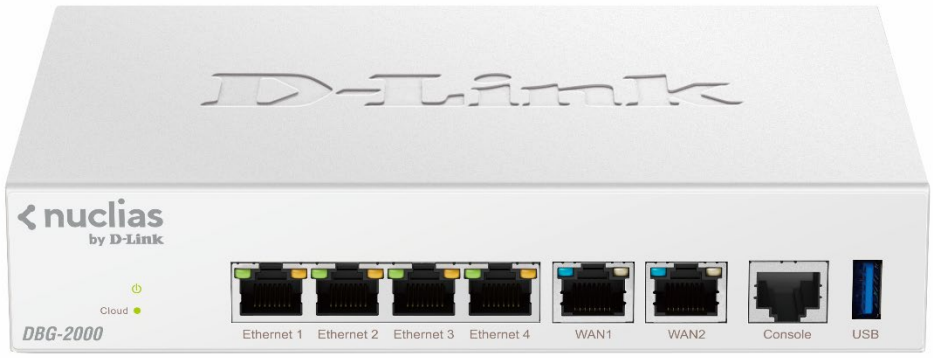
Version 2.2.0.9 | 21/11/2023



Mode d'emploi

Passerelle Nuclias Cloud

DBG-2000

Mode d'emploi

D-Link Nuclias Cloud Gateway, DBG-2000, offre plusieurs fonctionnalités à utiliser pour les applications réseau. Cependant, pour travailler efficacement avec l'appareil, vous devez comprendre ses fonctionnalités. Pour cela, nous vous recommandons de lire le Guide de l'utilisateur. Le guide de l'utilisateur comprend des détails sur tous les champs apparaissant sur chaque page de l'interface utilisateur de l'appareil.

Version V2.2.0.9

Agrandir Tout Réduire Tout

Préface

Les informations ici sont sujettes à changement sans préavis. Le fabricant ne fait aucune déclaration ou garantie concernant le contenu du présent document et décline spécifiquement toute garantie implicite de qualité marchande ou d'adéquation à un usage particulier. Le fabricant se réserve le droit de réviser cette publication et d'apporter des modifications de temps à autre à son contenu sans obligation pour le fabricant d'informer quiconque de ces révisions ou modifications.

Copyright notice

Limitations of liability

EN AUCUN CAS D-LINK OU SES FOURNISSEURS NE SERONT RESPONSABLES DES DOMMAGES DE QUELQUE CARACTÈRE (PAR EXEMPLE DOMMAGES POUR PERTE DE PROFIT, RESTAURATION DU LOGICIEL, ARRÊT DE TRAVAIL, PERTE DE DONNÉES SAUVEGARDÉES OU TOUT AUTRE DOMMAGE OU PERTE COMMERCIAL) RÉSULTANT DE L'APPLICATION OU D'UNE MAUVAISE UTILISATION DU PRODUIT D-LINK OU DÉFAILLANCE DU PRODUIT, MÊME SI D-LINK EST INFORMÉ DE LA POSSIBILITÉ DE TELS DOMMAGES. DE PLUS, D-LINK NE SERA PAS RESPONSABLE DES RÉCLAMATIONS DE TIERS CONTRE LE CLIENT POUR PERTES OU DOMMAGES. D-LINK NE SERA EN AUCUN CAS RESPONSABLE DE TOUT DOMMAGE DÉPASSANT LE MONTANT D-LINK REÇU DE L'UTILISATEUR FINAL POUR LE PRODUIT.

Safety instructions

Pour réduire le risque de blessure physique, de choc électrique, d'incendie et de dommage à l'équipement, respectez les précautions suivantes :

- Observez et suivez les marquages de service.
  - Ne réparez aucun produit sauf comme expliqué dans la documentation de votre système. Par exemple, ouvrir ou retirer les couvercles marqués du symbole triangulaire avec un éclair peut vous exposer à un choc électrique.
  - Seul un technicien de service qualifié doit entretenir les composants à l'intérieur de ces compartiments.
- Si l'une des conditions suivantes se produit, débranchez le produit de la prise électrique et remplacez la pièce ou contactez votre fournisseur de services qualifié :
  - Le câble d'alimentation, la rallonge ou la fiche est endommagé.
  - Un objet est tombé dans le produit. Le
  - produit a été exposé à l'eau. Le produit est
  - tombé ou est endommagé.
  - Le produit ne fonctionne pas correctement lorsque vous suivez les instructions d'utilisation. Gardez
- votre système éloigné des radiateurs et des sources de chaleur. Ne bloquez pas non plus les bouches d'aération.
- Ne renversez pas de nourriture ou de liquides sur les composants de votre système et n'utilisez jamais le produit dans un environnement humide. Si le système est mouillé, consultez la section appropriée de votre guide de dépannage ou contactez votre fournisseur de services qualifié.
- Ne poussez aucun objet dans les ouvertures de votre système. Cela pourrait provoquer un incendie ou un choc électrique en court-circuitant les composants intérieurs.
- Utilisez le produit uniquement avec un équipement approuvé.
- Laissez le produit refroidir avant de retirer les couvercles ou de toucher les composants internes.

- Faites fonctionner le produit uniquement à partir du type de source d'alimentation externe indiqué sur l'étiquette signalétique électrique. Si vous n'êtes pas sûr du type de source d'alimentation requis, consultez votre fournisseur de services ou votre compagnie d'électricité locale.
- Assurez-vous également que les appareils connectés sont électriquement conçus pour fonctionner avec la puissance disponible dans votre emplacement.

- Utilisez uniquement des câbles d'alimentation approuvés. Si vous n'avez pas reçu de câble d'alimentation pour votre système ou pour toute option alimentée en CA destinée à votre système, achetez un câble d'alimentation dont l'utilisation est approuvée dans votre pays. Le câble d'alimentation doit être adapté au produit et la tension et le courant doivent être indiqués sur l'étiquette électrique du produit. La tension et le courant nominal du câble doivent être supérieurs à ceux indiqués sur le produit.
- Pour éviter les chocs électriques, branchez les câbles d'alimentation du système et des périphériques dans des prises électriques correctement mises à la terre.
- Ces câbles sont équipés de fiches à trois broches pour garantir une mise à la terre adéquate. N'utilisez pas de fiches d'adaptateur et ne retirez pas la broche de mise à la terre d'un câble. Si vous devez utiliser une rallonge, utilisez un câble à 3 fils avec des fiches correctement mises à la terre.
- Respectez les valeurs nominales des rallonges et des multiprises. Assurez-vous que l'ampérage total de tous les produits branchés sur la rallonge ou la multiprise ne dépasse pas 80 % de la limite d'ampérage de la rallonge ou de la multiprise.
- Pour protéger votre système contre les augmentations et diminutions soudaines et transitoires de la puissance électrique, utilisez un suppresseur de surtension, un conditionneur de ligne ou une alimentation sans interruption (UPS).
- Positionnez soigneusement les câbles du système et les câbles d'alimentation ; acheminez les câbles de manière à ce qu'il ne soit pas possible de marcher dessus ou de trébucher. Assurez-vous que rien ne repose sur les câbles.

- Ne modifiez pas les câbles d'alimentation ou les fiches. Consultez un électricien agréé ou votre compagnie d'électricité pour les modifications du site.
- Suivez toujours vos règles de câblage locales/nationales.
- Lors de la connexion ou de la déconnexion de l'alimentation des blocs d'alimentation enfichables à chaud, si proposés avec votre système, respectez les directives suivantes :
    - Installez le bloc d'alimentation avant de connecter le câble d'alimentation au bloc d'alimentation.
    - Débranchez le câble d'alimentation avant de retirer le bloc d'alimentation.
    - Si le système dispose de plusieurs sources d'alimentation, débranchez l'alimentation du système en débranchant tous les câbles d'alimentation des blocs d'alimentation.
- Déplacez les produits avec soin ; assurez-vous que toutes les roulettes et/ou stabilisateurs sont fermement connectés au système. Évitez les arrêts brusques et les surfaces inégales.

Protection contre les décharges électrostatiques

L'électricité statique peut endommager les composants délicats de votre système. Pour éviter les dommages causés par l'électricité statique, déchargez l'électricité statique de votre corps avant de toucher l'un des composants électroniques, tels que le microprocesseur. Vous pouvez le faire en touchant périodiquement une surface métallique non peinte du châssis.

Vous pouvez également prendre les mesures suivantes pour éviter les dommages dus aux décharges électrostatiques (ESD) :

- Lorsque vous déballez un composant sensible à l'électricité statique de son carton d'expédition, ne retirez pas le composant du matériau d'emballage antistatique tant que vous n'êtes pas prêt à l'installer dans votre système. Juste avant de déballer l'emballage antistatique, veillez à décharger l'électricité statique de votre corps.
- Lors du transport d'un composant sensible, placez-le dans un conteneur ou un emballage antistatique.
- Manipulez tous les composants sensibles dans une zone antistatique. Si possible, utilisez des patins antistatiques pour le sol, des patins pour établi et une sangle de mise à la terre antistatique.

Commencer

Version : V2.2.0.9

Le guide de l'utilisateur de la passerelle D-Link Nuclias Cloud Gateway DBG-2000 comprend des informations sur toutes les fonctionnalités prises en charge par la passerelle. Cependant, avant de découvrir les fonctionnalités, vous devez savoir comment utiliser et installer la passerelle, ses fonctionnalités et où naviguer pour quoi. Vous obtiendrez un aperçu complet de ces éléments et découvrirez également la configuration de quelques paramètres dans cette section.

Introduction

D-Link Nuclias Cloud Gateway DBG-2000 offre une solution réseau sécurisée et hautes performances basée sur le cloud pour répondre aux besoins croissants des petites et moyennes entreprises. La sécurité réseau optimale est assurée via des fonctionnalités telles que les tunnels de réseau privé virtuel (VPN), la sécurité IP (IPSec), le protocole de tunneling point à point (PPTP), le protocole de tunneling de couche 2 (L2TP) et OpenVPN. Offrez à vos itinérants un accès à distance partout et à tout moment grâce aux tunnels OpenVPN. Avec la passerelle cloud D-Link Nuclias, DBG-2000, vous pouvez bénéficier de nombreux avantages.

- **Capacités de gestion complètes**
  Le DBG-2000 inclut WAN-Gigabit Ethernet, qui fournit une gestion des services basée sur des politiques garantissant une productivité maximale pour vos opérations commerciales. Le*basculement*La fonctionnalité maintient le trafic de données sans se déconnecter en cas de perte d'une connexion fixe. Le*Équilibrage de charge sortant*La fonctionnalité ajuste le trafic sortant sur les interfaces WAN et optimise les performances du système, ce qui entraîne une haute disponibilité. De plus, la solution prend en charge la configuration d'un port en tant que port DMZ dédié vous permettant d'isoler les serveurs de votre LAN.
- **Approvisionnement sans contact**
  DBG-2000 est une passerelle prise en charge par le cloud qui est synchronisée avec le cloud pour atteindre toutes ses fonctionnalités. Le D-Link Nuclias Cloud peut gérer virtuellement les passerelles largement déployées et leur transmettre instantanément la configuration. De plus, la fonctionnalité de configuration et d'association de profils à plusieurs passerelles déployées d'une organisation les aide à fonctionner avec la même configuration.
- **Fonctionnalités VPN robustes**
  Un réseau privé virtuel (VPN) complet fournit à vos travailleurs mobiles et à vos succursales un lien sécurisé vers votre réseau. Le DBG-2000 peut gérer plusieurs tunnels VPN simultanément, permettant ainsi à vos utilisateurs mobiles de fournir un accès à distance à une base de données centrale d'entreprise. Les tunnels VPN site à site utilisent le protocole de sécurité IP (IPSec), le protocole de tunneling point à point (PPTP) ou le protocole de tunneling de couche 2 (L2TP) pour faciliter la connectivité des succursales via des liaisons virtuelles cryptées. Hub and Spoke est une nouvelle topologie site à site qui désigne une passerelle DBG-2000 comme « Hub » et tous les sites distants comme « Spokes ». Le mode Hub-and-Spoke est avantageux dans les organisations où plusieurs sites auxiliaires nécessitent une connexion au siège. Avec cette topologie, la communication entre les deux sites ne pourrait s'effectuer que via le Hub. De cette façon, le Hub est toujours informé chaque fois que deux sites communiquent entre eux.

DBG-2000 Quick Start Guide

Le Guide de démarrage rapide du DBG-2000 comprend les rubriques suivantes :

Installation

Déballez le produit

Ouvrez le carton d'expédition et déballez soigneusement son contenu. Veuillez consulter la liste de colisage suivante pour vous assurer que tous les articles sont présents et en bon état. Si un élément est manquant ou endommagé, veuillez contacter votre revendeur D-Link local pour un remplacement.

- Une (1) passerelle Nuclias Cloud DBG-2000 Un
- (1) adaptateur secteur
- Un (1) câble de console (câble RJ-45 vers DB-9) Un (1)
- câble Ethernet (CAT5 UTP/Straight-Through) Un (1)
- guide d'installation rapide
- Deux (2) supports de montage en rack

Avant que tu commences

Assurez-vous de suivre les précautions indiquées ci-dessous pour éviter les arrêts, les pannes d'équipement et les blessures :

- Assurez-vous que la pièce dans laquelle vous utilisez l'appareil dispose d'une circulation d'air adéquate et que la température ambiante ne dépasse PAS 40 °C (104 °F).
- Prévoyez 1 mètre (3 pieds) d'espace libre à l'avant et à l'arrière de l'appareil.
- Ne placez PAS l'appareil dans un cadre de rack d'équipement qui bloque les bouches d'aération sur les côtés du châssis. Assurez-vous également que les racks fermés sont équipés de ventilateurs et de volets latéraux.
- Avant l'installation, veuillez corriger les conditions dangereuses suivantes : sols humides ou mouillés, fuites, câbles d'alimentation non mis à la terre ou effilochés, ou mise à la terre de sécurité manquante.

Connectez-vous à votre réseau

Les informations de base sur la connexion physique du DBG-2000 à un réseau sont les suivantes :

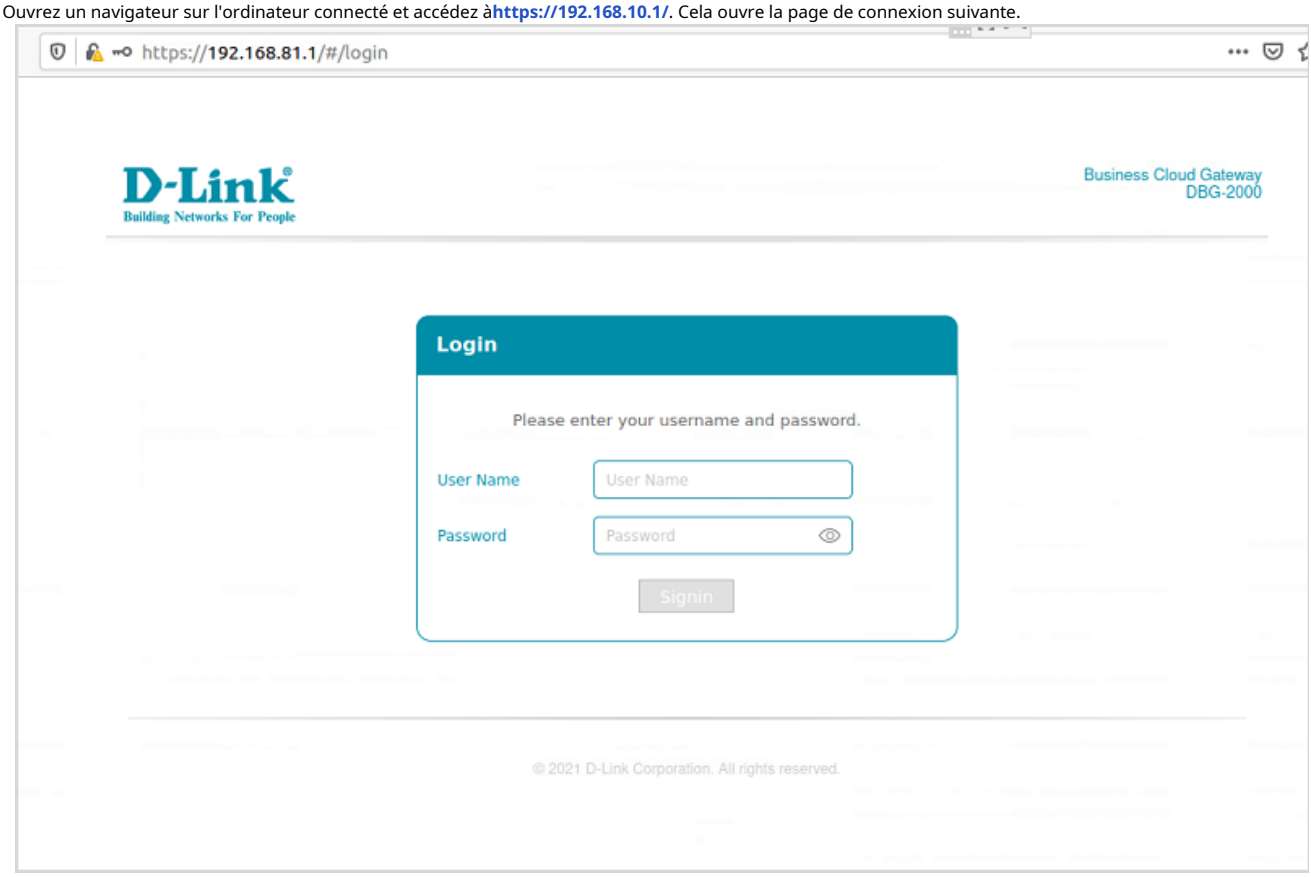
- Connectez un câble Ethernet du port étiqueté Ethernet 1 au routeur externe, au modem ou au FAI. Le port Ethernet 1 est alloué au segment du réseau WAN.
- Connectez un câble Ethernet de l'un des ports LAN (Ethernet 2, Ethernet 3 ou Ethernet 4) à un commutateur ou à un ordinateur du segment de réseau LAN.

Configuration requise

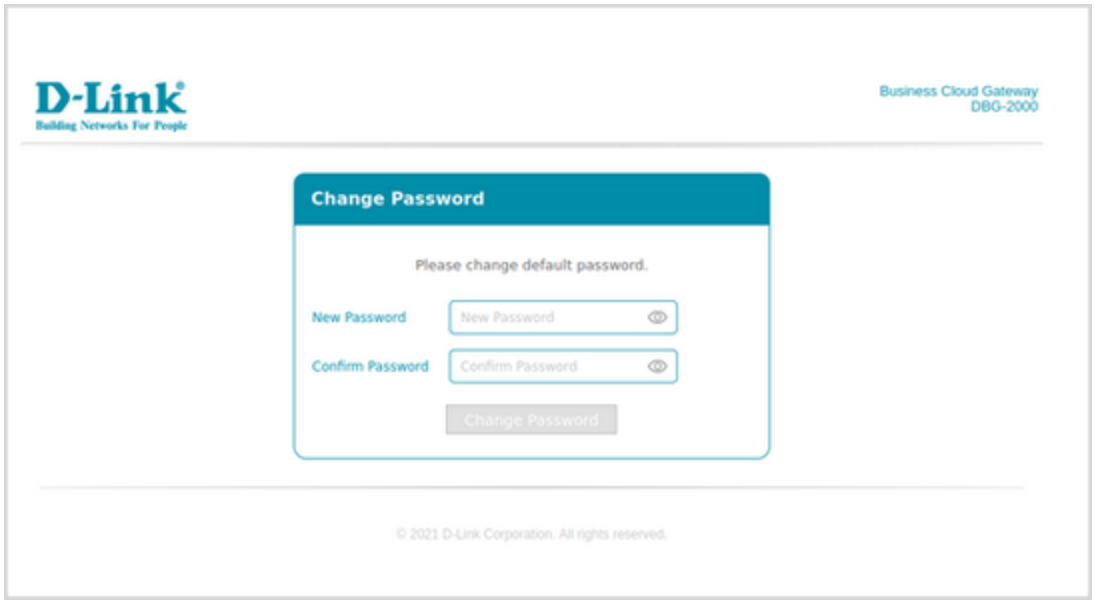
- Une connexion Internet haut débit
- Un ordinateur avec l'un des navigateurs suivants :
  - Microsoft Internet Explorer (version 9.0 ou supérieure)
  - Mozilla Firefox (version 20 ou supérieure)
  - Opera (version 77.0 ou supérieure)
  - Apple Safari (version 5.0 ou supérieure)
  - Google Chrome (version 25 ou supérieure)

Configuration basée sur le Web

1. Ouvrez un navigateur sur l'ordinateur connecté et accédez à**https://192.168.10.1/**. Cela ouvre la page de connexion suivante.



2. Entrer**administrateur**comme nom d'utilisateur et**administrateur123 $**comme mot de passe.
3. Si vous vous connectez pour la première fois et que l'appareil n'est pas synchronisé avec le cloud Nuclias, vous serez redirigé vers le**Changer le mot de passe**page. Vous devez modifier le mot de passe par défaut et saisir un nouveau mot de passe. Si l'appareil est synchronisé avec le cloud Nuclias, vous ne pouvez pas modifier le mot de passe.



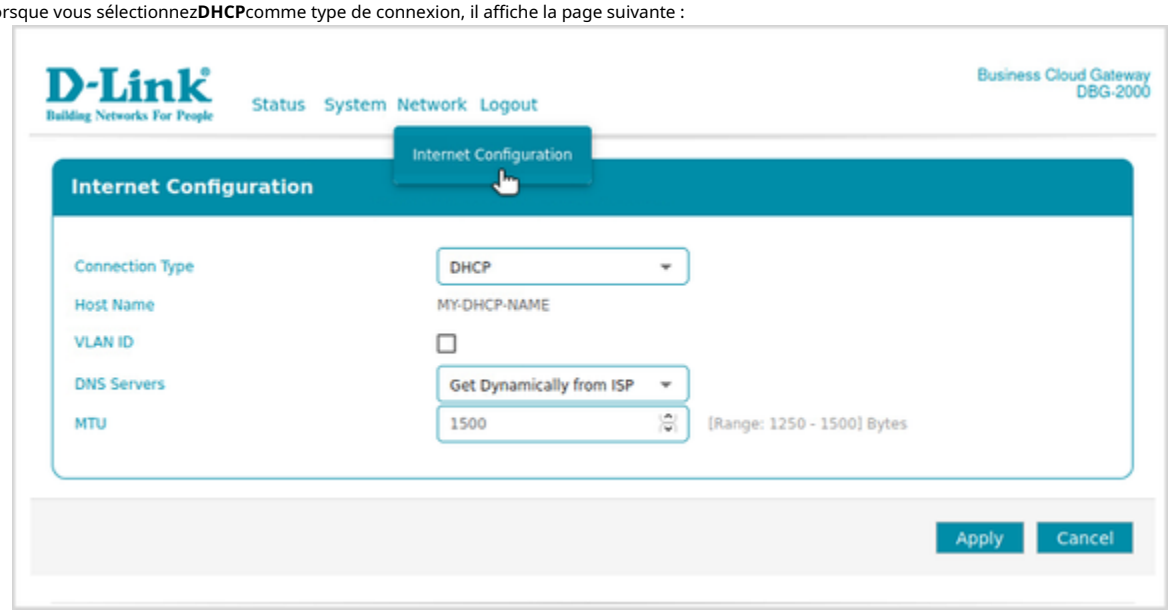
4. Saisissez votre nouveau mot de passe et saisissez-le à nouveau pour confirmer le nouveau mot de passe.
5. Cliquez sur**Changer le mot de passe**.
6. Si l'appareil est synchronisé avec le cloud Nuclias avant de se connecter à l'appareil, l'utilisateur n'est pas redirigé vers la page « Modifier le mot de passe ». Au lieu de cela, l'utilisateur peut se connecter directement avec le mot de passe de l'interface utilisateur cloud Nuclias pour le profil associé.
7. Après une connexion réussie, le**Aperçu**apparaîtra.

Comment connecter votre appareil à Internet ?

Pour vous connecter au cloud Nuclias, vous devez configurer la configuration Internet.

Note:*Les ports Ethernet 1 et Ethernet 4 sont configurés respectivement comme ports WAN et LAN par défaut.*

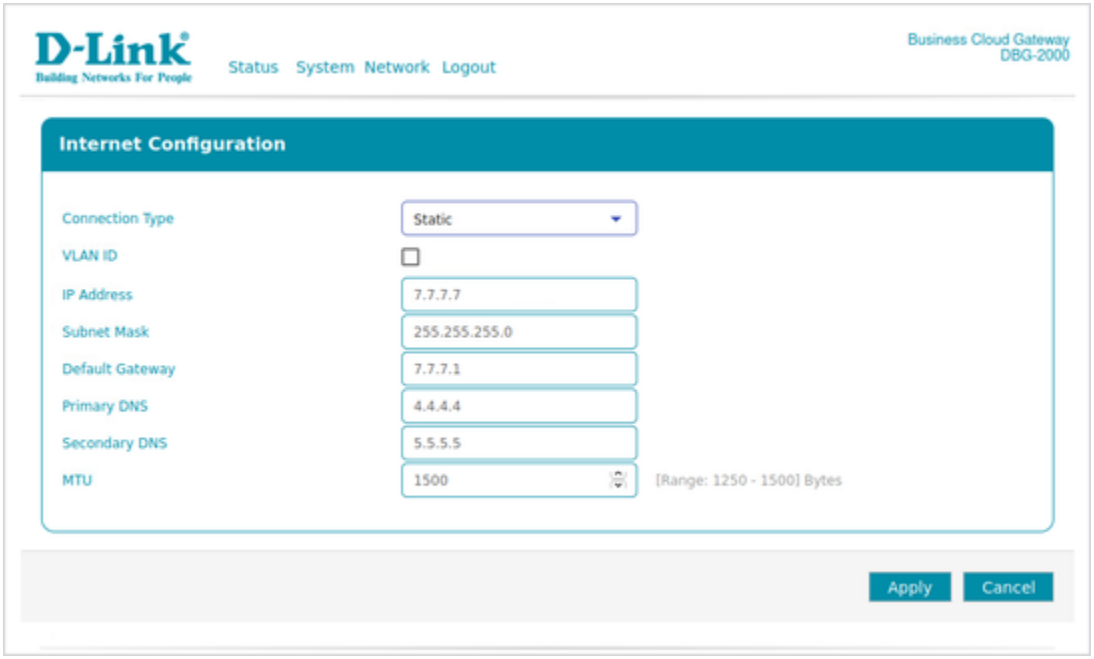
1. Accédez au**Réseau**menu, puis cliquez sur**Configuration Internet**.
2. Sélectionnez le type de connexion en fonction de votre FAI dans la liste déroulante. Les options sont DHCP, Statique, PPTP, L2TP et PPPoE.
3. Activez ou désactivez l'ID VLAN sur le port WAN configuré. Si vous activez l'ID VLAN, entrez le**ID de VLAN**.
4. Entrez les détails selon le type de connexion sélectionné.
   un. Lorsque vous sélectionnez**DHCP**comme type de connexion, il affiche la page suivante :



Des champs	Description
DHCP	

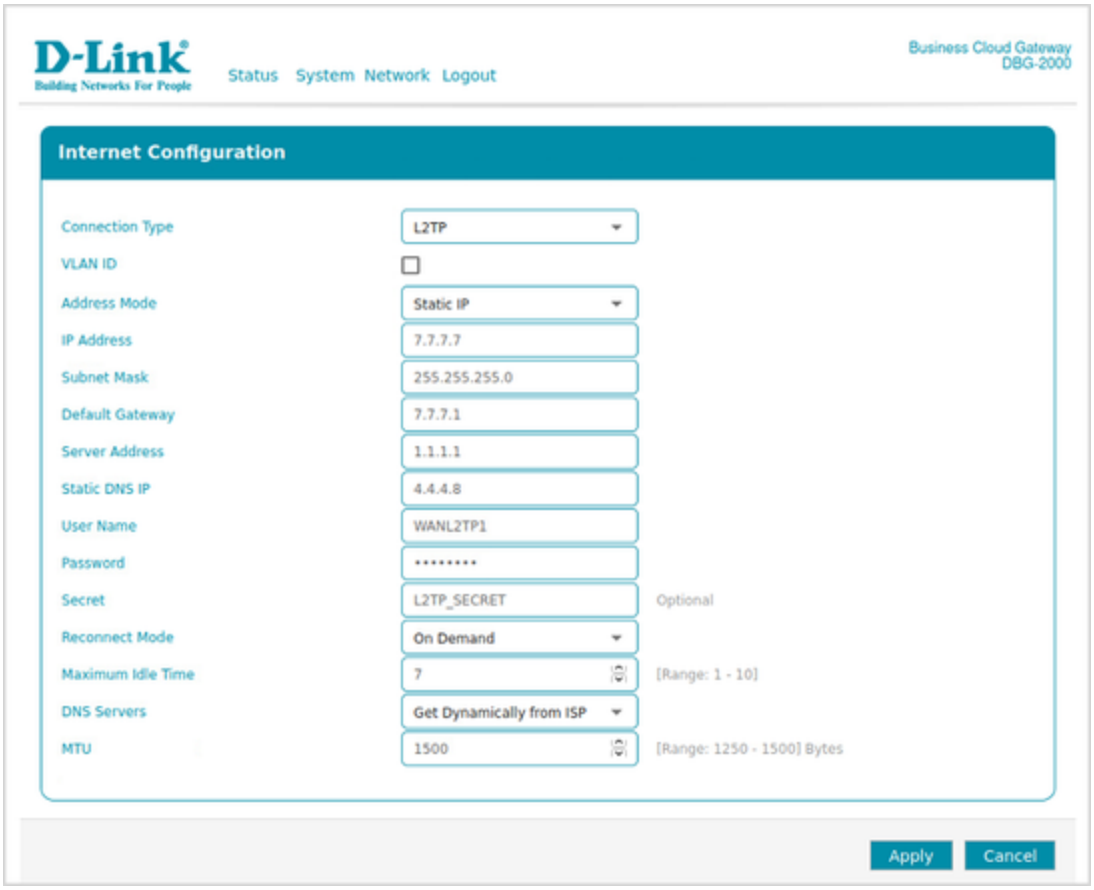
Nom d'hôte	Entrez le nom d'hôte si votre FAI l'exige.
Serveurs DNS	Sélectionnez soit**Obtenez dynamiquement du FAI**ou**Utilisez ces serveurs DNS**pour entrer manuellement les serveurs DNS.
DNS primaire	Si vous sélectionnez**Utilisez ces serveurs DNS**, saisissez l'adresse IP du serveur DNS principal.
DNS secondaire	Si vous sélectionnez**Utilisez ces serveurs DNS**, saisissez l'adresse IP du serveur DNS secondaire. C'est un champ facultatif.
MTU	Le MTU (Maximum Transmit Unit) est le plus gros paquet pouvant être envoyé sur le réseau. La valeur MTU standard pour les réseaux Ethernet est généralement de 1 500 octets.

b. Lorsque vous sélectionnez**Statique**comme type de connexion, il affiche la page suivante :



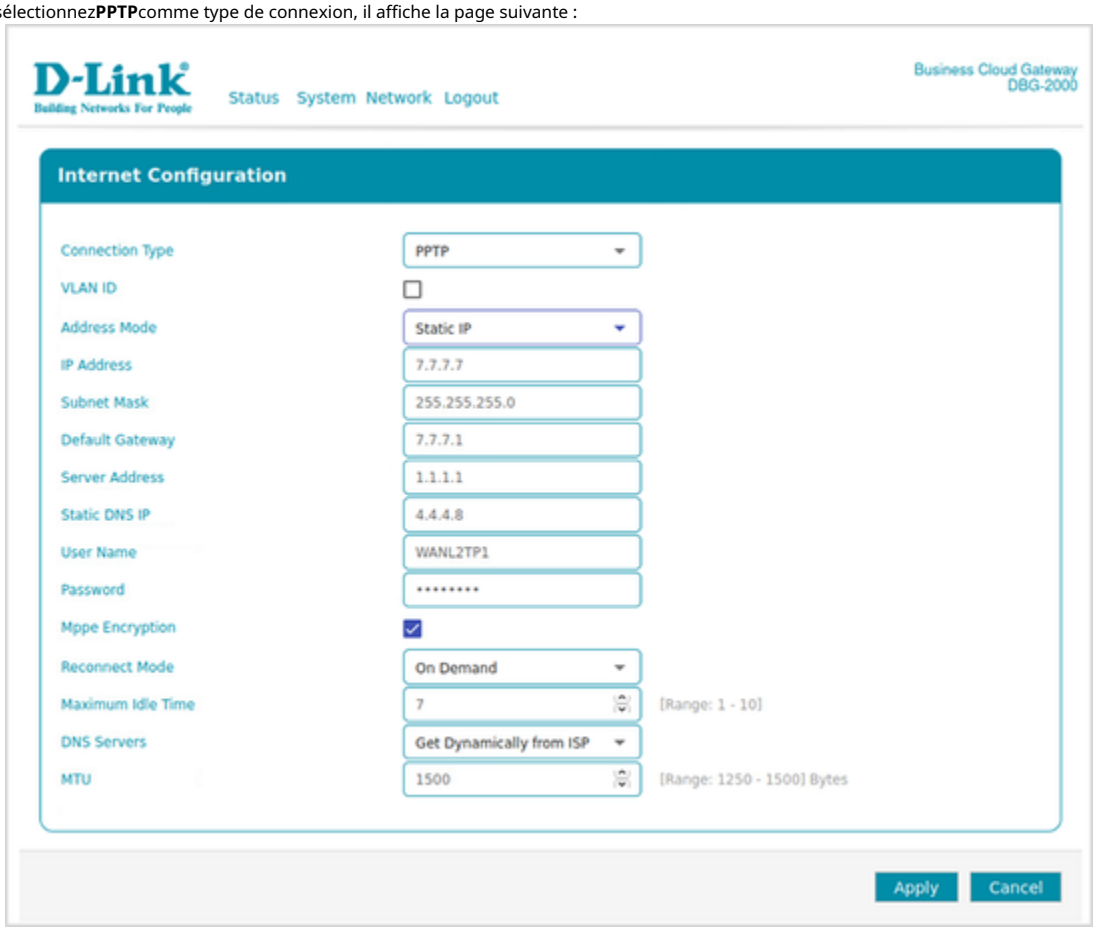
Des champs	Description
Statique	
adresse IP	Saisissez l'adresse statique que votre FAI vous a attribuée. Cette adresse identifiera le routeur auprès de votre FAI.
Masque de sous-réseau	Entrez le masque de sous-réseau IP.
Passerelle par défaut	Entrez l'adresse IP de la passerelle par défaut.
DNS primaire	Saisissez l'adresse IP du serveur DNS principal.
DNS secondaire	Saisissez l'adresse IP du serveur DNS secondaire. C'est un champ facultatif.
MTU	Le MTU (Maximum Transmit Unit) est le plus gros paquet pouvant être envoyé sur le réseau. Par exemple, la valeur MTU standard pour les réseaux Ethernet est généralement de 1 500 octets.

c. Lorsque vous sélectionnez**L2TP**comme type de connexion, il affiche la page suivante :



Des champs	Description
L2TP	
Mode adresse	Sélectionner**IP dynamique**ou**I.P statique**(Paramètres IP fournis par votre FAI).
Adresse du serveur	Entrez l'adresse de votre serveur L2TP.
adresse IP	Si vous sélectionnez**I.P statique**comme mode d'adresse, entrez l'adresse IP fournie par votre FAI.
Masque de sous-réseau	Si vous sélectionnez**I.P statique**comme mode d'adresse, entrez le masque de sous-réseau fourni par votre FAI.
Passerelle par défaut	Si vous sélectionnez**I.P statique**comme mode d'adresse, entrez l'adresse IP de la passerelle fournie par votre FAI.
IP DNS statique	Si vous sélectionnez**I.P statique**comme mode d'adresse, entrez l'adresse IP DNS statique dans le sous-réseau correspondant.
Nom d'utilisateur	Entrez votre nom d'utilisateur L2TP.
Mot de passe	Entrez votre mot de passe L2TP.
Secrète	Saisissez un secret partagé.
Mode reconnexion	Certains FAI peuvent vous demander de payer pour la durée d'utilisation. Sélectionner**Sur demande**si c'est le cas. La passerelle se connectera alors à Internet uniquement lorsque vous établirez une connexion Internet. Sélectionner**Toujours activé**pour que la passerelle reste connectée à Internet.
Temps d'inactivité maximum	Entrez le nombre de minutes dans le*Temps d'inactivité maximum*champ. Cette fonctionnalité est utile si votre FAI vous facture en fonction de la durée de votre connexion. Ce champ est disponible uniquement lorsque **Sur demande**est sélectionné.
Serveurs DNS	Sélectionnez soit**Obtenez dynamiquement du FAI**ou**Utilisez ces serveurs DNS**pour entrer manuellement les serveurs DNS.
MTU	Le MTU (Maximum Transmit Unit) est le plus gros paquet pouvant être envoyé sur le réseau. Par exemple, pour toutes les connexions L2TP, la MTU est de 1 460 octets.

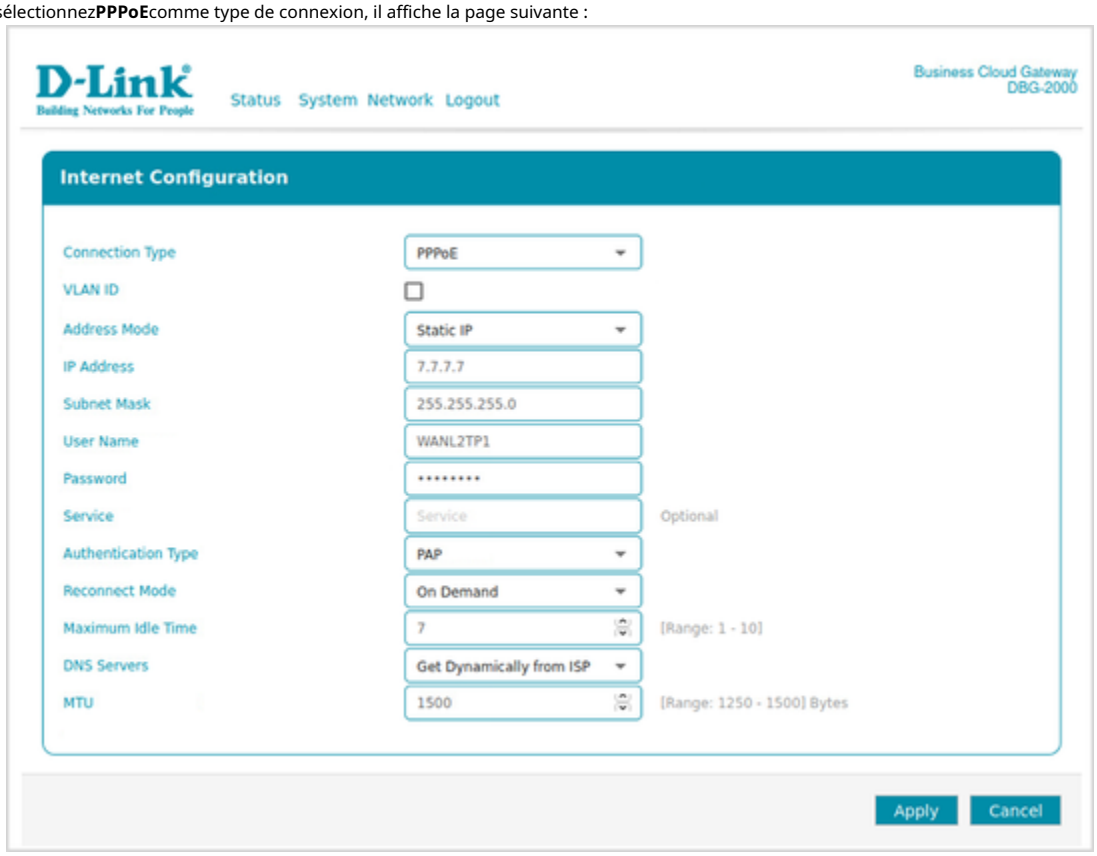
d. Lorsque vous sélectionnez**PPTP**comme type de connexion, il affiche la page suivante :



Des champs	Description
PPTP	
Mode adresse	Sélectionner**IP dynamique**ou**I.P statique**(Paramètres IP fournis par votre FAI).
adresse IP	Si vous sélectionnez**I.P statique**comme mode d'adresse, entrez l'adresse IP fournie par votre FAI.
Masque de sous-réseau	Si vous sélectionnez**I.P statique**comme mode d'adresse, entrez le masque de sous-réseau fourni par votre FAI.
Passerelle par défaut	Si vous sélectionnez**I.P statique**comme mode d'adresse, entrez l'adresse IP de la passerelle fournie par votre FAI.
Adresse du serveur	Entrez l'adresse de votre serveur PPTP.
IP DNS statique	Si vous sélectionnez**I.P statique**comme mode d'adresse, entrez l'adresse IP DNS statique dans le sous-réseau correspondant.
Nom d'utilisateur	Entrez votre nom d'utilisateur PPTP.
Mot de passe	Entrez votre mot de passe PPTP.
Cryptage MPPE	Activez-le si le serveur PPTP prend en charge cette fonctionnalité.
Mode reconnexion	Certains FAI peuvent vous demander de payer pour la durée d'utilisation. Sélectionner**Sur demande**si c'est le cas. La passerelle se connectera alors à Internet uniquement lorsque vous établirez une connexion Internet. Sélectionner**Toujours activé**pour que la passerelle reste connectée à Internet.
Temps d'inactivité maximum	Entrez le nombre de minutes dans le*Temps d'inactivité maximum*champ. Cette fonctionnalité est utile si votre FAI vous facture en fonction de la durée de votre connexion. Ce champ est disponible uniquement lorsque **Sur demande**est sélectionné.
Serveurs DNS	Sélectionnez soit**Obtenez dynamiquement du FAI**ou**Utilisez ces serveurs DNS**pour entrer manuellement les serveurs DNS.

MTU	Le MTU (Maximum Transmit Unit) est le plus gros paquet pouvant être envoyé sur le réseau. Pour les connexions PPTP, il s'agit de 1 492 octets.

e. Lorsque vous sélectionnez**PPPoE**comme type de connexion, il affiche la page suivante :

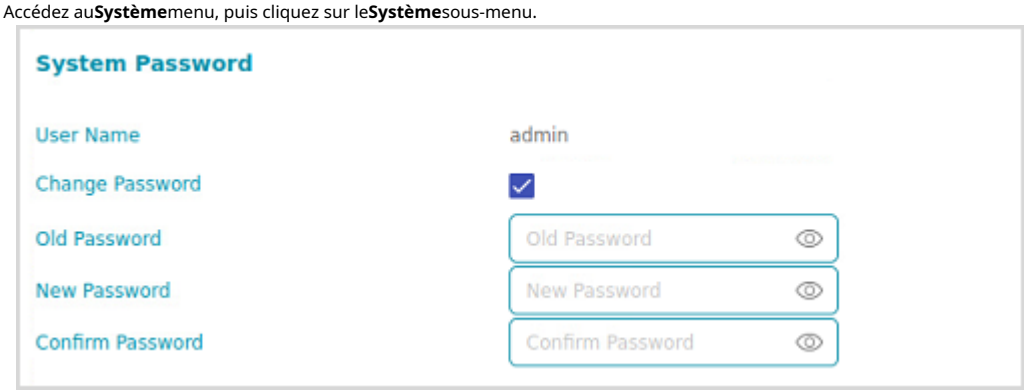


Des champs	Description
PPPoE	
Mode adresse	Sélectionner**IP dynamique**ou**I.P statique**(Paramètres IP fournis par votre FAI).
adresse IP	Si vous sélectionnez**I.P statique**comme mode d'adresse, entrez l'adresse IP fournie par votre FAI.
Masque de sous-réseau	Si vous sélectionnez**I.P statique**comme mode d'adresse, entrez le masque de sous-réseau fourni par votre FAI.
Nom d'utilisateur	Entrez votre nom d'utilisateur PPPoE.
Mot de passe	Entrez votre mot de passe PPPoE.
Service	Si votre FAI prend en charge le service, saisissez le nom du service. C'est un champ facultatif.
Type d'identification	Sélectionnez le type d'authentification à utiliser (négociation automatique, PAP, CHAP, MS-CHAP ou MS-CHAPv2).
Mode reconnexion	Sélectionnez l'une des options suivantes : • **Toujours allumé :**La connexion est toujours active. • **Sur demande:**La connexion est automatiquement interrompue si elle est inactive pendant un nombre de minutes spécifié.
Temps d'inactivité maximum	Entrez le nombre de minutes dans le*Temps d'inactivité maximum*champ. Cette fonctionnalité est utile si votre FAI vous facture en fonction de la durée de votre connexion. Ce champ est disponible uniquement lorsque**Sur demande**est sélectionné.
Serveurs DNS	Sélectionnez soit**Obtenez dynamiquement du FAI**ou**Utilisez ces serveurs DNS**pour entrer manuellement les serveurs DNS.
MTU	Le MTU (Maximum Transmit Unit) est le plus gros paquet pouvant être envoyé sur le réseau. Pour les connexions PPPoE, il s'agit de 1 492 octets.

5. Cliquez sur**Appliquer**pour appliquer vos paramètres à l'appareil.

Comment changer votre mot de passe ?

1. Accédez au**Système**menu, puis cliquez sur le**Système**sous-menu.



2. Sélectionnez le**Changer le mot de passe**case à cocher.
3. Entrez votre**Ancien mot de passe**.
4. Entrez votre**nouveau mot de passe**.
5. Retapez votre nouveau mot de passe pour le confirmer et cliquez sur**Appliquer**.

Comment changer de serveur NTP ?

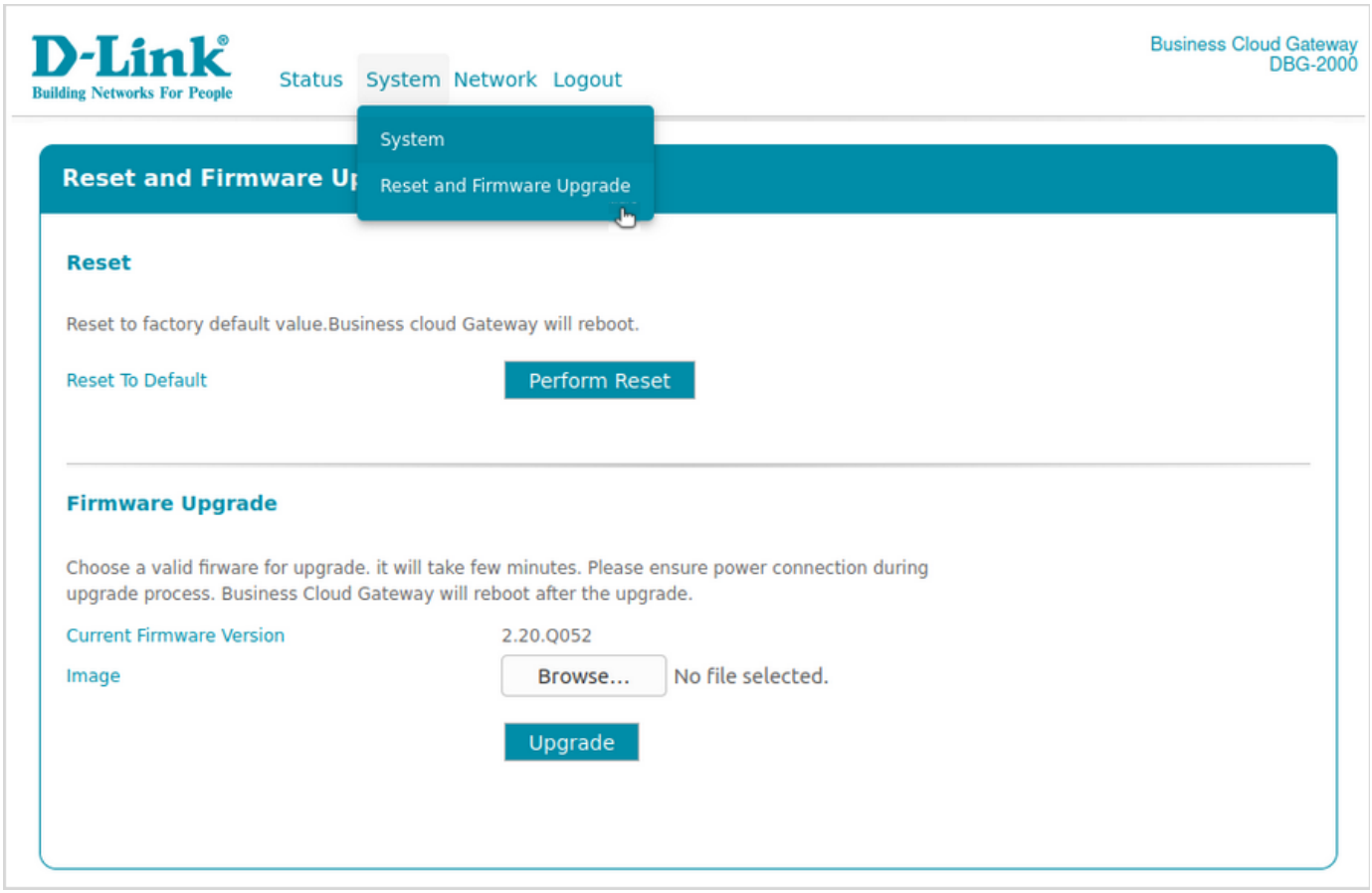
1. Accédez au**Système**menu et cliquez sur le**Système**sous-menu.

2. Sous Synchronisation de l'heure, entrez l'adresse IP du serveur ou le nom de domaine sur lequel le serveur NTP est exécuté.
3. Vous configurerez les serveurs NTP primaires, secondaires et tertiaires.
4. Cliquez sur**Appliquer**.

Comment réinitialiser et mettre à niveau le micrologiciel ?

Pour réinitialiser l'appareil et mettre à jour son micrologiciel, accédez à***Système > Réinitialisation et mise à niveau du micrologiciel***.

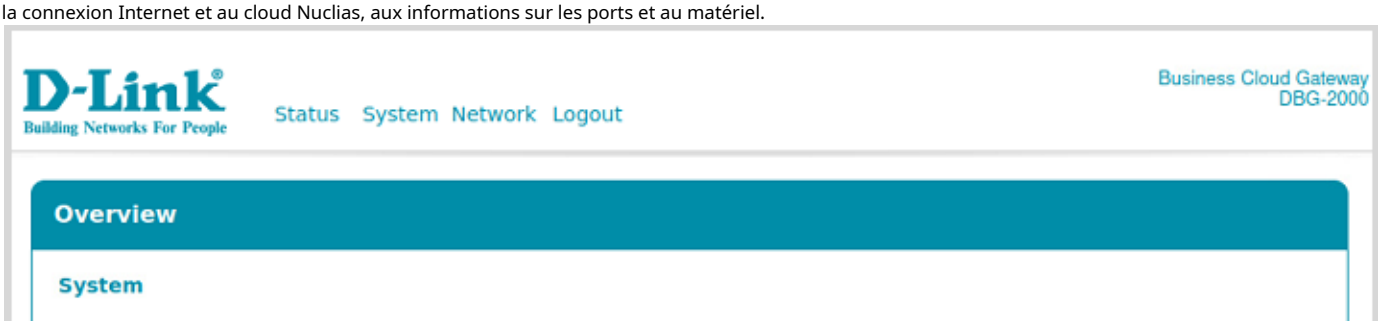
Remarque : Vous pouvez effectuer une réinitialisation uniquement via l'interface graphique de l'appareil et non depuis le portail Nuclias Cloud.



Des champs	Description
Réinitialiser	
Réinitialiser aux valeurs par défaut	Si vous réinitialisez l'appareil à ses paramètres par défaut, il revient à l'état dans lequel il était neuf : toutes les modifications que vous avez apportées à la configuration par défaut sont perdues. *Remarque : Si votre appareil est synchronisé avec le cloud Nuclias, il est associé à un profil et les paramètres de configuration Internet sont enregistrés dans ce profil. Après la réinitialisation, lorsque l'appareil est synchronisé avec le cloud Nuclias, par défaut, la même configuration est transmise à l'appareil.*
Mise à jour du firmware	
Version actuelle du micrologiciel	Il affiche la version du firmware exécuté sur la passerelle.
Image	Cliquez sur**Parcourir**et localisez le fichier du micrologiciel.
Mise à niveau	Cliquez sur**Mise à niveau**pour démarrer la mise à niveau du micrologiciel.

Aperçu du statut

Le**Statut**Le menu de la passerelle donne un bref aperçu de l'état de l'appareil et de sa configuration. De plus, il fournit des détails relatifs au système, à la connexion Internet et au cloud Nuclias, aux informations sur les ports et au matériel.



Model	DBG-2000
Current Firmware	2.20.Q049
Local Time	Wed Apr 07 2021 02:42:58 PM

Internet Connection

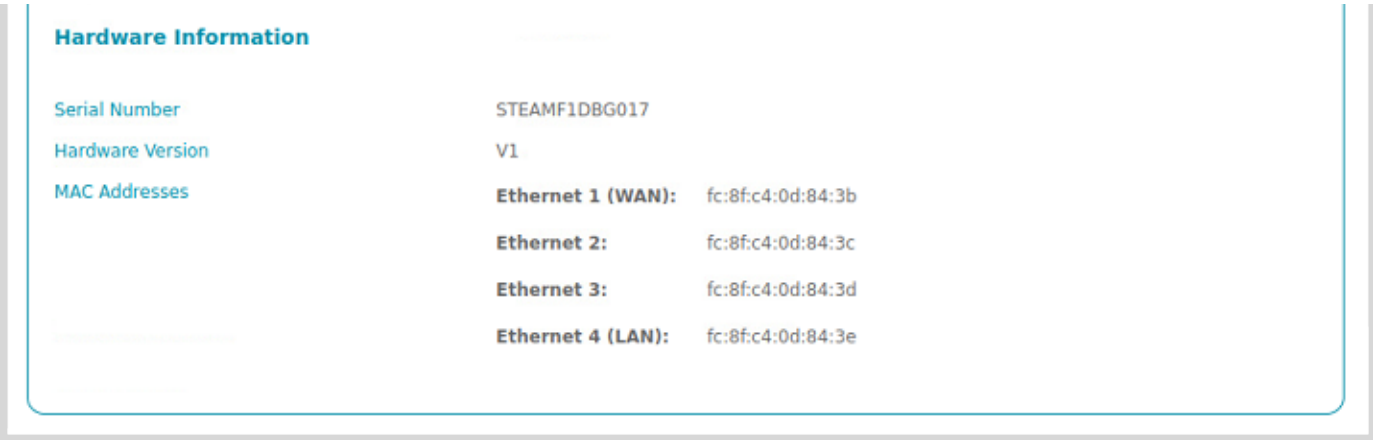
WAN1	**Connection Type:**	DHCP
	Address:	192.168.98.121
	Netmask:	255.255.248.0
	Gateway:	192.168.98.1
	DNS1:	192.168.98.1
	DNS2:	0.0.0.0
	Connected:	01h 45m 04s

Cloud Details

Cloud Connectivity Status	Connected
Internet Status	Connected
Device UID	TEAMF1DBG017
Registered	Yes
Registered Date	2021-04-06 16:59:53.261491
Nuclias	https://login.nuclias.com

Port Information

Ethernet 4 (LAN)	**IP Address:**	192.168.81.1
	Subnet Mask:	255.255.255.0
	DHCP Server:	Enabled
	Starting IP:	192.168.22.2
	Ending IP:	192.168.22.50
	Default Gateway:	192.168.22.1
	Domain Name:	lan.nuclias.com
	Lease Time:	1440
Ethernet 3 (LAN)	**IP Address:**	192.168.121.1
	Subnet Mask:	255.255.255.0
	DHCP Server:	Enabled
	Starting IP:	192.168.121.2
	Ending IP:	192.168.121.50
	Default Gateway:	192.168.121.1
	Domain Name:	lan.nuclias.com
	Lease Time:	1440



Des champs	Description
Système	
Modèle	Il affiche le nom du modèle.
Version actuelle	Il affiche la version du firmware exécuté sur la passerelle.
Heure locale	Il affiche l'heure selon le fuseau horaire défini sur la passerelle.
Connexion Internet	
WAN1	
Type de connexion	Il affiche le type de connexion utilisé pour établir une connexion Internet.
Adresse	Il affiche l'adresse IP obtenue ou configurée pour l'interface WAN.
Masque de réseau	Il affiche le masque de sous-réseau pour l'adresse IP.
passerelle	Il affiche l'adresse IP de la passerelle.
DNS1	Il affiche l'adresse IP du serveur DNS principal.
DNS2	Il affiche l'adresse IP du serveur DNS secondaire.
Connecté	Il fournit l'état de la connexion Internet.
Détails du nuage	
État de la connectivité cloud	Il indique si l'appareil est connecté au Nuclias Cloud ou non.
Statut Internet	Il fournit l'état Internet de votre connexion.
UID de l'appareil	Il affiche l'identification unique de l'appareil.
Inscrit	Il indique si votre appareil est enregistré sur le cloud Nuclias.
Date d'enregistrement	Si votre appareil est enregistré, il affiche la date et l'heure auxquelles il a été enregistré.
Nuclies	Il affiche le lien du site Web du cloud Nuclias.
Informations portuaires	
Ethernet	
adresse IP	Il affiche l'adresse IP de la passerelle.
Masque de sous-réseau	Il affiche le masque de sous-réseau du réseau.
Serveur DHCP	Il indique si le serveur DHCP est activé ou désactivé.
IP de départ	Il affiche l'adresse IP de départ.
Fin de la propriété intellectuelle	Il affiche l'adresse IP de fin.

Passerelle par défaut	Il affiche l'adresse IP de la passerelle par défaut.
Nom de domaine	Il affiche le nom de domaine pour la configuration LAN.
Durée du bail	Il affiche la durée pendant laquelle les adresses IP seront louées aux clients.
Informations sur le matériel	
Numéro de série	Il affiche le numéro de série de votre passerelle.
Version matérielle	Il affiche la version du matériel de votre appareil.
Adresse Mac	Il affiche l'adresse MAC de chaque port.

Vous souhaitez en savoir plus sur le portail Nuclias Cloud ? Aller àOù aller en partant d'ici.

Where to Go from Here

Après avoir installé la passerelle cloud Nuclias, vous pouvez la faire fonctionner en utilisant les paramètres d'usine par défaut. Ces paramètres devraient convenir à la plupart des utilisateurs et dans la plupart des situations. De plus, Nuclias Cloud Gateway fournit des paramètres de configuration de base et avancés que les utilisateurs peuvent utiliser selon leurs besoins. Les chapitres suivants fournissent les paramètres avancés de la passerelle cloud :

Chapitre 1 - Base

Ce chapitre décrit les informations sur le périphérique, son emplacement, l'interface WAN, ainsi que le site et le profil.

Chapitre 2 - Résumé

Ce chapitre décrit l'état, les statistiques, le DHCP et l'état VPN de la passerelle cloud.

Chapitre 3 - Réseau

Ce chapitre décrit Ethernet, l'adressage, le routage, les services, la gestion du trafic et la haute disponibilité.

Chapitre 4 - Sécurité

Ce chapitre décrit le pare-feu, IPS, ALG, WCF et Application Control.

Chapitre 5 - VPN

Ce chapitre décrit les sites VPN site à site, PPTP/L2TP, OpenVPN et GRE Tunnel.

Chapitre 6 - Outils

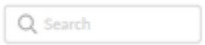
Ce chapitre décrit les outils de diagnostic pris en charge.

Chapitre 7 - Licence

Ce chapitre fournit des informations sur la licence.

Standard Web Management Interface Features

Les fonctionnalités standard disponibles sur l'interface de gestion Web sont les suivantes :



Recherche de contenu de tableauvous permet de rechercher des informations dans le tableau en tapant un mot dans la zone de recherche. Le champ de recherche est toujours situé dans le coin supérieur droit du tableau.

Précédent Suivant(sur la table) : les informations sont affichées sur plusieurs pages. Utilisez Précédent ou Suivant pour changer de page, et entre elles, le numéro de page actuel est affiché. La pagination est toujours située dans le coin inférieur droit du tableau.

Il indique le nombre d'entrées affichées sur le tableau sur une page. Le système peut répertorier 5, 10, 20, 40 et 100 entrées sur une seule page.

Le**Ajouter**Le bouton ajoute une nouvelle entrée à la table actuelle et le**Supprimer**Le bouton supprime l'entrée sélectionnée ou plusieurs entrées. Le**Ajouter**et**Supprimer**les boutons sont situés dans le coin supérieur gauche du tableau.

Il vous aide à filtrer le contenu que vous souhaitez afficher dans le tableau. Cliquez sur la flèche et cochez les cases des éléments que vous souhaitez ajouter en tant que colonnes dans le tableau. Cette icône est toujours située dans le coin supérieur droit du tableau.

Le**Appliquer**Le bouton pousse la configuration vers l'appareil connecté. Ce bouton est présent dans le coin supérieur gauche à côté des onglets du périphérique et est disponible uniquement pour les onglets suivants : De base, Réseau, Sécurité et VPN.

Configuration pages

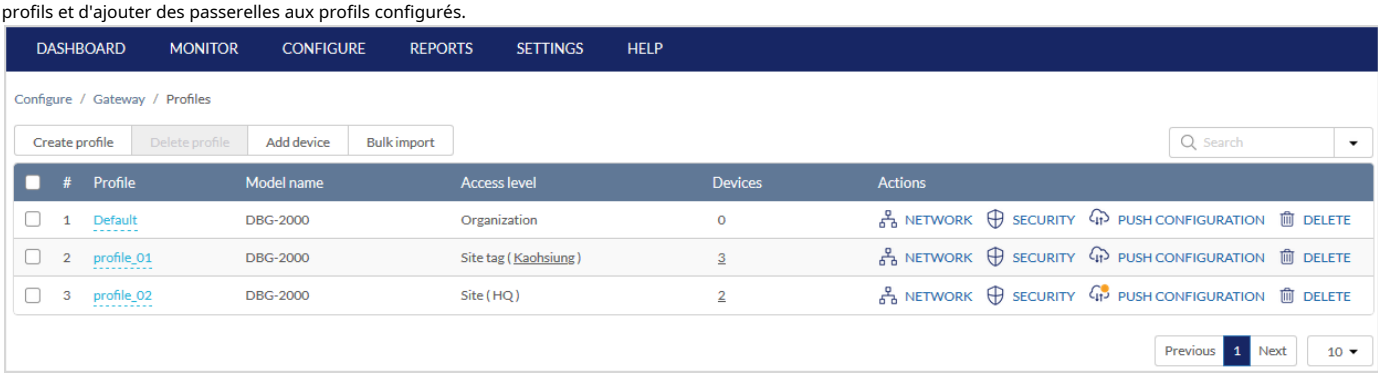
Cette section du guide de l'utilisateur comprend un ensemble de pages d'interface utilisateur utilisées pour configurer les paramètres importants, tels que les profils, les appareils, les serveurs d'authentification, les politiques de planification et l'éditeur de page de démarrage. Ces paramètres sont en outre requis pour configurer quelques fonctionnalités de la passerelle cloud Nuclias. Les pages de configuration fournissent une liste des paramètres configurés et vous aident également à les configurer.

Cette section comprend les sujets suivants :

Profils

Un profil est défini comme une configuration prédéfinie qui est directement transmise à toutes les passerelles nouvellement ajoutées ou existantes et partagée entre plusieurs passerelles. Plutôt que de configurer chaque appareil ajouté indépendamment, un ensemble de paramètres de paramètres réseau et de sécurité peut être enregistré en tant que profils. Lorsqu'un appareil est ajouté au cloud, il doit être associé à l'un de ces profils configurés. Vous pouvez également modifier cette configuration de profil en fonction des besoins.

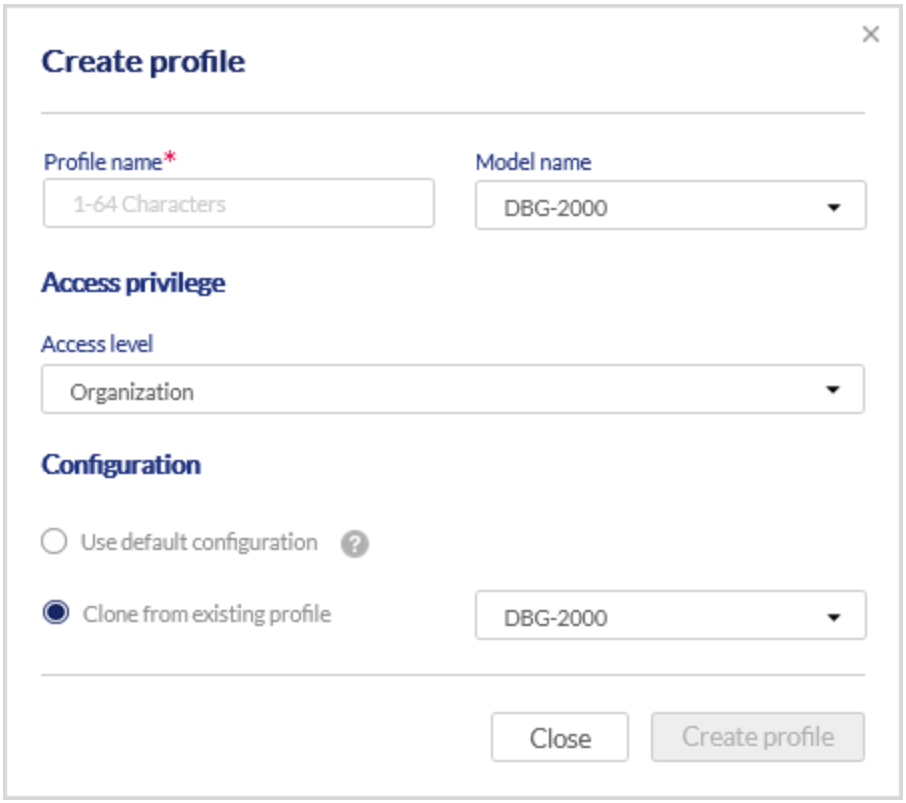
Le chemin pour atteindre le*Profils*la page est*Configurer > Passerelle > Profils*. Cette page répertorie tous les profils configurés et permet à l'utilisateur de créer des profils et d'ajouter des passerelles aux profils configurés.



Les champs présents dans le tableau sont les suivants :

Champ	Description
Profil	Il affiche le nom du profil.
Nom du modèle	Il affiche le nom du modèle associé au profil.
Niveau d'accès	Il affiche le niveau où l'utilisateur peut l'utiliser.
Dispositifs	Il affiche le nombre d'appareils associés au profil.
Actions	Il affiche les actions suivantes : • **Réseau**: Clique le**Réseau**lien, et il vous redirigera vers l'onglet Réseau de l'appareil pour configurer les paramètres liés au réseau commeEthernet,Adressage,Prestations de service, Gestion du trafic, etPortail captif. • **Sécurité**: Clique le**Sécurité**lien, et il vous redirigera vers l'onglet Sécurité de l'appareil pour configurer les paramètres de sécurité commePare-feu,IPS,Filtre de contenu Web, etUn contrôle d'application. • **Configuration poussée**: Cliquez sur**Configuration poussée**pour configurer tous les appareils associés à ce profil en une seule fois. • **Supprimer**: Cliquez sur**Supprimer**pour supprimer le profil.

Pour créer un nouveau profil, cliquez sur le**Créer un profil**bouton. Cela ouvre le*Créer un profil*page.



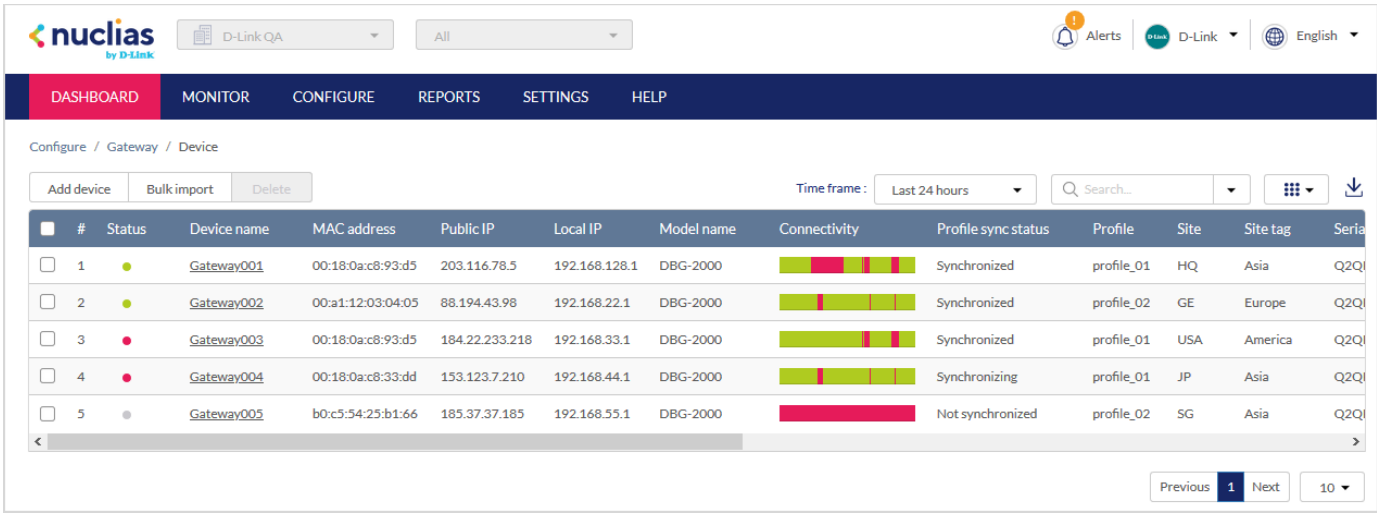
Les champs disponibles sur cette page sont les suivants :

Champ	Description
Nom de profil	Entrez un nom descriptif du profil.
Nom du modèle	Sélectionnez le nom du modèle que vous souhaitez associer au profil.
Niveau d'accès	Sélectionnez le niveau où l'utilisateur peut utiliser ce profil. Les options sont Organisation, Balise de site et Site. En fonction du niveau d'accès, sélectionnez le**Balise du site géré**et le**Site géré**.
Balise du site géré	Sélectionnez la balise du site géré dans la liste déroulante. Ce champ est disponible lorsque vous sélectionnez « Tag du site géré » comme**Niveau d'accès**.
Site géré	Sélectionnez le site géré dans la liste déroulante. Ce champ est disponible lorsque vous sélectionnez « Site géré » comme**Niveau d'accès**.
Configuration	
Utiliser la configuration par défaut	Choisissez cette option si vous souhaitez utiliser les paramètres par défaut du profil. Vous pouvez modifier la configuration à tout moment.
Cloner à partir d'un profil existant	Si vous souhaitez utiliser la configuration de l'un des profils configurés, choisissez cette option puis sélectionnez ce profil. Ce champ est disponible lorsque vous sélectionnez « Organisation » comme**Niveau d'accès**.
Créer un profil	Cliquez sur**Créer un profil**pour enregistrer le nouveau profil.
Fermer	Cliquez sur**Fermer**fermer le*Créer un profil*page.

Pour ajouter un appareil, cliquez sur**Ajouter un appareil**. Cela ouvre le*Ajouter un appareil*page. Se référer auAppareilpour plus de détails.

Appareil

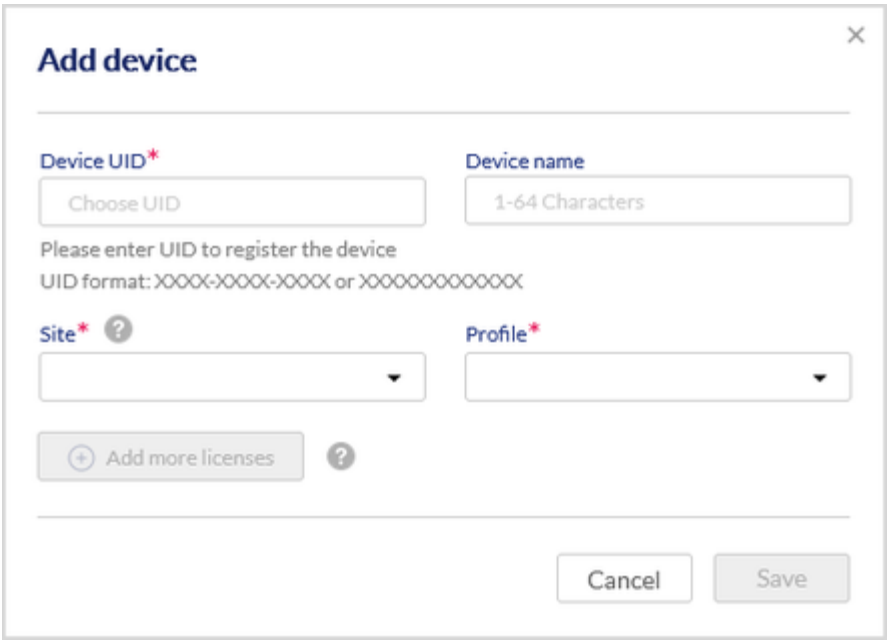
Le chemin pour atteindre le*Appareil*la page est*Configurer > Passerelle > Périphérique*. Le*Appareil*La page se compose d'une liste des appareils présents dans le groupe d'appareils pour la période sélectionnée. Il affiche les détails du matériel et du micrologiciel des appareils ainsi que les profils auxquels ces appareils sont associés. Il permet également à l'utilisateur d'ajouter de nouveaux appareils à la liste, soit séparément, soit par importation groupée.



Les champs suivants sont affichés sur cette page :

Champ	Description
Statut	Il affiche l'état de l'appareil présent dans le groupe d'appareils. Le**Vert**Le point indique que l'appareil est connecté au cloud et que le**Rouge**Le point indique que l'appareil n'est pas connecté au cloud.
Nom de l'appareil	Il affiche le nom de l'appareil.
Adresse Mac	Il affiche l'adresse MAC de l'appareil présent dans le groupe de périphériques.
IP publique	Il affiche l'adresse IP via laquelle DBG est connecté au serveur cloud.
IP locale	Il affiche l'adresse IP de l'appareil.
Nom du modèle	Il affiche le nom du modèle de l'appareil.
Connectivité	Il fournit l'historique de l'état de la connectivité de cet appareil sous la forme d'une barre. Lorsque vous survolez la barre, elle affiche quand et pendant combien de temps l'appareil a été connecté ou déconnecté. La zone verte indique une passerelle connectée et la zone rouge indique « aucune connectivité ».
État de synchronisation du profil	Lorsque vous poussez une configuration et que l'appareil est accessible, il affiche**Synchronisé**, et si l'appareil n'est pas accessible, il affiche**Non synchronisé**.
Profil	Il affiche le profil utilisé.
Site	Il affiche le site où l'appareil est utilisé.
Balise du site	Il affiche le nom du sous-site auquel il appartient.
Numéro de série	Il affiche le numéro de série de l'appareil.
Version du firmware	Il affiche la version actuelle du micrologiciel exécuté sur l'appareil.
Vu pour la dernière fois	Il affiche la date et l'heure de la dernière connexion de l'appareil.
Statut de la licence	Il indique si la licence est active ou non.
UID de l'appareil	Il affiche l'identification unique de l'appareil générée par l'équipe Cloud.
Date d'activation	Il affiche l'heure à laquelle la licence a été activée.
Date d'expiration	Il affiche l'heure à laquelle la licence expirera.

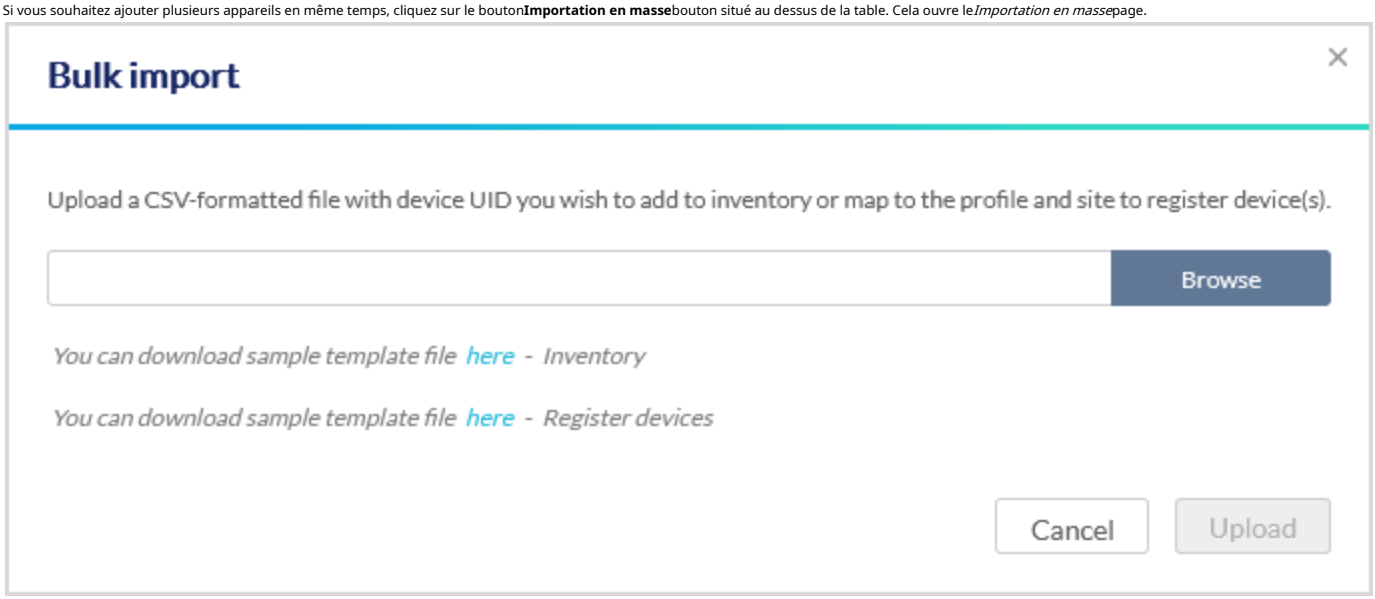
Pour ajouter un nouvel appareil au groupe d'appareils, cliquez sur l'icône**Ajouter un appareil**bouton situé au dessus de la table. Cela ouvre le*Ajouter un appareil*page. Pour supprimer plusieurs entrées à la fois, cochez les cases correspondantes des entrées que vous souhaitez supprimer, puis cliquez sur**Supprimer**.



Les champs disponibles sur cette page sont indiqués ci-dessous.

Champ	Description
UID de l'appareil	Saisissez l'identification unique de l'appareil générée par l'équipe Cloud.
Nom de l'appareil	Entrez le nom de l'appareil.
Site	Sélectionnez le site sur lequel l'appareil est utilisé.
Profil	Sélectionnez l'un des profils configurés que vous souhaitez utiliser.
Clé de licence n°1	Cliquez dans la case pour sélectionner l'une des licences disponibles.
Ajouter plus de licences	Clique le**Ajouter plus de licences**bouton pour ajouter plus de licences.
Sauvegarder	Cliquez sur**Sauvegarder**pour enregistrer les détails de votre appareil.
Annuler	Cliquez sur**Annuler**fermer le*Ajouter un appareil*page.

Si vous souhaitez ajouter plusieurs appareils en même temps, cliquez sur le bouton**Importation en masse**bouton situé au dessus de la table. Cela ouvre le*Importation en masse*page.



Cliquez sur**Parcourir**pour sélectionner et ouvrir le fichier au format CSV, puis cliquez sur**Télécharger**. Cela téléchargera le fichier avec l'UID de l'appareil soit vers l'inventaire, soit vers le profil et le site pour enregistrer le ou les appareils. Vous pouvez également télécharger les exemples de modèles pour l'inventaire et enregistrer les appareils ici.

Authentification

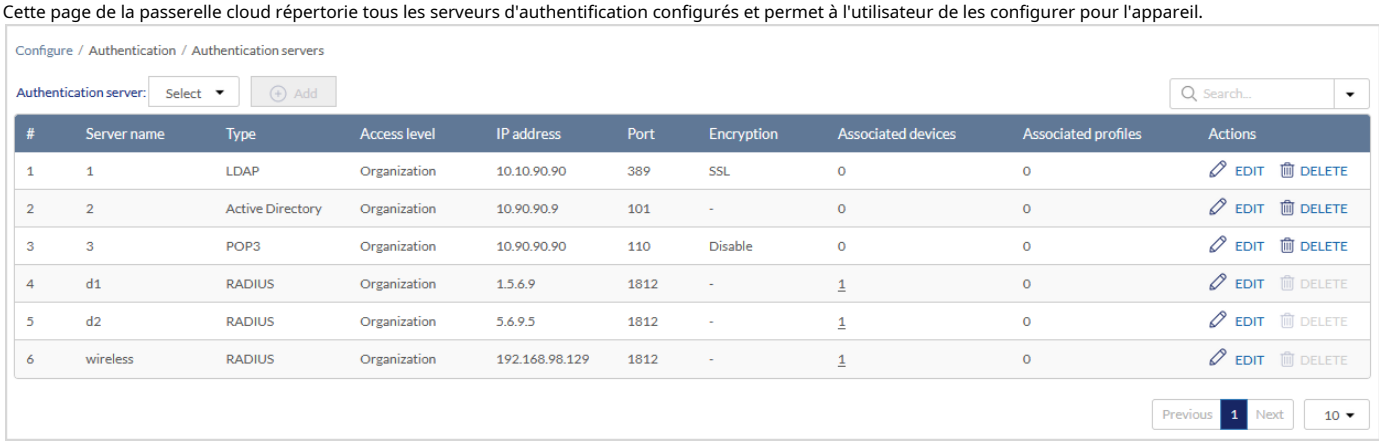
L'authentification réseau fait référence au processus lié à la sécurité requis lorsqu'un client tente de se connecter à votre réseau. La passerelle cloud Nuclias prend en charge le processus d'authentification de différentes manières, qui inclut le serveur d'authentification local et les serveurs d'authentification externes. Cette section du guide de l'utilisateur vous parlera de ces serveurs et de leur configuration.

Il comprend les thèmes suivants :

Serveurs d'authentification

Le chemin pour le**Serveurs d'authentification**la page est*Configurer > Authentification > Serveurs d'authentification*. Un serveur d'authentification est un service réseau qui fournit des informations d'identification aux utilisateurs authentifiés pour accéder au réseau. Lorsqu'un utilisateur saisit ces informations d'identification sur la page de connexion, l'accès au réseau est accordé. De plus, le serveur d'authentification gère une base de données d'utilisateurs ou une configuration de serveur d'authentification externe.

Cette page de la passerelle cloud répertorie tous les serveurs d'authentification configurés et permet à l'utilisateur de les configurer pour l'appareil.



Les champs disponibles dans le tableau sont les suivants :

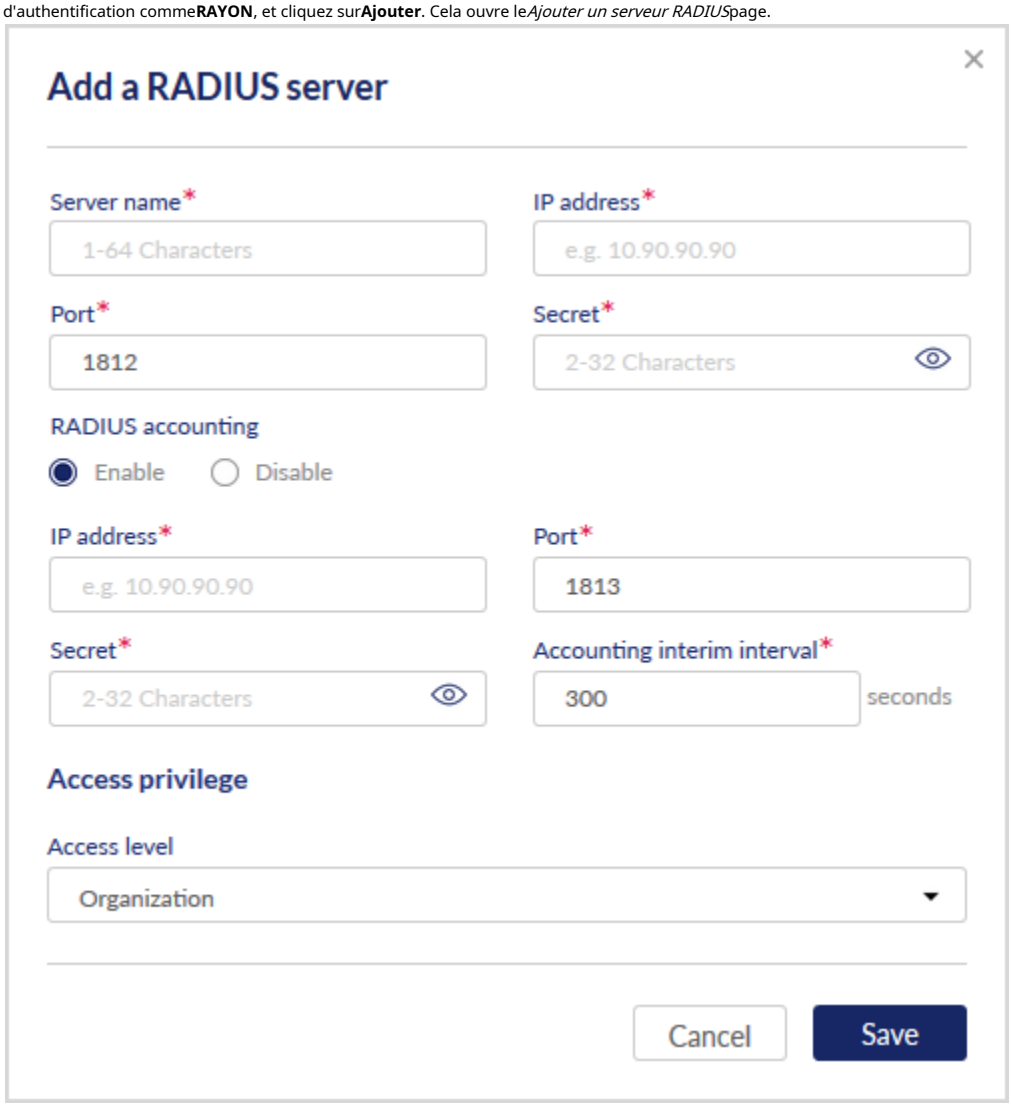
Champ	Description
Nom du serveur	Il affiche le nom du serveur.
Taper	Il affiche le type de serveur. Il peut s'agir de l'un des types de serveur suivants : RADIUS, LDAP, Active Directory, POP3 ou domaine NT.
Niveau d'accès	Il affiche le niveau d'accès autorisé à utiliser le serveur configuré.
adresse IP	Il affiche l'adresse IP du serveur d'authentification.
Port	Il affiche le port du serveur d'authentification.
Chiffrement	Il s'affiche si le cryptage est activé.
Appareils associés	Il affiche les appareils associés au serveur.
Profils associés	Il affiche le nombre de profils associés aux appareils utilisant le serveur d'authentification.
Actions	Vous pouvez modifier ou supprimer le serveur d'authentification configuré. Cliquez sur**Modifier**pour apporter des modifications au serveur d'authentification existant. Cela ouvre la page de configuration.

Pour ajouter un nouveau serveur d'authentification, sélectionnez le type de serveur d'authentification dans la liste déroulante présente au-dessus du tableau, puis cliquez sur l'icône **Ajouter** bouton. Cela ouvre la page de configuration du type de serveur sélectionné. Sélectionnez l'un des types de serveur d'authentification suivants :

- RAYON
- LDAP
- POP3
- Active Directory
- Domaine NT

RAYON

Un serveur RADIUS peut être configuré et accessible par la passerelle pour authentifier les connexions client. Pour ajouter un serveur Radius, sélectionnez le serveur d'authentification comme**RAYON**, et cliquez sur**Ajouter**. Cela ouvre le*Ajouter un serveur RADIUS*page.



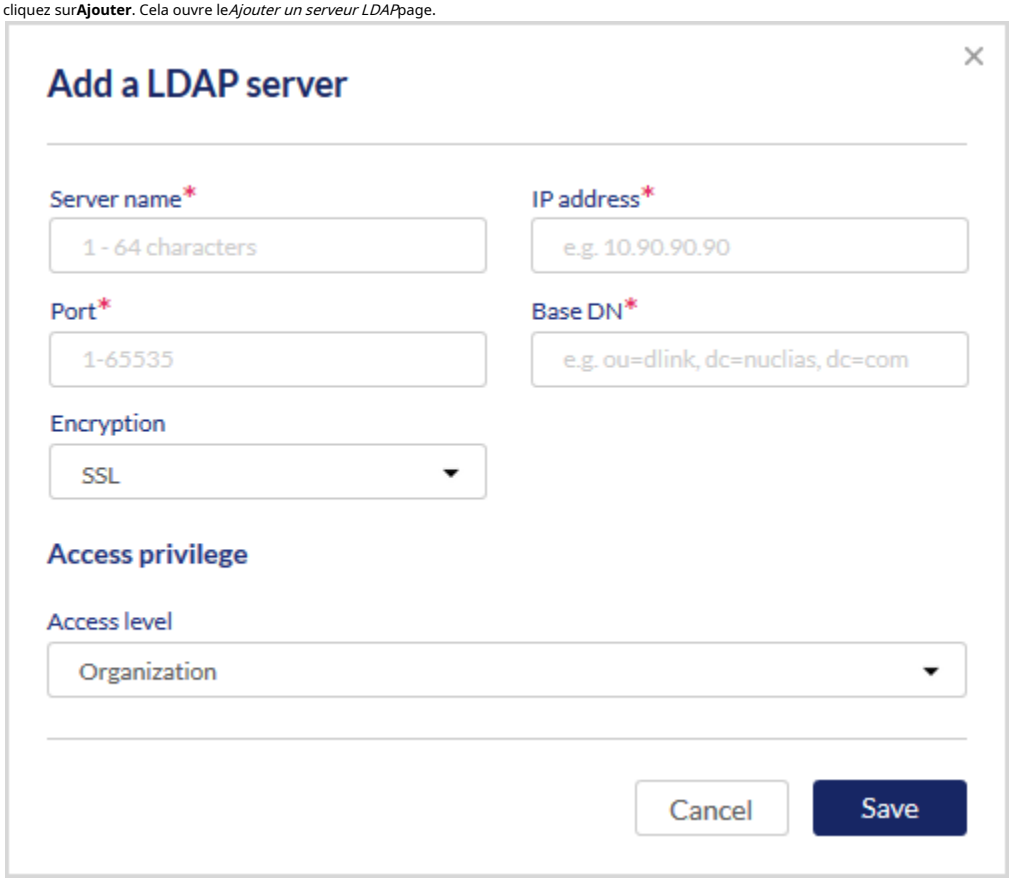
Les champs disponibles sur cette page sont les suivants :

Champ	Description
Nom du serveur	Entrez le nom du serveur.
adresse IP	Saisissez l'adresse IP du serveur d'authentification.
Port	Entrez le port du serveur d'authentification RADIUS.
Secrète	Entrez la clé secrète qui permet à l'appareil de se connecter au serveur RADIUS configuré. Il doit correspondre au secret du serveur RADIUS.
Comptabilité RAYON	Activez cette fonctionnalité pour configurer l'intervalle intermédiaire de comptabilité (en secondes), auquel l'appareil envoie les statistiques de trafic d'une session dans des messages de comptabilité au serveur Radius configuré.
adresse IP	Saisissez l'adresse IP du serveur de comptabilité RADIUS.
Port	Entrez le port de comptabilité RADIUS.
Secrète	Entrez la clé secrète qui permet à l'appareil de s'authentifier auprès du serveur de comptabilité RADIUS. Toutes les transactions comptables Radius entre le client et le serveur comptable RADIUS sont authentifiées grâce à ce secret partagé.

Intervalle comptable	Entrez l'intervalle intermédiaire, en secondes, auquel l'appareil doit envoyer les paquets Radius Accounting (Interim-Update). La valeur doit être comprise entre 300 et 3 600. Par défaut, elle est de 300.
Privilège d'accès	
Niveau d'accès	Le niveau d'accès décide des appareils qui peuvent utiliser ce serveur. Sélectionnez le niveau d'accès.
Sauvegarder	Cliquez sur**Sauvegarder**pour enregistrer le serveur d'authentification.
Annuler	Cliquez sur**Annuler**pour revenir aux paramètres précédents.

LDAP

La méthode d'authentification LDAP utilise LDAP pour échanger les informations d'authentification entre la passerelle et un serveur externe. Le serveur LDAP gère une grande base de données d'utilisateurs dans une structure de répertoires, de sorte que les utilisateurs portant le même nom d'utilisateur mais appartenant à des groupes différents peuvent être authentifiés puisque les informations utilisateur sont stockées hiérarchiquement. Notez également que la configuration d'un serveur LDAP sur des serveurs Windows ou Linux est considérablement moins complexe que la configuration de serveurs de domaine NT ou Active Directory pour l'authentification des utilisateurs. Pour ajouter un serveur LDAP, sélectionnez le serveur d'authentification comme**LDAP**, et cliquez sur**Ajouter**. Cela ouvre le*Ajouter un serveur LDAP*page.



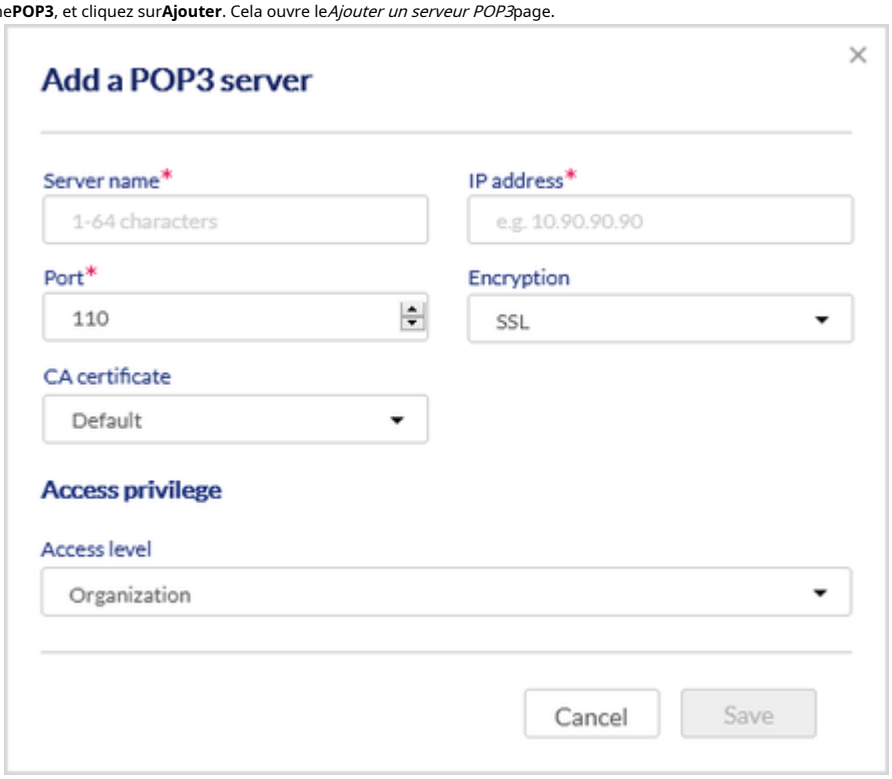
Les champs disponibles sur cette page sont les suivants :

Champ	Description
Nom du serveur	Entrez le nom du serveur.
adresse IP	Saisissez l'adresse IP du serveur LDAP.
Port	Entrez le port du serveur d'authentification LDAP.
DN de base	Entrez le nom de domaine de base.
Chiffrement	Vous pouvez activer le cryptage en sélectionnant SSL ou TLS dans la liste déroulante.
Privilège d'accès	
Niveau d'accès	Le niveau d'accès décide des appareils qui peuvent utiliser ce serveur. Sélectionnez le niveau d'accès.

Sauvegarder	Cliquez sur**Sauvegarder**pour enregistrer le serveur d'authentification.
Annuler	Cliquez sur**Annuler**pour revenir aux paramètres précédents.

POP3

POP3 est un protocole de couche application le plus couramment utilisé pour le courrier électronique via une connexion TCP/IP. Le serveur d'authentification peut être utilisé avec le cryptage SSL sur le port 995 pour envoyer du trafic crypté au serveur POP3. Un certificat CA vérifie le certificat du serveur POP3. Pour ajouter un serveur POP3, sélectionnez le serveur d'authentification comme**POP3**, et cliquez sur**Ajouter**. Cela ouvre le*Ajouter un serveur POP3*page.

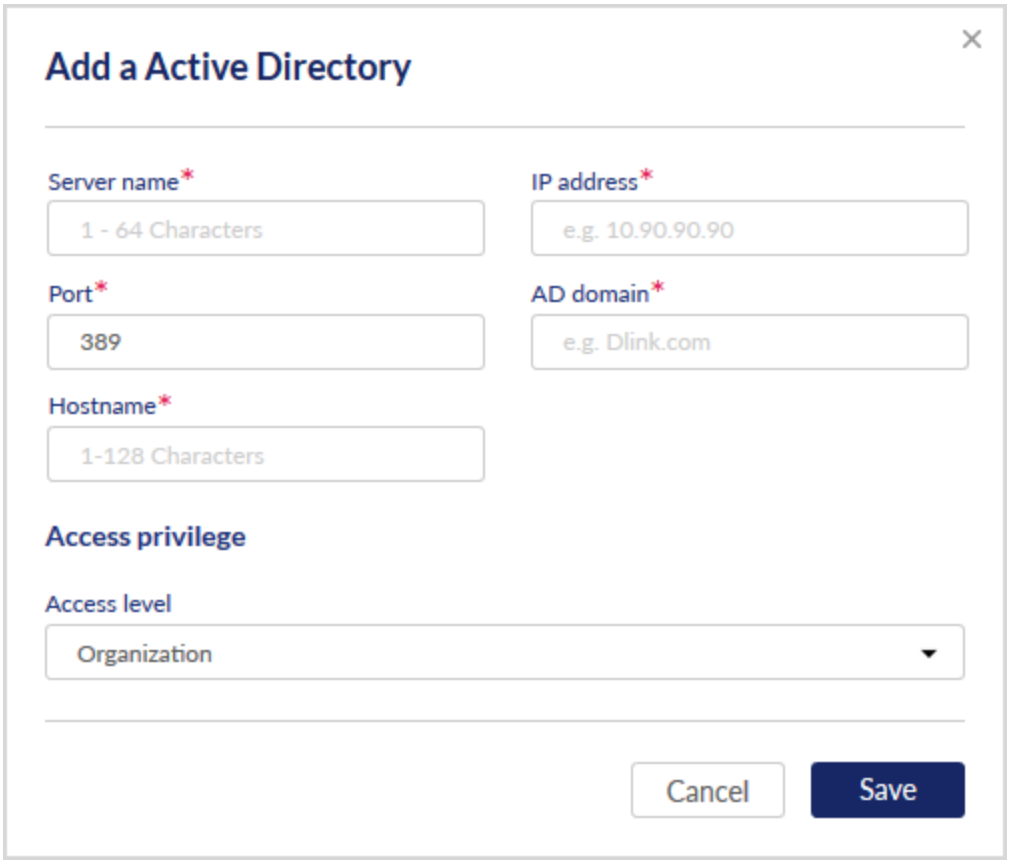


Les champs disponibles sur cette page sont les suivants :

Champ	Description
Nom du serveur	Entrez le nom du serveur.
adresse IP	Saisissez l'adresse IP du serveur POP3.
Port	Entrez le port du serveur d'authentification POP3.
Chiffrement	Vous pouvez activer ou désactiver la prise en charge SSL pour POP3. Si cette option est activée, il est obligatoire de sélectionner une autorité de certification pour celle-ci.
Certificat d'autorité de certification	Sélectionnez une autorité de certification pour vérifier le certificat du serveur POP3.
Privilège d'accès	
Niveau d'accès	Le niveau d'accès décide des appareils qui peuvent utiliser ce serveur. Sélectionnez le niveau d'accès.
Sauvegarder	Cliquez sur**Sauvegarder**pour enregistrer le serveur d'authentification.
Annuler	Cliquez sur**Annuler**pour revenir aux paramètres précédents.

Active Directory

L'authentification Active Directory est une version améliorée de l'authentification de domaine NT. Le protocole Kerberos est utilisé pour l'authentification des utilisateurs regroupés en unités organisationnelles (UO). Les serveurs d'authentification et le(s) domaine(s) Active Directory configurés sont utilisés pour valider l'utilisateur avec l'annuaire des utilisateurs sur le serveur Windows externe. Pour ajouter un serveur Active Directory, sélectionnez le serveur d'authentification comme **Active Directory**, et cliquez sur**Ajouter**. Cela ouvre le*Ajouter un Active Directory*page.

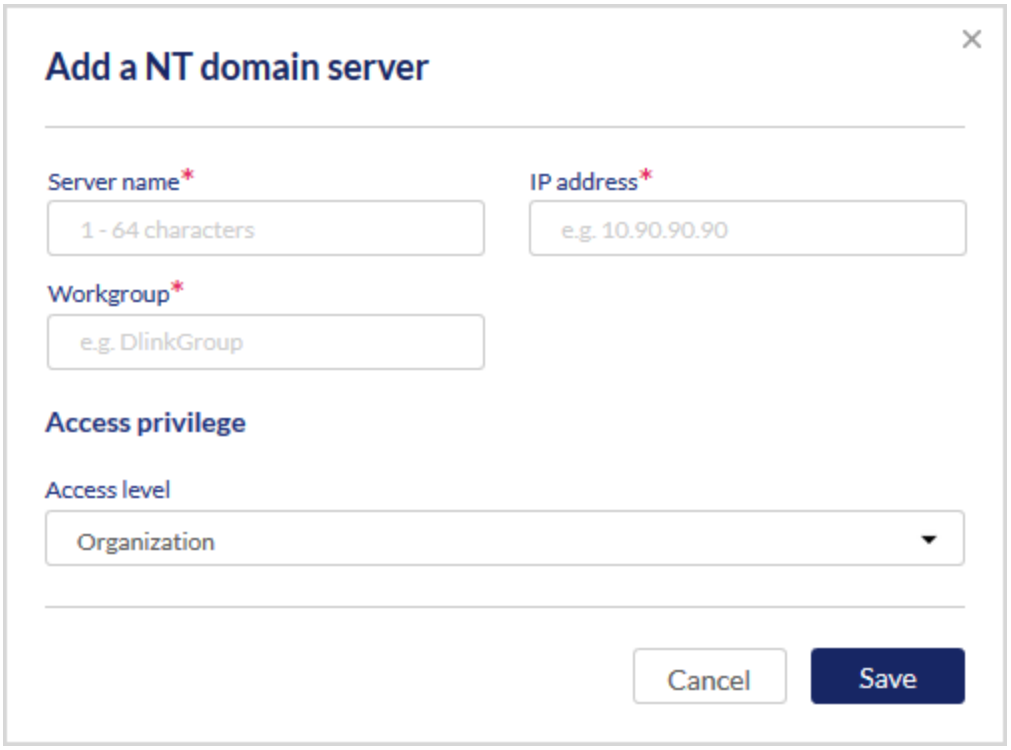


Les champs disponibles sur cette page sont les suivants :

Champ	Description
Nom du serveur	Entrez le nom du serveur.
adresse IP	Saisissez l'adresse IP du serveur Active Directory.
Port	Entrez le port du serveur d'authentification Active Directory.
Domaine AD	Active Directory étant le type d'authentification choisi, vous devez saisir le nom de domaine Active Directory dans ce champ. Les utilisateurs enregistrés dans la base de données Active Directory peuvent désormais accéder au portail VPN SSL en utilisant leur nom d'utilisateur et leur mot de passe Active Directory.
Nom d'hôte	Entrez le nom d'hôte du serveur pour Active Directory.
Privilège d'accès	
Niveau d'accès	Le niveau d'accès décide des appareils qui peuvent utiliser ce serveur. Sélectionnez le niveau d'accès.
Sauvegarder	Cliquez sur**Sauvegarder**pour enregistrer le serveur d'authentification.
Annuler	Cliquez sur**Annuler**pour revenir aux paramètres précédents.

Domaine NT

Le serveur de domaine NT permet aux utilisateurs et aux hôtes de s'authentifier via un groupe de travail préconfiguré
champ. Généralement, les serveurs Windows ou Samba sont utilisés pour gérer le domaine d'authentification du répertoire centralisé des utilisateurs autorisés. Pour ajouter un serveur de domaine NT, sélectionnez**Domaine NT**comme le*Serveur d'authentification*,et cliquez**Ajouter**. Cela ouvre le*Ajouter un serveur de domaine NT*page.

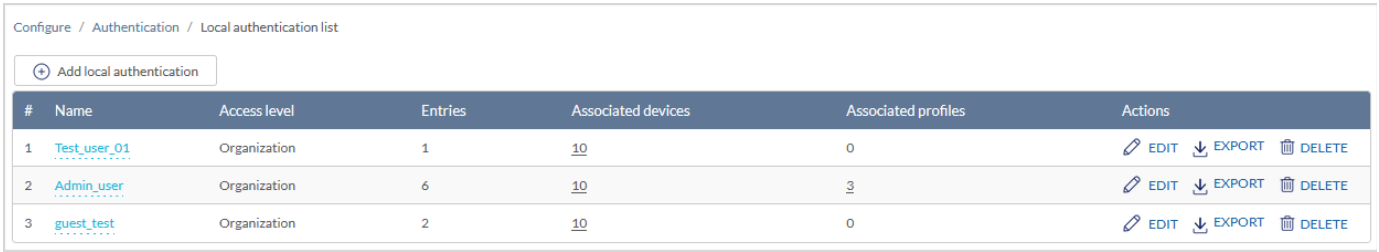


Les champs disponibles sur cette page sont les suivants :

Champ	Description
Nom du serveur	Entrez le nom du serveur.
adresse IP	Saisissez l'adresse IP du serveur d'authentification.
Groupe de travail	Entrez le(s) nom(s) du ou des groupes de travail NT.
Privilège d'accès	
Niveau d'accès	Le niveau d'accès décide des appareils qui peuvent utiliser ce serveur. Sélectionnez le niveau d'accès.
Sauvegarder	Cliquez sur**Sauvegarder**pour enregistrer le serveur d'authentification.
Annuler	Cliquez sur**Annuler**pour revenir aux paramètres précédents.

Liste d'authentification locale

Le chemin pour le**Liste d'authentification locale**la page est*Configurer > Authentification > Liste d'authentification locale*. Cette section répertorie toutes les authentifications locales enregistrées dans l'appareil et permet d'ajouter une nouvelle authentification locale.

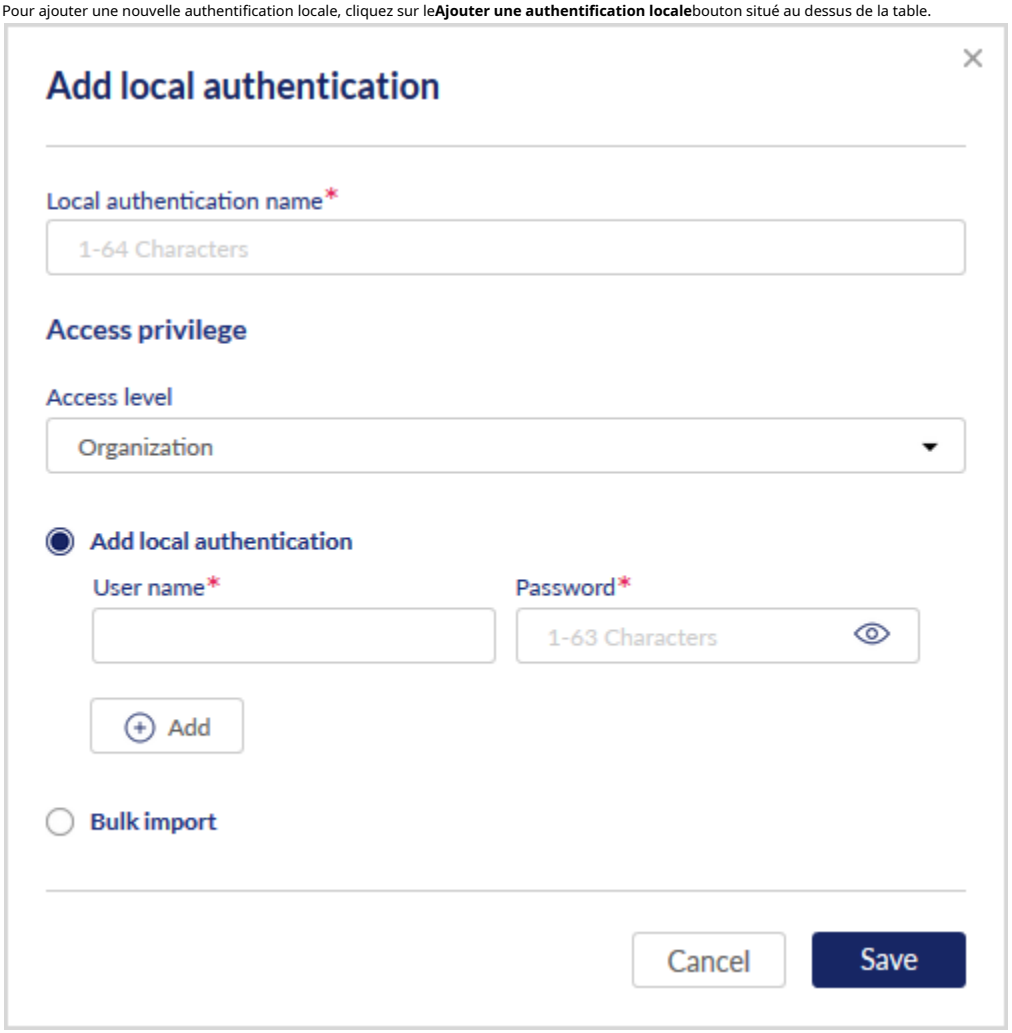


Les champs affichés dans la liste sont les suivants :

Champ	Description
Nom	Il affiche le nom du serveur.
Niveau d'accès	Il affiche le niveau d'accès autorisé à utiliser l'authentification locale.

Entrées	Il affiche le nombre d'identifiants de connexion enregistrés sous ce nom.
Appareils associés	Il affiche le nombre de périphériques associés au serveur.
Profils associés	Il affiche le nombre de profils associés aux appareils utilisant l'authentification locale.
Actions	Vous pouvez modifier ou supprimer le serveur d'authentification configuré. Cliquez sur**Modifier**pour apporter des modifications aux détails d'authentification existants. Cela ouvre le*Modifier l'authentification locale*page. Vous pouvez exporter les détails en cliquant sur**Exporter**.

Pour ajouter une nouvelle authentification locale, cliquez sur le**Ajouter une authentification locale**bouton situé au dessus de la table.



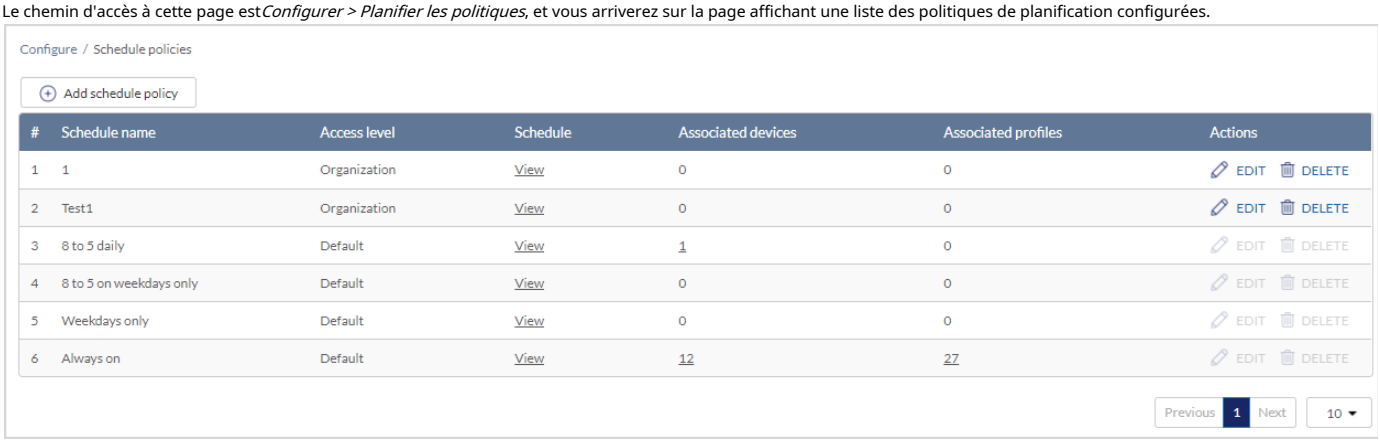
Les champs disponibles sur cette page sont les suivants :

Champ	Description
Nom d'authentification local	Entrez le nom du serveur.
Niveau d'accès	Sélectionnez le niveau d'accès dans la liste déroulante. Les appareils qui relèvent de ce niveau peuvent accéder à l'authentification locale configurée.
Ajouter une authentification locale	Entrez le nom d'utilisateur et le mot de passe. Pour ajouter d'autres entrées, cliquez sur le**Ajouter**bouton.
Importation en masse	Pour ajouter plusieurs entrées à la fois, sélectionnez**Importation en masse**. Cliquez sur**Parcourir**pour localiser et sélectionner le fichier au format *.csv et télécharger les entrées. Vous pouvez également télécharger l'exemple de fichier de modèle ici.
Sauvegarder	Cliquez sur**Sauvegarder**pour enregistrer vos paramètres.
Annuler	Cliquez sur**Annuler**pour revenir aux paramètres précédents.

Politiques de planification

Le*Politiques de planification*La page affiche toutes les politiques de planification par défaut et configurées pour les appareils. Ces plannings permettent d'activer quelques fonctionnalités de la passerelle pendant une certaine période de temps. Ainsi, pour des fonctionnalités telles que le filtre de contenu Web, le contrôle d'accès, etc., vous pouvez configurer les planifications sur cette page, puis sélectionner l'une de ces planifications dans la liste déroulante lors de la configuration de ces fonctionnalités.

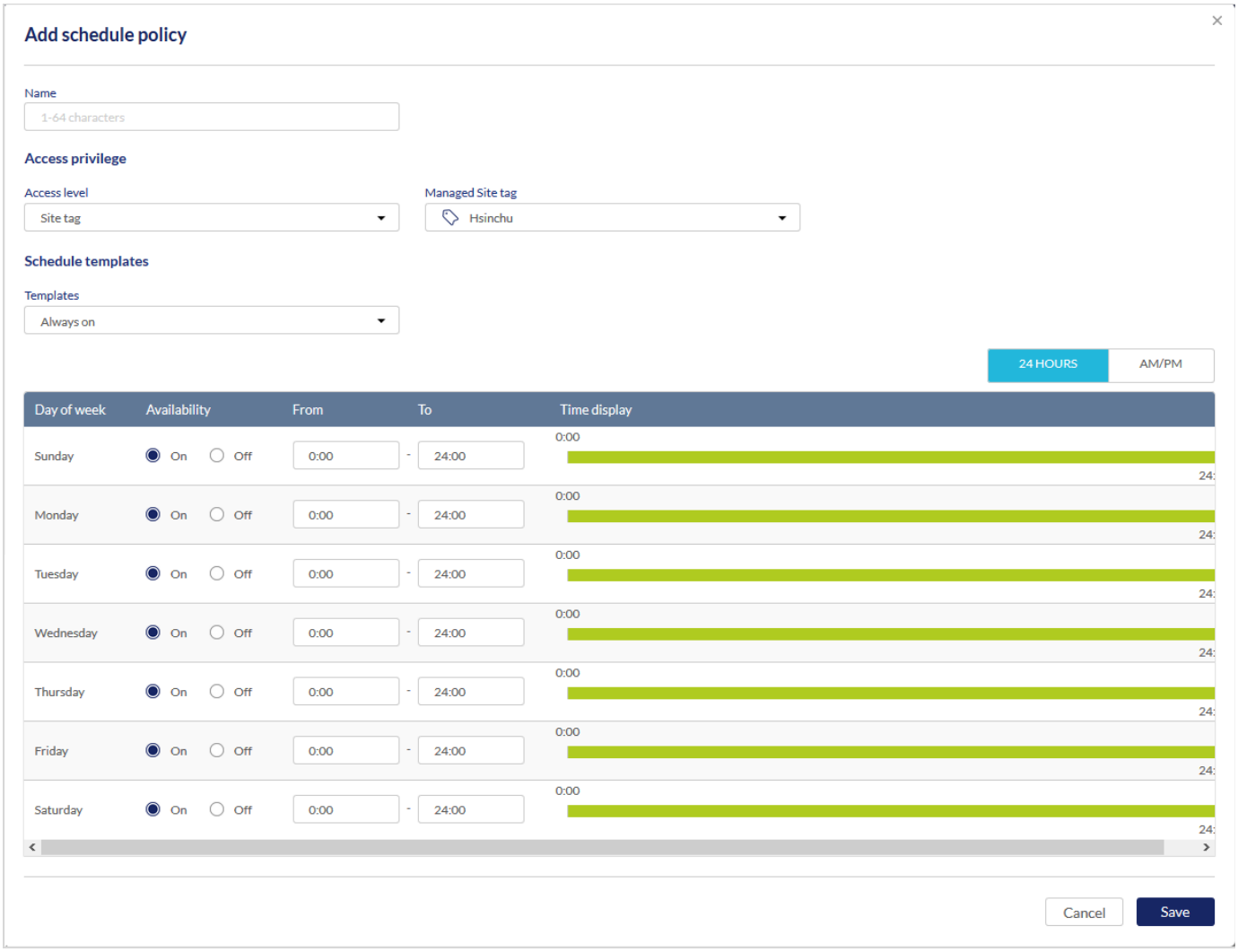
Le chemin d'accès à cette page est*Configurer > Planifier les politiques*, et vous arriverez sur la page affichant une liste des politiques de planification configurées.



Les champs affichés dans le tableau sont les suivants :

Champ	Description
Nom du programme	Il affiche le nom du planning configuré.
Niveau d'accès	Il affiche le niveau auquel le planning est appliqué.
Calendrier	Cliquez sur**Voir**pour voir le détail du planning.
Appareils associés	Il affiche le nombre de périphériques associés à cette stratégie particulière.
Profils associés	Il affiche le nombre de profils associés aux appareils utilisant la politique de planification particulière.
Actions	Vous pouvez cliquer**Modifier**ou**Supprimer**pour modifier ou supprimer ceux existants. ***Note:****Les stratégies avec le niveau d'accès par défaut sont des stratégies de modèles et ne peuvent pas être modifiées ou supprimées ; par conséquent, les options d'édition et de suppression ne sont pas disponibles.*

Pour ajouter une nouvelle politique de planification, cliquez sur le bouton**Ajouter une politique de planification**bouton. Cela ouvre le*Ajouter une politique de planification*page.



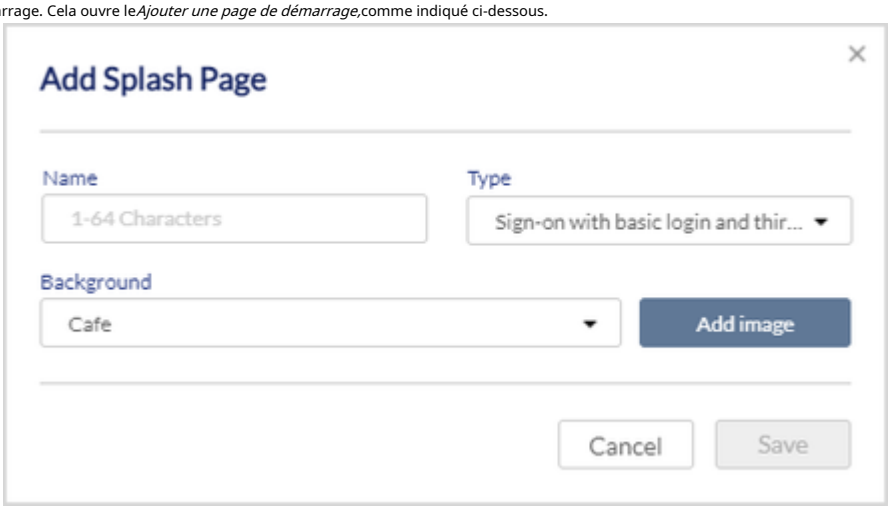
Les champs disponibles sur cette page sont les suivants :

Champ	Description
Nom	Entrez un nom descriptif pour le planning.
Privilège d'accès	
Niveau d'accès	Sélectionnez le niveau auquel la planification doit être appliquée. Les options sont Organisation, Site et Balise de site.
Balise du site géré	Sélectionnez le site tag auquel l'utilisateur pourra appliquer cette règle de planification. Ce champ est disponible uniquement lorsque vous sélectionnez le**Balise du site**dans le champ Niveau d'accès.
Site géré	Sélectionnez le site sur lequel cette politique sera disponible pour que l'utilisateur puisse l'appliquer. Ce champ est disponible uniquement lorsque vous sélectionnez**Site**dans le champ Niveau d'accès.
Modèles de planning	
Modèle	Sélectionnez l'un des modèles planifiés préconfigurés suivants :*8 à 5 par jour*,*8h à 17h en semaine uniquement*,*en semaine uniquement*, et*Toujours allumé*.
Jour de la semaine	Cette colonne affiche les jours de la semaine.
Disponibilité	Il indique si la règle est appliquée le jour sélectionné à la plage horaire mentionnée ou non. Si la fonctionnalité de disponibilité est**Sur**, la règle s'applique pendant la plage horaire mentionnée, et si elle est**Désactivé**, la règle s'applique en dehors de la plage horaire mentionnée. Par exemple, le créneau horaire sélectionné est de 15h00 à 18h00. Si la disponibilité est On, alors la règle s'applique pendant ces heures (3 heures), et si elle est Off, la règle s'applique aux heures autres que 15h00 à 18h00, soit pour le reste des 21h.

Depuis	Entrez l'heure de début à laquelle la stratégie est appliquée ou non.
À	Entrez l'heure de fin à laquelle la stratégie est appliquée ou non.
Affichage de l'heure	Il affiche le format (24 heures ou 12 heures) dans lequel vous souhaitez voir l'heure.
Sauvegarder	Cliquez sur**Sauvegarder**pour ajouter une nouvelle politique de planification.
Annuler	Cliquez sur**Annuler**pour revenir aux paramètres précédents.

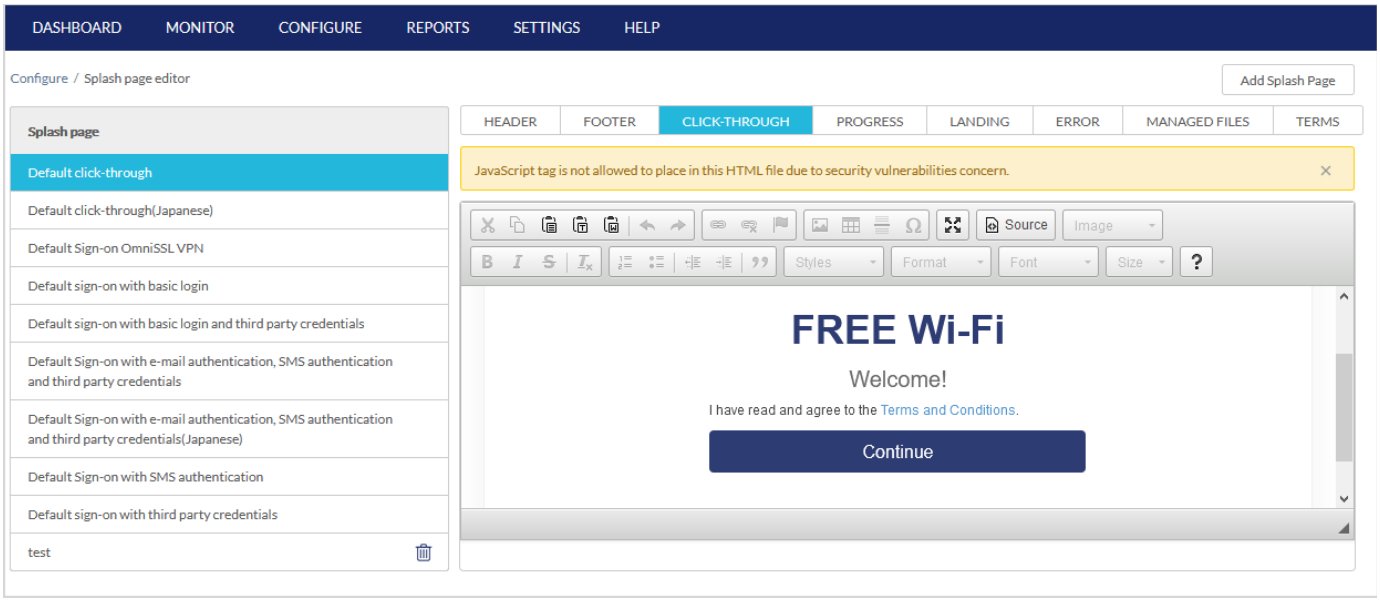
Éditeur de page de garde

La passerelle cloud Nuclias, DBG-2000, permet à ses utilisateurs de personnaliser la page d'accueil selon leurs besoins, par exemple, ils peuvent ajouter un logo d'entreprise ou modifier la palette de couleurs. Il vous permet de créer, modifier ou supprimer les pages de démarrage existantes. Clique le**Ajouter une page Splash**bouton présent dans le coin supérieur droit de la page pour ajouter une nouvelle page de démarrage. Cela ouvre le*Ajouter une page de démarrage,*comme indiqué ci-dessous.



Les champs disponibles sur le*Ajouter une page de garde*sont les suivants:

Champ	Description
Nom	Entrez un nom pour la page de garde d'une longueur de 1 à 64 caractères.
Taper	Sélectionnez l'un des types de pages de démarrage que vous souhaitez créer. Vous pouvez créer plusieurs pages de garde pour le même type. • Clic • Connexion par clic (japonais) • avec connexion de base • Connectez-vous avec une connexion de base et des informations d'identification tierces • Connectez-vous avec l'authentification par e-mail, l'authentification par SMS et les informations d'identification de tiers • Connectez-vous avec l'authentification par e-mail, l'authentification par SMS et les informations d'identification de tiers (japonais) • Connectez-vous avec l'authentification SMS Connectez- • vous avec des informations d'identification tierces ***Note**: Actuellement, le DBG-2000 ne prend pas en charge l'authentification SMS et l'authentification e-mail.*
Arrière-plan	Vous pouvez soit sélectionner l'un des arrière-plans disponibles, soit également ajouter une image. Cliquez sur**Ajouter une image**pour télécharger votre image personnalisée pour l'arrière-plan.
Sauvegarder	Cliquez sur**Sauvegarder**pour enregistrer vos paramètres.
Annuler	Cliquez sur**Annuler**pour revenir aux paramètres précédents.

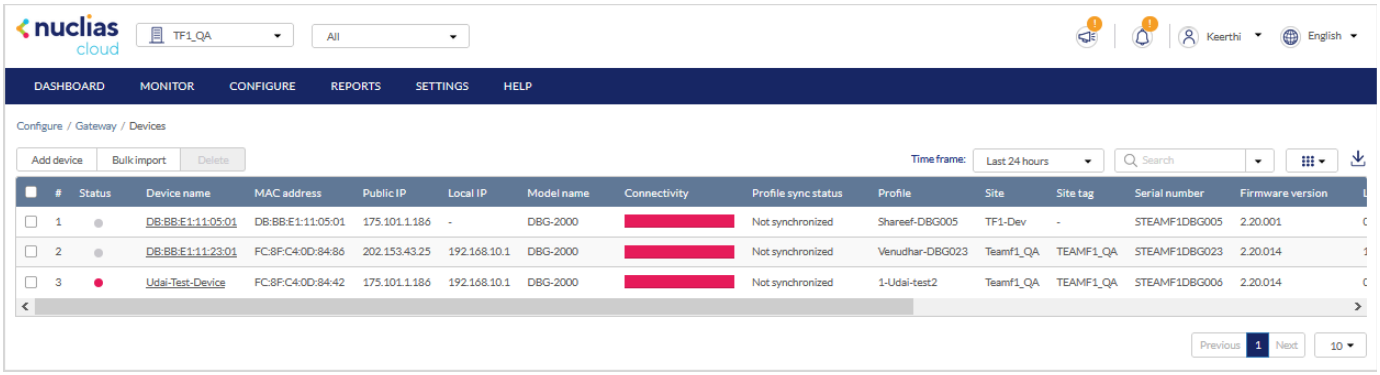


Les champs disponibles sur le*Éditeur de page de garde*page sont les suivantes :

Champ	Description
Page d'accueil	Il répertorie tous les types de pages de démarrage. Cliquez sur le type d'authentification requis du portail captif et ajoutez/modifiez/supprimez la page.
Entête	Vous pouvez modifier le style et le format de l'en-tête de la page de démarrage.
Bas de page	Vous pouvez modifier le style et le format du pied de page de la page de démarrage.
Clic	Vous pouvez modifier le style et le format de la page cliquable. Cet onglet est disponible en sélectionnant soit**Clic par défaut**ou**Clic par défaut (japonais)**comme les types de page de démarrage.
Se connecter	La page de connexion affiche la page de connexion en fonction du type de page de démarrage de connexion sélectionné.
Progrès	Il affiche la page indiquant que l'authentification est en cours.
Atterrissage	Il affiche la page qui apparaît après une authentification réussie.
Erreur	Il affiche les erreurs à afficher lorsque l'authentification échoue.
Fichiers gérés	Vous pouvez télécharger des fichiers spécifiques à un utilisateur ou à une organisation.
Termes	Il affiche les termes et conditions que vous devez suivre lors de l'utilisation du portail captif.
Sauvegarder	Cliquez sur**Sauvegarder**pour enregistrer vos paramètres.
Annuler	Cliquez sur**Annuler**pour revenir aux paramètres précédents.

Chapitre 1 Base

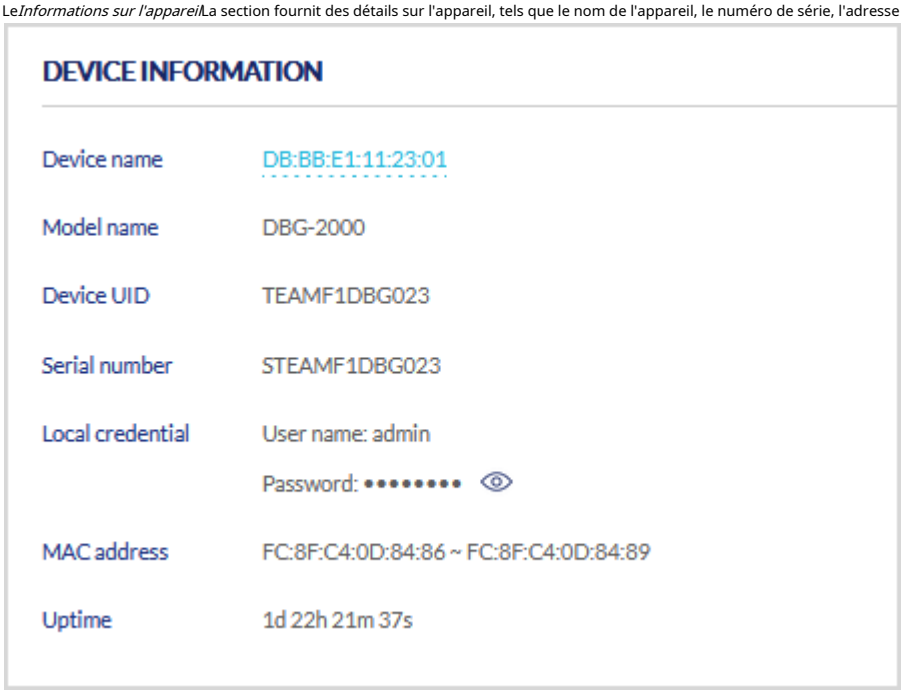
Ce chapitre fournit un aperçu des informations relatives à l'appareil. Pour ouvrir le*Basique*page, suivez le chemin*Configurer > Passerelle > Périphériques*, c'est-à-dire dans le **Configurer**menu, cliquez sur**passerelle**, puis cliquez sur**Dispositifs**. Cela ouvre le**Dispositifs**page. Il se compose d'une liste d'appareils présents dans le groupe d'appareils pour la période sélectionnée. Dans le**Nom de l'appareil**colonne, cliquez sur n'importe quelle entrée pour ouvrir la*Basique*page du DBG-2000. Le*Basique*La page affiche les informations suivantes : informations sur le périphérique, emplacement, interface WAN, site et profil. Pour enregistrer les modifications, cliquez sur**Sauvegarder**, et pour revenir aux paramètres précédents, cliquez sur**Annuler**.



Ce chapitre couvre les sujets suivants:

Device Information

Le*Informations sur l'appareil*La section fournit des détails sur l'appareil, tels que le nom de l'appareil, le numéro de série, l'adresse MAC et les informations d'identification locales.

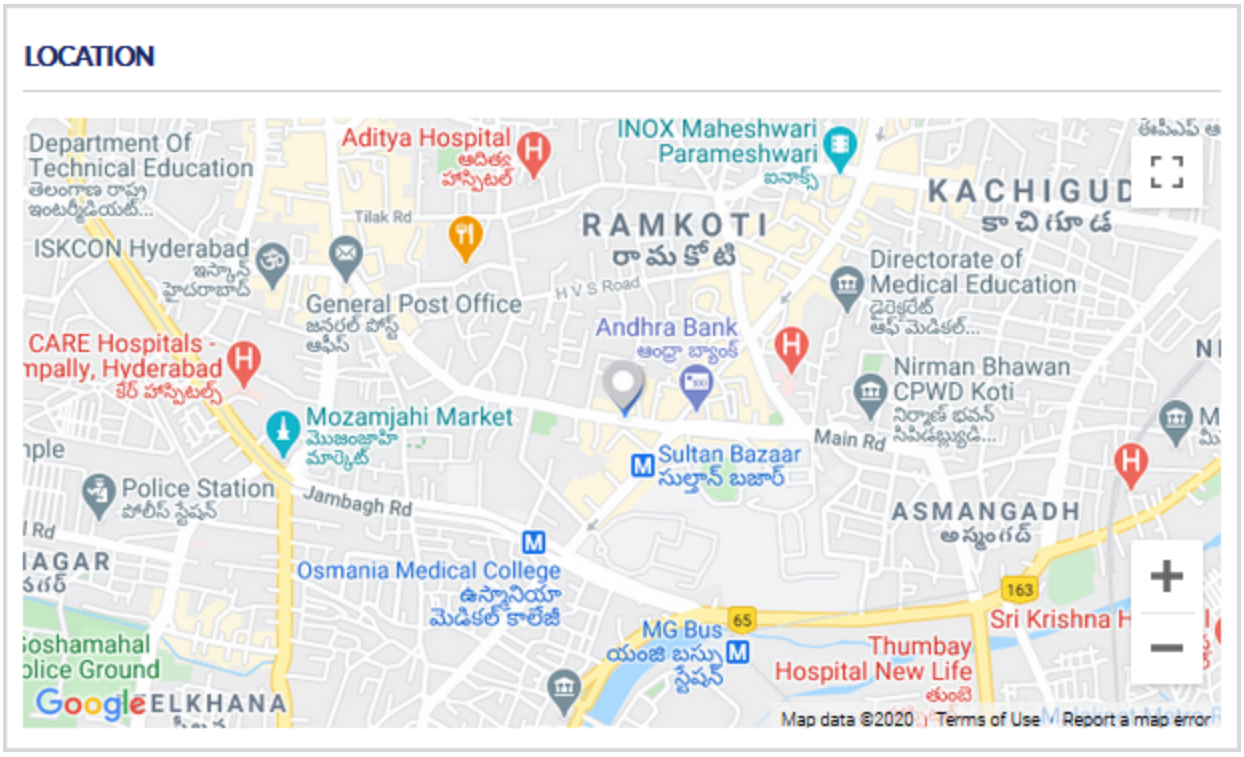


Les champs disponibles sur cette page sont les suivants :

Champ	Description
Nom de l'appareil	Il indique le nom de l'appareil. Vous pouvez cliquer et modifier le nom de l'appareil.
Nom du modèle	Il affiche le nom du modèle de votre appareil.
UID de l'appareil	Il affiche l'identification unique de l'appareil générée par l'équipe Cloud pour les fonctionnalités liées aux licences.
Numéro de série	Il affiche le numéro de série de votre appareil.
Identifiants locaux	Il affiche le nom d'utilisateur et le mot de passe pour se connecter à l'interface Web du DBG-2000.
Adresse Mac	Il affiche la plage d'adresses MAC.
Temps de disponibilité	Il affiche la durée depuis le dernier redémarrage.

Location

Le*Emplacement*La section indique l'endroit sur la carte où l'appareil est déployé.



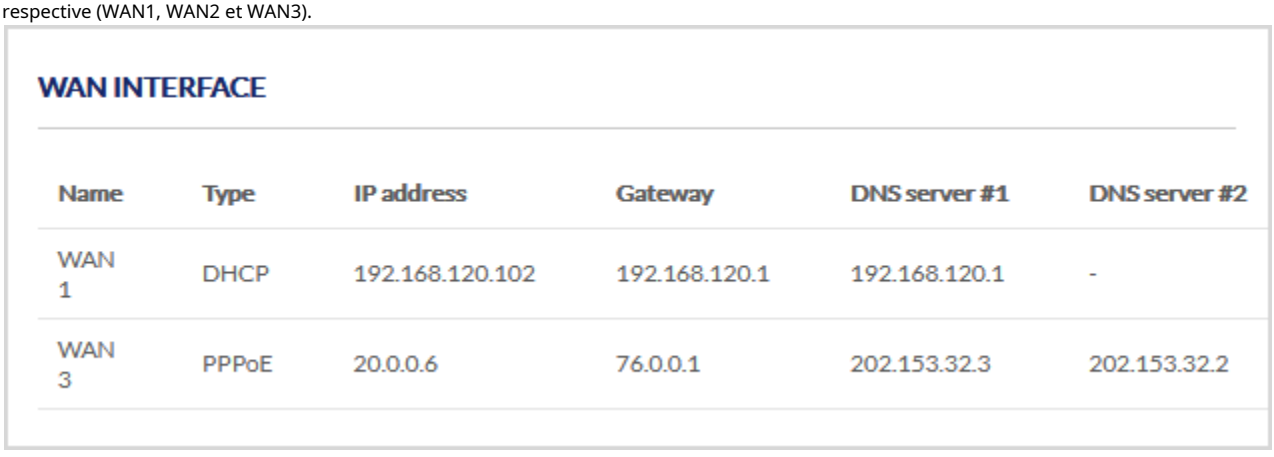
Utilisez l'une des méthodes suivantes pour ajuster la taille de la carte :

- **Contrôle**touche + défilement pour zoomer ou dézoomer sur la carte
- Cliquez sur "**+**" et "**-**", situés dans le coin inférieur droit de la carte, pour zoomer et dézoomer, respectivement.

Dans le coin supérieur droit, sélectionnez l'icône plein écran pour afficher la carte en plein écran. Pour quitter le mode plein écran, appuyez sur la touche**Échap**ou cliquez sur l'icône de réduction dans le coin supérieur droit pour la faire basculer vers le petit écran.

WAN Interface

Sur la page De base, cette section fournit des détails sur l'interface WAN du périphérique et affiche les informations suivantes pour l'interface WAN respective (WAN1, WAN2 et WAN3).



WAN INTERFACE

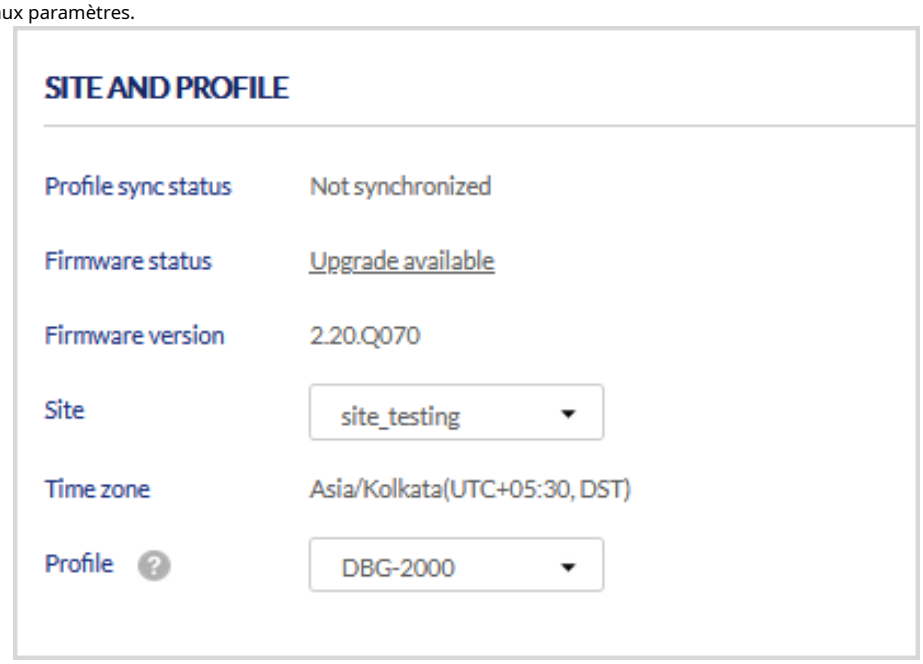
Name	Type	IP address	Gateway	DNS server #1	DNS server #2
WAN 1	DHCP	192.168.120.102	192.168.120.1	192.168.120.1	-
WAN 3	PPPoE	20.0.0.6	76.0.0.1	202.153.32.3	202.153.32.2

Champ	Description
Nom	Il affiche le nom de l'interface WAN.
Taper	Il affiche le type de connexion Internet utilisé pour le port WAN respectif.
adresse IP	Il affiche l'adresse IP obtenue ou configurée pour l'interface WAN.
passerelle	Il affiche l'adresse IP de la passerelle.
Serveur DNS 1	Il affiche l'adresse IP du serveur DNS principal.

Serveur DNS 2	Il affiche l'adresse IP du serveur DNS secondaire.

Site et profil

Le*Site et profil*La section détaille la synchronisation du profil, le micrologiciel et le profil utilisé. De plus, il vous permet de modifier le profil et de reconfigurer l'appareil avec les nouveaux paramètres.



Champ	Description
État de synchronisation du profil	Lorsque vous poussez une configuration et que l'appareil est accessible, il affiche**Synchronisé**, et si l'appareil n'est pas accessible, il affiche**Non synchronisé**.
État du micrologiciel	Ce champ vous permet de savoir si des mises à jour du firmware sont disponibles sur le serveur.
Version du firmware	Il affiche la version actuelle du micrologiciel exécuté sur votre appareil.
Site	Il affiche le site auquel appartient l'appareil.
Fuseau horaire	Il affiche le fuseau horaire actuel de l'appareil.
Profil	Il affiche la configuration du profil appliquée à l'appareil.

Résumé du chapitre 2

Ce chapitre fournit des détails sur la connectivité des ports du périphérique DBG-2000. Il indique la quantité de données téléchargées ou téléchargées depuis les interfaces WAN et informe sur l'utilisation d'Internet et son trafic sur chaque port. Il comprend également un aperçu de l'utilisation du VPN et de l'état VPN de chaque type de VPN.

Ce chapitre couvre les sujets suivants:

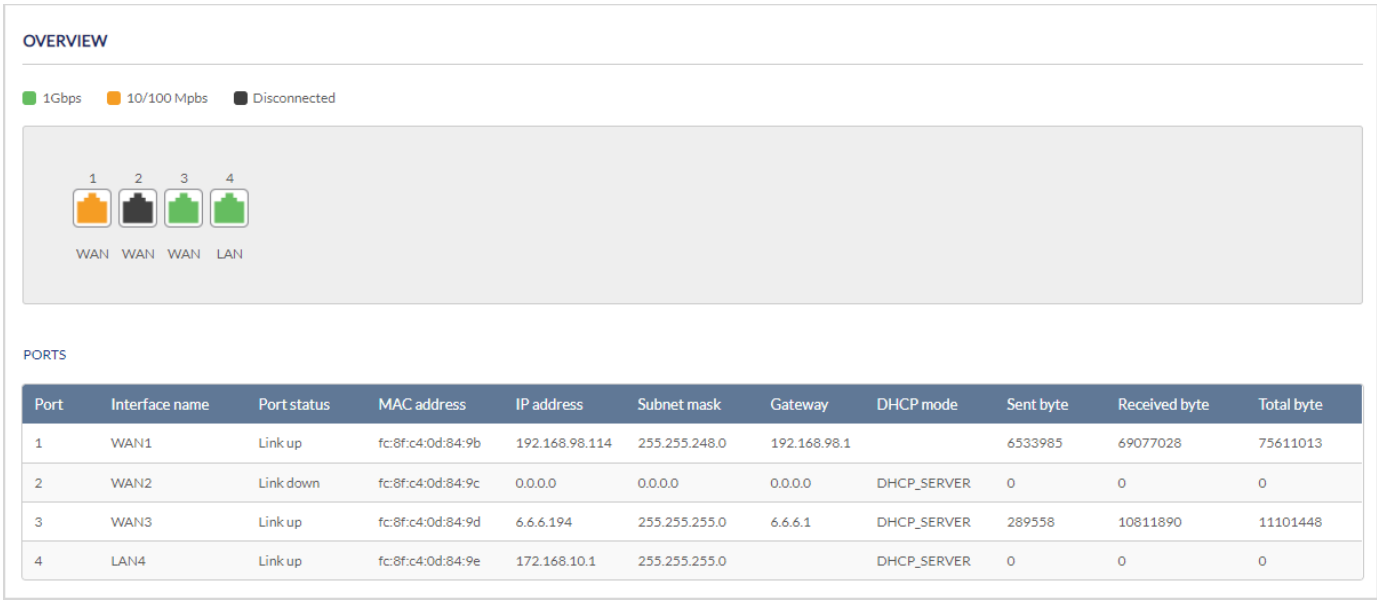
Statut

Le**Statut**L'onglet de l'interface de gestion Web de la passerelle fournit l'état du périphérique qui inclut l'état du port, le trafic Internet et l'utilisation d'Internet. Cette page couvre les sujets suivants :

- Aperçu
- Circulation du Internet
- Utilisation d'Internet

Aperçu

Sous**Aperçu**, vous trouverez des détails sur tous les ports de votre appareil. Les ports 1 Gbit/s connectés sont indiqués dans**Vert**couleur. Si l'interface est en panne, déconnectée ou si les ports sont désactivés, ils sont indiqués dans**Noir**, et les ports 10/100Mbps connectés sont indiqués dans**Orange**.



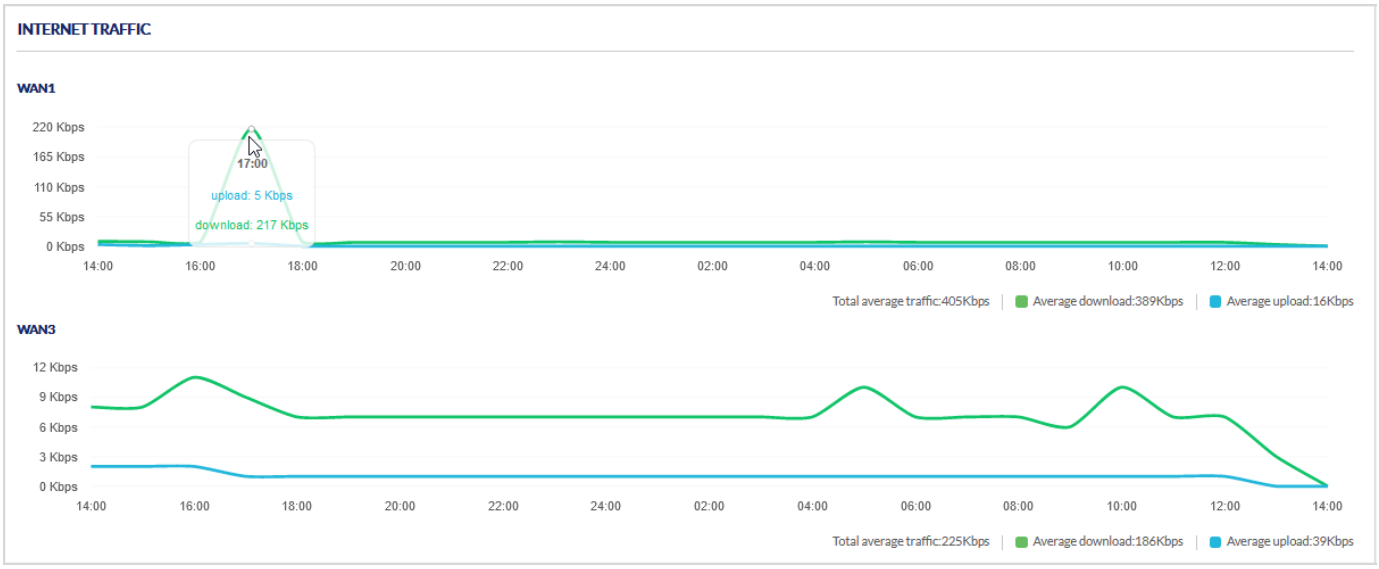
Port	Interface name	Port status	MAC address	IP address	Subnet mask	Gateway	DHCP mode	Sent byte	Received byte	Total byte
1	WAN1	Link up	fc:8f:c4:0d:84:9b	192.168.98.114	255.255.248.0	192.168.98.1		6533985	69077028	75611013
2	WAN2	Link down	fc:8f:c4:0d:84:9c	0.0.0.0	0.0.0.0	0.0.0.0	DHCP_SERVER	0	0	0
3	WAN3	Link up	fc:8f:c4:0d:84:9d	6.6.6.194	255.255.255.0	6.6.6.1	DHCP_SERVER	289558	10811890	11101448
4	LAN4	Link up	fc:8f:c4:0d:84:9e	172.168.10.1	255.255.255.0		DHCP_SERVER	0	0	0

Les champs affichés dans le*Ports*le tableau est le suivant :

Champ	Description
Port	Il affiche les numéros de port.
Nom de l'interface	Il affiche les interfaces de l'appareil.
Statut du port	Il indique si le port est connecté vers le haut ou vers le bas.
Adresse Mac	Il affiche l'adresse MAC du port.
adresse IP	Il affiche l'adresse IP du port.
Masque de sous-réseau	Il affiche le masque de sous-réseau du port.
passerelle	Il affiche l'adresse IP de la passerelle du port.
Mode DHCP	Il affiche le mode DHCP du port. Il pourrait être**Aucun**,**Serveur DHCP**,ou**Relais DHCP**.
Octet envoyé	Il affiche le nombre d'octets transmis depuis cette interface.
Octet reçu	Il affiche le nombre d'octets reçus sur cette interface.
Octet total	Il affiche le nombre total d'octets envoyés et reçus sur cette interface.

Circulation du Internet

Cette section affiche graphiquement la vitesse des données sur les ports WAN configurés au cours des dernières 24 heures. Il indique la vitesse moyenne de téléchargement et la vitesse moyenne de téléchargement du trafic Internet. Lorsque la souris survole le graphique, elle spécifie la vitesse de téléchargement et de téléchargement à un moment précis.

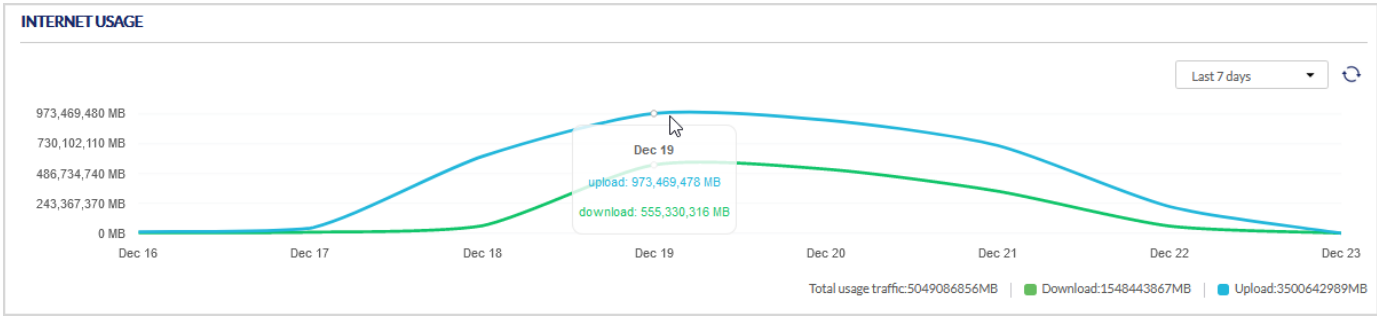


Les champs affichés dans le graphique du trafic Internet sont les suivants :

Champ	Description
Trafic moyen total	Il indique la moyenne du trafic total transitant via le port WAN.
Téléchargement moyen	Il indique la vitesse moyenne de téléchargement.
Téléchargement moyen	Il indique la vitesse de téléchargement moyenne.

Utilisation d'Internet

Cette section affiche graphiquement l'utilisation d'Internet. Il indique le téléchargement, le téléchargement et l'utilisation totale d'Internet pour la période sélectionnée. Vous pouvez sélectionner la période dans la liste déroulante située dans le coin supérieur droit du graphique. Pour mettre à jour le graphique avec les dernières données, cliquez sur le bouton *Rafraîchir*icône à côté de*Laps de temps*boîte. Lorsque la souris survole le graphique, elle spécifie les données de téléchargement et les données de téléchargement à un moment précis.



Les champs affichés dans le graphique d'utilisation d'Internet sont les suivants :

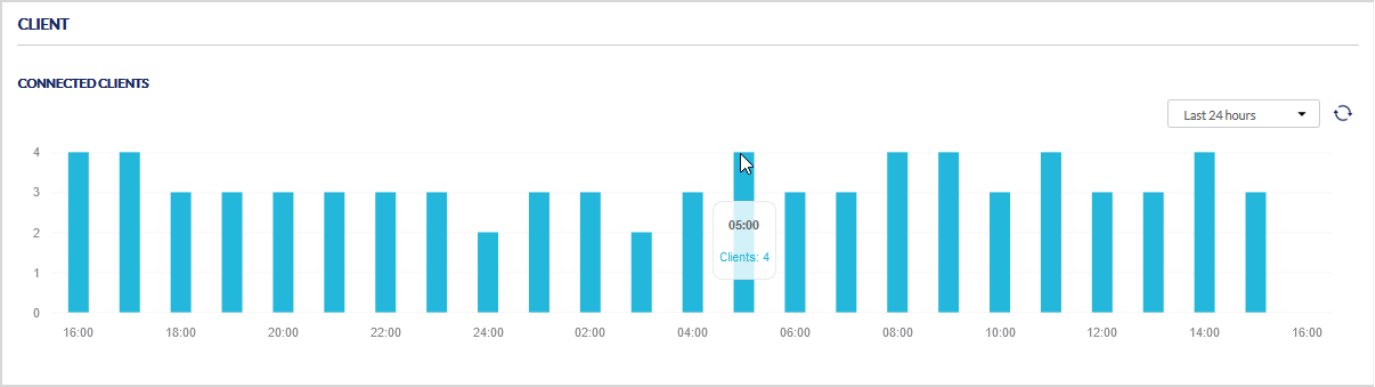
Champ	Description
Laps de temps	Sélectionnez la durée pendant laquelle les données d'utilisation d'Internet sont affichées.
Trafic d'utilisation total	Il indique le total des données transférées via les ports WAN pour la période sélectionnée.
Télécharger	Il indique le total des données téléchargées via les ports WAN pour la période sélectionnée.
Télécharger	Il indique le total des données téléchargées via les ports WAN pour la période sélectionnée.

Statistic

Le*Statistique*La page fournit un aperçu du nombre de clients connectés à votre passerelle, des ports WAN de la passerelle et de l'utilisation du VPN. Il collecte les données de l'appareil et les représente graphiquement, à savoir. graphique à barres ou graphique linéaire.

Client

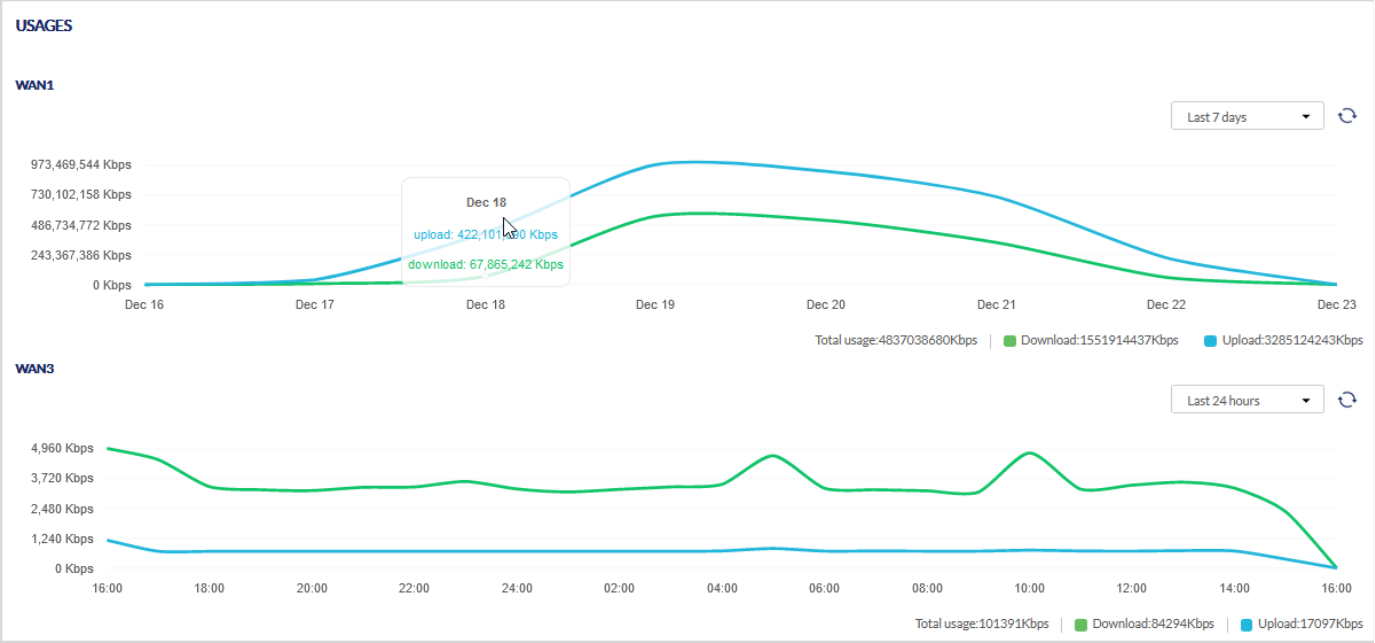
Cette section affiche un graphique à barres du nombre de clients connectés à votre passerelle pour la période sélectionnée. Le*Laps de temps*Le champ vous permet de sélectionner le nombre de jours pendant lesquels vous souhaitez voir le graphique à barres. Vous pouvez cliquer sur le*Rafraîchir*icône pour mettre à jour le graphique avec les dernières lectures. Lorsque la souris survole le graphique, elle affiche le nombre de clients connectés à cet instant.



Coutumes

BLÊME

Cette section affiche la vitesse à laquelle les données sont téléchargées depuis le port WAN particulier pour la période sélectionnée. Vous pouvez sélectionner le*Laps de temps*dans la liste déroulante située dans le coin supérieur droit du graphique, puis cliquez sur le bouton*Rafraîchir*icône pour mettre à jour le graphique avec les dernières lectures. Lorsque la souris survole le graphique, elle affiche la vitesse de téléchargement et de téléchargement à un moment donné.

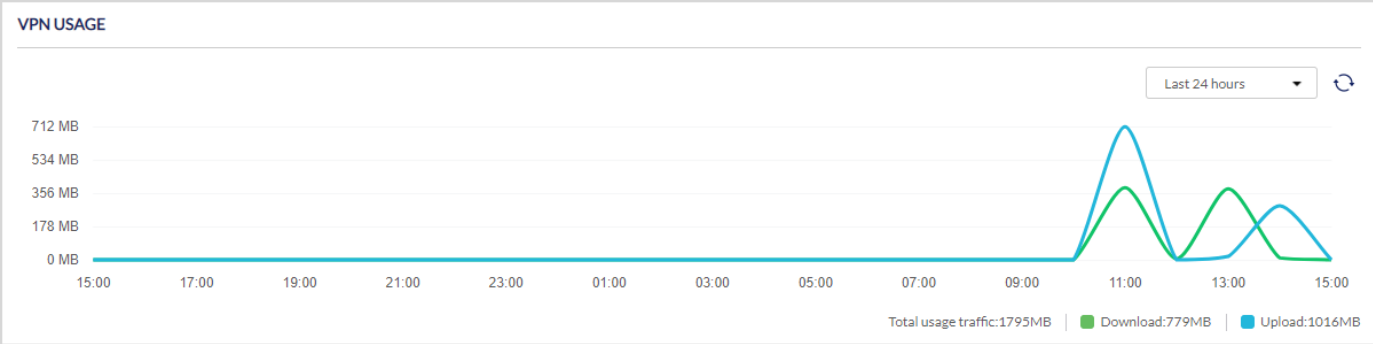


Les champs affichés dans le*Utilisation du réseau étendu*le graphique est le suivant :

Champ	Description
Utilisation totale	Il indique la vitesse totale à laquelle le trafic a transité via le port WAN au cours de la période sélectionnée. Il est situé dans le coin inférieur droit du graphique.
Télécharger	Il indique la vitesse à laquelle les données sont téléchargées via le port WAN dans le laps de temps sélectionné.
Télécharger	Il indique la vitesse à laquelle les données sont téléchargées via le port WAN dans le laps de temps sélectionné.

UTILISATION DU VPN

L'utilisation du VPN affiche l'utilisation totale du tunnel VPN pour le téléchargement et le chargement des données. Vous pouvez sélectionner le*Laps de temps*pour afficher l'utilisation du VPN. Lorsque la souris survole le graphique, elle affiche la quantité de données téléchargées et téléchargées via le tunnel VPN à cet instant.



Les champs affichés dans le*Utilisation du VPN*e graphique est le suivant :

Champ	Description
Utilisation totale	Il indique le total des données téléchargées via le tunnel VPN pendant la période sélectionnée.
Télécharger	Il indique la quantité de données téléchargées via le tunnel VPN pendant la période sélectionnée.
Télécharger	Il indique la quantité de données téléchargées via le tunnel VPN pendant la période sélectionnée.

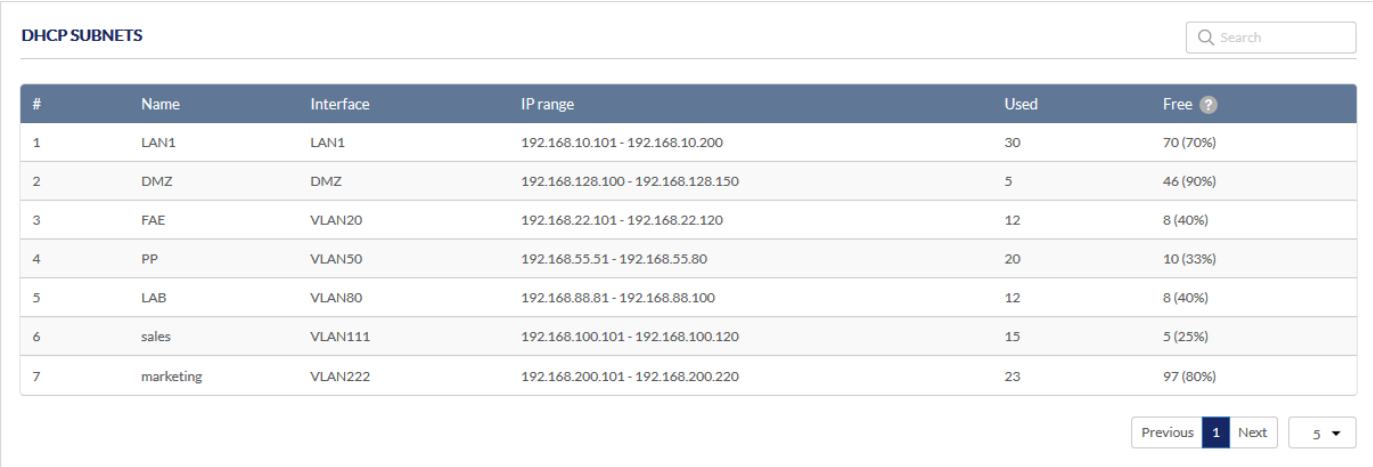
DHCP

Le**Protocole de configuration d'hôte dynamique**(DHCP) simplifie la configuration et la gestion de l'adresse IP des appareils comme les imprimantes, les ordinateurs portables, les ordinateurs de bureau, etc., présents sur le réseau. Cela se fait en attribuant un pool d'adresses IP aux appareils, et ce pool est appelé pool DHCP. Lorsqu'un appareil est ajouté à un réseau et qu'il est invité à obtenir dynamiquement son adresse IP auprès du serveur DHCP, l'une des adresses IP du pool DHCP configuré, ainsi que le masque de sous-réseau et la passerelle par défaut, sont attribués à l'appareil. Ces adresses IP ne sont attribuées aux clients que pour une durée limitée, et ce processus est appelé un**Bail DHCP**. Le bail DHCP est renouvelé automatiquement une fois la durée du bail expirée.

Cette page de la passerelle cloud détaille les*Sous-réseaux DHCP*et*Baux DHCP*configuré sur votre passerelle.

Sous-réseaux DHCP

Cette section fournit une liste de sous-réseaux DHCP précisant leur plage d'adresses IP, l'interface sur laquelle ils ont été configurés et le nombre d'adresses IP libres et utilisées.



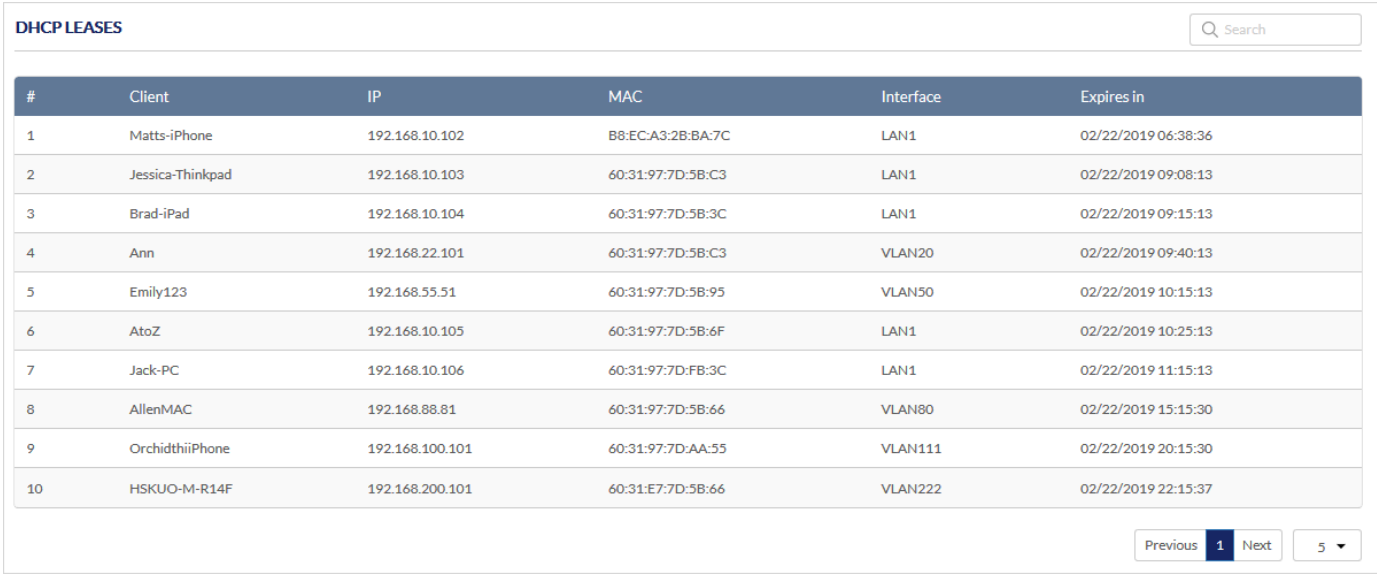
Les champs affichés dans le*Sous-réseaux DHCP*e tableau est le suivant :

Champ	Description
Nom	Il affiche le nom du sous-réseau DHCP.

Interface	Il affiche l'interface sur laquelle le sous-réseau DHCP a été configuré.
Plage ip	Il affiche la plage d'adresses IP pouvant être attribuées en location.
Utilisé	Il affiche le nombre d'adresses IP utilisées.
Gratuit	Il affiche le nombre d'adresses IP qui ne sont attribuées à personne.

Baux DHCP

Le*Durée du bail DHCP*fait référence à la durée pendant laquelle une adresse IP est attribuée au client par le serveur DHCP. Cette section répertorie tous les baux DHCP fournis aux clients sur le réseau. Il donne également un aperçu de l'interface utilisée et de l'expiration de chaque bail DHCP.

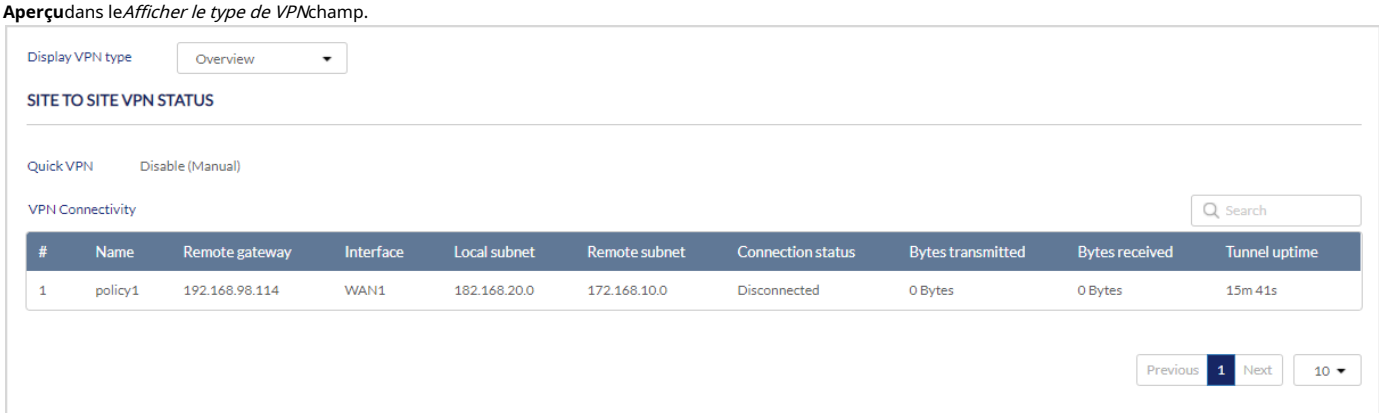


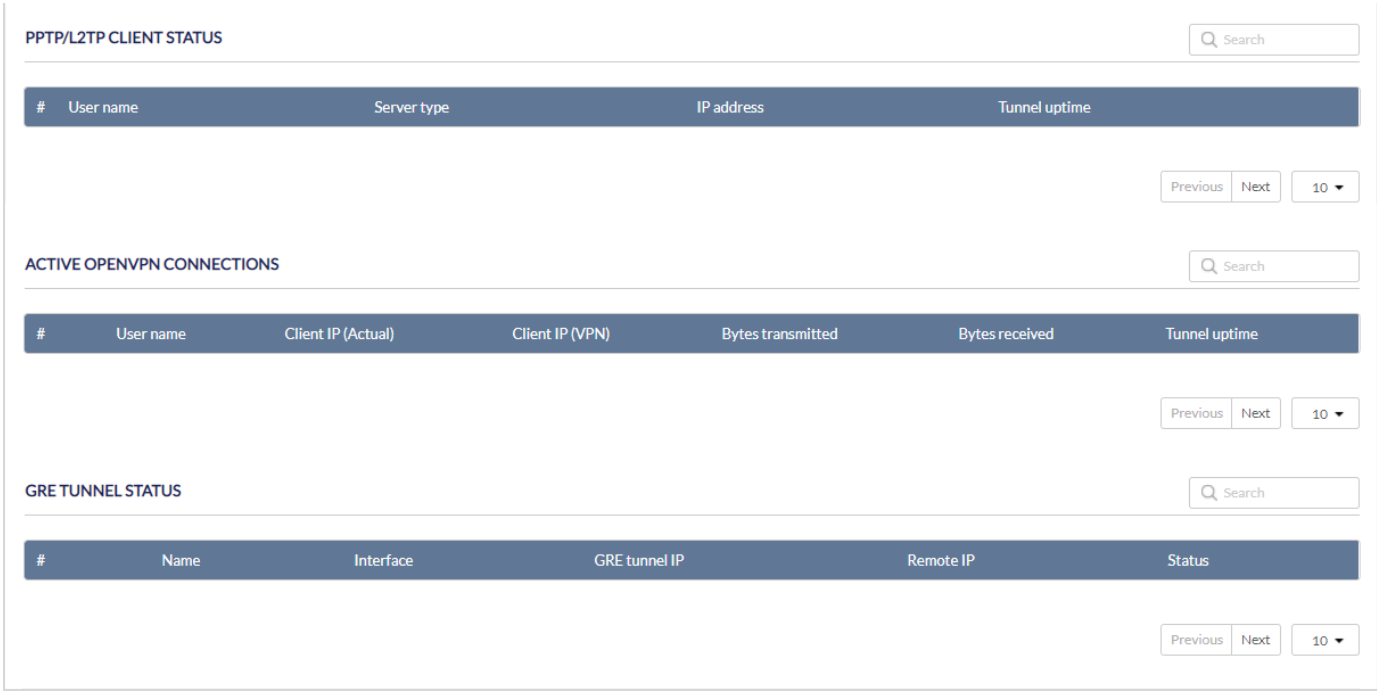
Les champs affichés dans le*Baux DHCP*e tableau est le suivant :

Champ	Description
Client	Il affiche le nom du client auquel l'adresse IP est attribuée.
IP	Il affiche l'adresse IP qui a été attribuée au client.
MAC	Il affiche l'adresse MAC du client pour lequel une adresse IP est réservée.
Interface	Il affiche l'interface via laquelle le client est connecté.
Expire dans	Il affiche la date et l'heure d'expiration du bail DHCP.

VPN

Vous pouvez visualiser l'état (connexion ou déconnexion) des associations/connexions VPN de la passerelle. La page répertorie l'association ou les connexions VPN actives, les détails du trafic et l'état du tunnel. Le trafic est une mesure cumulative des paquets transmis ou reçus depuis l'établissement du tunnel. Vous pouvez obtenir un aperçu de tous les types de VPN à la fois et également afficher chaque VPN séparément. Si vous souhaitez afficher l'état de tous les types de VPN, sélectionnez **Aperçu**dans le*Afficher le type de VPN*champ.

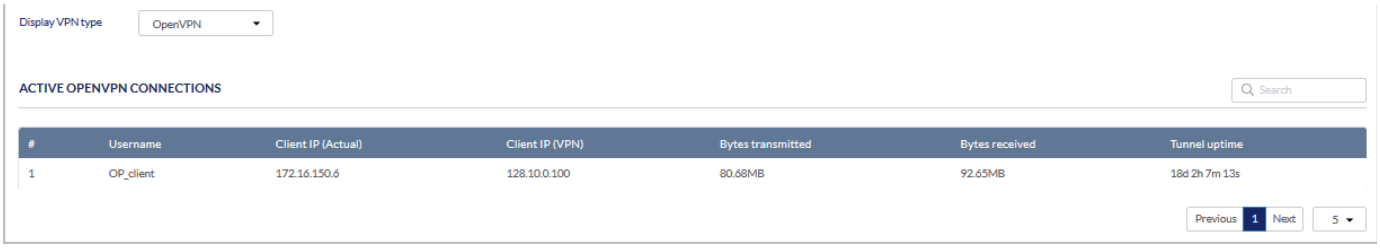




Champ	Description
Afficher le type de VPN	Sélectionnez le type de VPN que vous souhaitez afficher. Les options sont indiquées ci-dessous : • *Aperçu*: Il affiche un aperçu de tous les types de VPN. • *VPN rapide (manuel)*: Il affiche uniquement les détails du VPN site à site manuel. • *VPN rapide (site à site)*: Il affiche les détails du VPN site à site. *VPN rapide (Hub-and-* • *Spoke)*: Il affiche les détails du VPN Hub-and-Spoke. *PPTP/L2TP*: Il affiche • uniquement les détails de l'état du client PPTP/L2TP. *OpenVPN*: Il affiche • uniquement l'état du client OpenVPN. *Tunnel GRE*: Il affiche uniquement les détails • du client GRE Tunnel. ***Note:****Les VPN manuels, site à site et Hub-and-Spoke sont disponibles uniquement lorsque l'un d'entre eux est configuré sur le serveur.VPN site à siteen sélectionnant le type de VPN dans le champ « Quick VPN ».*
Statut VPN site à site	
VPN rapide	Quick VPN est une technologie VPN site à site à provisionnement automatique Nuclias qui vous permet de créer rapidement et facilement des tunnels VPN entre les appareils de passerelle Nuclias sans configuration VPN manuelle fastidieuse. Si*Désactiver (manuel)*est sélectionné, configurez le VPN manuellement dans Configuration VPN manuelle pour établir une connexion VPN avec d'autres partenaires.
Désactiver (manuel)	
Nom	Il affiche le nom du VPN.
Passerelle distante	Il affiche l'adresse IP ou le nom de domaine du homologue distant.
Interface	Il affiche l'interface sur laquelle le tunnel VPN est établi.
Sous-réseau local	Il affiche le sous-réseau local utilisé par cette connexion VPN.
Sous-réseau distant	Il affiche le sous-réseau distant utilisé par cette connexion VPN.
Statut de connexion	Il affiche si la connexion VPN est connectée ou déconnectée.
Octets transmis	Il affiche le nombre d'octets transmis via le tunnel.
Octets reçus	Il affiche le nombre d'octets reçus via le tunnel.
Temps de disponibilité du tunnel	Il affiche la durée pendant laquelle le tunnel est en service.

Statut VPN site à site (site à site)	
VPN rapide	Si*Site à site*est sélectionné, les connexions site à site entre les appareils DBG2000 de la même organisation et leurs politiques VPN sont configurées par le cloud Nuclias.
Description	Il affiche la description des réseaux locaux sur lesquels le tunnel VPN IPSec a été configuré.
Point de contact (adresse IP)	Il affiche l'adresse IP publique via laquelle l'appareil est connecté.
Nom de l'appareil	Il affiche le nom du périphérique distant du tunnel site à site.
adresse IP	Il affiche l'adresse IP (réelle) du client.
Site	Il affiche le nom du site du homologue distant.
Sous-réseau(s)	Il affiche les sous-réseaux homologues distants pour lesquels le tunnel VPN site à site est établi.
Statut de connexion	Il indique si le tunnel est connecté ou déconnecté.
Octets transmis	Il affiche le nombre d'octets transmis depuis le tunnel.
Octets reçus	Il affiche le nombre d'octets reçus par le tunnel.
Temps de disponibilité du tunnel	Il affiche la durée active du tunnel.
Statut VPN site à site (Hub-and-Spoke)	
VPN rapide	Hub-and-Spoke est utilisé lorsqu'il existe plusieurs passerelles d'approvisionnement (Spokes) avec une passerelle centrale appelée Hub.
Description	Il affiche la description des réseaux locaux sur lesquels le tunnel VPN IPSec a été configuré.
Point de contact (adresse IP)	Il affiche l'adresse IP publique via laquelle l'appareil est connecté.
Nom de l'appareil	Il affiche le nom de périphérique du homologue distant.
adresse IP	Il affiche l'adresse IP du homologue distant avec lequel le tunnel est établi.
Site	Il affiche le nom du site du homologue distant.
Sous-réseau(s)	Il affiche les sous-réseaux homologues distants pour lesquels le tunnel sera établi.
Rôle	Il indique si le client connecté agit en tant que hub ou Spoke.
Statut de connexion	Il indique si le tunnel est connecté ou déconnecté.
Octets transmis	Il affiche le nombre d'octets transmis depuis le tunnel.
Octets reçus	Il affiche le nombre d'octets reçus par le tunnel.
Temps de disponibilité du tunnel	Il affiche la durée pendant laquelle le tunnel est en place.

Champ	Description
Nom d'utilisateur	Il affiche le nom d'utilisateur PPTP/L2TP.
Type de serveur	Il affiche le type de serveur (PPTP ou L2TP) sur lequel le tunnel est établi.
adresse IP	Il affiche l'adresse IP du client PPTP/L2TP connecté.
Temps de disponibilité du tunnel	Il affiche la durée pendant laquelle le tunnel est en service.



Champ	Description
Connexions OpenVPN actives	
Nom d'utilisateur	Il affiche le nom des clients connectés au serveur.
IP client (réelle)	Il affiche l'adresse IP via laquelle le client est connecté.
IP client (VPN)	Il affiche l'adresse IP virtuelle du client connecté.
Octets transmis	Il affiche le nombre d'octets transmis depuis le tunnel.
Octets reçus	Il affiche le nombre d'octets reçus par le tunnel.
Temps de disponibilité du tunnel	Il affiche la durée pendant laquelle le tunnel est en place.

Champ	Description
Statut du tunnel GRE	
Nom	Il affiche le nom du tunnel.
Interface	Il affiche l'interface où le tunnel est créé.
IP du tunnel GRE	Il affiche l'adresse IP du tunnel GRE.
IP distante	Il affiche l'adresse IP de la passerelle du point de terminaison distant.
Statut	Il indique si le tunnel GRE est connecté ou non.

Chapitre 3 Réseau

Clique le**Réseau**pour modifier ou configurer le réseau (LAN, WAN ou DMZ). Ce chapitre traite des différents paramètres requis pour configurer un réseau. Les paramètres de basculement automatique et d'équilibrage de charge de cette section vous permettent de configurer un flux de trafic simple et continu sur le réseau. De même, les protocoles de routage de la passerelle aident à sélectionner un chemin optimal pour que le trafic circule de la source à sa destination, et les différents services pris en charge fournissent un réseau sécurisé à ses utilisateurs finaux. La gestion du trafic est une autre configuration importante pour un réseau qui régule le flux de trafic des ports LAN vers les ports WAN. Ainsi, ce chapitre vous aide à configurer les éléments clés du réseau tels que les ports de l'appareil, les protocoles de routage, les services, la gestion du trafic et les fonctionnalités de haute disponibilité.

Ce chapitre couvre les sujets suivants:

Ethernet

Cette section fournit un aperçu schématique de l'état du port. Il indique les ports de l'appareil avec différentes couleurs en fonction de la connectivité des ports. Vous pouvez configurer les ports WAN, LAN et DMZ sur cette page. La passerelle cloud Nuclias, DBG-2000, prend en charge plusieurs ports WAN et vous permet donc d'utiliser des techniques de basculement et d'équilibrage de charge pour hiérarchiser les services Internet lors d'une connexion WAN instable.

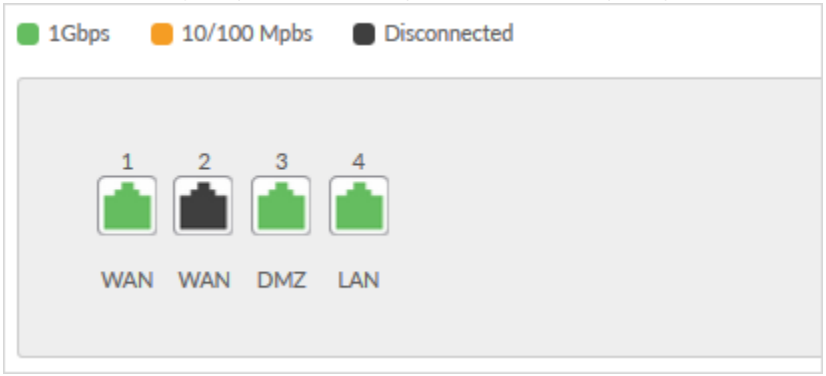
Une autre fonctionnalité prise en charge par la passerelle cloud est le DNS dynamique (DDNS), c'est-à-dire un service Internet qui permet de localiser des routeurs avec différentes adresses IP publiques à l'aide de noms de domaine Internet. Vous pouvez également configurer le*Alias IP*fonctionnalité pour associer une autre adresse IP à l'interface.

Le*Ethernet*La section comprend les sujets suivants :

Statut du port

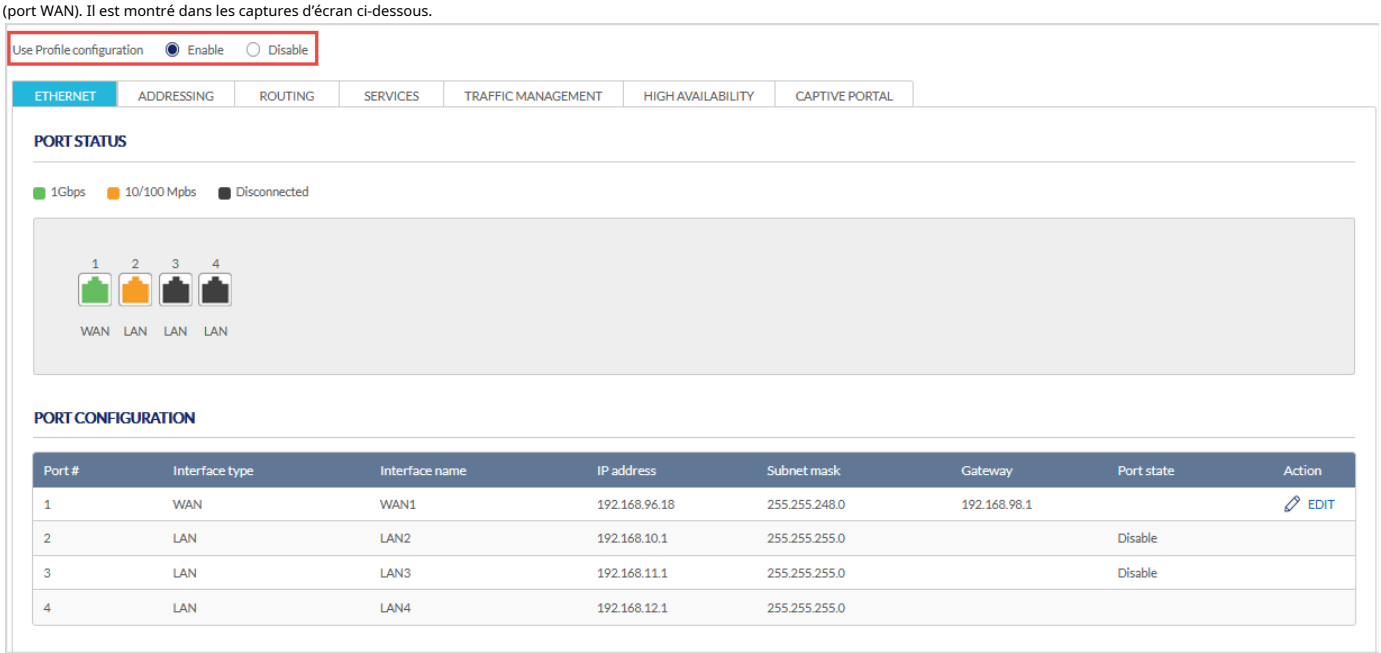
Les ports Ethernet, disponibles sur la passerelle cloud, prennent en charge 10/100/1000 Mbps et utilisent la vitesse commune la plus élevée entre les appareils d'envoi et de réception. Le*Statut du port*affiche les quatre ports de l'appareil et indique la connectivité de chaque port dans les trois couleurs suivantes :

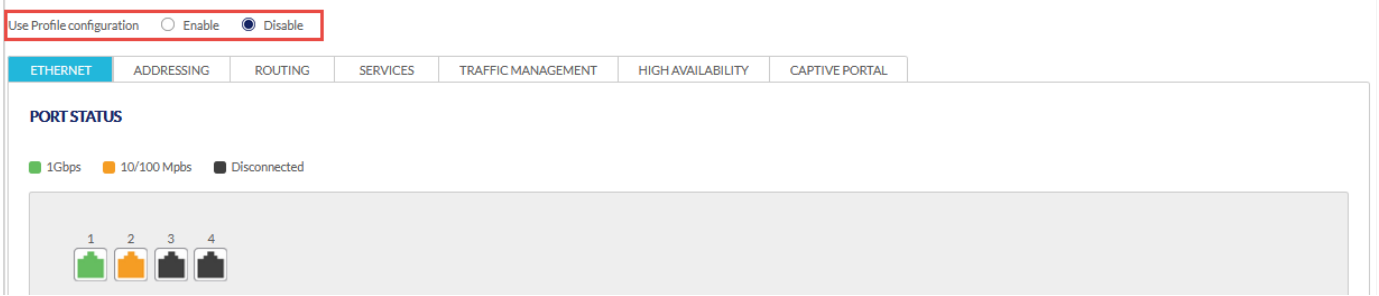
- **Vert**: Cela signifie que le port transmet à 1 Gbps. **Orange**:
- Cela signifie que le port transmet à 10/100Mbps.
- **Noir**: Cela signifie que l'interface est en panne, déconnectée ou que les ports sont désactivés.

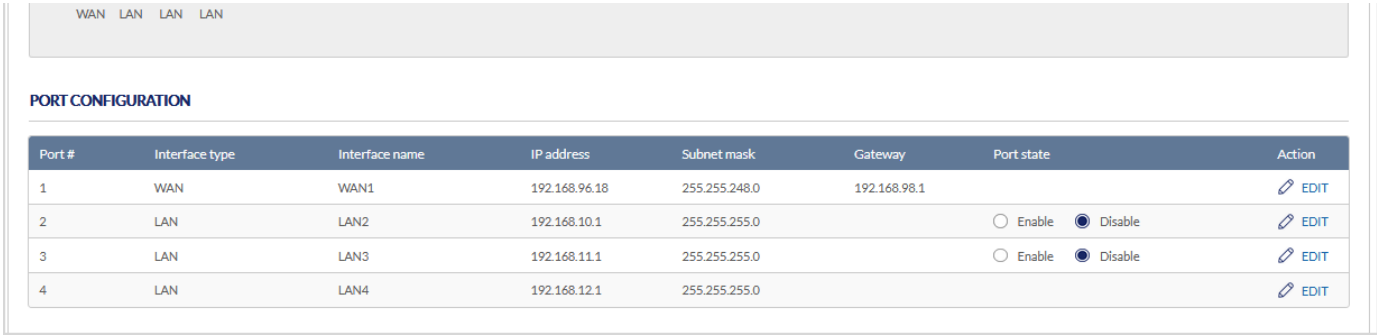


Configuration des ports

Pour configurer un port, vous devez désactiver le*Utiliser la configuration du profil*champ présent au-dessus du**Statut du port**. Si ce champ est activé, vous pouvez modifier uniquement le port 1 (port WAN). Il est montré dans les captures d'écran ci-dessous.







Les champs disponibles dans le*Configuration des ports*le tableau est le suivant :

Champ	Description
Port	Il affiche le numéro de port.
Type d'interface	Il affiche le type d'interface. Les options sont WAN, DMZ et LAN.
Nom de l'interface	Il affiche le nom de l'interface.
adresse IP	Il affiche l'adresse IP du port sélectionné.
Masque de sous-réseau	Il affiche le masque de sous-réseau pour l'adresse IP.
passerelle	Il affiche l'adresse IP de la passerelle.
État du port	Vous pouvez activer ou désactiver l'état du port uniquement lorsque le*Utiliser la configuration du profil*le champ est désactivé.
Actions	Vous pouvez modifier tous les ports uniquement lorsque le*Utiliser la configuration du profil*le champ est désactivé ; sinon, vous ne pouvez modifier que le port 1.

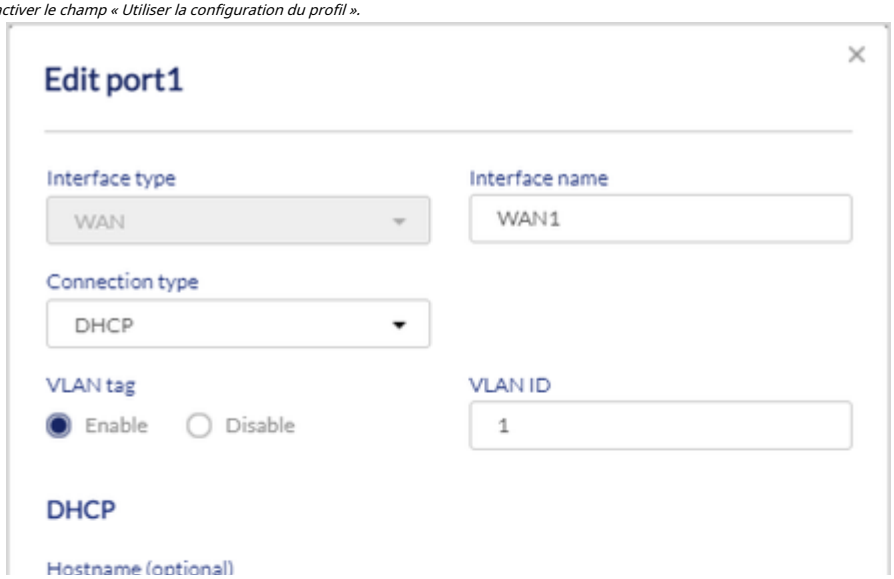
Le*Configuration des ports*La section explique comment configurer les ports suivants :

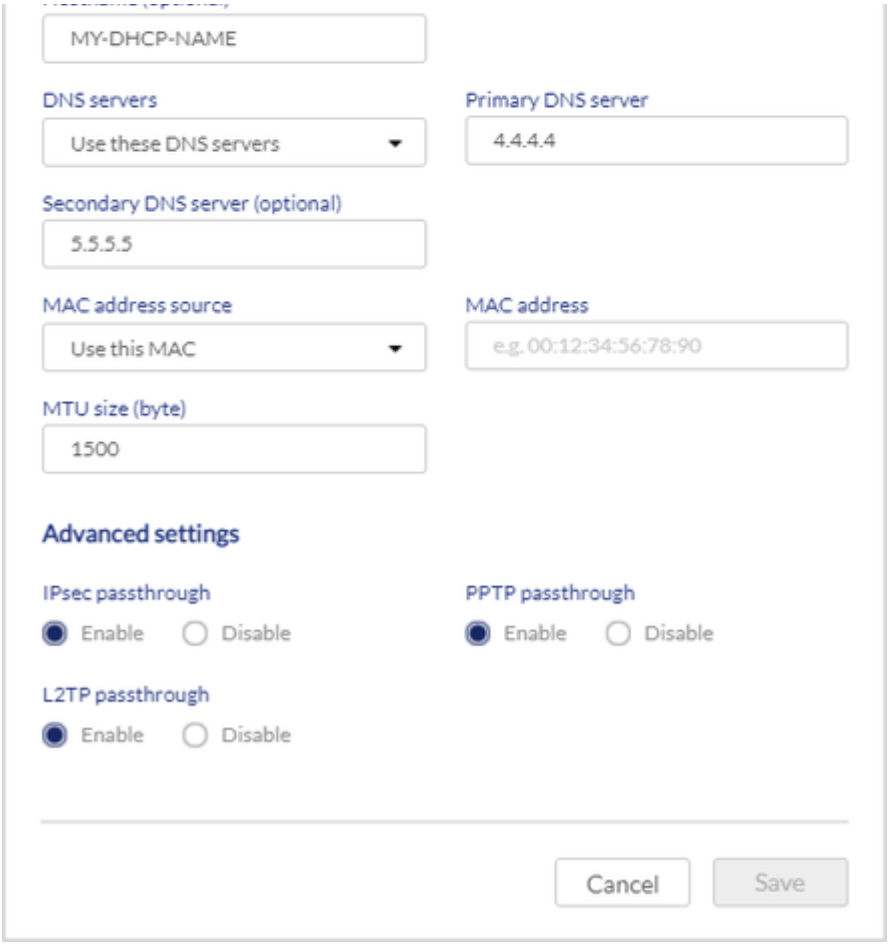
- Port WAN
- Port DMZ
- Port LAN

Port WAN

La passerelle dispose d'un total de quatre ports, parmi lesquels le port 1, le port 2 et le port 3 peuvent être utilisés comme ports WAN pour établir une connexion à Internet. Le port 1 ne peut être configuré qu'en tant que port WAN, tandis que les ports 2 et 3 peuvent être configurés en tant que port LAN, WAN ou DMZ. Il est supposé que vous avez organisé un service Internet avec votre fournisseur d'accès Internet (FAI). Veuillez contacter votre FAI ou votre administrateur réseau pour obtenir les informations de configuration requises pour configurer la passerelle cloud Nuclias.

Vous pouvez configurer le port WAN dans le*Configuration des ports*section. Cliquez sur**Modifier**pour ouvrir la page de configuration du port correspondant. ***Note**: Pour configurer le port, vous devez désactiver le champ « Utiliser la configuration du profil ».*





Les champs disponibles sur cette page sont les suivants :

Champ	Description
Type d'interface	Sélectionnez le type d'interface. Les options sont WAN, DMZ et LAN. ***Note:****Vous ne pouvez pas modifier ce champ pour les interfaces Port 1 et Port 4. Le port 1 ne peut être configuré que comme port WAN et le port 4 comme port LAN.*
Nom de l'interface	Entrez un nom pour l'interface.
Type de connexion	Sélectionnez un type de connexion parmi les options suivantes : DHCP, IP statique, PPPoE, PPTP et L2TP.
Balise VLAN	Activez ou désactivez la balise VLAN sur le port WAN configuré.
ID de VLAN	Si la balise VLAN est activée, entrez le**ID de VLAN**.
DHCP	
Nom d'hôte (facultatif)	Entrez le nom d'hôte si votre FAI l'exige.
Serveurs DNS	Sélectionnez soit**Obtenez dynamiquement du FAI**ou**Utilisez ces serveurs DNS**pour entrer manuellement les serveurs DNS.
Serveur DNS primaire	Si vous sélectionnez**Utilisez ces serveurs DNS**, saisissez l'adresse IP du serveur DNS principal.
Serveur DNS secondaire (facultatif)	Si vous sélectionnez**Utilisez ces serveurs DNS**, saisissez l'adresse IP du serveur DNS secondaire. C'est un champ facultatif.
Source de l'adresse MAC	Sélectionner**Utiliser le MAC par défaut**pour utiliser l'adresse MAC du port WAN configuré à associer à votre modem/FAI, ou**Utiliser ce MAC**pour saisir manuellement une adresse MAC.
Adresse Mac	Si vous sélectionnez**Utiliser ce MAC**, saisissez l'adresse MAC que vous souhaitez associer à votre FAI.
Taille MTU (octet)	

	Le MTU (Maximum Transmit Unit) est le plus gros paquet pouvant être envoyé sur le réseau. La valeur MTU standard pour les réseaux Ethernet est généralement de 1 500 octets, et pour les connexions PPPoE/PPTP, elle est de 1 492 octets. Pour toutes les connexions L2TP, il s'agit de 1 460 octets.
I.P statique	
adresse IP	Saisissez l'adresse statique que votre FAI vous a attribuée.
Masque de sous-réseau IP	Entrez le masque de sous-réseau IP.
Adresse IP de la passerelle	Entrez l'adresse IP de la passerelle par défaut.
Configuration PPPoE	
Mode adresse	Sélectionnez soit**IP dynamique**ou**I.P statique**.
adresse IP	Si vous sélectionnez**I.P statique**, saisissez l'adresse IP qui vous a été fournie par votre FAI.
Masque de sous-réseau IP	Si vous sélectionnez**I.P statique**, saisissez le masque de sous-réseau fourni par votre FAI.
Nom d'utilisateur	Entrez votre nom d'utilisateur PPPoE.
Mot de passe	Entrez votre mot de passe PPPoE.
Service (facultatif)	Si votre FAI prend en charge le nom du service, saisissez-le ici.
Type d'identification	Sélectionnez le type d'authentification à utiliser (négociation automatique, PAP, CHAP, MS-CHAP ou MS-CHAPv2).
Mode reconnexion	Sélectionnez l'une des options suivantes : • **Toujours allumé :**La connexion est toujours active. • **Sur demande:**La connexion est automatiquement interrompue si elle est inactive pendant un nombre de minutes spécifié.
Temps d'inactivité maximum (minutes)	Entrez le nombre de minutes dans le*Temps d'inactivité maximum*champ. Cette fonctionnalité est utile si votre FAI vous facture en fonction de la durée de votre connexion. Ce champ est disponible uniquement lorsque**Sur demande**est sélectionné.
PPTP	
Mode adresse	Sélectionner**IP dynamique**ou**I.P statique**(Paramètres IP fournis par votre FAI).
Nom du serveur	Saisissez l'adresse IP de votre serveur PPTP ou le nom de domaine.
Nom d'utilisateur	Entrez votre nom d'utilisateur PPTP.
Mot de passe	Entrez votre mot de passe PPTP.
adresse IP	Si vous sélectionnez**I.P statique**comme mode d'adresse, entrez l'adresse IP fournie par votre FAI.
Masque de sous-réseau IP	Si vous sélectionnez**I.P statique**comme mode d'adresse, entrez le masque de sous-réseau fourni par votre FAI.
Adresse IP de la passerelle	Si vous sélectionnez**I.P statique**comme mode d'adresse, entrez l'adresse IP de la passerelle fournie par votre FAI.
IP DNS statique	Si vous sélectionnez**I.P statique**comme mode d'adresse, entrez l'adresse IP DNS statique dans le sous-réseau correspondant.
Cryptage MPPE	Activez-le si le serveur PPTP prend en charge cette fonctionnalité.
Mode reconnexion	Certains FAI peuvent vous demander de payer pour la durée d'utilisation. Sélectionner**Sur demande**si c'est le cas. La passerelle se connectera alors à Internet uniquement lorsque vous établirez une connexion Internet. Sélectionner**Toujours activé**pour que la passerelle reste connectée à Internet.
Temps d'inactivité maximum (minutes)	Entrez le nombre de minutes dans le*Temps d'inactivité maximum*champ. Cette fonctionnalité est utile si votre FAI vous facture en fonction de la durée de votre connexion. Ce champ est disponible uniquement lorsque**Sur demande**est sélectionné.
L2TP	
Mode adresse	Sélectionner**IP dynamique**ou**I.P statique**(Paramètres IP fournis par votre FAI).
Nom du serveur	Saisissez l'adresse IP de votre serveur L2TP ou le nom de domaine.

adresse IP	Si vous sélectionnez**I.P statique**comme mode d'adresse, entrez l'adresse IP fournie par votre FAI.
Masque de sous-réseau IP	Si vous sélectionnez**I.P statique**comme mode d'adresse, entrez le masque de sous-réseau fourni par votre FAI.
Adresse IP de la passerelle	Si vous sélectionnez**I.P statique**comme mode d'adresse, entrez l'adresse IP de la passerelle fournie par votre FAI.
IP DNS statique	Si vous sélectionnez**I.P statique**comme mode d'adresse, entrez l'adresse IP DNS statique dans le sous-réseau correspondant.
Nom d'utilisateur	Entrez votre nom d'utilisateur L2TP.
Mot de passe	Entrez votre mot de passe L2TP.
Secret (facultatif)	Entrez un secret partagé si votre FAI le prend en charge.
Mode reconnexion	Certains FAI peuvent vous demander de payer pour la durée d'utilisation. Sélectionner**Sur demande**si c'est le cas. La passerelle se connectera alors à Internet uniquement lorsque vous établirez une connexion Internet. Sélectionner**Toujours activé**pour que la passerelle reste connectée à Internet.
Temps d'inactivité maximum (minutes)	Entrez le nombre de minutes dans le*Temps d'inactivité maximum*champ. Cette fonctionnalité est utile si votre FAI vous facture en fonction de la durée de votre connexion. Ce champ est disponible uniquement lorsque**Sur demande**est sélectionné.
Réglages avancés	
Passage IPSec	Activez cette fonctionnalité pour autoriser le trafic VPN crypté pour les connexions par tunnel VPN IPSec via l'appareil.
Passage PPTP	Activez cette fonctionnalité pour autoriser le trafic VPN crypté pour les connexions par tunnel VPN PPTP via l'appareil.
Passage L2TP	Activez cette fonctionnalité pour autoriser le trafic VPN crypté pour les connexions par tunnel VPN L2TP via l'appareil.
Sauvegarder	Cliquez sur**Sauvegarder**pour enregistrer vos paramètres.
Annuler	Cliquez sur**Annuler**pour revenir aux paramètres précédents.

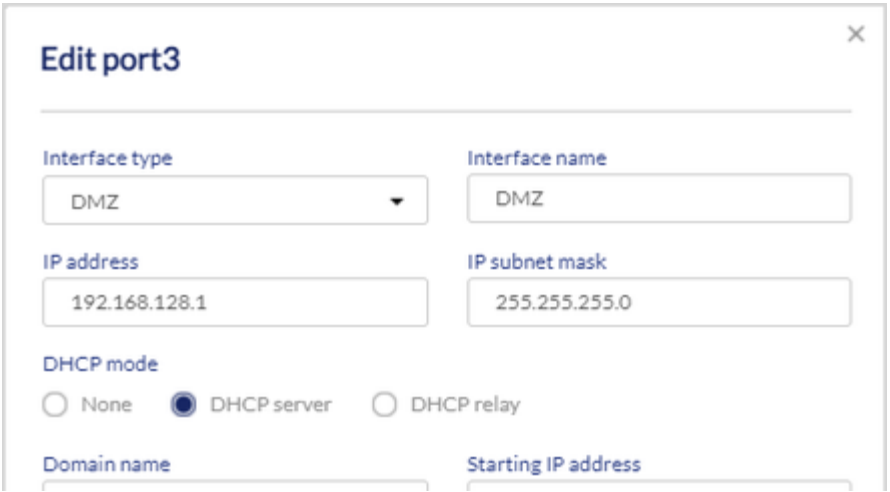
Port DMZ

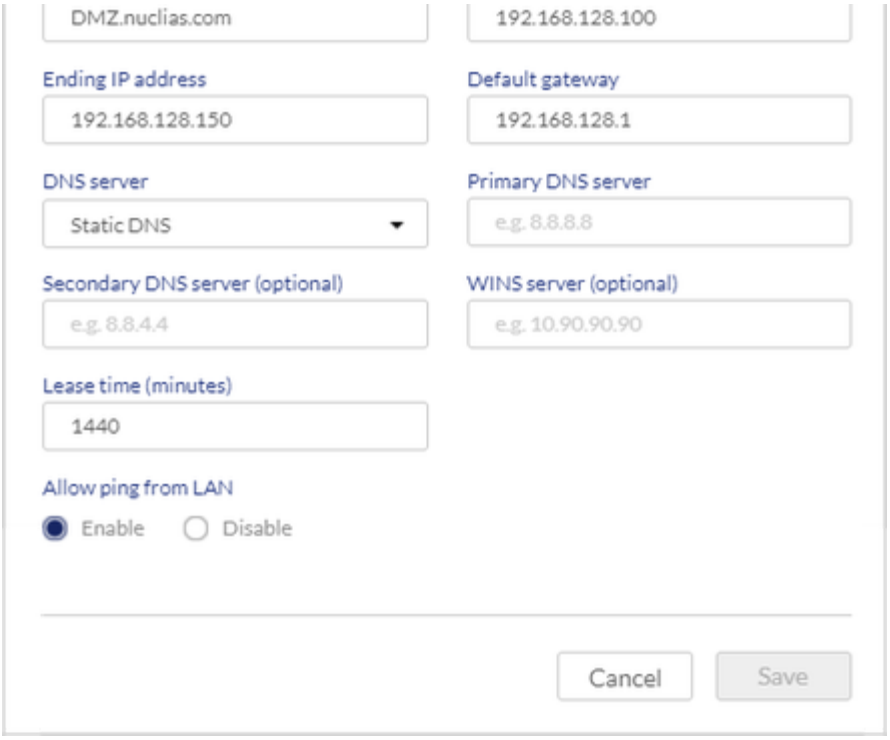
La passerelle prend en charge l'un des ports physiques à configurer en tant que port DMZ dédié. Une DMZ est un sous-réseau ouvert au public mais derrière le pare-feu. La DMZ assure la sécurité du réseau, car les services/ports spécifiques exposés à Internet sur la DMZ ne le sont pas sur l'intranet. Par conséquent, il est recommandé que les hôtes exposés à Internet (tels que les serveurs Web ou de messagerie) soient placés dans le réseau DMZ. Les règles de pare-feu peuvent permettre l'accès à des services/ports spécifiques vers la DMZ depuis un LAN ou un WAN. Lors d'une attaque contre l'un des nœuds DMZ, le réseau local n'est pas nécessairement vulnérable. La configuration DMZ est identique à la configuration LAN. Il n'y a aucune restriction sur l'adresse IP ou le sous-réseau attribué au port DMZ, autre que le fait qu'elle ne peut pas être identique à l'adresse IP donnée à l'interface LAN de cette passerelle.

Vous pouvez configurer le port 2 ou le port 3 en tant que ports DMZ dans le*Configuration des ports*section. Cliquez sur**Modifier**pour ouvrir la page de configuration du port correspondant.

***Note**:*

- *Pour configurer le port, vous devez désactiver le champ « Utiliser la configuration du profil ». Les*
- *ports 1 et 4 ne peuvent être configurés respectivement que comme ports WAN et LAN.*





Les champs disponibles sur cette page sont les suivants :

Champ	Description
Type d'interface	Sélectionner**DMZ**pour configurer le port comme port DMZ.
Nom de l'interface	Spécifiez le nom de votre interface DMZ.
adresse IP	Saisissez une nouvelle adresse IP pour l'appareil.
Masque de sous-réseau IP	Entrez le masque de sous-réseau de votre réseau.
Mode DHCP	Sélectionnez l'un des modes suivants : • **Aucun**-Sélectionner**Aucun**pour désactiver DHCP. • **Serveur DHCP**-Si cette option est sélectionnée, la passerelle agira en tant que serveur DHCP sur votre réseau. Par défaut, le « serveur DHCP » est sélectionné comme mode DHCP. • **Relais DHCP**-Si cette option est sélectionnée, les clients DHCP de votre réseau recevront des baux d'adresses IP d'un serveur DHCP sur un sous-réseau différent.
Nom de domaine	Entrez un nom de domaine pour la configuration DMZ.
Adresse IP de départ	Entrez l'adresse IP de départ.
Adresse IP de fin	Entrez l'adresse IP de fin.
Passerelle par défaut	Si vous sélectionnez**Serveur DHCP**comme mode DHCP, entrez la passerelle par défaut pour le mode serveur DHCP.
Serveur dns	Sélectionnez l'une des options suivantes pour les serveurs DNS pour les clients DHCP : • **Proxy DNS**: Activez ou désactivez le proxy DNS. Lorsque le champ Proxy DNS est sélectionné, l'appareil agit comme proxy pour toutes les requêtes DNS et communique avec les serveurs DNS du FAI. • **DNS du FAI**: Cette option envoie toutes les requêtes DNS aux serveurs DNS du FAI. **DNS statique**: • Cette option envoie toutes les requêtes DNS aux serveurs DNS statiques configurés.
Serveur DNS primaire	Entrez l'adresse IP du serveur DNS principal.
Serveur DNS secondaire (facultatif)	Entrez l'adresse IP du serveur DNS secondaire. C'est un champ facultatif.
Serveur WINS (facultatif)	

	Entrez l'adresse IP WINS dans la configuration DHCP. Un WINS (Windows Internet Naming Service Server) est l'équivalent d'un serveur DNS mais utilise le protocole NetBIOS pour résoudre les noms d'hôtes. C'est un champ facultatif.
Durée du bail (minutes)	Saisissez la durée (en minutes) pendant laquelle les adresses IP seront louées aux clients.
Passerelle relais	Saisissez l'adresse IP de la passerelle relais. Ce champ est disponible lorsque vous sélectionnez*Mode DHCP* comme **Relais DHCP**.
Autoriser le ping depuis le réseau local	Si cette option est désactivée, les requêtes ping vers l'interface LAN sont bloquées.
Proxy DNS	Lorsque le champ Proxy DNS est activé, l'appareil agit comme proxy pour toutes les requêtes DNS et communique avec les serveurs DNS du FAI. Ce champ est disponible lorsque vous sélectionnez**Relais DHCP**ou**Aucun**comme le mode DHCP.
Sauvegarder	Cliquez sur**Sauvegarder**pour enregistrer vos paramètres.
Annuler	Cliquez sur**Annuler**pour revenir aux paramètres précédents.

Port LAN

Par défaut, la passerelle fonctionne comme un serveur DHCP (Dynamic Host Configuration Protocol) pour les hôtes présents sur le réseau LAN. Avec DHCP, les PC et autres périphériques LAN peuvent se voir attribuer des adresses IP et des adresses pour les serveurs DNS, les serveurs Windows Internet Name Service (WINS) et la passerelle par défaut. L'adresse IP de la passerelle sert d'adresse de passerelle pour les clients LAN, avec le serveur DHCP activé. Les PC du réseau local se voient attribuer des adresses IP à partir d'un pool d'adresses si le serveur DHCP est configuré.

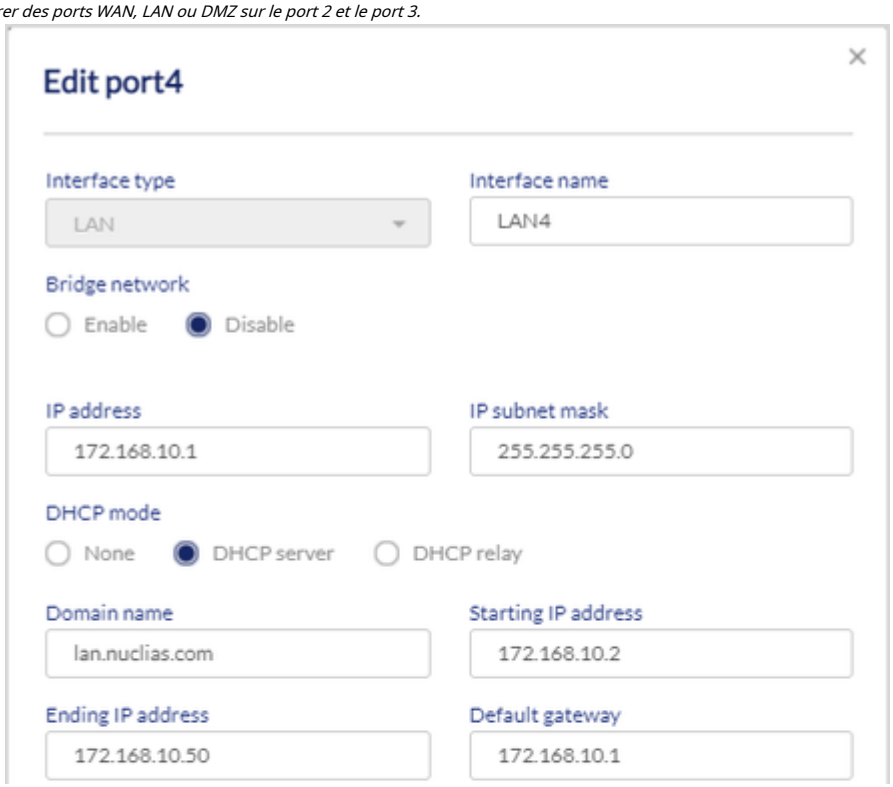
Pour la plupart des applications, les paramètres DHCP et TCP/IP par défaut sont satisfaisants. Si vous souhaitez qu'un autre PC de votre réseau soit le serveur DHCP ou si vous configurez manuellement les paramètres réseau de tous vos PC, définissez le mode DHCP sur « aucun ». Le relais DHCP peut transférer des paquets DHCP pour obtenir les informations de bail DHCP d'un autre serveur DHCP du réseau.

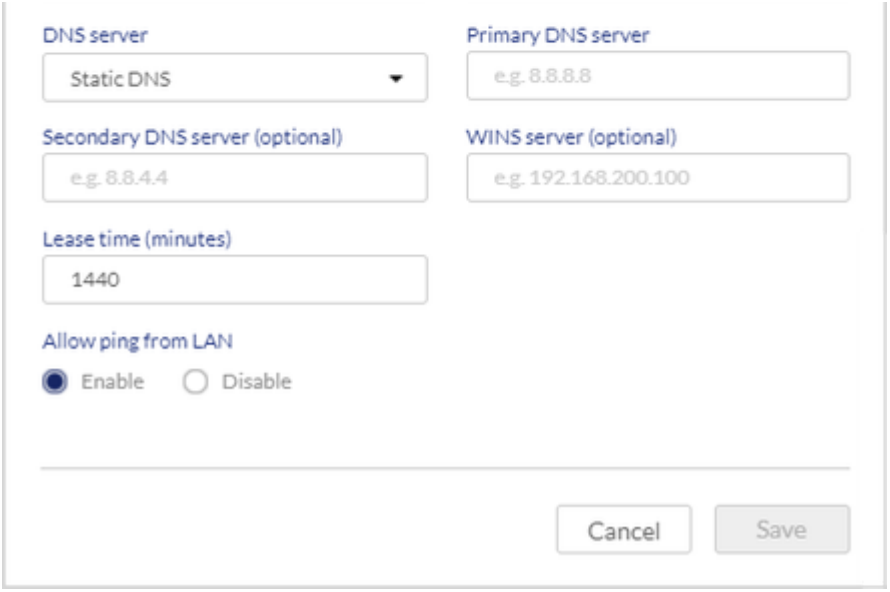
En plus d'un serveur DNS, vous pouvez également utiliser un serveur WINS (Windows Internet Naming Service). Un serveur WINS est l'équivalent d'un serveur DNS mais utilise le protocole NetBIOS pour résoudre les noms d'hôte. La passerelle inclut l'adresse IP du serveur WINS dans la configuration DHCP lors de l'accusé de réception d'une requête DHCP provenant d'un client DHCP.

Vous pouvez configurer le port LAN dans le*Configuration des ports*section. Cliquez sur**Modifier**pour ouvrir la page de configuration du port correspondant.

***Note**:*

- *Pour configurer le port, vous devez désactiver le champ « Utiliser la configuration du profil ».*
- *Les ports 1 et 4 sont respectivement des ports WAN et LAN.*
- *Vous pouvez configurer des ports WAN, LAN ou DMZ sur le port 2 et le port 3.*





Les champs disponibles sur cette page sont les suivants :

Champ	Description
Type d'interface	Sélectionner**Réseau local**pour configurer le port comme port LAN. ***Note:****Vous ne pouvez pas modifier ce champ pour les interfaces Port 1 et Port 4. Le port 1 ne peut être configuré que comme port WAN et le port 4 comme port LAN.*
Nom de l'interface	Spécifiez le nom de votre interface LAN.
Réseau de ponts	Activez ce champ pour relier ce LAN à un autre VLAN.
Réseau	Sélectionnez le réseau dans la liste déroulante. Ce champ est disponible lorsque vous activez le*Réseau de pont*champ.
adresse IP	Saisissez une nouvelle adresse IP pour la passerelle.
Masque de sous-réseau IP	Entrez le masque de sous-réseau de votre réseau.
Mode DHCP	Sélectionnez l'un des modes suivants : • **Aucun**-Sélectionner**Aucun**pour désactiver DHCP. • **Serveur DHCP**-Si cette option est sélectionnée, la passerelle agira en tant que serveur DHCP sur votre réseau. Par défaut, le « serveur DHCP » est sélectionné comme mode DHCP. • **Relais DHCP**-Si cette option est sélectionnée, les clients DHCP de votre réseau recevront des baux d'adresses IP d'un serveur DHCP sur un sous-réseau différent.
Nom de domaine	Entrez un nom de domaine pour la configuration LAN.
Adresse IP de départ	Entrez l'adresse IP de départ.
Adresse IP de fin	Entrez l'adresse IP de fin.
Passerelle par défaut	Si le mode DHCP est**Serveur DHCP**, entrez la passerelle par défaut pour le mode serveur DHCP.
Serveur dns	Sélectionnez l'une des options suivantes pour les serveurs DNS pour les clients DHCP : • **Proxy DNS**: Activez ou désactivez le proxy DNS sur ce VLAN. Lorsque le champ Proxy DNS est sélectionné, la passerelle agit comme proxy pour toutes les requêtes DNS et communique avec les serveurs DNS du FAI. • **DNS du FAI**: Cette option envoie toutes les requêtes DNS aux serveurs DNS du FAI. **DNS statique :** • Cette option envoie toutes les requêtes DNS aux serveurs DNS statiques configurés.
Serveur DNS primaire	Entrez l'adresse IP du serveur DNS principal.
Serveur DNS secondaire (facultatif)	Entrez l'adresse IP du serveur DNS secondaire. C'est un champ facultatif.

Serveur WINS (facultatif)	Entrez l'adresse IP WINS dans la configuration DHCP. Un WINS (Windows Internet Naming Service Server) est l'équivalent d'un serveur DNS mais utilise le protocole NetBIOS pour résoudre les noms d'hôtes. C'est un champ facultatif.
Durée du bail (minutes)	Saisissez la durée (en minutes) pendant laquelle les adresses IP seront louées aux clients.
Passerelle relais	Saisissez l'adresse IP de la passerelle relais. Ce champ est disponible lorsque vous sélectionnez*Mode DHCP* comme **Relais DHCP**.
Autoriser le ping depuis le réseau local	Si cette option est désactivée, les requêtes ping vers l'interface LAN sont bloquées.
Proxy DNS	Lorsque le champ Proxy DNS est activé, la passerelle agit comme proxy pour toutes les requêtes DNS et communique avec les serveurs DNS du FAI. Ce champ est disponible lorsque vous sélectionnez**Relais DHCP**ou**Aucun**comme le mode DHCP.
Sauvegarder	Cliquez sur**Sauvegarder**pour enregistrer vos paramètres.
Annuler	Cliquez sur**Annuler**pour revenir aux paramètres précédents.

Configuration du mode WAN

La passerelle cloud Nuclias prend en charge plusieurs liaisons WAN. Cela vous permet de profiter des fonctionnalités de rollover et d'équilibrage de charge pour garantir que certains services dépendants d'Internet sont prioritaires en cas de connectivité WAN instable sur l'un des ports.

Pour utiliser le basculement automatique ou l'équilibrage de charge, vous devez configurer la détection des défaillances de la liaison WAN. Cela implique d'accéder aux serveurs DNS sur Internet ou d'envoyer une requête ping à une adresse Internet (définie par l'utilisateur). Dans l'équilibrage de charge, vous pouvez également sélectionner*Aucun*pour désactiver la fonction de détection de panne. Lorsque la détection des échecs est activée, spécifiez l'intervalle de nouvelle tentative et le nombre de tentatives dont il dispose pour se connecter au serveur configuré. Si toutes les tentatives échouent, le port WAN est considéré comme indisponible.

Cette section traite des modes WAN suivants :

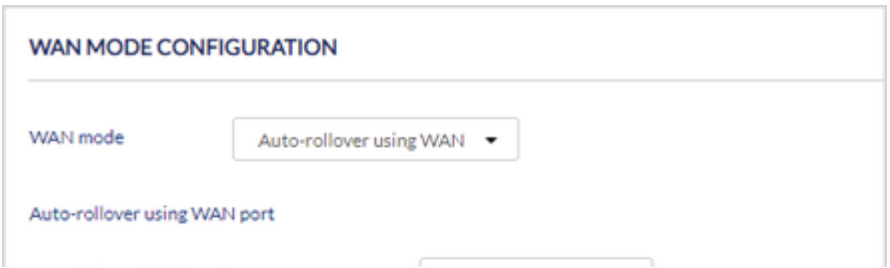
- Réseau étendu principal
- Rollover automatique à l'aide du WAN
- L'équilibrage de charge
  - Tournoi à la ronde
  - Mode débordement

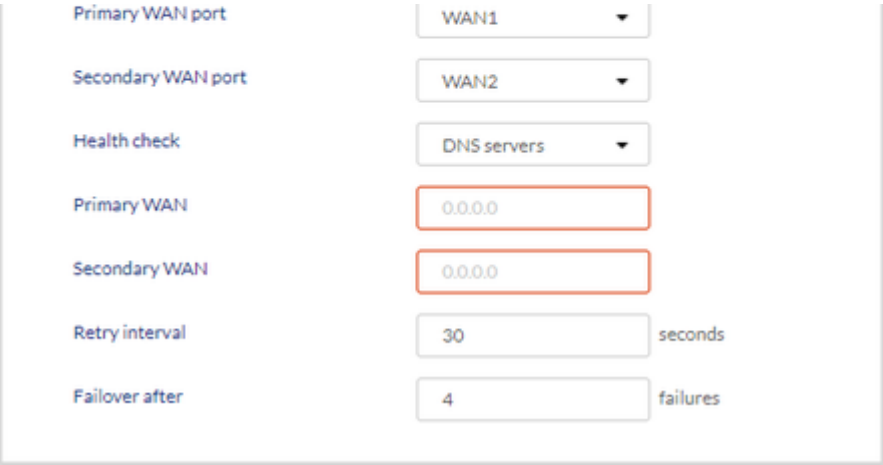
Réseau étendu principal

Si vous ne souhaitez pas utiliser le basculement automatique ou l'équilibrage de charge, sélectionnez**Réseau étendu principal**comme mode WAN et sélectionnez le port WAN que vous souhaitez définir comme port WAN principal.

Rollover automatique à l'aide du WAN

En mode Auto-rollover using WAN, l'un des ports WAN est attribué comme liaison Internet principale pour tout le trafic Internet ; le port WAN secondaire est utilisé pour la redondance si la liaison principale tombe en panne pour une raison quelconque. Les deux ports WAN (primaire et secondaire) doivent être configurés pour se connecter aux FAI respectifs avant d'activer cette fonctionnalité. Le port WAN secondaire restera déconnecté jusqu'à ce qu'une panne soit détectée sur la liaison principale (l'un ou l'autre des ports peut être attribué comme principal). Si une panne se produit sur le port principal, le trafic Internet sera transféré vers le port de sauvegarde. Lorsqu'il est configuré en mode Auto-rollover, l'état de la liaison du port WAN principal est vérifié à intervalles réguliers, comme défini par les paramètres de détection de panne.





Si vous souhaitez utiliser le survol automatique, sélectionnez*Rollover automatique à l'aide du WAN*comme mode WAN et entrez les détails suivants.

Champ	Description
Mode réseau étendu	Sélectionner*Rollover automatique à l'aide du WAN.*
Port WAN principal	Sélectionnez le port WAN principal.
Port WAN secondaire	Sélectionnez le port WAN secondaire.
Bilan de santé	Sélectionnez l'une des options suivantes pour la vérification de l'état : • **Serveurs DNS WAN**: Si vous sélectionnez cette option, il détecte l'état d'une liaison WAN à l'aide des serveurs DNS WAN configurés dans les pages Paramètres WAN. • **Serveurs DNS**: Si vous sélectionnez cette option, il détecte l'état du WAN à l'aide d'un serveur DNS spécifique. Sélectionnez Serveurs DNS et entrez les adresses IP des serveurs DNS personnalisés pour les WAN principal et secondaire. • **Adresse IP ping**: Si vous sélectionnez cette option, envoyez une requête ping à une adresse IP pour détecter l'état du WAN. Sélectionnez cette option et entrez les adresses IP dans les champs pour envoyer une requête ping à partir des réseaux WAN principal et secondaire. Assurez-vous que cet hôte de destination est fiable.
Réseau étendu principal	Entrez l'adresse IP dont l'état peut être vérifié à l'aide du port WAN principal.
Réseau étendu secondaire	Entrez l'adresse IP dont l'état peut être vérifié à l'aide du port WAN secondaire.
Intervalle de nouvelle tentative	Entrez la durée de la nouvelle tentative en secondes pour vérifier l'état du WAN. Par défaut, c'est toutes les 30 secondes.
Basculement après	Entrez le nombre d'échecs après lequel le port est considéré comme indisponible.

L'équilibrage de charge

La fonction d'équilibrage de charge vous permet d'utiliser simultanément plusieurs liaisons WAN (vraisemblablement plusieurs FAI). Après avoir configuré plusieurs ports WAN, l'option d'équilibrage de charge peut acheminer le trafic sur plusieurs liaisons. Les liaisons de protocole sont utilisées pour séparer et attribuer les services sur un port WAN afin de gérer le flux Internet. La méthode de détection de panne configurée est utilisée régulièrement sur tous les ports WAN configurés en mode Load Balancing.

L'équilibrage de charge est bénéfique lorsque la vitesse de connexion d'un port WAN diffère considérablement de celle d'un autre. Dans ce cas, vous pouvez définir des liaisons de protocole pour acheminer les services à faible latence (tels que VOIP) sur la liaison à vitesse plus élevée et laisser le trafic d'arrière-plan à faible volume (tel que SMTP) passer par la liaison à vitesse inférieure.

La passerelle prend actuellement en charge deux algorithmes pour l'équilibrage de charge :

- **Tournoi à la ronde**: Cet algorithme fonctionne selon un processus récurrent dans lequel les paquets sont acheminés vers les ports WAN disponibles dans une séquence quelle que soit la vitesse de connexion des ports WAN. Si un paquet est transféré vers un port WAN, le paquet suivant ira automatiquement au port WAN suivant. Cela garantit que la charge de trafic est répartie entre tous les ports WAN actifs.
- **Débordement**: Si la méthode Spillover est sélectionnée, un WAN agit comme un lien dédié jusqu'à ce qu'un seuil de bande passante défini soit atteint. Après cela, le prochain WAN sera utilisé pour de nouvelles connexions. Les connexions entrantes sur le WAN sont autorisées avec ce mode, car la logique de débordement régit les connexions sortantes se déplaçant d'un WAN à l'autre WAN.

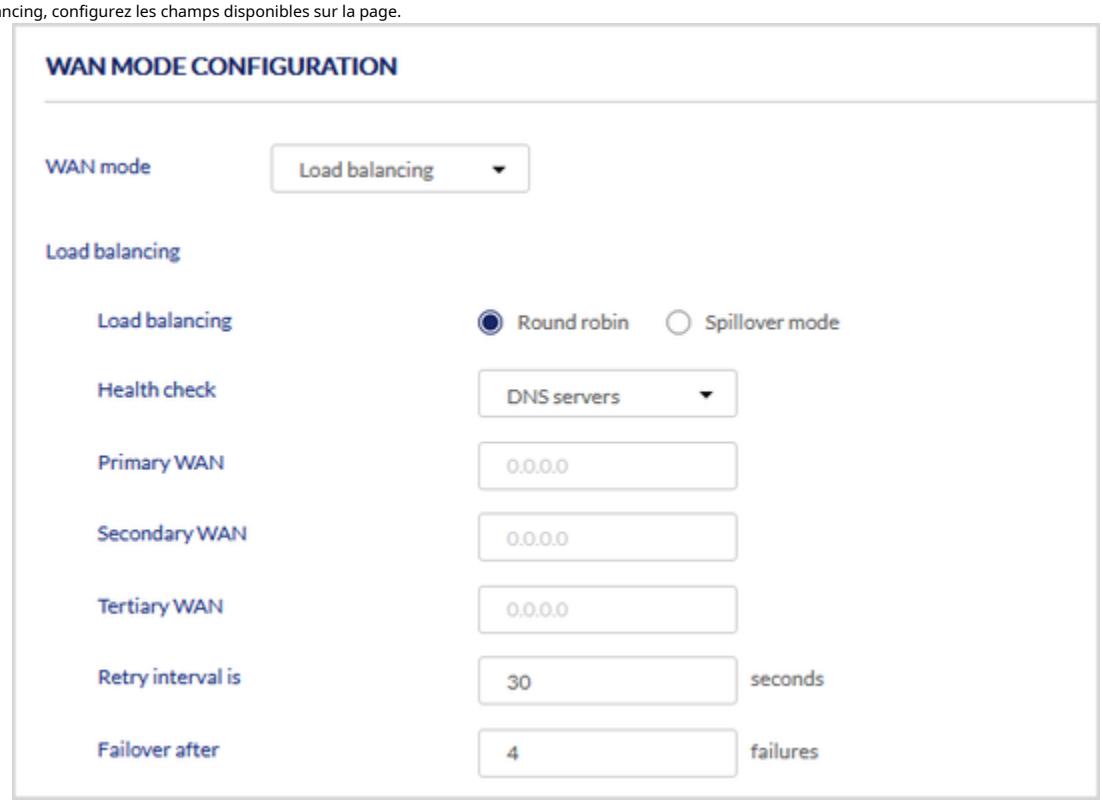
Vous pouvez configurer le mode de débordement à l'aide des options suivantes :

- **Tolérance de charge**: C'est le pourcentage de bande passante après lequel la passerelle passe au WAN secondaire.
- **Bande passante maximale**: Ceci définit la bande passante maximale tolérable par le WAN principal pour le trafic sortant.
  Si la bande passante de liaison du trafic sortant dépasse la valeur maximale de tolérance de charge de bande passante, la passerelle débordera sur les connexions suivantes vers le WAN suivant.

Par exemple, si la bande passante maximale d'un WAN est de 1 Kbps et que la tolérance de charge est définie sur 70. Désormais, chaque fois qu'une nouvelle connexion est établie, la bande passante augmente. Après un certain nombre de connexions, disons que la bande passante atteint 70 % de 1 Kbps, la passerelle diffusera de nouvelles connexions sortantes vers le prochain WAN. La valeur maximale de tolérance de charge est de 80 % et la valeur minimale est de 20 %.

Tournoi à la ronde

Le round robin est un algorithme d'équilibrage de charge et est utile lorsque la charge du trafic est répartie entre tous les ports WAN. Lorsque vous sélectionnez**Tournoi à la ronde** comme Load Balancing, configurez les champs disponibles sur la page.

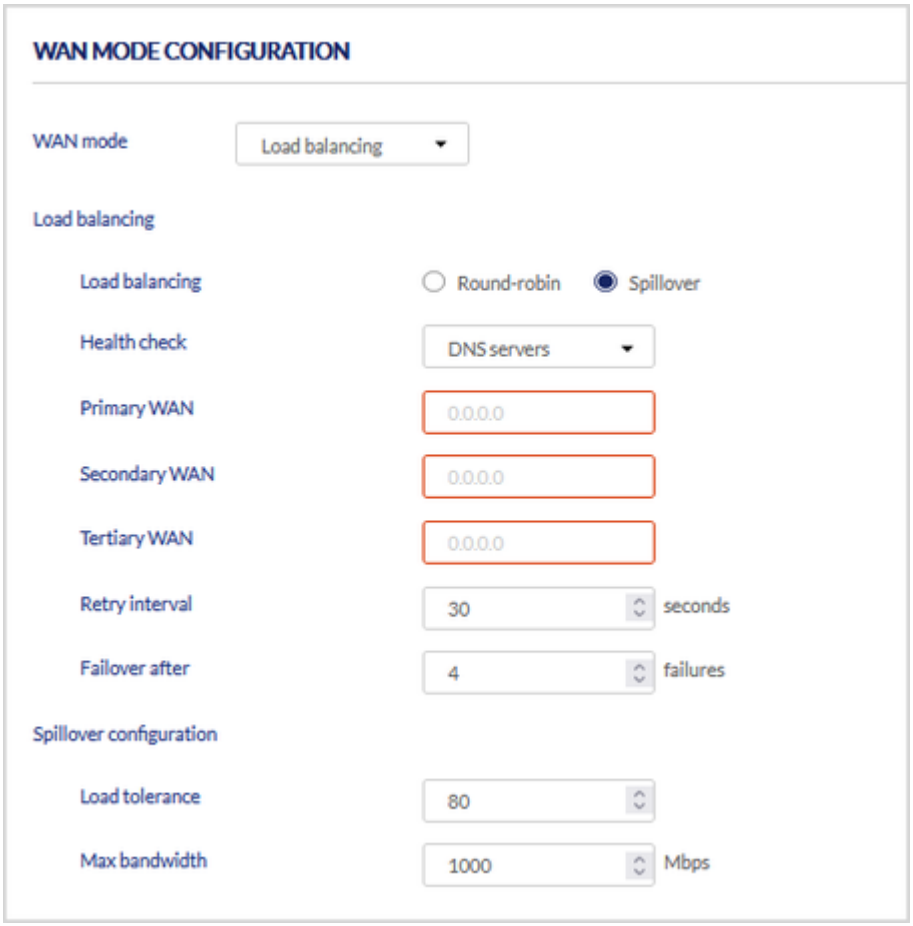


Champ	Description
L'équilibrage de charge	Sélectionner**Tournoi à la ronde**.
Bilan de santé	Sélectionnez l'une des options suivantes : • **Aucun**: sélectionnez cette option si vous ne souhaitez pas vérifier l'état du WAN. • **Serveurs DNS WAN**: sélectionnez cette option pour détecter l'état d'une liaison WAN à l'aide des serveurs DNS WAN configurés dans la page Paramètres WAN. • **Serveurs DNS**: sélectionnez cette option pour utiliser un serveur DNS spécifique pour détecter l'état du WAN, sélectionnez les serveurs DNS et entrez les adresses IP des serveurs DNS personnalisés pour les ports WAN principal, secondaire et tertiaire. • **Adresse IP ping**: sélectionnez cette option pour détecter l'état du WAN en envoyant une requête ping à une adresse IP, sélectionnez cette option et entrez les adresses IP dans les champs pour envoyer une requête ping à partir des ports WAN principal, secondaire et tertiaire.
Réseau étendu principal	Entrez le serveur DNS principal ou l'adresse IP principale à envoyer par ping.
Réseau étendu secondaire	Entrez le serveur DNS secondaire ou l'adresse IP secondaire à envoyer par ping.
WAN tertiaire	Entrez le serveur DNS tertiaire ou l'adresse IP tertiaire à envoyer par ping. Ce champ est disponible uniquement lorsque les trois WAN sont configurés.
L'intervalle de nouvelle tentative est	Entrez la durée de la nouvelle tentative en secondes pour vérifier l'état du WAN. Par défaut, c'est toutes les 30 secondes.

Basculement après	Entrez le nombre d'échecs après lequel le port est considéré comme indisponible.

Mode débordement

Sélectionner**Mode débordement**lorsque vous souhaitez qu'un WAN spécifique agisse comme un lien dédié jusqu'à ce qu'un seuil de bande passante défini soit atteint. Après cela, le prochain WAN est utilisé pour les nouvelles connexions. Lorsque vous sélectionnez le mode Spillover, configurez les champs suivants.



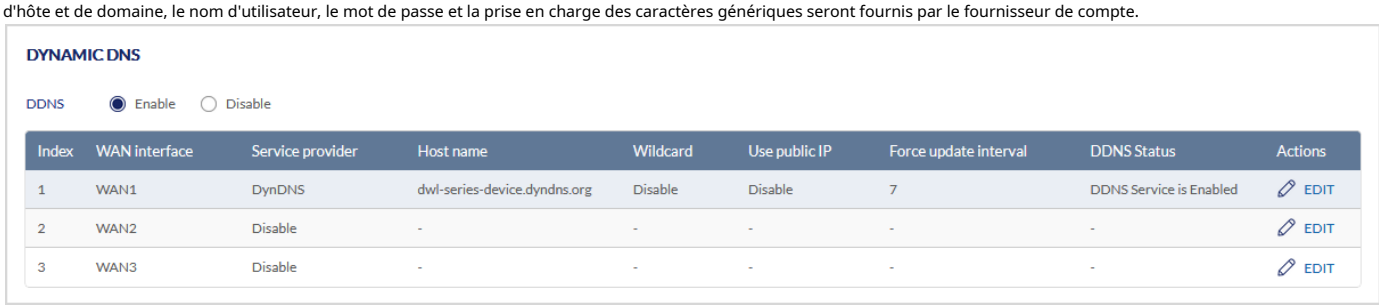
Champ	Description
L'équilibrage de charge	Sélectionner**Mode débordement**.
Bilan de santé	Sélectionnez l'une des options suivantes : • **Aucun**: sélectionnez cette option si vous ne souhaitez pas vérifier l'état du WAN. • **Serveurs DNS WAN**: sélectionnez cette option pour détecter l'état d'une liaison WAN à l'aide des serveurs DNS WAN configurés dans la page Paramètres WAN. • **Serveurs DNS**: sélectionnez cette option pour utiliser un serveur DNS spécifique pour détecter l'état du WAN. Sélectionnez Serveurs DNS et entrez les adresses IP des serveurs DNS personnalisés pour les ports WAN principal, secondaire et tertiaire. • **Adresse IP ping**: sélectionnez cette option pour détecter l'état du WAN en envoyant une requête ping à une adresse IP. Entrez les adresses IP dans les champs pour envoyer une requête ping à partir des ports WAN principal, secondaire et tertiaire.
Réseau étendu principal	Entrez le serveur DNS principal ou l'adresse IP principale à envoyer par ping.
Réseau étendu secondaire	Entrez le serveur DNS secondaire ou l'adresse IP secondaire à envoyer par ping.
WAN tertiaire	Entrez le serveur DNS tertiaire ou l'adresse IP tertiaire à envoyer par ping. Ce champ est disponible uniquement lorsque les trois WAN sont configurés.
L'intervalle de nouvelle tentative est	Entrez la durée de la nouvelle tentative en secondes pour vérifier l'état du WAN. Par défaut, c'est toutes les 30 secondes.

Basculement après	Entrez le nombre d'échecs après lequel le port est considéré comme indisponible.
Configuration de débordement	
Tolérance de charge	Entrez le pourcentage de bande passante, après quoi la passerelle passe au WAN suivant. La fourchette va de 20 à 80.
Bande passante maximale	Cela définit la bande passante maximale tolérable par le WAN pour le trafic sortant. La plage de bande passante maximale va de 1 à 1 000 Mbps.

DNS dynamique

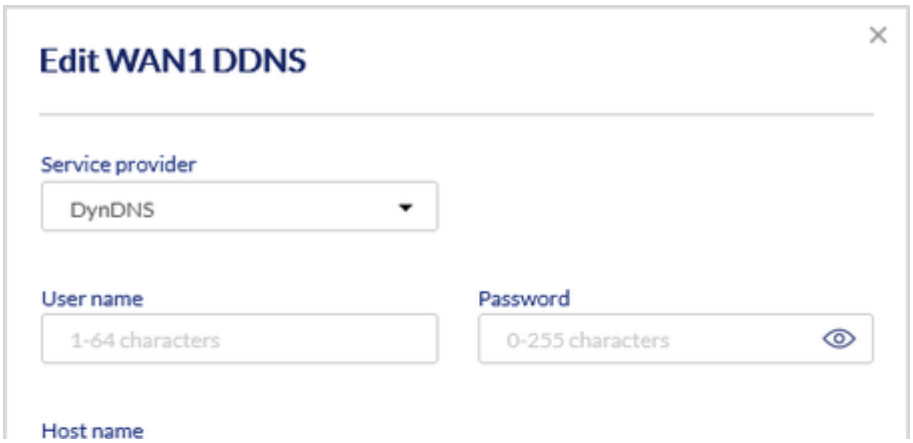
Le DNS dynamique (DDNS) est un service Internet qui permet de localiser des routeurs avec différentes adresses IP publiques.
en utilisant des noms de domaine Internet. Pour utiliser DDNS, vous devez créer un compte auprès d'un fournisseur DDNS tel que DynDNS, FreeDNS, NO-IP ou 3322.org.

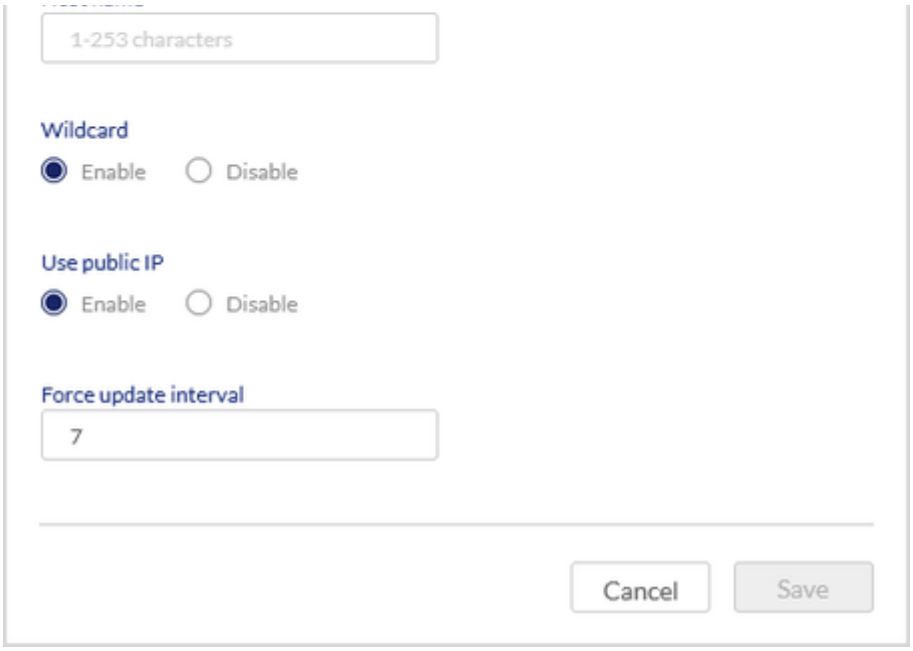
Chaque WAN configuré peut avoir un service DDNS différent si nécessaire. Une fois configurée, la passerelle mettra à jour les modifications des services DDNS dans l'adresse IP WAN. Il dirigera les fonctionnalités dépendant de l'accès au WAN de la passerelle via FQDN vers la bonne adresse IP. Lorsque vous créez un compte avec un service DDNS, le nom d'hôte et de domaine, le nom d'utilisateur, le mot de passe et la prise en charge des caractères génériques seront fournis par le fournisseur de compte.



Lorsque la fonctionnalité DDNS est activée, elle est appliquée à l'adresse IP WAN, qui est active, et les champs suivants sont affichés dans le tableau :

Champ	Description
Indice	Il affiche le numéro de série des entrées.
Interface WAN	Il affiche l'interface WAN sur laquelle le DDNS est appliqué.
Fournisseur de services	Il affiche les types de services utilisés par ce port WAN.
Nom d'hôte	Il affiche le nom d'hôte à mapper avec l'adresse IP de l'interface WAN dans le service DDNS sélectionné.
Caractère générique	Il indique si la fonctionnalité Wildcard est activée ou désactivée.
Utiliser une adresse IP publique	Il indique si cette option est activée ou désactivée. L'activation de cette option utiliserait une adresse IP externe (du routeur NAT) au lieu de l'adresse IP WAN de l'appareil.
Forcer l'intervalle de mise à jour	Il spécifie l'intervalle de mise à jour périodique pour automatiser la passerelle afin de mettre à jour les informations de l'hôte sur le service DDNS sélectionné.
Statut DDNS	Il affiche l'état DDNS du port WAN.
Actions	Cliquez sur**Modifier**pour modifier la configuration. Cela ouvre le*Modifier le DDNS WAN1/WAN2/WAN3*page.



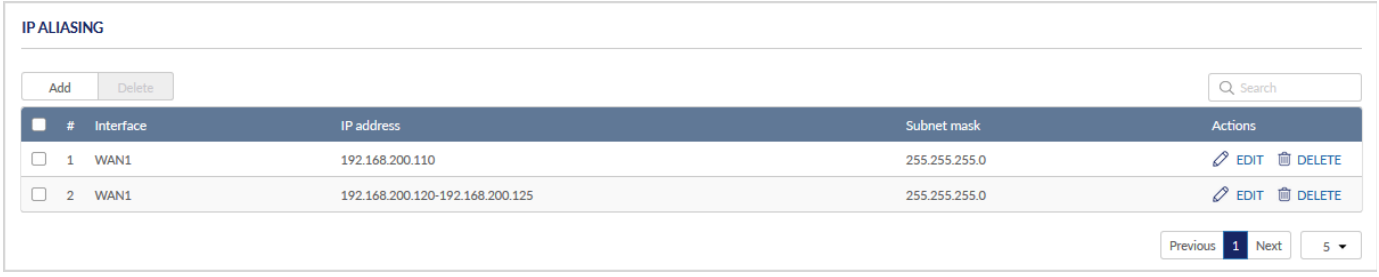


Les champs disponibles sur cette page sont les suivants :

Champ	Description
Fournisseur de services	Sélectionnez l'un des types de services suivants que ce port WAN doit utiliser : DynDNS, FreeDNS, NO-IP, 3322.org et Disable.
Nom d'utilisateur	Saisissez le nom d'utilisateur du compte pour les fournisseurs de services suivants : DynDNS, FreeDNS, NO-IP et 3322.org.
Mot de passe	Saisissez le mot de passe des comptes des fournisseurs de services ci-dessus.
Nom d'hôte	Spécifiez le nom d'hôte complet qui doit être mappé avec l'adresse IP de l'interface WAN dans le service DDNS sélectionné.
Caractère générique	La fonctionnalité de caractère générique permet à tous les sous-domaines de votre nom d'hôte DynDNS ou 3322.org de partager la même adresse IP publique que le nom d'hôte. Cette option peut être activée ici si elle n'est pas effectuée sur le site DynDNS. Ce champ est disponible lorsque vous sélectionnez**DynDNS**ou**3322.org**en tant que fournisseur de services.
Utiliser une adresse IP publique	L'activation de cette option utiliserait une adresse IP externe (du routeur NAT) au lieu de l'adresse IP WAN de l'appareil.
Forcer l'intervalle de mise à jour	Spécifiez l'intervalle de mise à jour périodique pour automatiser la passerelle afin de mettre à jour les informations de l'hôte sur le service DDNS sélectionné.
Sauvegarder	Cliquez sur**Sauvegarder**pour enregistrer vos paramètres.
Annuler	Cliquez sur**Annuler**pour revenir aux paramètres précédents.

Alias IP

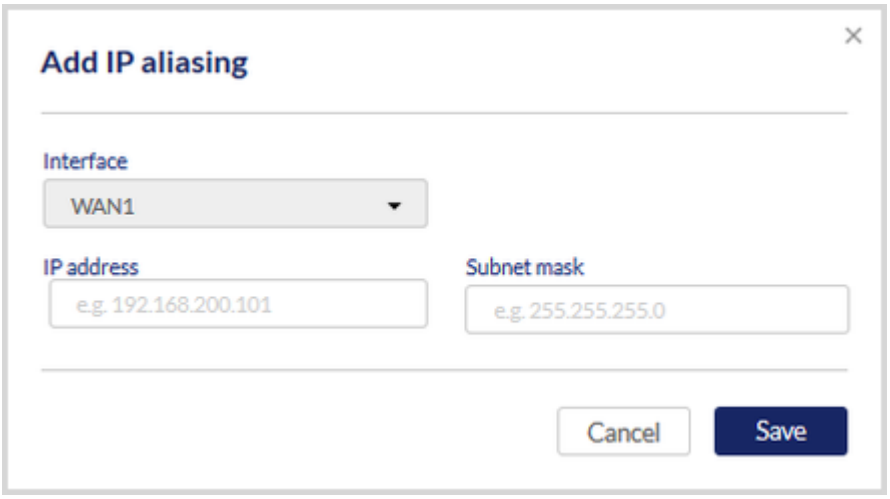
Un seul port Ethernet WAN est accessible via plusieurs adresses IP en ajoutant un alias au port. Cela se fait en configurant une adresse IP Alias. La section Alias IP répertorie les alias IP configurés sur les interfaces WAN. Vous pouvez ajouter un nouvel alias IP et modifier ou supprimer l'alias IP configuré.



Les champs affichés sur le*Alias IP*le tableau est le suivant :

Champ	Description
Interface	Il affiche le port WAN sur lequel l'alias IP est configuré.
adresse IP	Il affiche une adresse IP d'alias pour l'interface WAN que vous avez sélectionnée.
Masque de sous-réseau	Il affiche le masque de sous-réseau pour l'interface WAN que vous avez sélectionnée.
Actions	Vous pouvez modifier ou supprimer cette entrée. *Remarque : Cette colonne est disponible uniquement lorsque vous désactivez le champ « Utiliser la configuration du profil ».*

Pour supprimer plusieurs entrées à la fois, cochez les cases du*Alias IP*vous souhaitez supprimer, puis cliquez sur**Supprimer**. Cliquez sur**Ajouter**pour ajouter un nouvel alias IP. Cela ouvre le*Ajouter un alias IP*page.



Les champs disponibles sur cette page sont les suivants :

Champ	Description
Interface	Sélectionnez le port WAN.
adresse IP	Entrez une adresse IP d'alias pour l'interface WAN que vous avez sélectionnée.
Masque de sous-réseau	Entrez un masque de sous-réseau pour l'interface WAN que vous avez sélectionnée.
Sauvegarder	Cliquez sur**Sauvegarder**pour enregistrer vos paramètres.
Fermer	Cliquez sur**Fermer**pour revenir aux paramètres précédents.

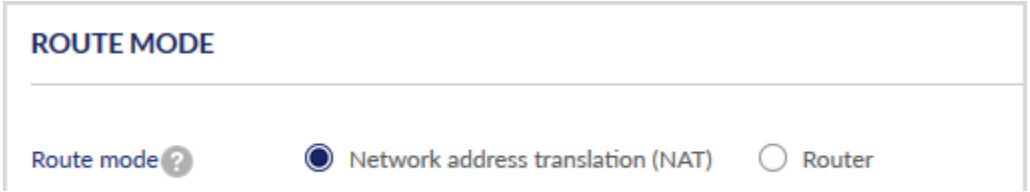
Adressage

Le*Adressage*La section présente diverses fonctionnalités que la passerelle cloud Nuclias utilise pour gérer le flux de trafic entre Internet et le réseau local sécurisé. Pour limiter les paquets de diffusion d'un appareil dans un grand réseau, la passerelle prend en charge les réseaux locaux virtuels. Ces réseaux locaux virtuels attribuent des identifiants de VLAN aux ports LAN pour isoler le trafic de ce port du réseau local général. Vous découvrirez tous ces sujets en détail dans cette section.

Le*Adressage*La section couvre les sujets suivants :

Mode itinéraire

Le routage entre le LAN et le WAN aura un impact sur la façon dont cette passerelle gère le trafic reçu sur l'une de ses interfaces physiques. Le mode de routage de la passerelle est au cœur du comportement du flux de trafic entre le réseau local sécurisé et Internet.



Avec le routeur (routage classique), les appareils du réseau local sont directement accessibles depuis Internet avec leurs adresses IP publiques (en supposant que les paramètres de pare-feu appropriés soient configurés). Si votre FAI a attribué une adresse IP à chacun des ordinateurs/appareils que vous utilisez, sélectionnez**Routeur**.

Traduction d'adresses réseau (NAT)est une technique qui permet à plusieurs ordinateurs et appareils de votre réseau local de partager une connexion Internet. Les ordinateurs du réseau local utilisent une plage d'adresses IP « privée », tandis que le port WAN de la passerelle est configuré avec une seule adresse IP « publique ». Outre le partage de connexion, NAT masque également les adresses IP internes des ordinateurs sur Internet. NAT est requis si votre FAI ne vous a attribué qu'une seule adresse IP. Les ordinateurs/appareils qui se connectent via la passerelle devront se voir attribuer des adresses IP à partir d'un sous-réseau privé.

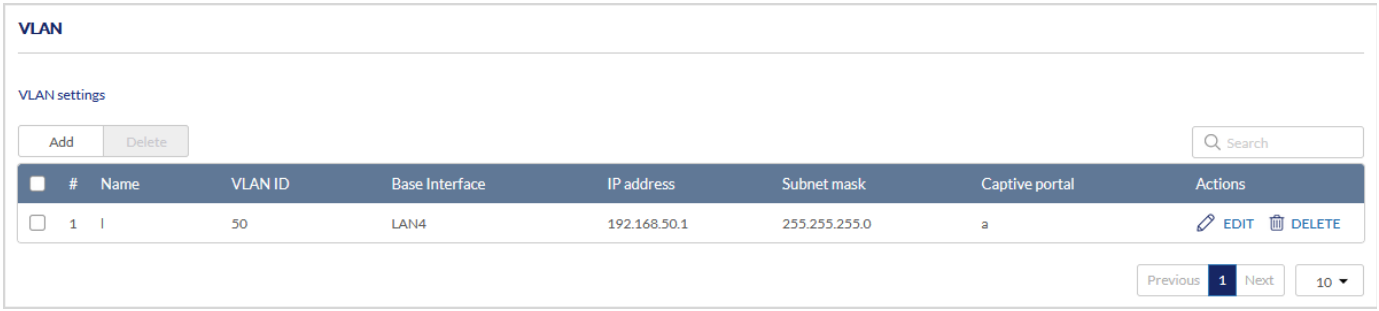
VLAN

La passerelle prend en charge l'isolation du réseau virtuel sur le réseau local à l'aide de VLAN. Vous pouvez configurer les périphériques LAN pour communiquer dans un sous-réseau défini par des identifiants VLAN. Un ID VLAN unique peut être attribué à chaque port LAN afin que le trafic vers et depuis le port physique puisse être isolé du LAN général.

Le filtrage VLAN est avantageux pour limiter les paquets de diffusion d'un appareil dans un grand réseau. Dans le*Ajouter un profil VLAN*page, définissez le réseau virtuel.

Paramètres VLAN

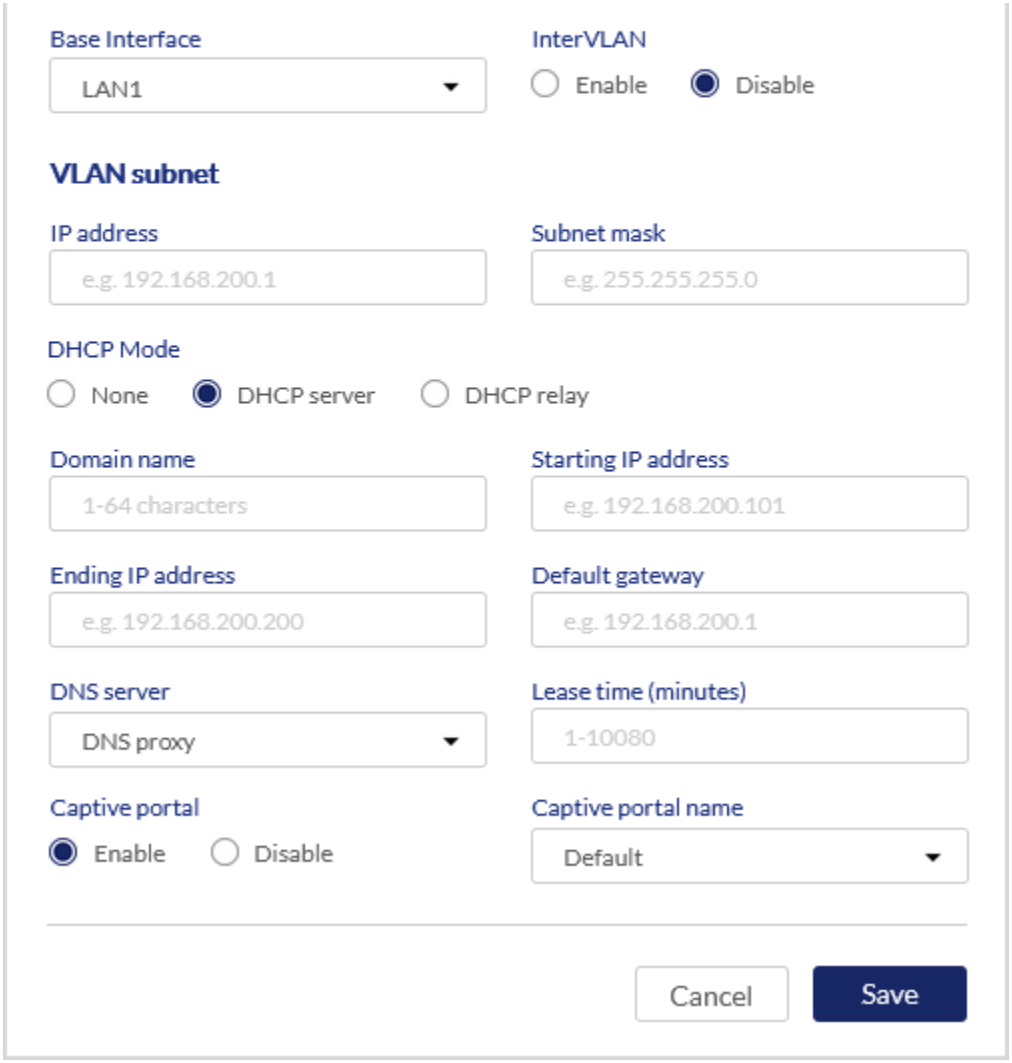
Le*Paramètres VLAN*La section affiche une liste des VLAN configurés par nom et ID de VLAN. Une adhésion à un VLAN peut être créée en cliquant sur le bouton**Ajouter** bouton présent au dessus de la liste.
La passerelle cloud prend en charge les ports LAN avec différents sous-réseaux pour chaque LAN, c'est-à-dire que pour le port 4, l'adresse IP attribuée est 192.168.10.1, pour le port 3, elle est 192.168.11.1 et pour le port 2, elle est 192.168.12.1. La valeur de l'ID VLAN peut être n'importe quel nombre compris entre 1 et 4 094. Par défaut, la passerelle cloud accepte uniquement le trafic non balisé sur l'interface LAN. Par conséquent, pour tout trafic balisé, l'utilisateur doit ajouter explicitement un VLAN.



Les champs disponibles sur le*Paramètres VLAN*e tableau est le suivant :

Champ	Description
Nom	Il affiche le nom du VLAN.
ID de VLAN	Il affiche la valeur numérique associée au VLAN.
Interface de base	Il affiche l'interface physique sur laquelle le VLAN est créé.
adresse IP	Il affiche l'adresse IP du VLAN.
Masque de sous-réseau	Il affiche le masque de sous-réseau du VLAN.
Portail captif	Si le portail captif est activé sur le VLAN, ce champ affiche le nom du portail captif.
Actions	Vous pouvez modifier ou supprimer le VLAN correspondant. *Remarque : Ce champ est disponible uniquement lorsque le champ « Utiliser la configuration du profil » est désactivé.*

Cliquez sur**Ajouter**pour ajouter un nouveau VLAN. Cela ouvre le*Ajouter un profil VLAN*page. Pour supprimer plusieurs entrées à la fois, cochez les cases des VLAN configurés que vous souhaitez supprimer, puis cliquez sur**Supprimer**.



Les champs disponibles sur le*Ajouter un profil VLAN*page sont les suivantes :

Champ	Description
Nom	Entrez un nom unique pour ce VLAN.
ID de VLAN	Entrez un ID unique pour ce VLAN (1 - 4094).
Interface de base	Sélectionnez l'interface physique sur laquelle le VLAN doit être créé.
InterVLAN	Il autorise ou refuse la communication entre les réseaux VLAN.
Sous-réseau VLAN	
adresse IP	Entrez une adresse IP pour le sous-réseau VLAN.
Masque de sous-réseau	Entrez le masque de sous-réseau pour le sous-réseau VLAN.
Mode DHCP	Sélectionnez l'un des modes suivants : • **Aucun:**Sélectionner**Aucun**pour désactiver DHCP. • **Serveur DHCP:**Si cette option est sélectionnée, l'appareil agira en tant que serveur DHCP sur votre réseau. • **Relais DHCP :**Si cette option est sélectionnée, les clients DHCP de votre réseau recevront des baux d'adresses IP d'un serveur DHCP sur un sous-réseau différent.
Nom de domaine	Spécifiez le nom de domaine. Ce champ est disponible uniquement lorsque**Serveur DHCP**est le*Mode DHCP*.
Adresse IP de départ	Entrez l'adresse IP de départ.

Adresse IP de fin	Entrez l'adresse IP de fin.
Passerelle par défaut	Si*Mode DHCP*est**Serveur DHCP**, entrez la passerelle par défaut pour le mode serveur DHCP.
Serveur dns	Sélectionnez l'une des options suivantes pour les serveurs DNS pour les clients DHCP : • **Proxy DNS**: Activez ou désactivez le proxy DNS sur ce VLAN. Si elle est activée, la passerelle agit comme un proxy pour toutes les requêtes DNS et communique avec les serveurs DNS du FAI. • **DNS du FAI**: Cette option envoie toutes les requêtes DNS aux serveurs DNS du FAI. **DNS statique :** • Cette option envoie toutes les requêtes DNS aux serveurs DNS statiques configurés.
Serveur DNS primaire	Entrez l'adresse IP du serveur DNS principal.
Serveur DNS secondaire	Entrez l'adresse IP du serveur DNS secondaire.
Serveur WINS (facultatif)	Entrez l'adresse IP WINS dans la configuration DHCP. Un WINS (Windows Internet Naming Service Server) est l'équivalent d'un serveur DNS mais utilise le protocole NetBIOS pour résoudre les noms d'hôtes. C'est un champ facultatif.
Durée du bail (minutes)	Saisissez la durée (en minutes) pendant laquelle les adresses IP seront louées aux clients DHCP.
Passerelle relais	Saisissez l'adresse IP de la passerelle relais.
Portail captif	Vous pouvez activer ou désactiver la fonctionnalité de portail captif sur le VLAN.
Nom du portail captif	Sélectionnez le nom du portail captif configuré dans la liste déroulante.
Proxy DNS	Lorsque le champ Proxy DNS est activé, la passerelle agit comme proxy pour toutes les requêtes DNS et communique avec les serveurs DNS du FAI. Ce champ est disponible lorsque vous sélectionnez**Relais DHCP**ou**Aucun**comme le mode DHCP.
Sauvegarder	Cliquez sur**Sauvegarder**pour enregistrer vos paramètres.
Fermer	Cliquez sur**Fermer**pour revenir aux paramètres précédents.

Liste de gestion IP

Le serveur DHCP de la passerelle peut attribuer des paramètres IP à vos clients sur votre réseau en ajoutant le MAC d'un client
et l'adresse IP à la base de données du serveur DHCP. Chaque fois que la passerelle reçoit une demande d'un client, l'adresse MAC de ce client est comparée à la liste d'adresses MAC présente dans la base de données et l'adresse IP correspondante est attribuée au client.

Une autre mesure de sécurité disponible consiste à autoriser le trafic sortant (du LAN au WAN) lorsque le nœud LAN possède une adresse IP correspondant à l'adresse MAC qui lui est liée. Il s'agit d'une liaison IP/MAC. En obligeant la passerelle à valider l'adresse IP du trafic source avec l'adresse MAC unique du nœud LAN configuré, l'administrateur peut garantir que le trafic provenant de cette adresse IP n'est pas usurpé. Si une violation (c'est-à-dire si l'adresse IP source du trafic ne correspond pas à l'adresse MAC source attendue) se produit, les paquets seront abandonnés.

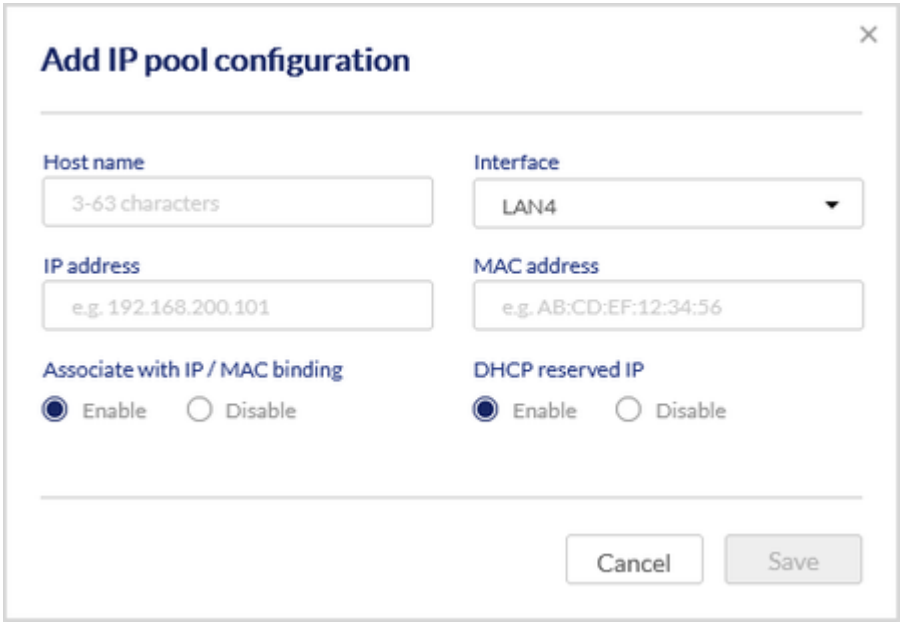
Cette section du VLAN affiche la liste de gestion IP.

Les champs affichés dans le*Liste de gestion IP*le tableau est le suivant :

Champ	Description
Nom d'hôte	Il affiche le nom d'hôte pour la paire d'adresses IP et MAC.
Interface	Il affiche l'interface à laquelle le client est connecté et le bail DHCP est fourni. Il peut inclure des noms d'interface VLAN personnalisés.
adresse IP	Il affiche l'adresse IP que vous avez attribuée à l'appareil.
Adresse Mac	

	Il affiche l'adresse MAC de l'hôte pouvant se connecter sur l'interface configurée et pour lequel une adresse IP est réservée.
IP réservée DHCP	Il indique si l'adresse IP réservée DHCP est activée ou désactivée.
Liaison IP/MAC	Il indique si la fonction de liaison IP/MAC est activée ou désactivée.
Actions	Vous pouvez modifier ou supprimer l'entrée sélectionnée. *Remarque : Ce champ est disponible uniquement lorsque le champ « Utiliser la configuration du profil » est désactivé.*

Cliquez sur**Ajouter**pour ajouter une nouvelle entrée. Cela ouvre le*Ajouter la configuration du pool IP*page. Pour supprimer plusieurs entrées à la fois, cochez les cases de la gestion IP que vous souhaitez supprimer, puis cliquez sur**Supprimer**.



Les champs disponibles sur le*Ajouter la configuration du pool IP*page sont les suivants :

Champ	Description
Nom d'hôte	Entrez le nom d'hôte pour la paire d'adresses IP et MAC.
Réseau	Sélectionnez le réseau dans la liste déroulante.
adresse IP	Saisissez l'adresse IP que vous souhaitez attribuer à cet appareil. *Remarque : Cette adresse IP doit être dans la même plage que l'adresse IP de début/fin sous les paramètres DHCP de cette interface.*
Adresse Mac	Saisissez l'adresse MAC (format xx:xx:xx:xx:xx:xx) de l'hôte pouvant être connecté sur LAN, pour lequel une adresse IP doit être réservée.
Associer à la liaison IP/MAC	Vous pouvez activer ou désactiver la fonctionnalité de liaison IP/MAC. S'il est activé, il associe les informations de l'hôte à la liaison IP/MAC.
IP réservée DHCP	Vous pouvez activer ou désactiver la fonctionnalité IP réservée DHCP.
Sauvegarder	Cliquez sur**Sauvegarder**pour enregistrer vos paramètres.
Fermer	Cliquez sur**Fermer**pour revenir aux paramètres précédents.

Routage

Le routage fait référence au chemin que suivent les paquets de la source à la destination de la manière la plus optimale. Cette section du Réseau vous fournit les champs de configuration requis pour gérer le processus de routage dans le réseau. Diverses méthodes sont prises en charge par la passerelle cloud Nuclias, telles que Static Route, Policy Route, RIP et OSPFv2. Le routage statique est une méthode conventionnelle dans laquelle la passerelle utilise le chemin de route configuré manuellement et si des modifications se produisent, la route statique doit être reconfigurée manuellement. Policy Route vous permet de configurer la politique de routage en fonction de certains paramètres tels que l'adresse source, l'adresse de destination, le port source ou le port de destination. Un autre protocole pris en charge par la passerelle cloud est le Routing Information Protocol (RIP). C'est un protocole qui contrôle le nombre de sauts qu'un paquet peut effectuer.

faire de sa source à sa destination. De même, vous apprendrez également à configurer OSPFv2 dans cette section. OSPFv2 est un protocole dynamique qui achemine les paquets IP (Internet Protocol) uniquement au sein d'un seul domaine de routage.

Cette section couvre les sujets suivants :

Itinéraire statique

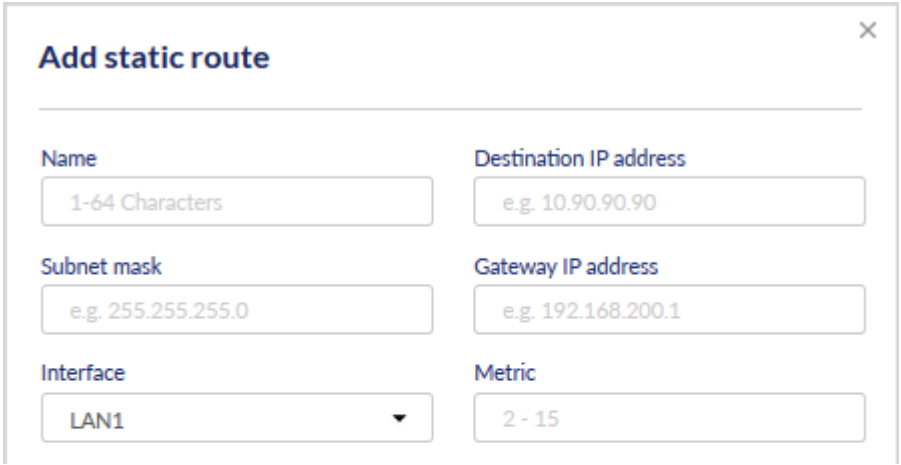
Le routage entre le LAN et le WAN aura un impact sur la façon dont cette passerelle gère le trafic reçu sur l'une de ses interfaces physiques. Le mode de routage de la passerelle est au cœur du comportement du flux de trafic entre le réseau local sécurisé et Internet.

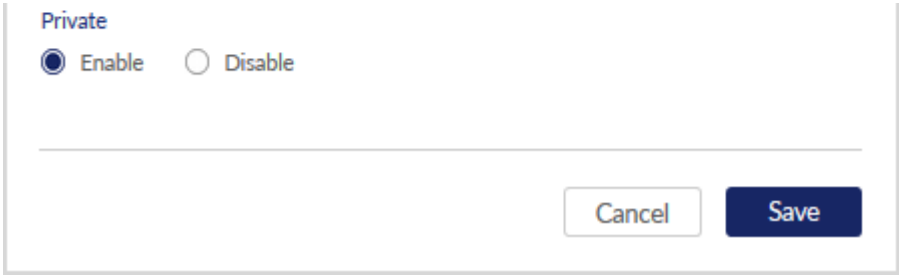
L'ajout manuel d'itinéraires statiques à cet appareil vous permet de définir la sélection du chemin de trafic d'une interface à l'autre. Il n'y a aucune communication entre cette passerelle et d'autres appareils pour tenir compte des changements de chemin ; une fois configurée, la route statique sera active et efficace jusqu'à ce que le réseau change.
La page Route statique affiche toutes les routes ajoutées manuellement par un administrateur et permet plusieurs opérations sur les routes statiques.

Vous trouverez une liste des routes statiques configurées sur la passerelle avec les détails suivants :

Champ	Description
Nom	Il affiche le nom de l'itinéraire.
Destination	Il affiche l'adresse IP de la destination de la route statique.
Masque de sous-réseau	Il affiche le masque de sous-réseau de la route statique.
passerelle	Il affiche l'adresse IP de la passerelle via laquelle l'hôte ou le réseau de destination peut être atteint.
Interface	Il affiche l'interface réseau physique (WAN, DMZ, VLAN ou LAN) via laquelle cette route est accessible.
Métrique	Il affiche une valeur comprise entre 2 et 15.
Actif	Sélectionnez activer ou désactiver pour activer ou désactiver cet itinéraire. ***Note**: Les options d'activation et de désactivation ne sont disponibles que si le champ « Utiliser la configuration du profil » est désactivé.*
Actions	Vous pouvez modifier ou supprimer l'itinéraire. ***Note**: Ce champ est disponible uniquement si le champ « Utiliser la configuration du profil » est désactivé.*

Cliquez sur**Ajouter**pour ajouter une nouvelle entrée. Cela ouvre le*Ajouter un itinéraire statique*page. Pour supprimer plusieurs entrées à la fois, cochez les cases de l'itinéraire statique configuré que vous souhaitez supprimer, puis cliquez sur**Supprimer**.





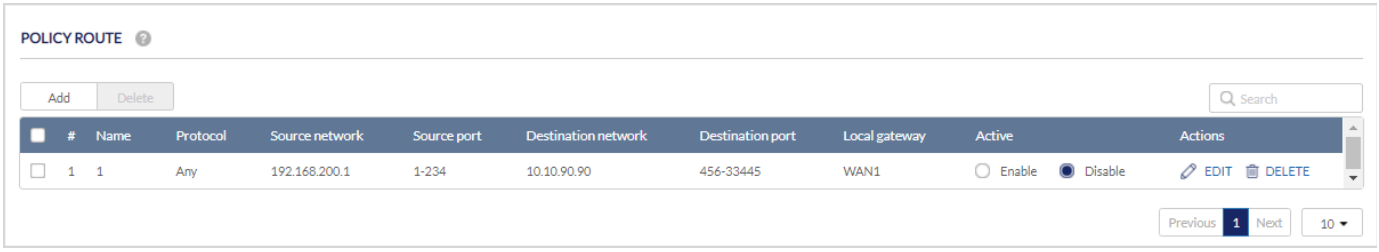
Les champs disponibles sur cette page sont les suivants :

Champ	Description
Nom	Entrez le nom de l'itinéraire.
Adresse IP de destination	Saisissez l'adresse IP de la destination de la route statique.
Masque de sous-réseau	Entrez le masque de sous-réseau de la route statique.
Adresse IP de la passerelle	Saisissez l'adresse IP de la passerelle via laquelle l'hôte ou le réseau de destination peut être atteint.
Interface	Sélectionnez une interface réseau physique (WAN, DMZ, VLAN ou LAN) via laquelle cette route est accessible.
Métrique	Saisissez une valeur comprise entre 2 et 15. Elle détermine la priorité de l'itinéraire. S'il existe plusieurs itinéraires vers la même destination, l'itinéraire avec la métrique la plus basse est choisi.
Privé	Activez cette fonctionnalité pour rendre cet itinéraire privé. Si la route est rendue privée, elle ne sera pas partagée dans un RIP.
Sauvegarder	Cliquez sur**Sauvegarder**pour enregistrer vos paramètres.
Annuler	Cliquez sur**Annuler**pour revenir aux paramètres précédents.

Voie politique

Les routes de stratégie sont utiles lorsque la fonctionnalité d'équilibrage de charge est utilisée. En sélectionnant TCP/UDP, vous pouvez attribuer le type de trafic à parcourir sur les ports WAN spécifiés. Le réseau source, l'adresse source, le réseau de destination, une adresse de destination, un service ou un protocole peuvent être associés à un port WAN particulier pour une flexibilité accrue.

Par exemple, le trafic VoIP d'un ensemble d'adresses IP LAN peut être attribué à un WAN, et tout trafic VoIP provenant des adresses IP restantes peut être attribué à l'autre liaison WAN. Les routes de stratégie ne sont applicables que lorsque le mode d'équilibrage de charge est activé et que plusieurs WAN sont configurés.

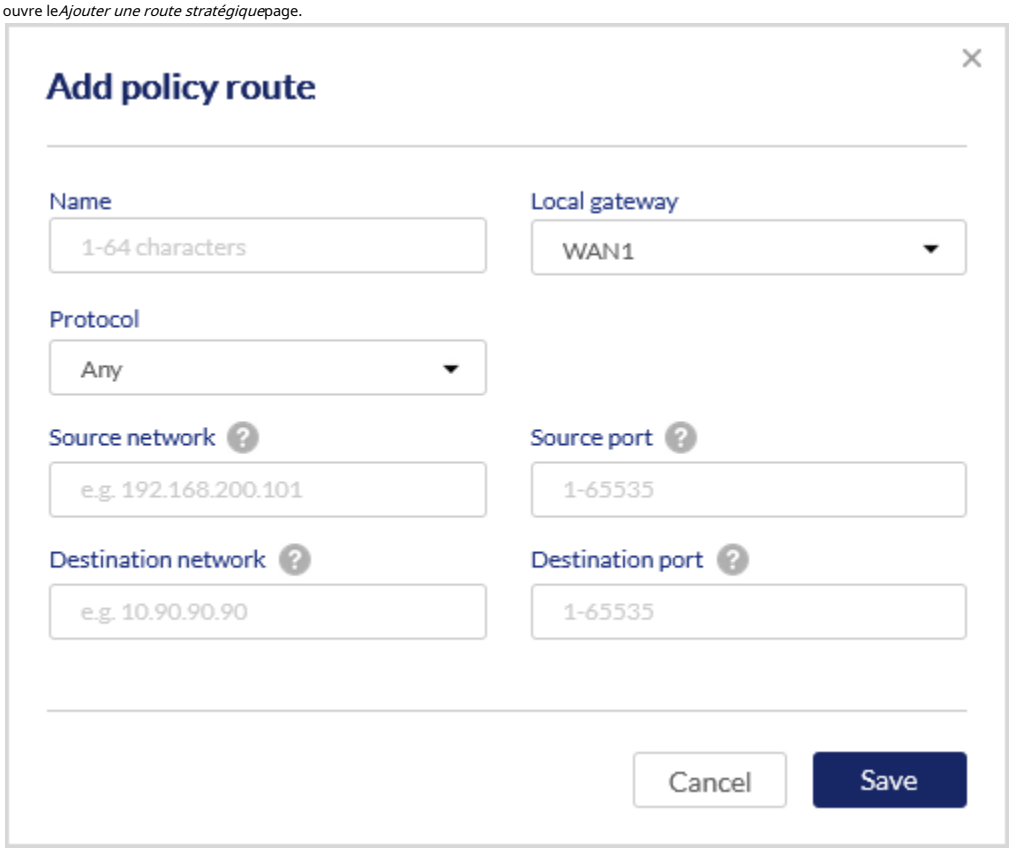


Cette section du routage affiche une liste des routes de stratégie configurées sur la passerelle avec les détails suivants :

Champ	Description
Nom	Il affiche le nom de la route politique.
Protocole	Il affiche le protocole placé dans les couches de transport de la suite de protocoles Internet.
Réseau source	Il affiche le réseau source. Ses options sont Any, une adresse IP et une plage d'adresses IP.
Port source	Il affiche un port source pour lequel la route de stratégie sera applicable.
Réseau de destination	Il affiche le réseau de destination. Ses options sont Any, une adresse IP et une plage d'adresses IP.

Le port de destination	Il affiche un port de destination pour lequel la route stratégique sera applicable.
Passerelle locale	Il affiche l'interface WAN.
Actif	Vous pouvez activer ou désactiver l'itinéraire de stratégie sélectionné. ***Note**: Les options d'activation et de désactivation ne sont disponibles que si le champ « Utiliser la configuration du profil » est désactivé.*
Actions	Vous pouvez modifier ou supprimer l'itinéraire. ***Note**: Ce champ est disponible uniquement si le champ « Utiliser la configuration du profil » est désactivé.*

Pour supprimer plusieurs entrées à la fois, cochez les cases de la route stratégique que vous souhaitez supprimer, puis cliquez sur**Supprimer**. Cliquez sur**Ajouter**pour ajouter plus d'entrées. Cela ouvre le*Ajouter une route stratégique*page.



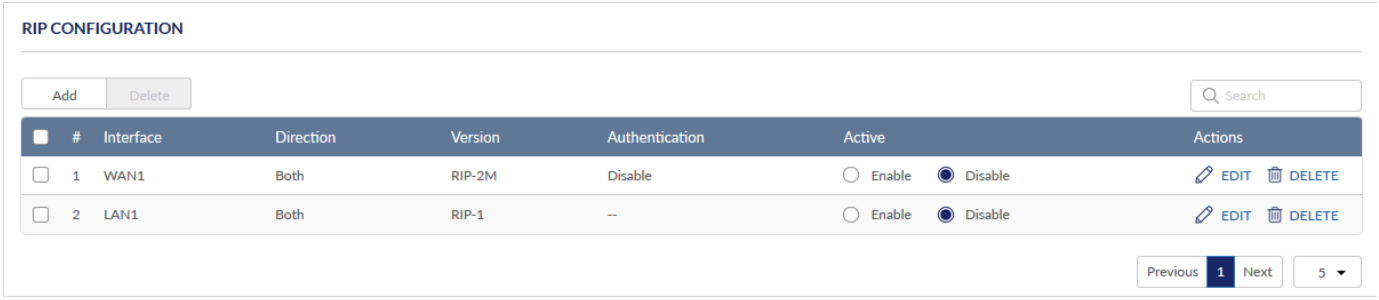
Les champs disponibles sur le*Ajouter une route stratégique*page sont les suivantes :

Champ	Description
Nom	Entrez le nom de la route stratégique.
Passerelle locale	Sélectionnez l'interface WAN.
Protocole	Sélectionnez l'un des protocoles généralement placés dans les couches de transport de la suite de protocoles Internet.
Réseau source	Entrez une adresse IP, une plage d'adresses IP ou Any comme réseau source.
Port source	Un port est un point de terminaison de communication. Les ports sont identifiés pour chaque combinaison de protocole et d'adresse par des nombres non signés de 16 bits, communément appelés numéro de port. Les protocoles les plus courants qui utilisent des numéros de port sont le Transmission Control Protocol (TCP) et le User Datagram Protocol (UDP). Ici le*Port source*est un nombre entier compris entre 1 et 65 535 initié à partir d'une application spécifique sur l'adresse IP source. Entrez un numéro de port source.
Réseau de destination	Entrez une adresse IP, une plage d'adresses IP ou Tout comme réseau de destination.
Le port de destination	Le port de destination est un nombre entier compris entre 1 et 65 535 destiné à une application spécifique sur l'adresse IP de destination. Entrez le numéro du port de destination.

Sauvegarder	Cliquez sur**Sauvegarder**pour enregistrer vos paramètres.
Fermer	Cliquez sur**Fermer**pour revenir aux paramètres précédents.

Configuration du RIP

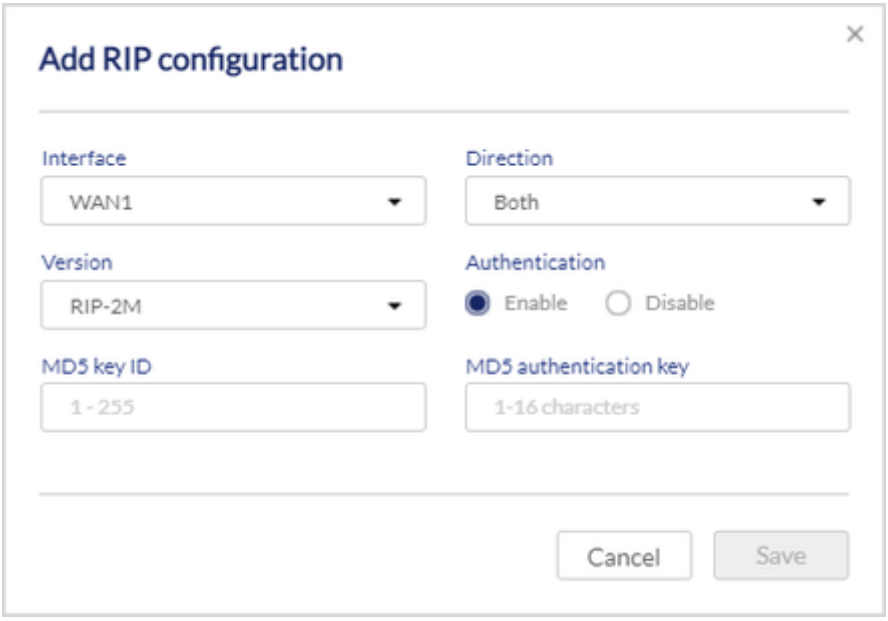
Le routage dynamique utilisant le Routing Information Protocol (RIP) est un protocole IGP (Interior Gateway Protocol) courant dans les réseaux locaux. Avec RIP, la passerelle cloud peut échanger des informations de routage avec d'autres passerelles prises en charge dans le LAN et permettre un ajustement dynamique des tables de routage pour s'adapter aux modifications du LAN sans interrompre le flux de trafic.



Les champs affichés sur la page sont les suivants :

Champ	Description
Interface	Il affiche l'interface sur laquelle le RIP est configuré.
Direction	Il affiche dans quelle direction les paquets RIP doivent être échangés.
Version	Il affiche la version RIP prise en charge par les périphériques de routage dans l'interface sélectionnée.
Authentification	Il indique si l'authentification est activée ou désactivée pour RIP-2M.
Actif	Vous pouvez activer ou désactiver le RIP configuré. ***Note**: Les champs d'activation et de désactivation ne sont disponibles que si le champ « Utiliser la configuration du profil » est désactivé.*
Actions	Vous pouvez modifier ou supprimer le RIP configuré. ***Note**: Ce champ est disponible uniquement si le champ « Utiliser la configuration du profil » est désactivé.*

Cliquez sur**Ajouter**pour ajouter une nouvelle entrée à la liste. Cela ouvre le*Ajouter une configuration RIP*page. Pour supprimer plusieurs entrées, cochez les cases correspondantes présentes dans la première colonne du tableau, puis cliquez sur**Supprimer**.

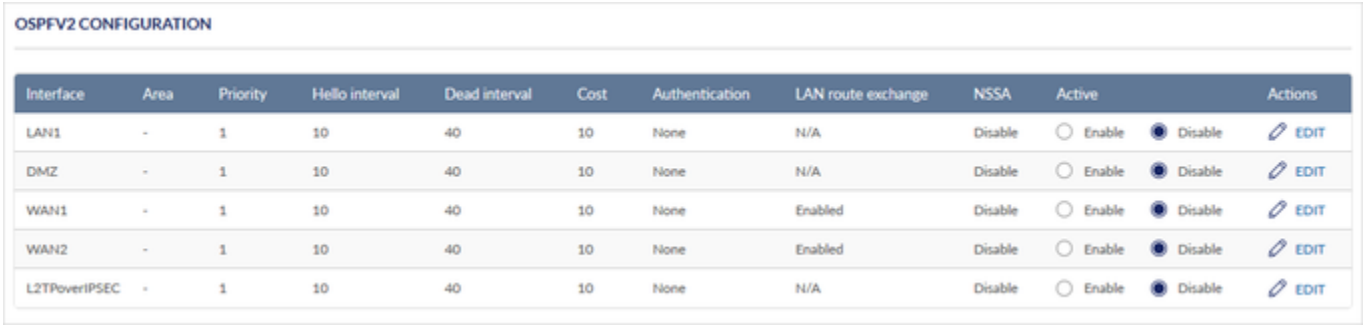


Les champs disponibles sur le*Ajouter une configuration RIP*page sont les suivantes :

Champ	Description
Interface	Sélectionnez l'interface sur laquelle vous souhaitez configurer le RIP.
Direction	La direction RIP définira comment cette passerelle envoie et reçoit les paquets RIP. Sélectionnez l'une des options suivantes : • **Les deux**: La passerelle diffuse à la fois sa table de routage et traite également les informations RIP reçues des autres routeurs. Il s'agit du paramètre recommandé pour utiliser pleinement les fonctionnalités RIP. • **Dans seulement**: La passerelle accepte les informations RIP des autres routeurs mais ne diffuse pas sa table de routage.
Version	La version RIP dépend de la prise en charge RIP des autres périphériques de routage du réseau local. • **RIP-1**: une version de routage basée sur les classes qui n'inclut pas les informations de sous-réseau. Il s'agit de la version la plus couramment prise en charge. • **RIP-2M**: Il inclut toutes les fonctionnalités de RIPv1 et prend en charge les informations de sous-réseau. RIP-2M envoie des données aux adresses de multidiffusion.
Authentification	Sélectionner**Activer**pour activer l'authentification pour RIP-2M. Par défaut, l'authentification RIP est désactivée.
ID de clé MD5	Entrez l'ID de clé MD5 unique.
Clé d'authentification MD5	Saisissez la clé d'authentification pour cette clé MD5.
Sauvegarder	Cliquez sur**Sauvegarder**pour enregistrer vos paramètres.
Annuler	Cliquez sur**Annuler**pour revenir à vos paramètres précédents.

Configuration OSPFv2

OSPF est un protocole de passerelle intérieure qui achemine les paquets IP (Internet Protocol) uniquement au sein d'un seul routage.
domaine. Il rassemble des informations sur l'état des liens auprès des routeurs disponibles et construit une carte topologique du réseau. OSPF version 2 est un protocole de routage décrit dans RFC2328 - OSPF Version 2. OSPF est un IGP (Interior Gateway Protocols) et est largement utilisé dans les grands réseaux tels que le réseau fédérateur des FAI et les réseaux d'entreprise.

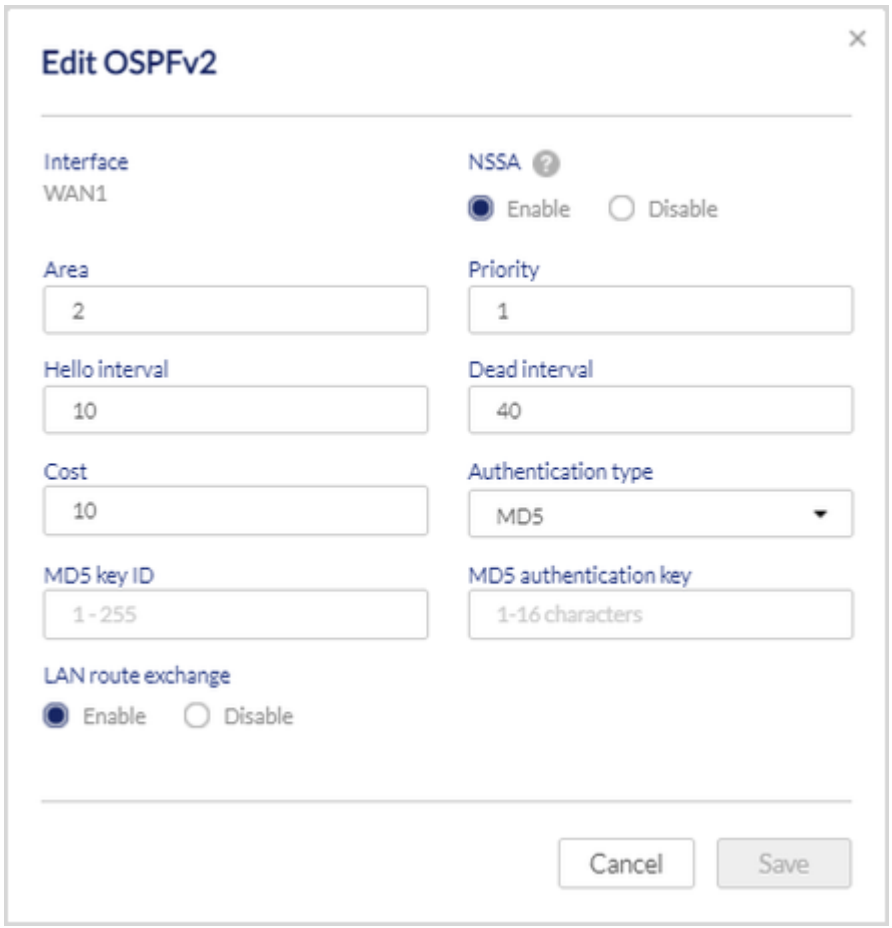


Les champs affichés sur le*Configuration OSPFV2*le tableau est le suivant :

Champ	Description
Interface	Il affiche l'interface réseau physique sur laquelle OSPFv2 est activé ou désactivé. *Note:* • *Pour l'interface « L2TP sur IPsec », suivez les étapes suivantes :* *1.Dans le portail cloud, accédez à VPN > PPTP/L2TP > Mode serveur/Mode client et cliquez sur**Ajouter**.* *2.Sélectionner**L2TP**comme type de serveur/client et activez**L2TP sur IPsec**. Configurez L2TP sur IPsec côté serveur/côté client.* *3.Enregistrez la configuration. Pour plus de détails, reportez-vous àPPTP/L2TP.* • *De même, pour l'« interface DMZ », vous devez configurer DMZ sur la page Configuration du port (Réseau > Ethernet > Configuration du port). Pour plus de détails, reportez-vous àConfiguration des ports .*
Zone	Il affiche la zone à laquelle appartient l'interface.

Priorité	Il affiche la priorité du routeur pour devenir le routeur désigné.
Bonjour intervalle	Il affiche le nombre de secondes pendant lesquelles le paquet hello est envoyé.
Intervalle mort	Il affiche le temps (nombre de secondes) pendant lequel les paquets Hello d'un périphérique ne doivent pas avoir vu avant que ses voisins déclarent le routeur OSPF hors service.
Coût	Il affiche le coût d'envoi d'un paquet sur une interface OSPFv2.
Authentification	Il affiche le type d'authentification.
Échange de routes LAN	Il affiche l'état de l'échange de route LAN pour une interface WAN.
NSSA	Il indique si NSSA est activé ou désactivé.
Actif	Vous pouvez activer ou désactiver l'interface correspondante. ***Note**: Les options d'activation et de désactivation ne sont disponibles que si le champ « Utiliser la configuration du profil » est désactivé.*
Actions	Vous pouvez modifier l'interface configurée. ***Note**: Ce champ est disponible uniquement si le champ « Utiliser la configuration du profil » est désactivé.*

Cliquez sur**Modifier**pour ouvrir le*Modifier OSPFv2*page. Pour supprimer plusieurs entrées à la fois, cochez les cases OSPFv2 que vous souhaitez supprimer, puis cliquez sur**Supprimer** .



Les champs disponibles sur le*Modifier OSPFv2*page sont les suivantes :

Champ	Description
Interface	Il affiche l'interface réseau physique sur laquelle OSPFv2 est activé ou désactivé.
NSSA	Activez cette option pour permettre aux zones de stub OSPF de transporter des routes externes.
Zone	

	Entrez la zone à laquelle appartient l'interface. Deux routeurs ayant un segment commun ; leurs interfaces doivent appartenir à la même zone sur ce segment. Les interfaces doivent appartenir au même sous-réseau et doivent avoir un masque similaire.
Priorité	Cela aide à déterminer la passerelle désignée OSPFv2 pour un réseau. La passerelle ayant la priorité la plus élevée sera plus éligible pour devenir un routeur désigné. La définition de la valeur sur 0 rend le routeur inéligible pour devenir un routeur désigné. La valeur par défaut est 1. Une valeur plus faible signifie une priorité plus élevée.
Bonjour intervalle	Entrez le numéro, en secondes, lorsque le paquet Hello doit être envoyé. Cette valeur doit être la même pour toutes les passerelles attachées à un réseau commun. La valeur par défaut est de 10 secondes.
Intervalle mort	Entrez le nombre de secondes pendant lesquelles les paquets Hello d'un périphérique ne sont pas vus avant que ses voisins déclarent le routeur OSPF hors service. Cette valeur doit être la même pour tous les routeurs connectés à un réseau commun. La valeur par défaut est de 40 secondes. OSPF exige que ces intervalles soient les mêmes entre deux voisins. Si l'un de ces intervalles est différent, ces routeurs ne deviendront pas voisins sur un segment particulier.
Coût	Saisissez le coût d'envoi d'un paquet sur une interface OSPFv2.
type d'identification	Sélectionnez l'un des types d'authentification suivants : • **Aucun**: L'interface n'authentifie pas les paquets OSPF. **Simple**: Les paquets • OSPF sont authentifiés à l'aide de simples clés de texte. **MD5**: L'interface • authentifie les paquets OSPF avec l'authentification MD5.
Clé d'authentification	Entrez la clé d'authentification. Ce champ est disponible lorsque vous sélectionnez**Simple**comme le*Type d'identification*.
ID de clé MD5	Si vous sélectionnez**MD5**comme le*type d'identification*, saisissez l'ID de la clé MD5.
Clé d'authentification MD5	Si vous sélectionnez**MD5**comme le*type d'identification*, saisissez la clé d'authentification MD5.
Échange de routes LAN	Il affiche l'état de l'échange de route LAN pour une interface WAN.
Sauvegarder	Cliquez sur**Sauvegarder**pour enregistrer vos paramètres.
Annuler	Cliquez sur**Annuler**pour revenir aux paramètres précédents.

Services

Le**Prestations de service**La section de l'interface utilisateur Web de la passerelle cloud Nuclias traite des multiples services permettant de fournir un réseau sécurisé et rapide à ses utilisateurs. Des services tels que la trame Jumbo améliorent les performances du réseau en utilisant une unité de transmission maximale (MTU) efficace. La surveillance IGMP filtre le trafic de multidiffusion sur le réseau et la fonctionnalité UPnP permet de découvrir les périphériques du réseau qui peuvent communiquer avec la passerelle et se configurer automatiquement. Cette section du réseau expliquera également la gestion des services et les passerelles de couche application, prises en charge par la passerelle cloud Nuclias.

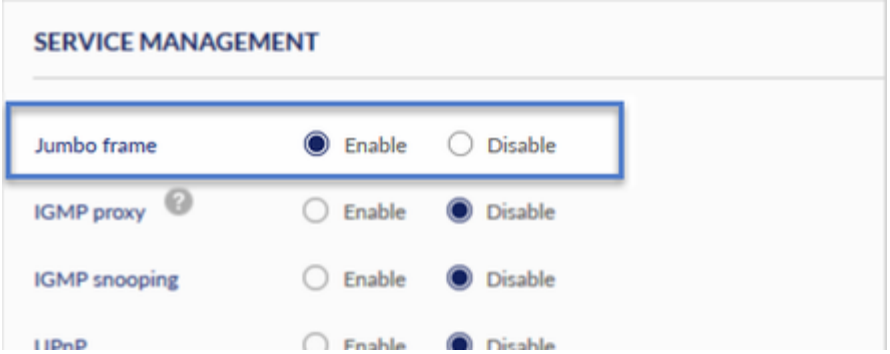
Cette section couvre les sujets suivants :

La gestion des services

Cette section de l'interface utilisateur Web traite des services suivants pris en charge par la passerelle cloud Nuclias :

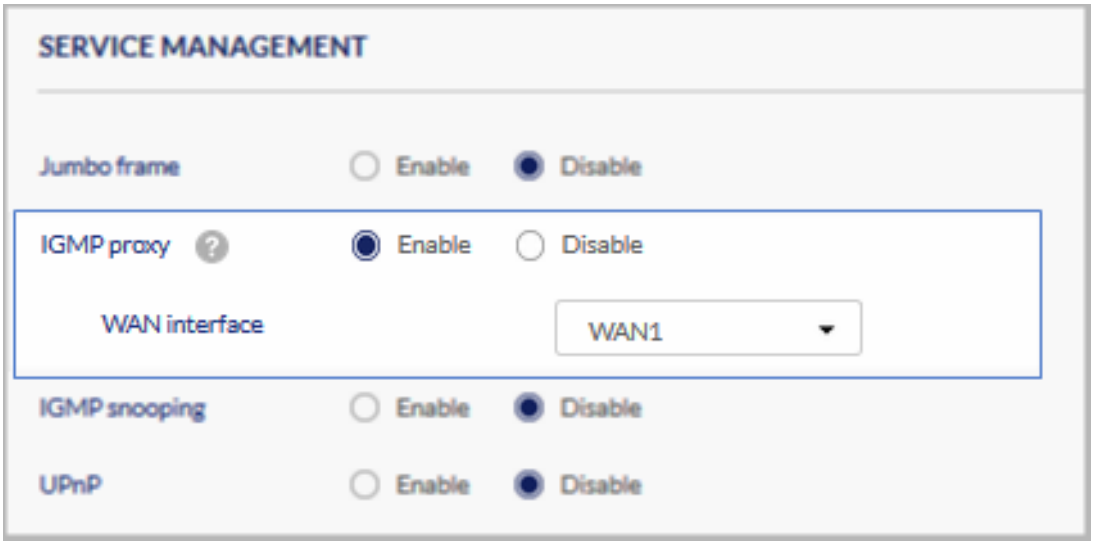
Cadre géant

Les trames Jumbo sont des trames Ethernet contenant plus de 1 500 octets de charge utile. Lorsque cette fonctionnalité est activée, les périphériques LAN peuvent échanger des informations au débit de trames Jumbo. Vous pouvez activer ou désactiver cette fonctionnalité.



Proxy IGMP

Le protocole IGMP (Internet Group Management Protocol) est utilisé par les hôtes et les routeurs sur un réseau IP pour créer des adhésions à des groupes de multidiffusion. L'IGMP peut être utilisé pour les applications Web et de support telles que le streaming en ligne de vidéos et de jeux. Le proxy IGMP permet à la passerelle d'émettre des messages IGMP au nom des clients derrière elle. Si la fonctionnalité proxy IGMP est activée, sélectionnez l'interface WAN sur laquelle elle doit être appliquée.



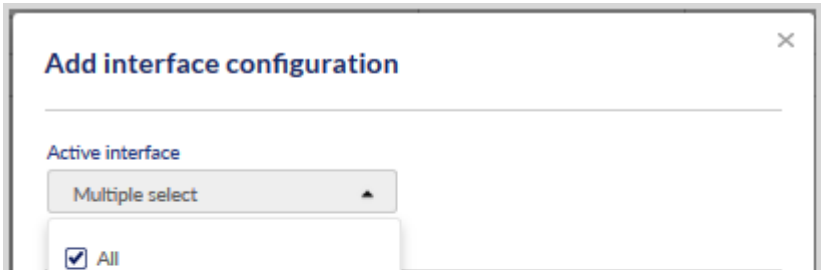
Surveillance IGMP

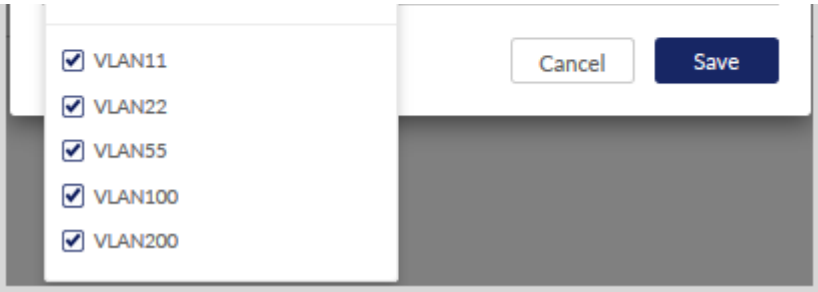
La surveillance IGMP permet à la passerelle d'« écouter » le trafic réseau IGMP via la passerelle. Cela permet à la passerelle de filtrer le trafic de multidiffusion et de le diriger uniquement vers les hôtes qui ont besoin de ce flux. Ceci est utile lorsqu'il y a beaucoup de trafic de multidiffusion sur le réseau et que tous les hôtes du réseau local n'ont pas besoin de recevoir ce trafic de multidiffusion.

Les champs disponibles dans le*Configuration*le tableau est le suivant :

Champ	Description
Interface	Il affiche l'interface sur laquelle la surveillance IGMP est configurée.
Surveillance IGMP	Il indique si la surveillance IGMP est activée ou désactivée.
Actions	Il vous permet de supprimer la surveillance IGMP configurée une par une.

Cliquez sur**Ajouter**pour ajouter une nouvelle interface. Cela ouvre le*Ajouter une configuration d'interface*page. Pour supprimer plusieurs surveillances IGMP configurées, cochez la case de l'interface configurée correspondante, puis cliquez sur**Supprimer**.





Les champs disponibles sur le*Ajouter une configuration d'interface*page sont les suivantes :

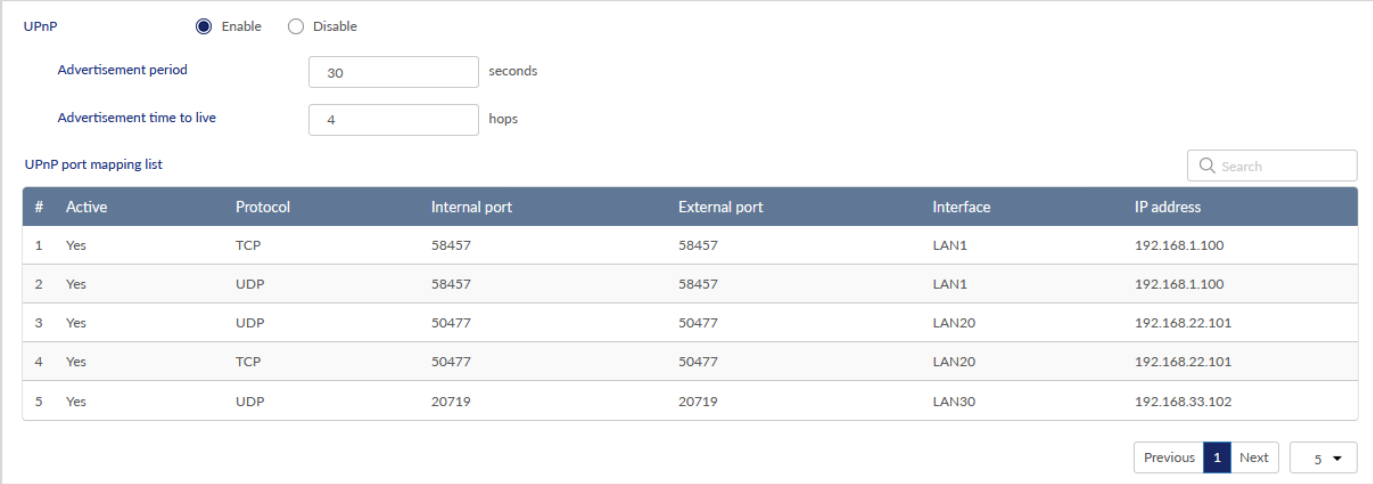
Champ	Description
Interface active	Sélectionnez l'interface active. ***Note**: La surveillance IGMP prend uniquement en charge le VLAN.*
Sauvegarder	Cliquez sur**Sauvegarder**pour enregistrer vos paramètres.
Annuler	Cliquez sur**Annuler**pour revenir à vos paramètres précédents.

UPnP

Universal Plug and Play (UPnP) est une fonctionnalité qui permet à la passerelle cloud de trouver les appareils sur le réseau qui peuvent communiquer avec la passerelle et permettre une configuration automatique. Si UPnP détecte un périphérique réseau, la passerelle peut ouvrir des ports internes ou externes pour le protocole de trafic requis par ce périphérique réseau. Si la fonctionnalité UPnP est désactivée, la passerelle ne peut pas configurer de périphérique automatique et vous devrez peut-être ouvrir/transférer manuellement les ports pour permettre aux applications de fonctionner.

Sélectionner**Activer**pour configurer UPnP et afficher la liste de mappage des ports UPnP.

***Note**: Vous pouvez modifier la fonctionnalité UPnP uniquement si le champ « Utiliser la configuration du profil » est désactivé.*



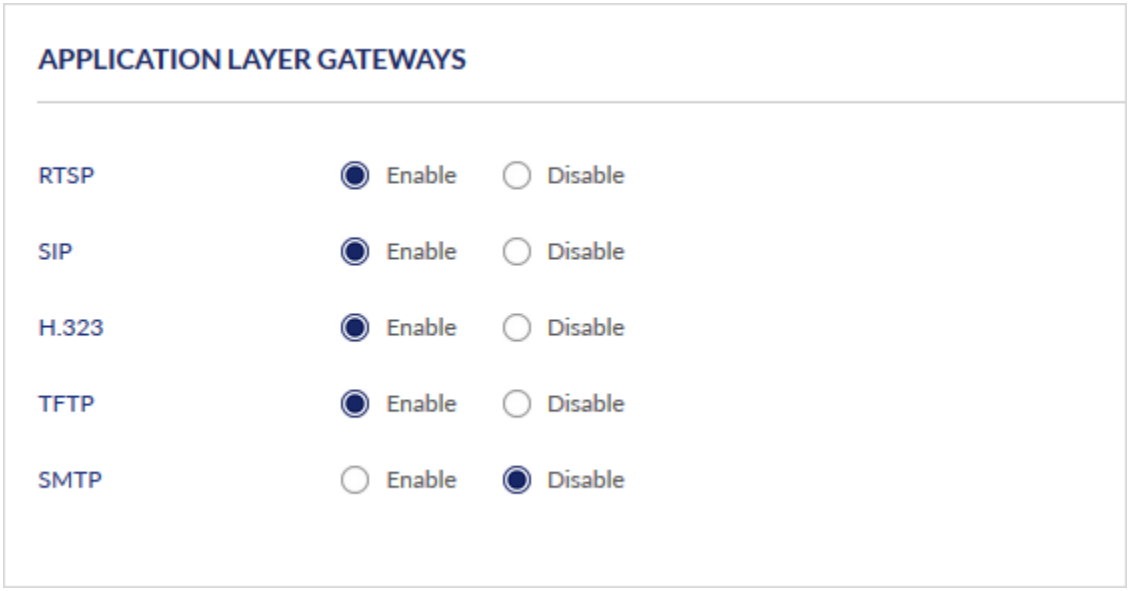
Le*Liste de mappage de ports UPnP*contient les détails des appareils UPnP qui répondent aux publicités de la passerelle. Les informations suivantes sont affichées pour chaque périphérique détecté :

Champ	Description
UPnP	Vous pouvez activer ou désactiver la fonctionnalité UPnP.
Période de publicité	Entrez une valeur pour la période de publication. Il s'agit de la fréquence à laquelle la passerelle diffuse les informations UPnP sur le réseau. Une valeur élevée minimisera le trafic réseau mais entraînera des retards dans l'identification des nouveaux périphériques UPnP sur le réseau.
Il est temps de vivre	Entrez une valeur pour la durée de vie de la publicité. Il s'agit du nombre de sauts qu'un paquet est autorisé à propager avant d'être rejeté. De petites valeurs limiteront la plage de diffusion UPnP. Une valeur par défaut de 4 est typique pour les réseaux comportant quelques nombres de commutateurs.
Liste de mappage de ports UPnP	

Actif	Il indique si le port UPnP est toujours ouvert dans l'appareil ou non.
Protocole	Il affiche le protocole réseau utilisé par la passerelle.
Port interne	Il affiche les ports internes ouverts par UPnP (le cas échéant).
Port externe	Il affiche les ports externes ouverts par UPnP (le cas échéant).
Interface	Il fait référence au segment LAN/VLAN sur lequel l'option UPnP est activée.
adresse IP	Il affiche l'adresse IP du périphérique UPnP détecté par la passerelle.

Passerelles de couche d'application (ALG)

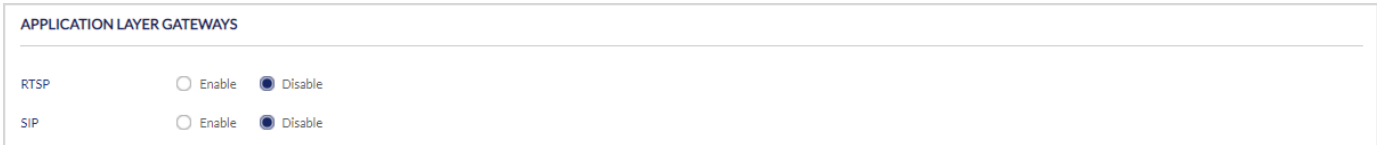
Les passerelles de niveau application (ALG) sont des composants de sécurité qui améliorent la prise en charge du pare-feu et du NAT du système.
passerelle pour prendre en charge de manière transparente les protocoles de couche application. Dans certains cas, l'activation de l'ALG permettra au pare-feu d'utiliser des ports TCP/UDP dynamiques et éphémères pour communiquer avec les ports connus dont une application client particulière (telle que H.323 ou RTSP) a besoin ; sinon, l'administrateur devrait ouvrir un grand nombre de ports pour obtenir le même support. ALG comprend le protocole utilisé par l'application spécifique qu'il prend en charge. Il s'agit d'un moyen très sécurisé et efficace d'introduire des applications clientes via le pare-feu de la passerelle.

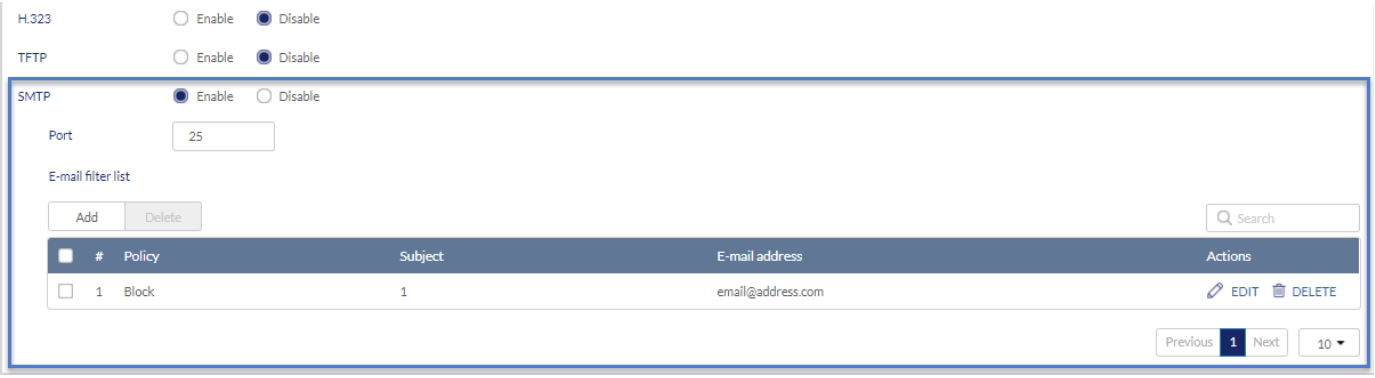


Champ	Description
RTSP	Activez-le pour permettre aux applications qui utilisent le protocole de diffusion en temps réel de recevoir des médias en streaming depuis Internet. QuickTime et Real Player sont quelques-unes des applications courantes utilisant ce protocole.
siroter	Activez-le pour permettre aux appareils et aux applications utilisant la VoIP (Voice over IP) de communiquer via NAT.
H.323	Activez-le pour permettre aux clients H.323 (en particulier Microsoft Netmeeting) de communiquer via NAT.
TFTP	Activez-le pour permettre aux clients et serveurs Trivial FTP (TFTP) de transférer des données via NAT.
SMTP	Activez-le pour transférer le courrier électronique entre les serveurs de messagerie via Internet et entrez le **port**auquel les paquets SMTP sont inspectés.

Liste de filtres de courrier électronique

Le*Liste de filtres de courrier électronique*apparaît uniquement lorsque le SMTP est activé. Simple Mail Transfer Protocol (SMTP) est un protocole textuel utilisé pour transférer des e-mails entre serveurs de messagerie via Internet. En règle générale, le serveur SMTP local est situé sur une DMZ afin que le courrier envoyé par les serveurs SMTP distants traverse la passerelle pour atteindre le serveur local. Les utilisateurs locaux utilisent ensuite un logiciel client de messagerie pour récupérer leur courrier électronique sur le serveur SMTP local. SMTP est également utilisé lorsque les clients envoient des e-mails. De plus, SMTP ALG peut surveiller le trafic SMTP provenant à la fois des clients et des serveurs.

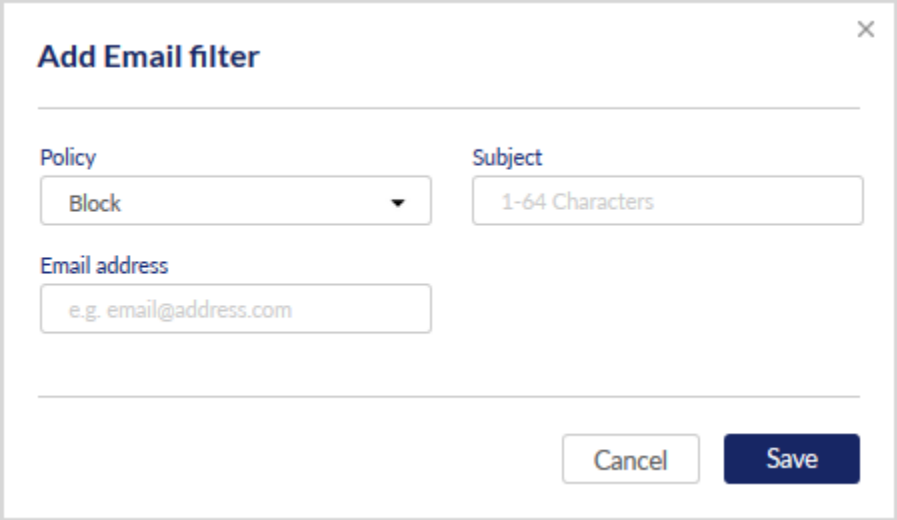




Le tableau répertorie tous les sujets ainsi que les adresses e-mail bloquées ou autorisées.

Champ	Description
Politique	Il affiche la politique pour autoriser ou bloquer l'adresse e-mail.
Sujet	Il affiche le sujet.
Adresse e-mail	Il affiche l'adresse e-mail.
Actions	Vous pouvez cliquer**Modifier**pour modifier l'entrée et cliquez**Supprimer**pour supprimer toute l'entrée.

Cliquez sur**Ajouter**pour ouvrir le*Ajouter un filtre de courrier électronique*page pour ajouter une nouvelle entrée. Pour supprimer plusieurs entrées à la fois, cochez les cases des entrées que vous souhaitez supprimer, puis cliquez sur**Supprimer**.



Les champs disponibles sur le*Ajouter un filtre de courrier électronique*page sont les suivantes :

Champ	Description
Politique	Sélectionnez une politique. Cela peut être soit**Permettre**ou**Bloc**.
Sujet	Entrez le sujet. La plage va de 1 à 64 caractères.
Adresse e-mail	Entrez une adresse email.
Sauvegarder	Cliquez sur**Sauvegarder**pour enregistrer vos paramètres.
Annuler	Cliquez sur**Annuler**pour revenir aux paramètres précédents.

Traffic Management

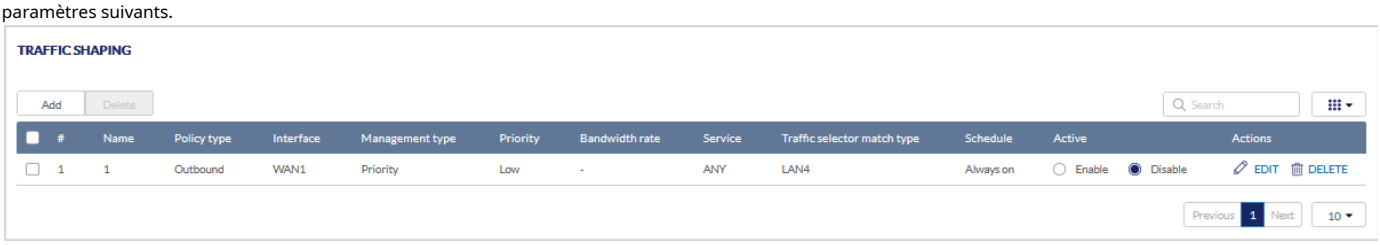
La fonction de gestion du trafic vous permet de réguler le flux de trafic du LAN vers le WAN. Ceci est utile pour garantir que les utilisateurs du réseau local à faible priorité (comme les invités ou le service HTTP) ne monopolisent pas la bande passante disponible du WAN à des fins d'économies ou d'allocation de priorité de bande passante.

Cette section vous aidera à comprendre et à configurer la fonction de contrôle de la bande passante à partir de l'interface utilisateur Web et à ajouter un profil qui définit les paramètres de contrôle. Vous pouvez ensuite associer le profil à un sélecteur de trafic pour appliquer le profil de bande passante au trafic, en faisant correspondre les sélecteurs. Les sélecteurs sont des éléments tels que des adresses IP ou des services qui déclencheraient la régulation de bande passante configurée.

Le*gestion du trafic*La section couvre les sujets suivants :

Façonnage du trafic

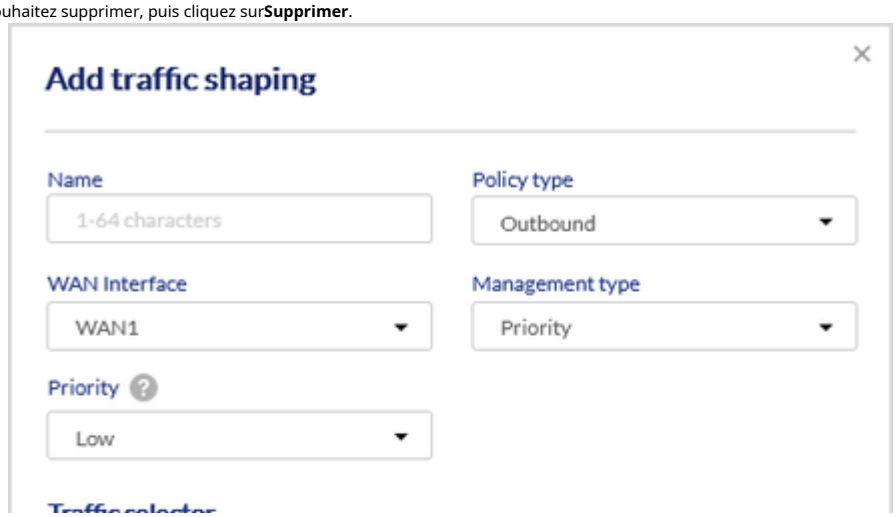
Le sélecteur de trafic est une règle basée sur un service à laquelle l'utilisateur peut attacher des profils de gestion du trafic. Une fois un profil créé, il peut ensuite être associé au flux de trafic du LAN vers le WAN. La configuration du sélecteur de trafic lie un profil de bande passante à un type ou une source de trafic LAN avec les paramètres suivants.

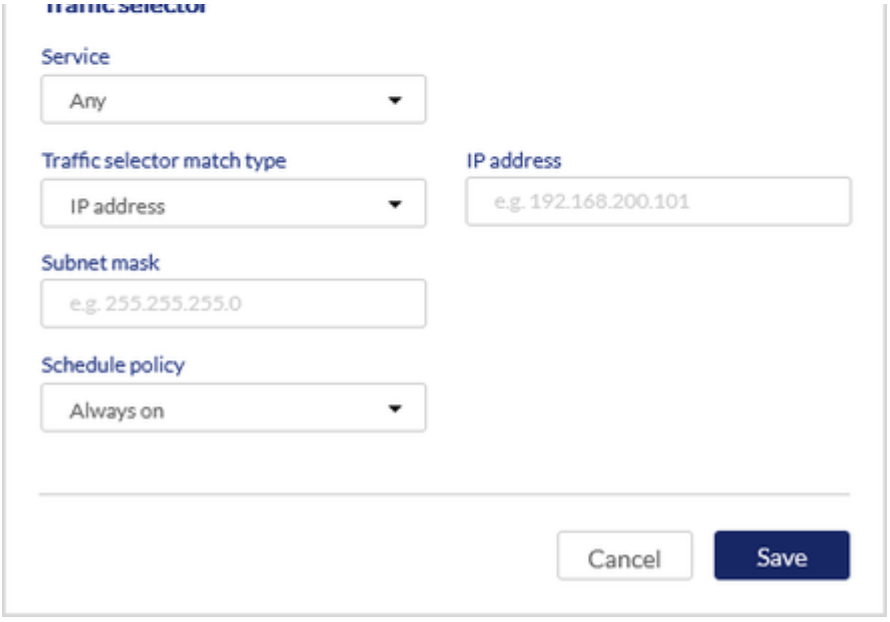


Les champs affichés dans le*Façonnage du trafic*e tableau est le suivant :

Champ	Description
Nom	Il affiche le nom de votre profil.
Type de politique	Il affiche le type de politique (**Entrant**ou**Sortant**).
Interface	Il affiche l'interface à laquelle le profil est associé.
Type de gestion	Il s'affiche comme**Priorité**ou**Taux**.
Priorité	Il affiche le niveau de priorité, c'est-à-dire faible, moyen ou élevé.
Taux de bande passante	Il affiche la plage de débits de bande passante.
Service	Il affiche le service.
Type de correspondance du sélecteur de trafic	Il affiche le type de correspondance du sélecteur de trafic.
Calendrier	Il affiche le calendrier de la mise en forme du trafic sélectionnée.
Actif	Vous pouvez activer ou désactiver la politique de gestion du trafic correspondante. ***Note**: Ce champ est disponible uniquement si le champ « Utiliser la configuration du profil » est désactivé.*
Actions	Vous pouvez modifier ou supprimer la politique de gestion du trafic sélectionnée. ***Note**: Ce champ est disponible uniquement si le champ « Utiliser la configuration du profil » est désactivé.*

Cliquez sur**Ajouter**pour ajouter une nouvelle entrée au tableau. Cela ouvre le*Ajouter une gestion du trafic*page. Pour supprimer plusieurs entrées, cochez la case des politiques de gestion du trafic que vous souhaitez supprimer, puis cliquez sur**Supprimer**.





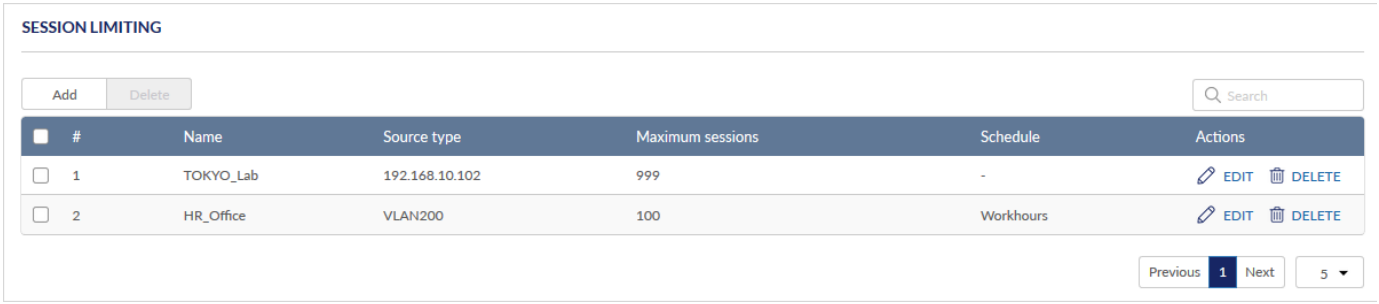
Les champs disponibles sur le*Ajouter une gestion du trafic*page sont les suivantes :

Champ	Description
Nom	Entrez un nom pour votre profil. Cet identifiant permet d'associer le profil configuré au sélecteur de trafic.
Type de politique	Sélectionnez le type de politique (**Entrant**ou**Sortant**).
Interface WAN	Sélectionnez à laquelle des interfaces WAN disponibles vous souhaitez associer ce profil. Ce champ apparaît lorsque**Sortant**est sélectionné comme*Type de politique*.
Interface	Sélectionnez à laquelle des interfaces disponibles vous souhaitez associer ce profil. Ce champ apparaît lorsque**Entrant**est sélectionné comme*Type de politique*.
Type de gestion	Sélectionnez soit**Priorité**ou**Taux**.
Priorité	Si vous sélectionnez**Priorité**, précisez la priorité. Il pourrait être*Faible*,*Moyen*, ou*Haut*.
Max. débit de bande passante (Kbps)	Si vous sélectionnez**Taux**, entrez le débit de bande passante maximum.
Min. débit de bande passante (Kbps)	Si vous sélectionnez**Taux**, entrez le débit de bande passante minimum.
Sélecteur de trafic	
Service	Sélectionnez un service dans la liste déroulante.
Type de correspondance du sélecteur de trafic	Ce champ est disponible lorsque vous sélectionnez**Sortant**comme le*Type de politique*. Sélectionnez l'un des types de correspondance suivants : • **adresse IP**: Sélectionnez cette option pour associer ce sélecteur de trafic à une adresse IP d'un périphérique LAN. Une fois sélectionné, entrez l'adresse IP du périphérique LAN. • **Adresse Mac**: Sélectionnez cette option pour associer ce sélecteur de trafic à une adresse MAC spécifique sur le LAN. Une fois sélectionné, entrez une adresse MAC valide. • **Interface**: Si cette option est sélectionnée, sélectionnez l'interface.
Interface	Si vous sélectionnez**Interface**, sélectionnez une interface dans la liste déroulante.
adresse IP	Saisissez l'adresse IP de la source associée à ce profil.
Masque de sous-réseau	Entrez le masque de sous-réseau.
Adresse Mac	Si vous sélectionnez**Adresse Mac**, saisissez l'adresse MAC de la source associée à ce profil.
Politique de planification	Il permet de définir l'heure et le jour auxquels la règle de régulation du trafic doit être appliquée.
Sauvegarder	Cliquez sur**Sauvegarder**pour enregistrer vos paramètres.

Fermer	Cliquez sur**Fermer**pour revenir aux paramètres précédents.

Limitation de session

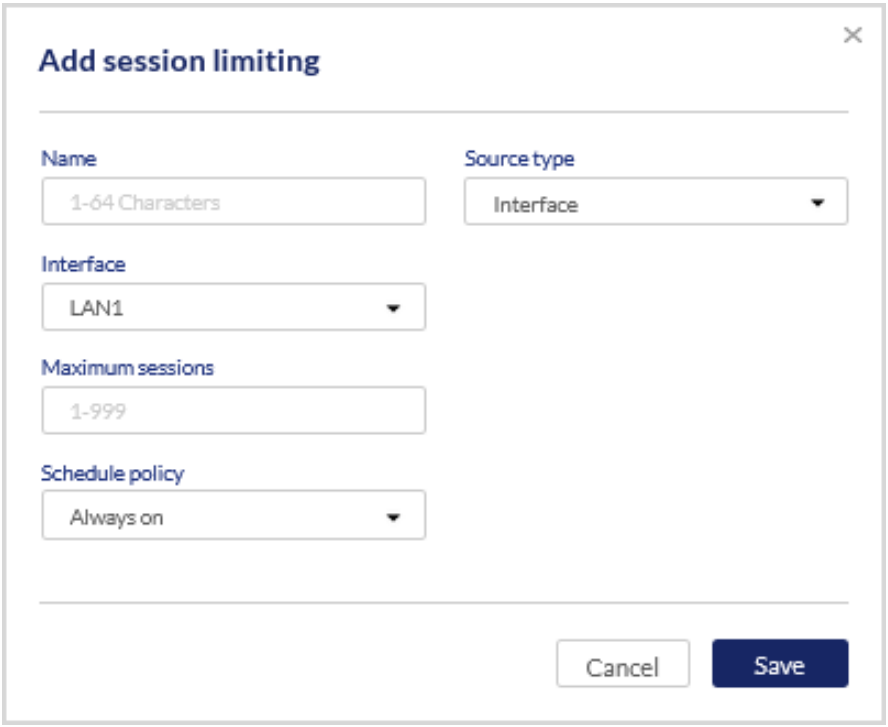
Le*Limitation de session*La section affiche une liste des profils de limitation de session configurés. Il permet à un utilisateur de limiter le nombre de sessions par adresse IP, plage d'adresses IP ou interface via l'appareil. Lorsque la limite de session est atteinte, un message d'avertissement s'affiche aux utilisateurs pour une session initiée depuis un navigateur Web. La configuration de la limitation de session comprend le nom du profil, le type de source, la planification et le nombre maximal de sessions.



Les champs affichés dans le*Limitation de session*le tableau est le suivant :

Champ	Description
Nom	Il affiche le nom du profil configuré pour un type de source particulier.
Type de Source	Il affiche le type de source sélectionné pour le profil.
Sessions maximales	Il affiche le nombre maximum de sessions autorisées sur le type de source sélectionné pour limiter les sessions.
Calendrier	Il affiche la planification du profil de limite de session configuré.
Actions	Vous pouvez modifier ou supprimer une entrée.

Cliquez sur**Ajouter**pour ajouter une nouvelle entrée à la liste. Cela ouvre le*Ajouter une limitation de session*page. Pour supprimer plusieurs entrées, cochez les cases des entrées que vous souhaitez supprimer, puis cliquez sur**Supprimer**.



Les champs disponibles sur le*Ajouter une limitation de session*page sont les suivantes :

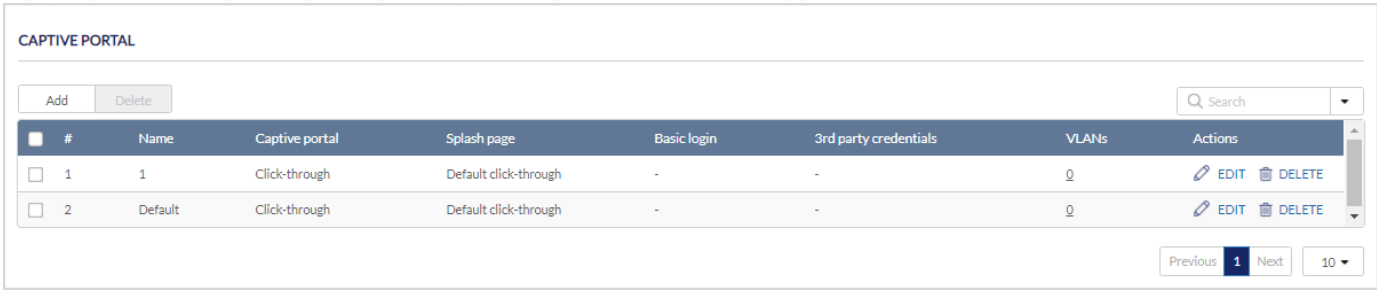
Champ	Description

Nom	Entrez le nom du profil à configurer pour un type de source particulier.
Type de Source	Sélectionnez un type de source pour le profil. Les options sont l'adresse IP, la plage IP et l'interface.
adresse IP	Entrez l'adresse IP du client/hôte à contrôler dans le profil Limite de session lorsque le type de source sélectionné est**adresse IP**.
Adresse IP de départ	Saisissez l'adresse IP de départ des clients à contrôler dans le profil Session Limit lorsque le type de source sélectionné est**Plage ip**.
Adresse IP de fin	Entrez l'adresse IP de fin des clients à contrôler dans le profil Limite de session lorsque le type de source sélectionné est**Plage ip**.
Interface	Sélectionnez l'interface dans la liste déroulante pour sélectionner le réseau complet contrôlé dans le profil Limite de session lorsque le type de source sélectionné est**Interface**.
Sessions maximales	Entrez le nombre maximum de sessions autorisées sur le type de source pour limiter les sessions.
Politique de planification	Il permet de définir l'heure et le jour où le profil de limitation de session doit être utilisé. Sélectionnez l'un des programmes configurés dans la liste déroulante.
Sauvegarder	Cliquez sur**Sauvegarder**pour enregistrer vos paramètres.
Annuler	Cliquez sur**Annuler**pour revenir aux paramètres précédents.

Captive Portal

UN*portail captif*(également connue sous le nom de « page de démarrage ») est une page Web qui apparaît lorsqu'un utilisateur non authentifié tente d'accéder à Internet. Lorsque le portail captif est configuré, l'utilisateur doit être vérifié et authentifié, puis seul l'accès à Internet est accordé. Cela se fait soit en saisissant les identifiants de connexion, soit en acceptant les termes et conditions de service. Cela aide la passerelle à surveiller et à contrôler l'utilisation d'Internet.

La passerelle cloud Nuclias, DBG-2000, permet à ses utilisateurs de configurer la page du portail captif et propose diverses méthodes d'authentification. Le*Portail captif* La page répertorie tous les profils de portail captif configurés. Vous pouvez les modifier ou les supprimer selon les besoins.

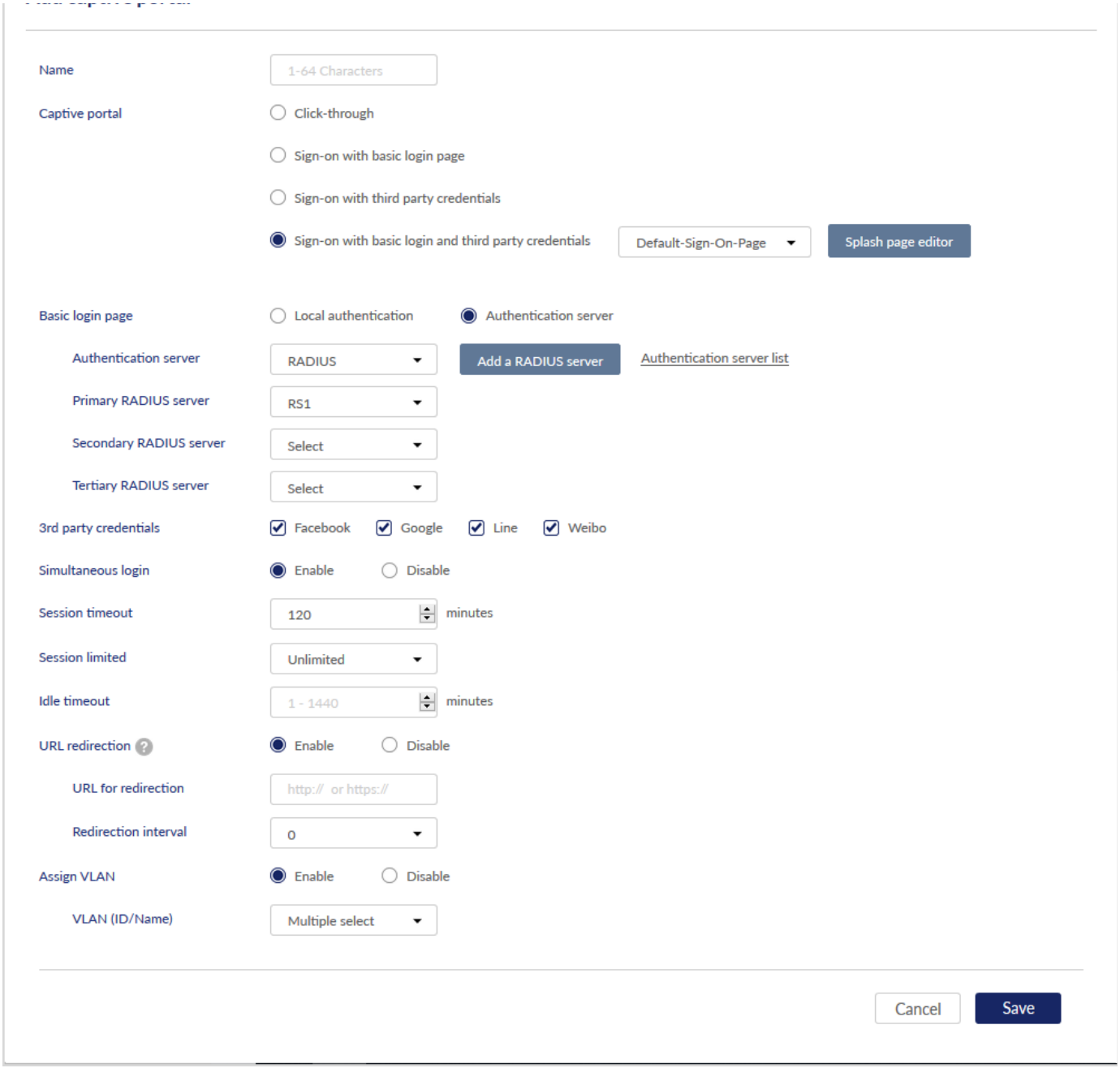


Les champs affichés dans le*Portail captif*le tableau est le suivant :

Champ	Description
Nom	Il indique le nom des profils de portail captif configurés.
Portail captif	Il affiche le type d'authentification utilisé pour le portail captif configuré.
Page d'accueil	Il affiche le nom de la page de démarrage créée.
Connexion de base	Il indique le serveur d'authentification utilisé pour la connexion de base.
Identifiants tiers	Il affiche les tiers dont les informations d'identification seront utilisées pour la connexion.
VLAN	Il affiche l'ID du VLAN sur lequel le portail captif est configuré.
Actions	Vous pouvez modifier ou supprimer le profil de portail captif sélectionné. Lorsque vous cliquez**Modifier**, il ouvre le *Modifier le portail captif*page. *Remarque : Cette colonne est disponible uniquement lorsque vous désactivez le champ « Utiliser la configuration du profil ».*

Cliquez sur**Ajouter**pour ajouter un nouveau profil de portail captif. Cela ouvre le*Ajouter un portail captif*page. Si vous souhaitez supprimer plusieurs entrées à la fois, cochez les cases correspondantes et cliquez sur**Supprimer**.

*Noter la**Ajouter**et**Supprimer**les boutons situés au-dessus du tableau ne sont disponibles que lorsque le champ « Utiliser la configuration du profil » est désactivé.*



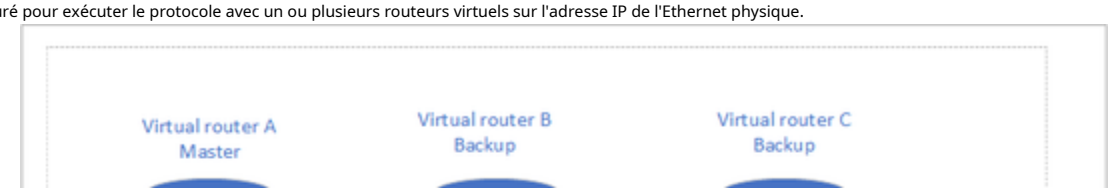
Les champs disponibles sur le*Ajouter un portail captif*page sont les suivantes :

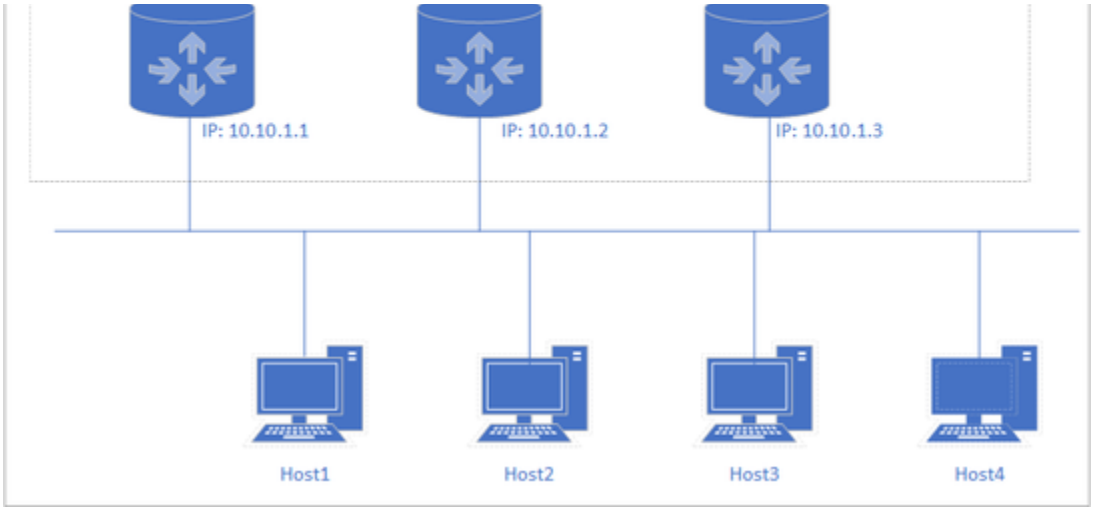
Champ	Description
Nom	Entrez un nom descriptif pour le profil du portail captif.
Portail captif	Sélectionnez l'un des types d'authentification suivants à utiliser pour le portail captif : • **Clic**: L'authentification par clic est une méthode de connexion alternative qui ne nécessite pas que l'utilisateur final crée un compte pour accéder au service. L'utilisateur final clique sur un bouton et peut ensuite accéder à Internet. • **Connectez-vous avec la page de connexion de base**: Ce type d'authentification fournit un accès à Internet après avoir saisi avec succès le nom d'utilisateur et le mot de passe. • **Connectez-vous avec des informations d'identification tierces**: Si vous sélectionnez ce type d'authentification, il utilise les informations d'identification tierces hébergées sur un serveur externe. Les utilisateurs doivent fournir des informations de connexion pour accéder au réseau. • **Connectez-vous avec une connexion de base et des informations d'identification tierces :**L'utilisateur peut se connecter soit en utilisant une page de connexion de base, soit via des informations d'identification tierces.

Éditeur de page de garde	Cliquez sur ce bouton pour modifier la page de démarrage existante ou ajouter une nouvelle page de démarrage pour le type d'authentification correspondant. Pour plus de détails, veuillez vous référer auÉditeur de page de gardepage.
Page de connexion de base	Sélectionnez l'une des méthodes d'authentification. Les informations d'identification saisies sur la page de connexion sont validées par l'un des serveurs d'authentification suivants : • **Authentification locale :**L'authentification locale est une méthode par laquelle l'utilisateur final est redirigé vers une page qui propose des options pour saisir un nom d'utilisateur et un mot de passe validés par rapport à la base de données utilisateur configurée de l'appareil. • **Serveur d'authentification :**Si cette option est sélectionnée, l'utilisateur final est redirigé vers une page proposant des options permettant de saisir un nom d'utilisateur et un mot de passe validés par le serveur d'authentification externe configuré. La liste des serveurs comprend RADIUS, LDAP, POP3, Active Directory et le domaine NT.
Authentification locale	Sélectionnez un serveur d'authentification local dans la liste déroulante. Ce champ est disponible lorsque vous sélectionnez **Authentification locale**comme le*Page de connexion de base*.
Serveur d'authentification	Sélectionnez l'un des serveurs d'authentification externes dans la liste déroulante, puis sélectionnez le **Primaire**,**Secondaire**, et**Tertiaire**serveurs pour le serveur d'authentification externe sélectionné. Si vous souhaitez ajouter un serveur d'authentification externe, cliquez sur le bouton**Ajouter un serveur**bouton. Cela ouvre le *Ajouter un serveur*page du type de serveur sélectionné. Pour plus de détails, veuillez vous référer auServeurs d'authentificationpage. Si vous souhaitez voir une liste des serveurs d'authentification configurés, cliquez sur le bouton**Serveur d'authentification**liste. Vous serez redirigé vers leServeurs d'authentificationpage.
Identifiants tiers	Cochez la case du serveur tiers externe sur lequel les utilisateurs fournissent leurs informations d'identification pour accéder à Internet.
Connexion simultanée	Il permet à plusieurs clients de se connecter avec les mêmes informations d'identification.
Expiration de la session	Le délai d'expiration de la session est le délai configuré pour que les clients connectés à la passerelle se réauthentifient afin de continuer à utiliser les services Internet. Entrez ou sélectionnez le délai d'expiration de la session en minutes. La plage va de 1 à 1440.
Session limitée	Vous pouvez limiter le nombre de sessions utilisateur actives pour chaque compte. Par exemple, si vous sélectionnez «*Illimité*», cela signifie qu'un nombre illimité d'utilisateurs peuvent utiliser le même compte.
Délai d'inactivité	Le délai d'inactivité fait référence à la fin de la session lorsqu'aucun trafic de données n'est observé pendant la durée donnée. Le client connecté à la passerelle doit se réauthentifier une fois le délai d'inactivité respecté pour accéder à Internet. Cette valeur est par passerelle et applicable à tous les clients connectés à la passerelle. La plage de délai d'inactivité est comprise entre 1 et 1 440 minutes.
Redirection d'URL	Si cette option est activée, l'utilisateur est redirigé vers l'URL configurée après l'authentification réussie.
URL de redirection	Entrez l'URL vers laquelle vous souhaitez que l'utilisateur soit redirigé après une connexion réussie.
Intervalle de redirection	Sélectionnez l'intervalle de temps périodique pendant lequel l'utilisateur sera redirigé vers l'URL mentionnée dans le champ ci-dessus.
Attribuer un VLAN	Activez cette fonctionnalité si vous souhaitez attribuer le portail captif à n'importe quel VLAN.
VLAN (ID/Nom)	Sélectionnez l'ID ou le nom du VLAN sur lequel le portail captif doit être activé.
Sauvegarder	Cliquez sur**Sauvegarder**pour enregistrer vos paramètres.
Annuler	Cliquez sur**Annuler**pour revenir aux paramètres précédents.

High Availability

La haute disponibilité fait référence à la disponibilité du chemin par défaut sans configurer de protocoles de routage dynamique ou de découverte de routeur sur chaque hôte. La fonctionnalité utilisée pour fournir un chemin par défaut est**Protocole de redondance de routeur virtuel (VRRP)**. VRRP est un protocole d'élection qui attribue dynamiquement un routeur virtuel à l'un des routeurs VRRP d'un réseau local. Un routeur virtuel est un routeur qui fait office de routeur par défaut pour les hôtes du réseau local partagé. Un routeur VRRP est configuré pour exécuter le protocole avec un ou plusieurs routeurs virtuels sur l'adresse IP de l'Ethernet physique.

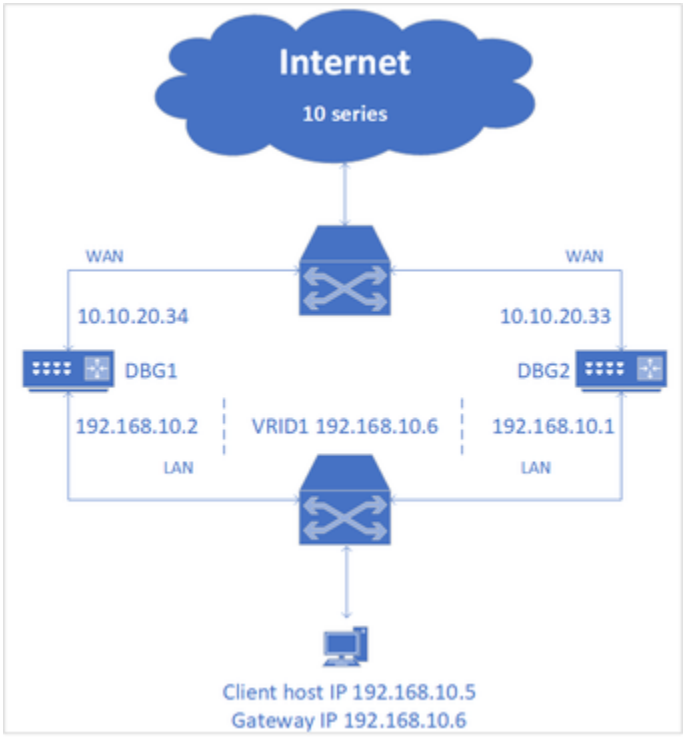




Dans VRRP, au lieu d'avoir un seul routeur, un groupe de routeurs virtuels est fourni ; Si l'un tombe en panne, l'autre prendra le relais du routeur défaillant et de ses adresses IP et fournira un service ininterrompu aux hôtes. Dans la configuration ci-dessus, les hôtes finaux installent une route par défaut vers l'adresse IP du routeur virtuel A, et les trois routeurs exécutent VRRP. Le routeur A devient le routeur virtuel maître et les deux autres routeurs deviennent les routeurs de secours. En cas de panne du routeur virtuel maître A, il transmet les paquets au routeur virtuel de secours, sélectionné en fonction de la priorité donnée aux routeurs de secours. Le routeur de secours (disons « Routeur virtuel B ») devient immédiatement le maître et maintient la connectivité entre les hôtes. Une fois que le routeur virtuel maître défaillant devient fonctionnel, le routeur de sauvegarde (routeur virtuel B) transmet les paquets via le routeur virtuel A récupéré.

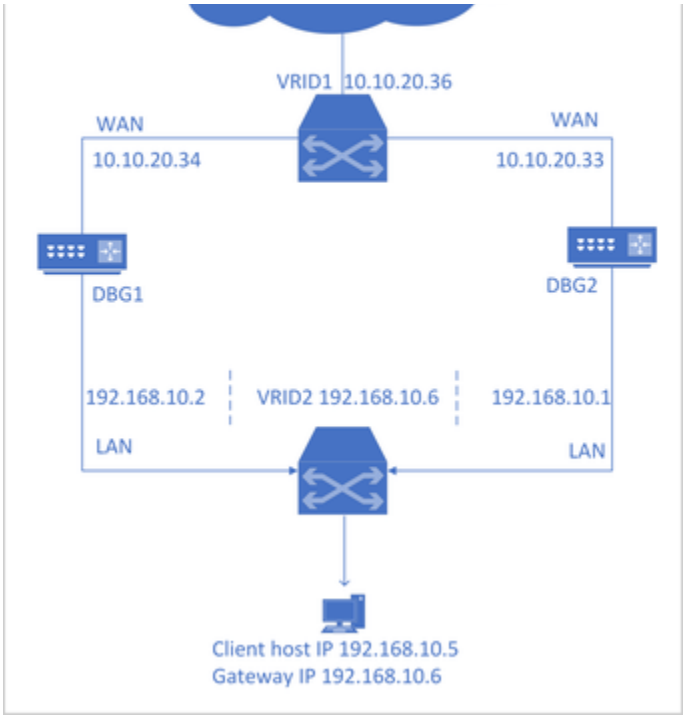
DBG-2000 prend en charge la fonctionnalité VRRP, et elle a été décrite en détail à l'aide des deux scénarios de test suivants et de leurs topologies :

1. Cas de test 1



Les routeurs (DBG1 et DBG2) ont été configurés avec la fonctionnalité VRRP pour l'interface LAN et reçoivent des numéros de priorité. Par exemple, disons que la priorité de DBG1 est de 200 et celle de DBG2 de 100. Ensuite, lorsque le client essaie de se connecter à Internet, il suit le DBG avec un numéro de priorité plus élevé. Ici, il suit DBG1. Mais si DBG1 est déconnecté ou inaccessible, il se connecte au deuxième routeur DBG2 et lorsque DBG1 retrouve ses fonctionnalités, il passe à DBG1.

2. Cas de test 2

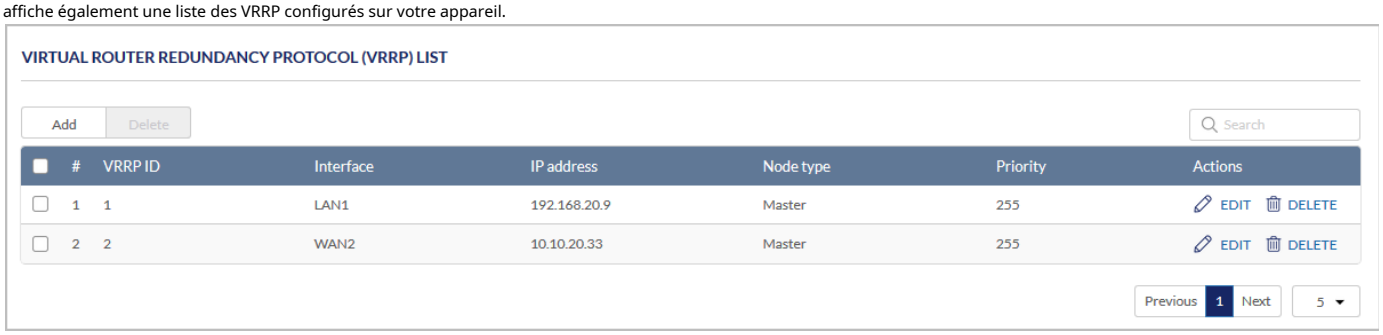


Les routeurs (DBG1 et DBG2) ont été configurés avec la fonctionnalité VRRP pour les deux interfaces (LAN et WAN) et reçoivent des numéros prioritaires. Ensuite, lorsque le client tente de se connecter à Internet, il suit le routeur avec un numéro de priorité plus élevé (par exemple DBG1). Lorsque le WAN DBG1 n'est pas accessible ou déconnecté de la topologie, il se connecte au WAN DBG2, et lorsque le WAN DBG1 est connecté ou devient fonctionnel, il passe à nouveau sur DBG1.

Pour configurer votre DBG-2000, reportez-vous àListe et configuration VRRP

. **Liste et configuration VRRP**

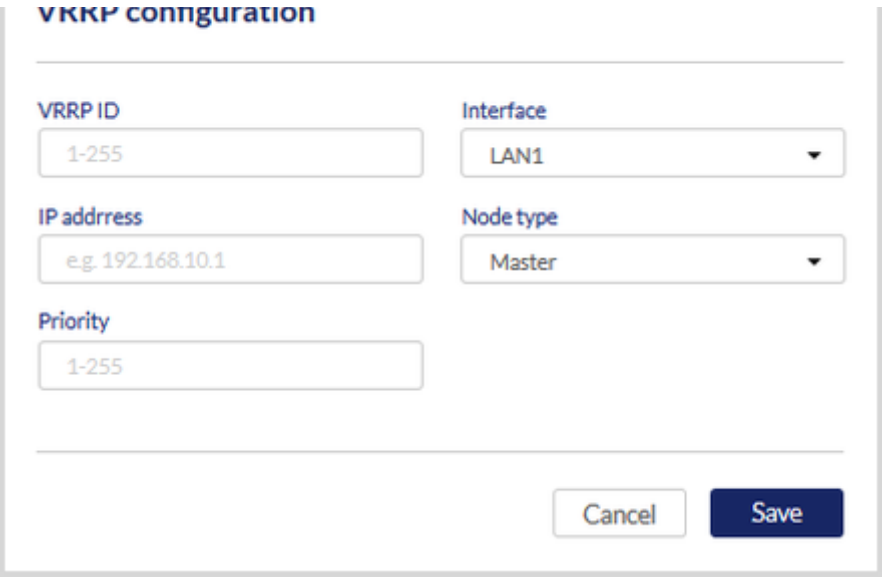
Cette page de l'interface utilisateur de la passerelle cloud Nuclias vous permet de configurer le VRRP, c'est-à-dire le Virtual Router Redundancy Protocol, sur votre appareil. Il affiche également une liste des VRRP configurés sur votre appareil.



Les champs affichés dans le*Liste du protocole de redondance de routeur virtuel (VRRP)*sont les suivants:

Champ	Description
ID VRRP	Il affiche l'ID attribué aux routeurs VRRP.
Interface	Il affiche l'interface sur laquelle le VRRP a été configuré.
adresse IP	Il affiche l'adresse IP du routeur VRRP.
Type de nœud	Il indique si le routeur VRRP sélectionné fonctionne comme un**Maître**routeur ou un**Sauvegarde**routeur.
Priorité	Il indique la priorité donnée au routeur VRRP configuré.
Actions	Vous pouvez modifier ou supprimer le VRRP sélectionné.

Cliquez sur**Ajouter**pour ajouter une nouvelle entrée à la liste. Cela ouvre le*Configuration VRRP*page. Si vous souhaitez supprimer plusieurs entrées à la fois, cochez les cases correspondantes et cliquez sur**Supprimer**.



Les champs disponibles sur le*Configuration VRRP*page sont les suivantes :

Champ	Description
ID VRRP	Spécifiez un ID pour le routeur VRRP.
Interface	Sélectionnez l'interface sur laquelle vous souhaitez configurer VRRP.
adresse IP	Saisissez l'adresse IP du routeur VRRP.
Type de nœud	Sélectionnez le type de nœud pour le routeur VRRP. Sélectionner**Maître**si vous souhaitez que le routeur VRRP fonctionne en tant que maître, puis sélectionnez**Sauvegarde**si vous voulez que ce soit le routeur de secours.
Priorité	Il indique la priorité donnée au routeur respectif. Si le maître n'est pas disponible, la sauvegarde de priorité la plus élevée transitera vers le maître, offrant ainsi une transition contrôlée de la responsabilité du routeur virtuel avec une interruption de service minimale.
Sauvegarder	Cliquez sur**Sauvegarder**pour enregistrer vos paramètres.
Annuler	Cliquez sur**Annuler**pour revenir aux paramètres précédents.

Chapitre 4 Sécurité

Ce chapitre vous présente les fonctionnalités de sécurité prises en charge par la passerelle cloud Nuclias. Ces fonctionnalités incluent le pare-feu, l'IPS, le filtrage du contenu Web et le contrôle des applications. Ce sont les différentes techniques utilisées pour bloquer toute attaque malveillante provenant d'Internet pour accéder à votre réseau. Vous pouvez également configurer vos propres politiques Internet pour autoriser uniquement certaines informations Web sélectionnées.

Ce chapitre couvre les sujets suivants:

Firewall

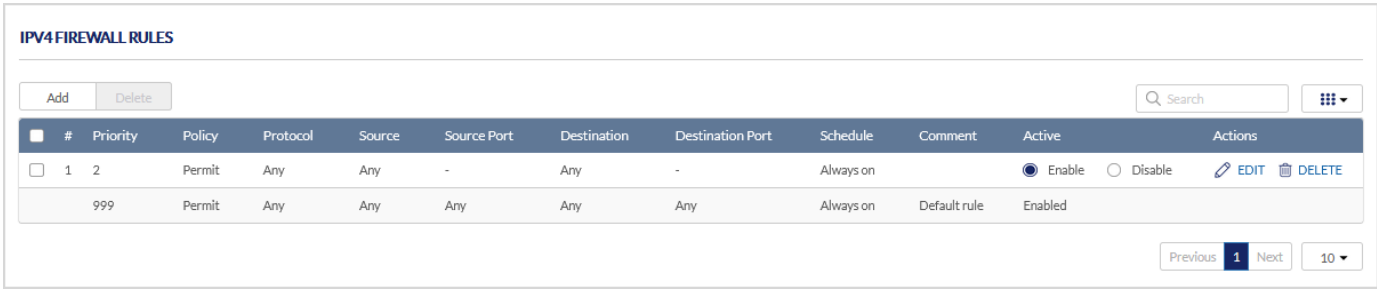
Le*Pare-feu*La section Sécurité traite des différentes méthodes adoptées par la passerelle cloud Nuclias pour garantir un réseau sûr et sécurisé. Dans cette section, vous découvrirez la configuration des règles de pare-feu sur les réseaux IPv4. Ce sont les règles définies pour contrôler le trafic entrant et sortant du réseau. Vous pouvez indiquer quel trafic doit être autorisé ou bloqué. De même, la méthode de redirection de port peut restreindre l'accès au trafic entrant sur votre réseau tout en permettant uniquement à des utilisateurs externes spécifiques d'accéder à des ressources locales spécifiques. Lorsque vous disposez de plusieurs adresses IP publiques et de plusieurs serveurs à travers le pare-feu, la méthode NAT 1:1 est utilisée.

Cette section couvre les sujets suivants :

Agrandir Tout Réduire Tout

Règles de pare-feu IPv4

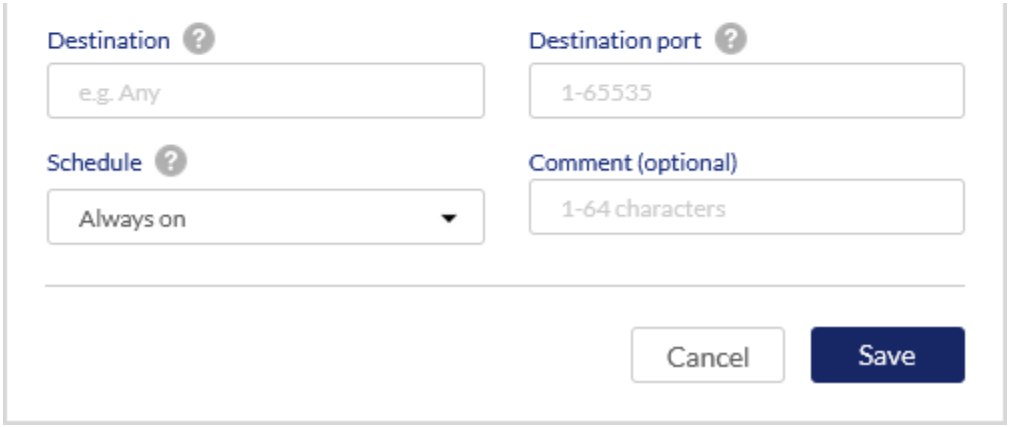
Les règles sortantes (LAN/DMZ vers WAN) restreignent l'accès au trafic sortant de votre réseau, permettant de manière sélective uniquement à des utilisateurs locaux spécifiques d'accéder à des ressources externes spécifiques. La règle sortante par défaut autorise l'accès depuis le zone sécurisée (LAN) vers la DMZ publique ou vers un WAN non sécurisé. D'un autre côté, la règle sortante par défaut consiste à refuser l'accès depuis la DMZ au WAN non sécurisé. De plus, vous pouvez restreindre le trafic VLAN à VLAN à l'aide des règles de pare-feu IPv4.



Les champs affichés dans le*Règles de pare-feu IPv4*le tableau est le suivant :

Champ	Description
Priorité	Il précise la priorité de la règle configurée.
Politique	Il affiche la politique appliquée à la règle de pare-feu particulière. C'est soit**Refuser**ou**Permis**.
Protocole	Il affiche le protocole pour lequel la règle de pare-feu est définie.
Source	Il affiche la plage d'adresses IP source, une adresse IP spécifique ou Any pour toutes les adresses IP sur lesquelles la règle de pare-feu est appliquée.
Port source	Il affiche une plage de ports, des ports spécifiques ou Any pour tous les ports source attribués au protocole configuré.
Destination	Il affiche la plage d'adresses IP de destination, une adresse IP spécifique ou Any pour toutes les adresses IP sur lesquelles la règle de pare-feu est appliquée.
Le port de destination	Il affiche une plage de ports, des ports spécifiques ou Any pour tous les ports de destination attribués au protocole configuré.
Calendrier	Il affiche le calendrier lorsque la règle de pare-feu est appliquée.
Commentaire	Il affiche le commentaire ajouté pour la règle de pare-feu.
Actif	Vous pouvez activer ou désactiver la règle de pare-feu IPv4 correspondante, à l'exception de la*Règle par défaut.* ***Note**: Vous pouvez modifier ce champ uniquement lorsque le champ « Utiliser la configuration du profil » est désactivé.*
Actions	Vous pouvez modifier ou supprimer la règle de pare-feu configurée, à l'exception de la*Règle par défaut.* ***Note**: Ce champ est disponible uniquement lorsque le champ « Utiliser la configuration du profil » est désactivé.*

Pour supprimer plusieurs entrées à la fois, cochez les cases des règles de pare-feu IPv4 que vous souhaitez supprimer, puis cliquez sur**Supprimer**. Cliquez sur**Ajouter**pour ajouter une nouvelle entrée à la liste. Cela ouvre le*Ajouter des règles de pare-feu IPv4*page.

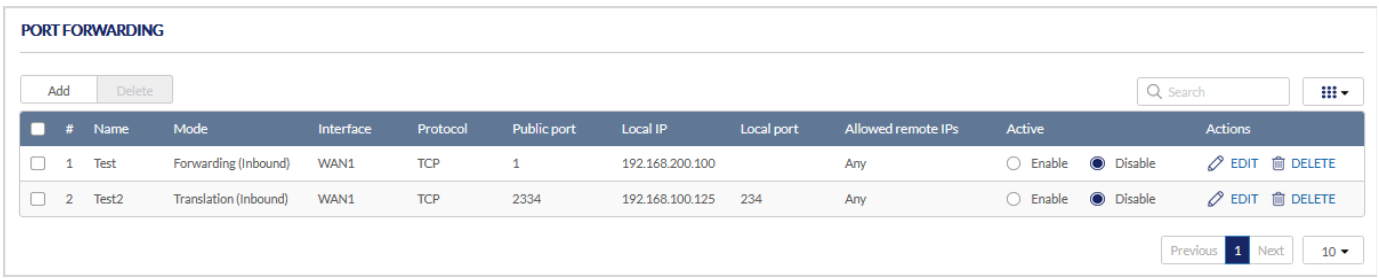


Les champs affichés sur cette page sont les suivants :

Champ	Description
Priorité	Définissez la priorité de la règle de pare-feu IPv4. Plus le nombre est petit, plus la priorité est élevée.
Politique	Sélectionnez soit**Refuser**ou**Permis**.
Protocole	Sélectionnez le protocole sur lequel vous souhaitez configurer la règle de pare-feu. Les options sont Any, TCP, UDP, TCP/UDP et ICMP.
Source	Entrez une adresse IP spécifique, une plage d'adresses IP ou toute adresse IP à partir de laquelle le trafic est envoyé.
Port source	Spécifiez un ou plusieurs ports sources où le trafic est généré. Ce champ apparaît uniquement lorsque vous sélectionnez les protocoles TCP, UDP ou TCP/UDP.
Destination	Entrez une adresse IP spécifique, une plage d'adresses IP ou toute adresse IP vers laquelle le trafic est envoyé.
Le port de destination	Spécifiez un ou plusieurs ports de destination qui recevront le trafic pour cette règle de pare-feu. Ce champ apparaît uniquement lorsque vous sélectionnez le protocole TCP, UDP ou TCP/UDP.
Calendrier	Sélectionnez un horaire dans la liste déroulante. Vous pouvez définir l'heure et le jour auxquels la règle de pare-feu IPv4 doit être appliquée. Pour configurer un horaire, reportez-vous auPolitiques de planificationsection.
Commentaire (facultatif)	Entrez le commentaire. Ce champ est facultatif.
Sauvegarder	Cliquez sur**Sauvegarder**pour enregistrer vos paramètres.
Annuler	Cliquez sur**Annuler**pour revenir aux paramètres précédents.

Redirection de port

La redirection de port est un processus visant à restreindre l'accès au trafic entrant sur votre réseau, permettant de manière sélective uniquement à des utilisateurs externes spécifiques d'accéder à des ressources locales spécifiques. Par défaut, tous les accès du côté WAN sont bloqués pour accéder au LAN sécurisé, sauf en réponse aux requêtes LAN ou DMZ. Pour autoriser les appareils externes à accéder aux services sur le réseau local sécurisé, vous devez créer une règle de redirection de port pour chaque service. Il prend également en charge la traduction (sortante).

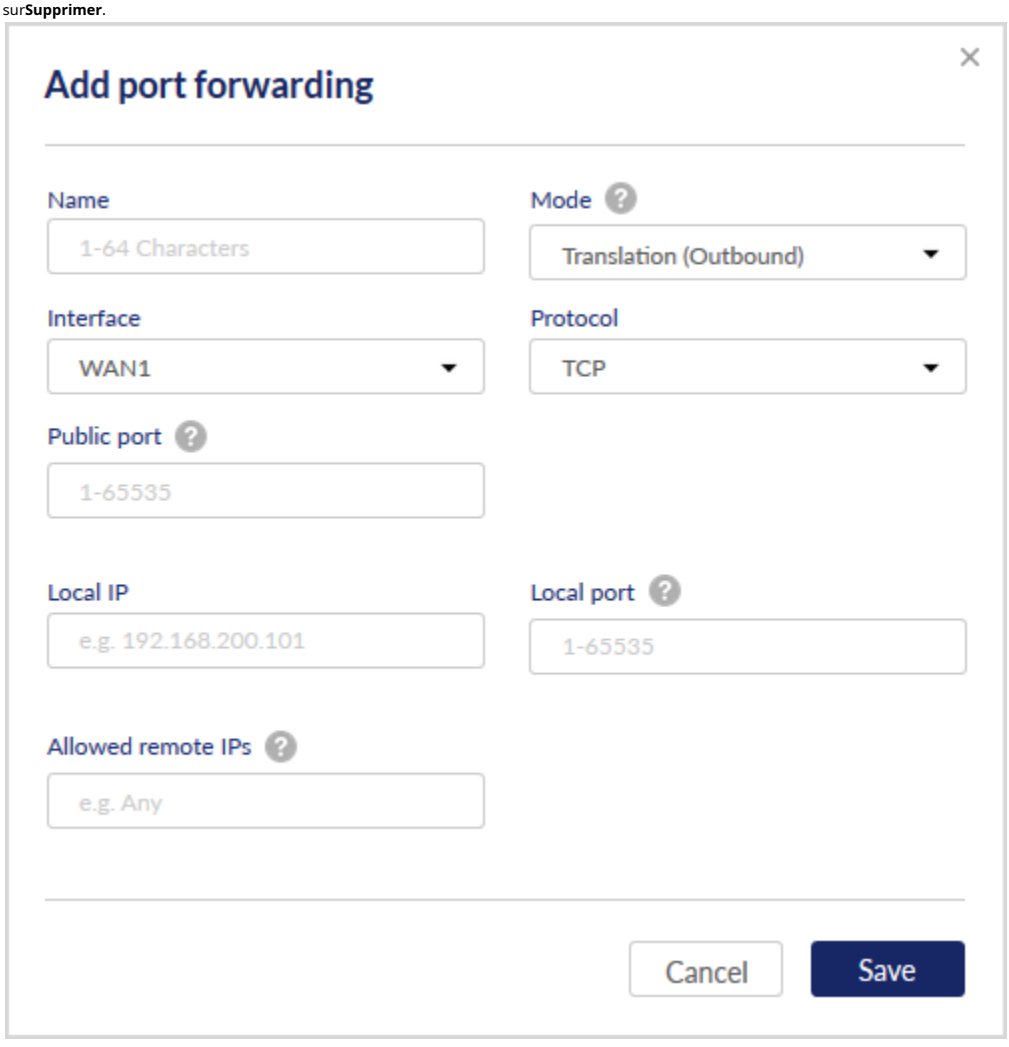


Les champs affichés dans le*Redirection de port*le tableau est le suivant :

Champ	Description
Nom	Il affiche le nom de la règle.

Mode	Il affiche le mode configuré pour la règle sélectionnée.
Interface	Il affiche l'interface sur laquelle la règle est configurée.
Protocole	Il affiche le protocole suivi pour la règle configurée.
Port public	Il affiche le numéro de port public.
IP locale	Il affiche l'adresse IP de l'hôte LAN.
Port local	Il affiche les numéros de port hôte LAN.
IP distantes autorisées	Il affiche les adresses IP qui peuvent accepter le trafic entrant et sortant.
Actif	Vous pouvez activer ou désactiver la règle correspondante. ***Note**: Vous pouvez modifier ce champ uniquement lorsque le champ « Utiliser la configuration du profil » est désactivé.*
Actions	Cliquez sur**Modifier**pour apporter des modifications à la règle de redirection de port existante. Cliquez sur**Supprimer**pour supprimer la règle. ***Note**: Cette colonne est disponible uniquement lorsque le champ « Utiliser la configuration du profil » est désactivé.*

Cliquez sur**Ajouter**pour ajouter une nouvelle entrée. Cela ouvre le*Ajouter une redirection de port*page. Pour supprimer plusieurs entrées, cochez les cases que vous souhaitez supprimer, puis cliquez sur**Supprimer**.



Les champs disponibles sur le*Ajouter une redirection de port*page sont les suivantes :

Champ	Description
Nom	Saisissez le nom de votre règle.

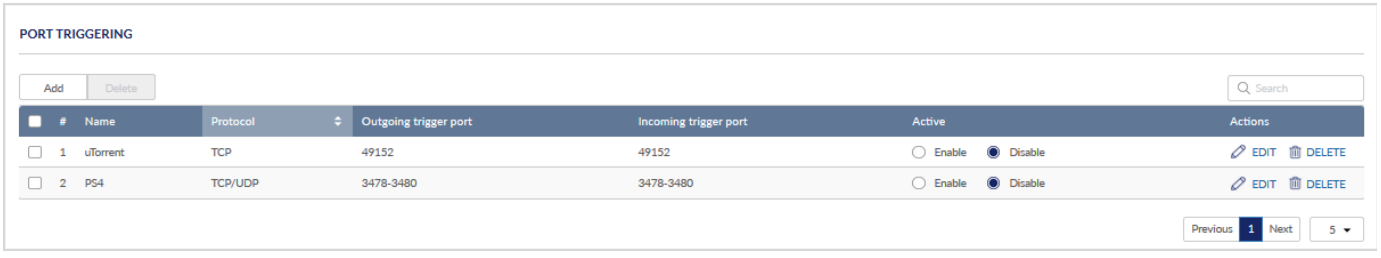
Mode	Sélectionnez l'un des modes suivants : • **Transfert (entrant)**: Si vous sélectionnez ce mode, le trafic passe de l'hôte WAN à l'hôte LAN pour un port de destination public. • **Traduction (sortante)** : Il traduit le trafic d'un numéro de port source local en numéro de port source public configuré pour l'hôte LAN vers le trafic de l'hôte WAN. • **Traduction (entrante)**: Si vous sélectionnez ce mode, le trafic passe de l'hôte WAN à l'hôte LAN et est traduit vers le port local de destination lorsque le trafic est envoyé sur le port de destination public. ***Note**: Les options Traduction (entrant) et Traduction (sortant) sont disponibles uniquement lorsque le mode de routage est configuré sur NAT sur leMode itinéraire page.*
Interface	Sélectionnez l'interface sur laquelle cette règle sera appliquée.
Protocole	Sélectionnez l'un des protocoles suivants : TCP, UDP ou TCP/UDP.
Port public	Entrez le numéro de port sur lequel les applications s'exécutent sur l'hôte WAN.
IP locale	Entrez l'adresse IP de l'hôte LAN. Pour la traduction (sortant), il s'agit de l'adresse IP d'où proviendra le trafic. Pour Traduction (Inbound) ou Forwarding (Inbound), il fait référence à l'adresse IP à laquelle le trafic sera envoyé. ***Note**: Ce champ n'est pas disponible uniquement lorsque vous configurez le mode route comme Routeur sur le Mode itinéraire page.*
Port local	Le port local fait référence aux numéros de port de l'hôte LAN. Pour les appels sortants, cela signifie le port source local et pour les appels entrants, cela signifie le port local de destination de l'hôte LAN. Ce champ est disponible uniquement lorsque vous sélectionnez**Traduction (sortante)**ou**Traduction (entrante)**mode. ***Note:*** • *En mappant une plage de ports publics à une plage de ports locaux, les plages doivent être de même longueur.* • *Ce champ n'est pas disponible uniquement lorsque vous configurez le mode de routage sur Routeur sur leMode itinéraire page.*
IP distantes autorisées	Entrez les adresses IP distantes autorisées. Les adresses IP distantes autorisées sont les adresses IP qui acceptent le trafic vers (pour la traduction sortante) et depuis (pour la traduction entrante et le transfert entrant).
Sauvegarder	Cliquez sur**Sauvegarder**pour enregistrer vos paramètres.
Annuler	Cliquez sur**Annuler**pour revenir aux paramètres précédents.

Déclenchement des ports

Le déclenchement de port permet aux appareils du LAN ou de la DMZ de demander qu'un ou plusieurs ports leur soient redirigés. Cette fonctionnalité attend une demande sortante du LAN ou de la DMZ sur l'un des ports sortants définis, puis ouvre un port entrant pour ce type de trafic. Il peut s'agir d'une forme de redirection de port dynamique pendant qu'une application transmet des données via le(s) port(s) sortant(s) ou entrant(s) ouvert(s).

Les règles d'application de déclenchement de port sont plus flexibles que la redirection de port statique, qui est une option lors de la configuration des règles de redirection. En effet, une règle de déclenchement de port ne fait pas référence à une adresse IP LAN ou à une plage IP spécifique. De plus, les ports ne sont pas laissés ouverts lorsqu'ils ne sont pas utilisés, offrant ainsi un niveau de sécurité que la redirection de port n'offre pas.

***Note**: Cette section est disponible uniquement lorsque vous configurez le mode de routage comme NAT sur leMode itinéraire page.*

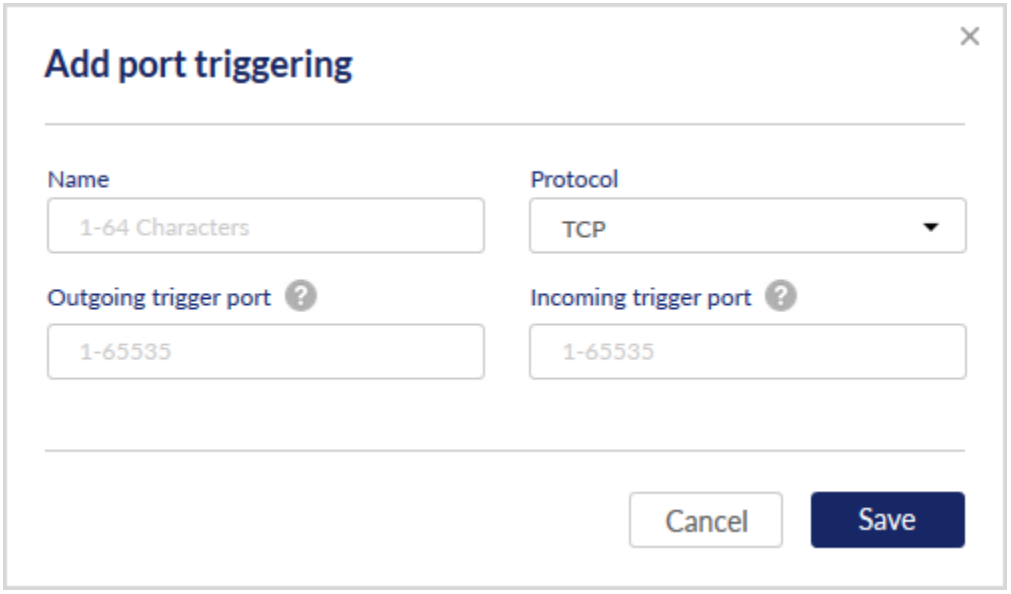


Les champs affichés dans le*Déclenchement des ports*le tableau est le suivant :

Champ	Description
Nom	Il affiche le nom de la règle de déclenchement du port.

Protocole	Il affiche le protocole sur lequel la règle est configurée. Il s'agit de TCP, UDP ou TCP/UDP.
Port de déclenchement sortant	Il affiche la plage de ports de déclenchement de début et de fin.
Port de déclenchement entrant	Il affiche une plage de ports ouverts pour recevoir le trafic.
Actif	Vous pouvez activer ou désactiver la règle de déclenchement de port. ***Note**: Vous pouvez modifier ce champ uniquement lorsque le champ « Utiliser la configuration du profil » est désactivé.*
Actions	Vous pouvez modifier ou supprimer la règle de déclenchement de port correspondante. ***Note**: Ce champ est disponible uniquement lorsque le champ « Utiliser la configuration du profil » est désactivé.*

Cliquez sur**Ajouter**pour ajouter une nouvelle entrée. Cela ouvre le*Ajouter un déclenchement de port*page. Pour supprimer plusieurs entrées, cochez les cases que vous souhaitez supprimer, puis cliquez sur**Supprimer**.



Les champs disponibles sur cette page sont les suivants :

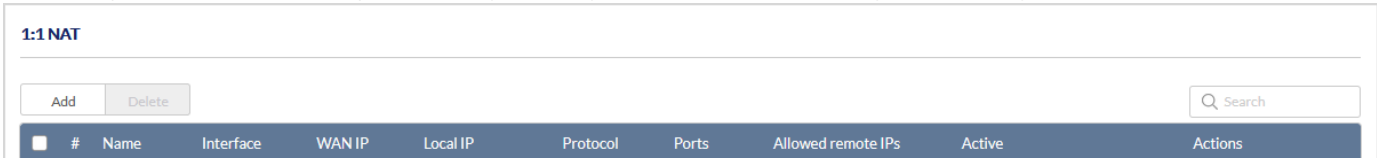
Champ	Description
Nom	Entrez le nom de la règle de déclenchement du port.
Protocole	Sélectionnez le protocole sur lequel la règle doit être configurée. Il s'agit de TCP, UDP ou TCP/UDP.
Port de déclenchement sortant	Entrez la plage de ports de déclenchement de début et de fin.
Port de déclenchement entrant	Entrez la plage de ports ouverte pour recevoir le trafic.
Sauvegarder	Cliquez sur**Sauvegarder**pour enregistrer vos paramètres.
Annuler	Cliquez sur**Annuler**pour revenir aux paramètres précédents.

NAT 1:1

1:1 NAT est une technique de pare-feu lorsque plusieurs adresses IP publiques et plusieurs serveurs sont disponibles à travers le pare-feu. Comme son nom l'indique, il mappe une adresse IP interne à une adresse IP externe. Pour mener à bien l'ensemble du processus, il doit d'abord configurer un alias d'adresse IP externe, puis mapper le trafic entrant et le rediriger vers la bonne adresse IP interne. De plus, il mappe également le trafic sortant de l'adresse IP interne et le dirige vers l'adresse IP externe destinée.

***Note**: Cette section est disponible uniquement lorsque vous configurez le mode de routage comme NAT sur le*Mode itinéraire*page.*

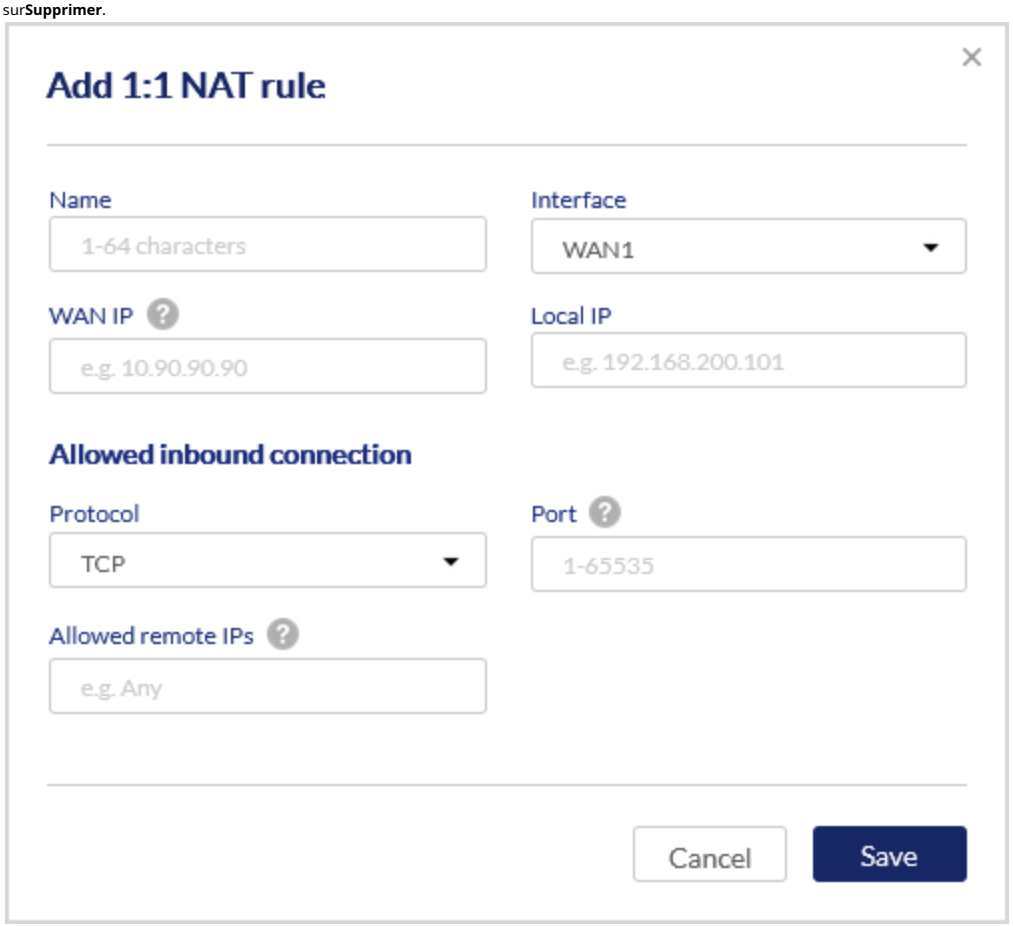
DBG-2000, la passerelle cloud Nuclias, vous permet de configurer des règles NAT 1:1 et affiche toutes les règles NAT 1:1 configurées.



Les champs affichés dans le*NAT 1:1*le tableau est le suivant :

Champ	Description
Nom	Il affiche le nom de la règle.
Interface	Il affiche le WAN pour lequel il est configuré.
IP WAN	Il affiche l'adresse IP publique pour laquelle l'adresse IP locale est mappée.
IP locale	Il affiche l'adresse IP locale à partir de laquelle l'adresse IP WAN est mappée.
Protocole	Il affiche le protocole sur lequel la règle a été configurée.
Ports	Il affiche le numéro de port ou une plage de ports autorisés à accéder à la ressource interne.
IP distantes autorisées	Il affiche les adresses IP à partir desquelles le pare-feu accepte le trafic.
Actif	Vous pouvez activer ou désactiver la règle sélectionnée. ***Note**: Vous pouvez modifier ce champ uniquement lorsque le champ « Utiliser la configuration du profil » est désactivé.*
Actions	Vous pouvez modifier ou supprimer la règle NAT 1:1 configurée. ***Note**: Cette colonne est disponible uniquement lorsque le champ « Utiliser la configuration du profil » est désactivé.*

Cliquez sur**Ajouter**pour ajouter une nouvelle entrée. Cela ouvre le*Ajouter une règle NAT 1:1*page. Pour supprimer plusieurs entrées, cochez les cases que vous souhaitez supprimer, puis cliquez sur**Supprimer**.



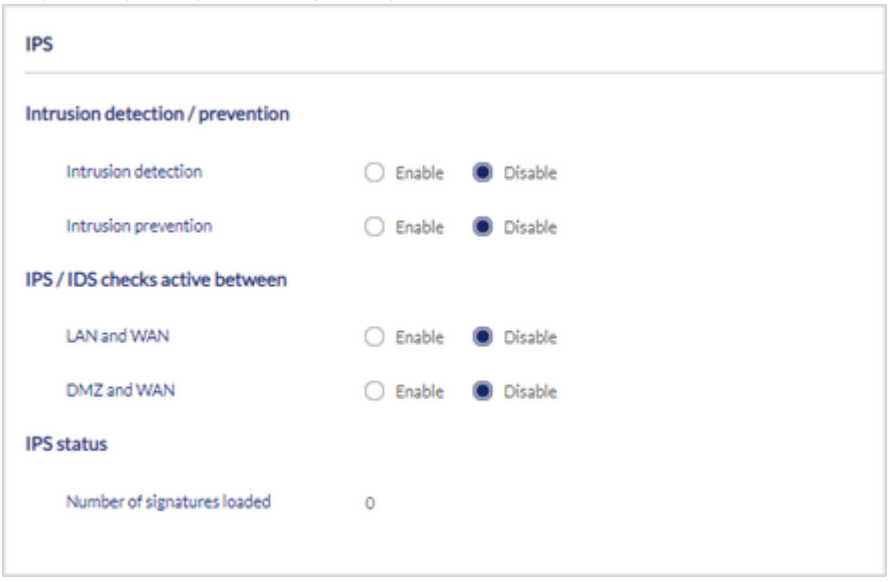
Les champs disponibles sur le*Ajouter une règle NAT 1:1*page sont les suivantes :

Champ	Description
Nom	Saisissez un nom descriptif pour la règle.
Interface	Sélectionnez l'interface WAN sur laquelle la règle sera appliquée.
IP WAN	Saisissez l'adresse IP publique pour laquelle l'adresse IP locale est mappée.
IP locale	Entrez l'adresse IP locale à partir de laquelle l'adresse IP WAN est mappée.
Connexion entrante autorisée	
Protocole	Sélectionnez un protocole à utiliser tout en autorisant la connexion entrante. Les options sont TCP, UDP et TCP/UDP.
Port	Sélectionnez le port ou une plage de ports à utiliser pour la connexion.
IP distantes autorisées	Saisissez les adresses IP distantes qui seront autorisées à établir les connexions entrantes.
Sauvegarder	Cliquez sur**Sauvegarder**pour enregistrer vos paramètres.
Annuler	Cliquez sur**Annuler**pour revenir aux paramètres précédents.

IPS

Le système de prévention des intrusions (IPS) de la passerelle empêche les attaques malveillantes provenant d'Internet d'accéder
le réseau privé. Les signatures d'attaque statiques chargées sur la passerelle permettent de détecter et de prévenir les attaques courantes. De plus, vous pouvez activer les vérifications entre le WAN et la DMZ ou le LAN.

***Note**: Vous pouvez modifier cette section uniquement lorsque le champ « Utiliser la configuration du profil » est désactivé.*



Les champs disponibles sur cette page sont les suivants :

Champ	Description
Détection/prévention des intrusions	
Détection d'intrusion	Activez ou désactivez la détection d'intrusion.
Prévention des intrusions	Activez ou désactivez la prévention des intrusions.
Contrôles IPS/IDS actifs entre	
LAN et WAN	Activez-le pour détecter les intrusions entre les interfaces LAN et WAN.
DMZ et WAN	Activez-le pour détecter les intrusions entre les interfaces DMZ et WAN.
Statut IPS	

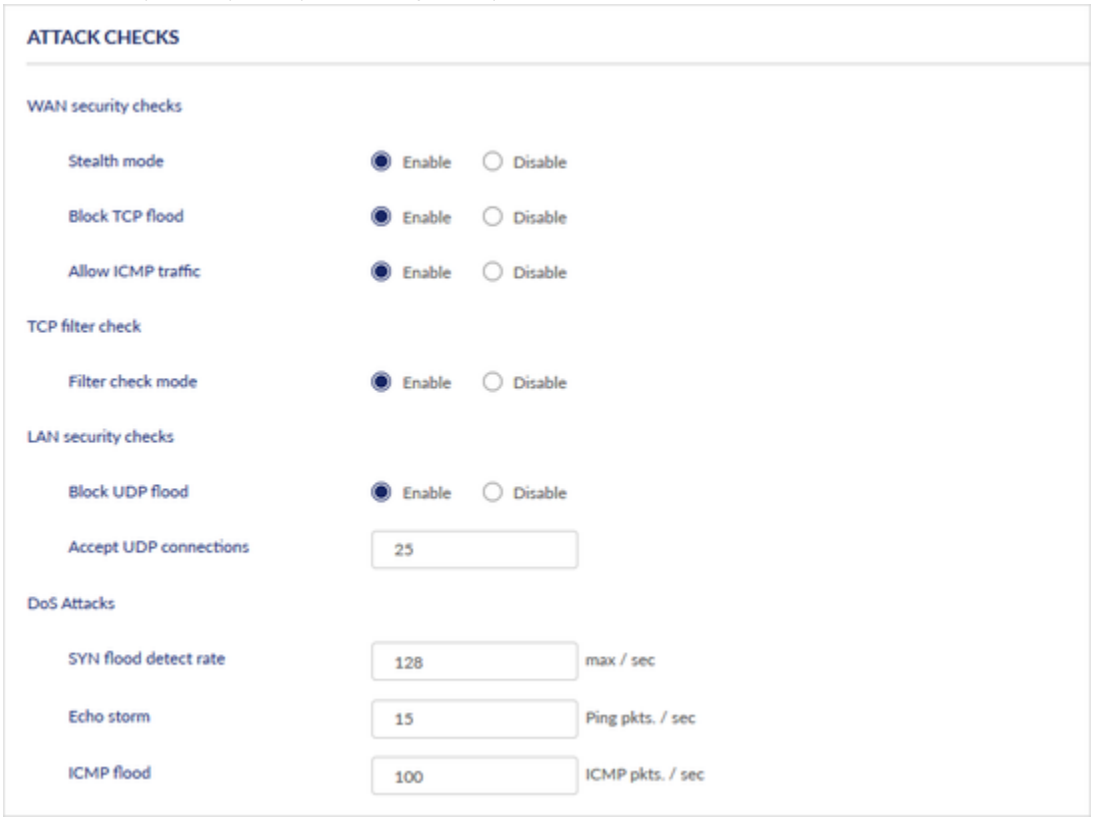
Nombre de signatures chargées	Il affiche le nombre de signatures chargées.

Vérifications d'attaque

Les attaques peuvent être des failles de sécurité malveillantes ou des problèmes de réseau involontaires qui rendent la passerelle inutilisable. Les contrôles d'attaques vous permettent de gérer les menaces de sécurité WAN, telles que les demandes ping continues et la découverte via les analyses ARP. Vous pouvez activer les contrôles d'attaque par inondation TCP et UDP pour gérer une utilisation extrême des ressources WAN.

De plus, vous pouvez bloquer certaines attaques par déni de service (DoS). Ces attaques, si elles ne sont pas inhibées, peuvent utiliser la puissance de traitement et la bande passante et empêcher les services réseau normaux. Vous pouvez également configurer les seuils d'inondation de paquets ICMP, d'inondation de trafic SYN et de tempête d'écho pour suspecter temporairement le trafic provenant de la source incriminée.

***Note**: Vous pouvez modifier cette section uniquement lorsque le champ « Utiliser la configuration du profil » est désactivé.*



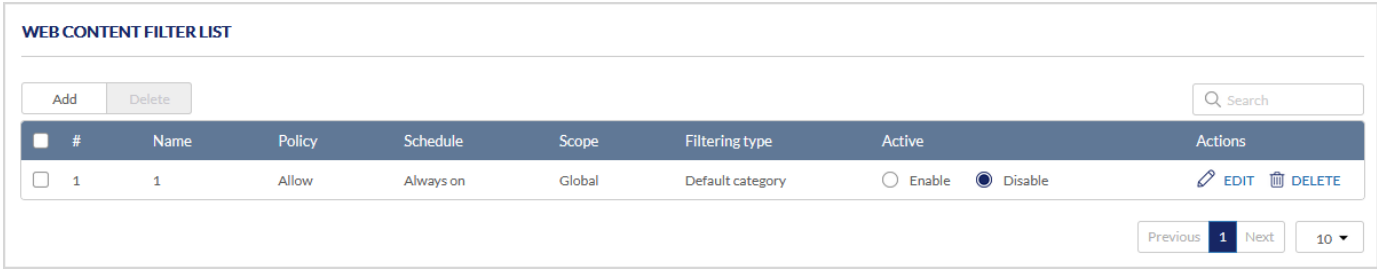
Les champs disponibles sur cette page sont les suivants :

Champ	Description
Contrôles de sécurité WAN	
Mode furtif	Si cette option est activée, la passerelle ne répondra pas aux analyses de ports du WAN. Cela le rend moins vulnérable aux découvertes et aux attaques.
Bloquer l'inondation TCP	Si cette option est activée, la passerelle supprime tous les paquets TCP non valides et est protégée contre l'attaque par inondation TCP.
Autoriser le trafic ICMP	Si cette option est activée, l'hôte WAN peut envoyer une requête ping au trafic vers l'interface WAN.
Vérification du filtre TCP	
Mode de vérification du filtre	Si cette option est activée, la passerelle abandonne les paquets TCP non valides (FIN, RST et ACK) accompagnés de SNAT pendant que la connexion est fermée. Certains autres paquets, comme TCP OUT-OF-WINDOW, sont également considérés comme non valides. Désactivez cette option lors de la prise de performances, car l'activation de cette option affectera le débit.
Contrôles de sécurité du réseau local	
Bloquer l'inondation UDP	Si cette option est activée, la passerelle n'acceptera pas plus que la valeur configurée dans*Accepter les connexions UDP*, indiquant des connexions UDP actives et simultanées à partir d'un seul ordinateur sur le réseau local.

Accepter les connexions UDP	Saisissez le nombre de connexions UDP acceptées simultanément par la passerelle à partir d'un seul ordinateur sur le LAN. Vous pouvez sélectionner n'importe quel nombre compris entre 25 et 500. Ce champ est disponible lorsque vous activez*Bloquer l'inondation UDP*.
Attaques DoS	
Taux de détection d'inondation SYN	Entrez la vitesse à laquelle le flux SYN peut être détecté.
Tempête d'écho	Entrez le nombre de paquets ping par seconde auquel la passerelle détecte une attaque Echo Storm provenant du WAN et empêche tout autre trafic ping provenant de cette adresse externe.
Inondation ICMP	Entrez le nombre de paquets ICMP par seconde auquel la passerelle détecte une attaque par inondation ICMP provenant du WAN et empêche la poursuite du trafic ICMP à partir de cette adresse externe.

Web Content Filter

La passerelle propose des options de filtrage Web standard pour filtrer la page Web affichée par les noms de domaine. Il vous permet de créer des politiques d'accès Internet entre LAN et WAN. Au lieu de créer des politiques basées sur le type de trafic (comme c'est le cas lors de l'utilisation de règles de pare-feu), le contenu Web lui-même peut être utilisé pour déterminer si le trafic est autorisé ou supprimé.

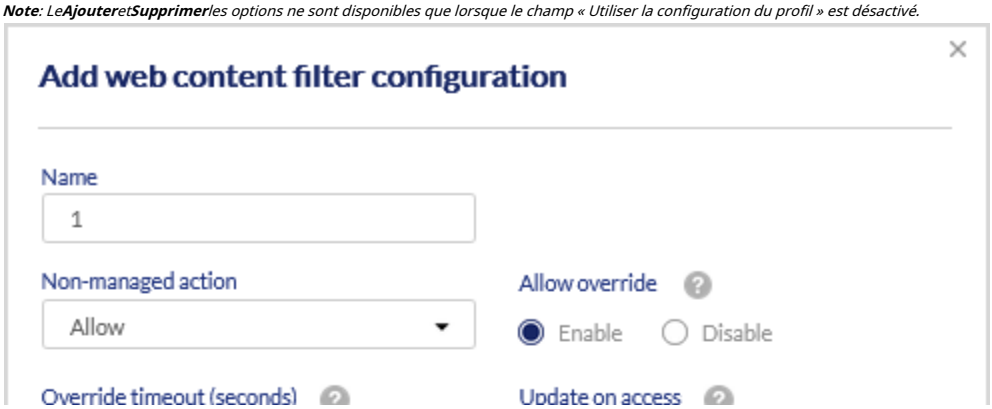


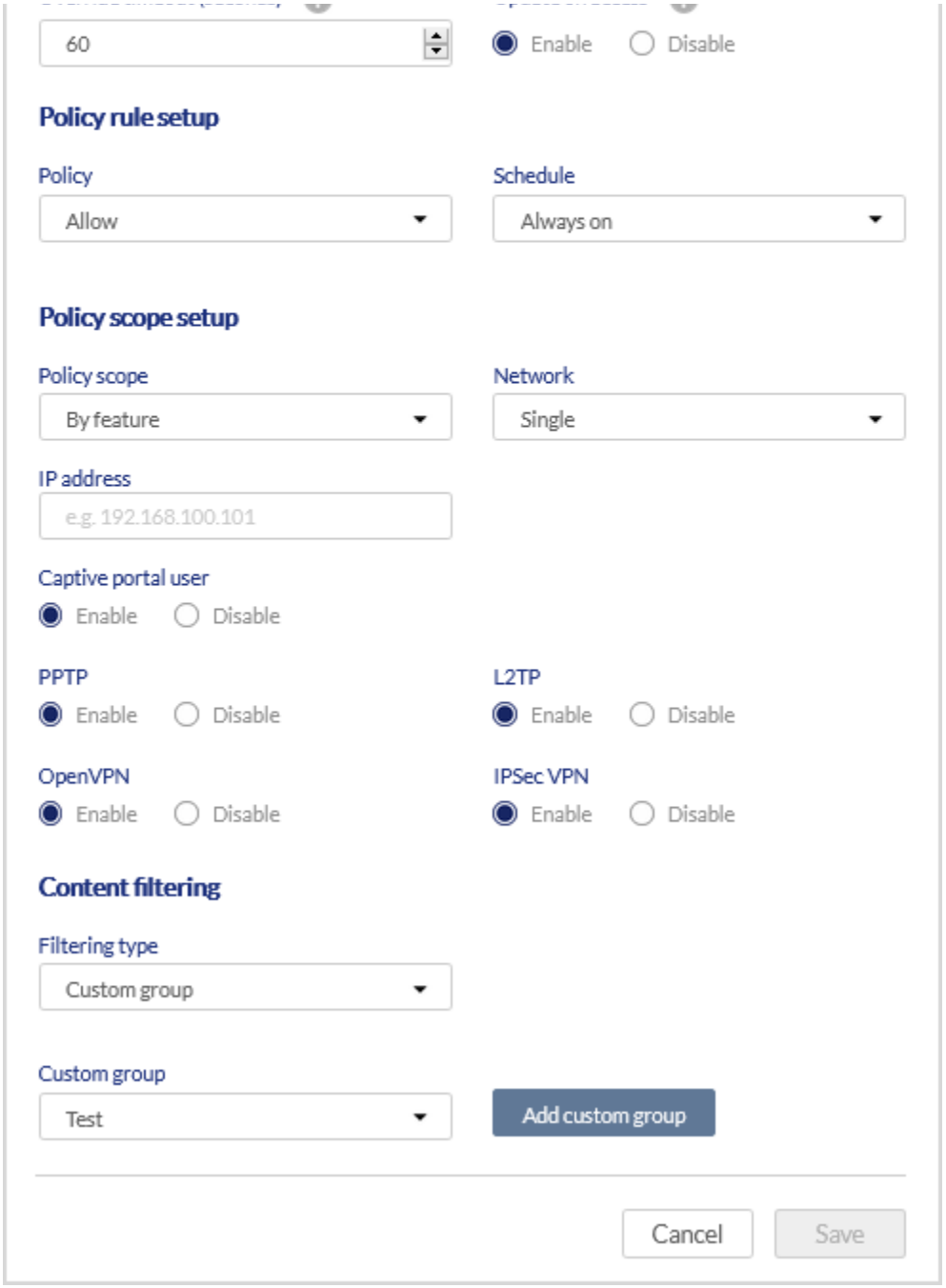
Les champs affichés dans le*Liste de filtres de contenu Web*sont les suivants:

Champ	Description
Nom	Il affiche le nom de la stratégie.
Politique	Il affiche la règle de politique.
Calendrier	Il affiche le calendrier sélectionné pour la politique.
Portée	Il affiche la portée. Il s'agit soit de Global, soit de Feature.
Type de filtrage	Il affiche le type d'informations que vous souhaitez filtrer avec cette stratégie.
Actif	Vous pouvez activer ou désactiver la stratégie. ***Note**: Vous pouvez modifier ce champ uniquement lorsque le champ « Utiliser la configuration du profil » est désactivé.*
Actions	Vous pouvez modifier ou supprimer la stratégie de filtrage de contenu Web sélectionnée. ***Note**: Ce champ est disponible uniquement lorsque le champ « Utiliser la configuration du profil » est désactivé.*

Cliquez sur**Ajouter**pour ajouter une nouvelle entrée. Cela ouvre le*Ajouter la configuration du filtre de contenu Web*page. Pour supprimer plusieurs entrées, cochez les cases du filtre de contenu Web que vous souhaitez supprimer, puis cliquez sur**Supprimer**.

***Note**: Le**Ajouter**et**Supprimer**les options ne sont disponibles que lorsque le champ « Utiliser la configuration du profil » est désactivé.*





Les champs disponibles sur le*Ajouter la configuration du filtre de contenu Web*page sont les suivantes :

Champ	Description
Nom	Entrez le nom de la stratégie.
Action non gérée	Il s'agit d'une action à entreprendre pour le Site Non Géré. Vous pouvez autoriser ou bloquer. Par défaut, il s'agit de Autoriser.
Autoriser Override	S'il est activé, il autorise les sites classés dans les catégories bloquées.
Délai d'expiration de remplacement (secondes)	Entrez la durée (en secondes) pendant laquelle toutes les catégories non autorisées seront autorisées.
Mise à jour sur l'accès	Activez le champ pour redémarrer le temporisateur de remplacement à chaque nouvel accès aux catégories non autorisées.
Configuration des règles de stratégie	
Politique	Sélectionnez la règle de stratégie. Les options sont*Permettre*et*Bloc*.

Calendrier	Sélectionnez le calendrier auquel la règle de stratégie doit être appliquée. Pour configurer un horaire, reportez-vous au Politiques de planificationpage.
Configuration de la portée de la stratégie	
Portée de la politique	Sélectionnez soit*Mondial*ou*Par fonctionnalité*comme le champ d'application de la politique. La politique globale affecte tous les types de trafic correspondant à la ou aux applications sélectionnées. Si vous sélectionnez*Par fonctionnalité*, les champs supplémentaires suivants seront disponibles.
Réseau	Sélectionnez l'un des profils réseau configurés. Vous pouvez sélectionner*Aucun, célibataire*,*Gamme*, ou*Interface*.
adresse IP	Si vous sélectionnez un**Célibataire**comme le*Réseau*, saisissez l'adresse IP.
Adresse IP de départ	Si vous sélectionnez**Gamme**comme le*Réseau*, saisissez l'adresse IP de départ de la plage IP.
Adresse IP de fin	Si vous sélectionnez**Gamme**comme le*Réseau*, saisissez l'adresse IP de fin de la plage IP.
Interface	Si vous sélectionnez**Interface**comme le*Réseau*, sélectionnez l'interface configurée dans la liste déroulante.
Utilisateur du portail captif	Activer ou désactiver le*Utilisateur du portail captif*option. L'activation de cette option permet à tous les clients du portail captif de suivre cette politique.
PPTP	Activez ou désactivez le VPN PPTP. L'activation de cette option permet au trafic PPTP de suivre cette politique.
L2TP	Activez ou désactivez le VPN L2TP. L'activation de cette option permet au trafic L2TP de suivre cette stratégie.
OpenVPN	Activez ou désactivez OpenVPN. L'activation de cette option permet au trafic OpenVPN de suivre cette politique.
VPN IPSec	Activez ou désactivez le VPN IPSec. L'activation de cette option permet au trafic IPSec de suivre cette stratégie.
Filtrage du contenu	
Type de filtrage	Ce champ vous permet de sélectionner le type d'informations que vous souhaitez filtrer. Sélectionnez l'une des options suivantes : • **Catégorie par défaut**: Sélectionnez les catégories par défaut que vous souhaitez filtrer. • **URL**: La section Filtrage des URL est disponible sur la page suivante. Clique le**Suivant**bouton situé dans le coin inférieur droit de la page pour ajouter des URL ou des mots-clés. • **Catégorie+URL par défaut**: sélectionnez une catégorie par défaut dans la liste déroulante et ajoutez des URL/mots-clés dans la section de filtrage d'URL disponible sur la page suivante. • **Groupe personnalisé**: Sélectionnez l'un des groupes personnalisés configurés ou créez un nouveau groupe.
Filtrage d'URL	Pour ajouter une URL (HTTP ou HTTPS), un nom de domaine ou un mot-clé, sélectionnez**Ajouter une URL/un mot clé**. Cliquez sur**+Ajouter**pour ajouter plusieurs entrées. Si vous souhaitez ajouter des URL ou des mots-clés en même temps, sélectionnez**Importation en masse**. Cliquez sur **Parcourir**et sélectionnez le fichier (au format CSV) dont vous souhaitez importer les informations dans la base de données. Vous pouvez télécharger l'exemple de fichier de modèle ici.*Notez que le nombre d'entrées est limité à un maximum de 512 URL.*
Catégorie par défaut	Ce champ est disponible lorsque vous sélectionnez le*Catégorie par défaut*ou*Catégorie+URL par défaut* comme type de filtrage. Sélectionnez le type de catégories à filtrer dans la liste déroulante.
Groupe personnalisé	Sélectionnez l'un des groupes personnalisés configurés dans la liste déroulante. Pour créer un nouveau groupe, cliquez sur **Ajouter un groupe personnalisé**. Cela ouvre le*Ajouter une configuration de groupe*page. Pour plus de détails, reportez-vous àListe de groupes personnalisée.
Précédent	Cliquez sur**Précédent**pour revenir à la page de configuration précédente.
Sauvegarder	Cliquez sur**Sauvegarder**pour enregistrer vos paramètres.
Annuler	Cliquez sur**Annuler**pour revenir aux paramètres précédents.

Liste de groupes personnalisée

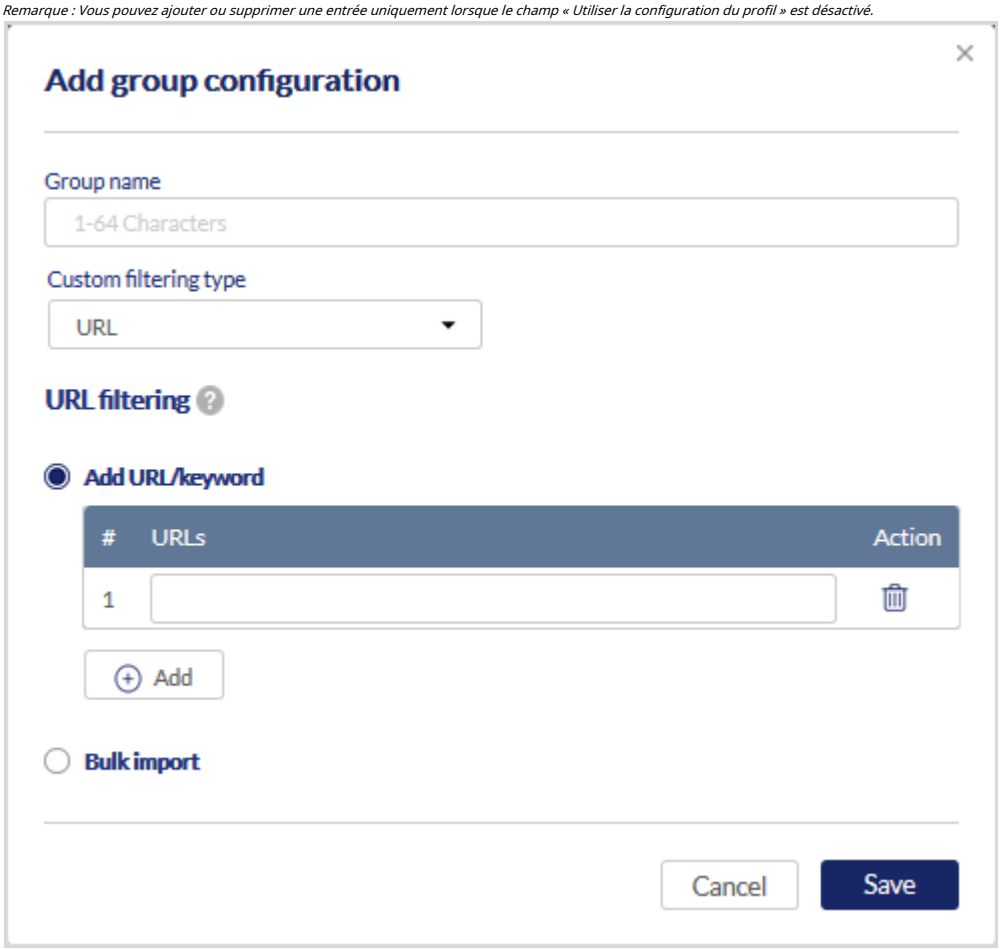
Les utilisateurs peuvent sélectionner une URL particulière ou sélectionner un groupe pour gérer les URL associées à ce groupe. Cette section affiche les groupes et les URL qui leur sont associés.

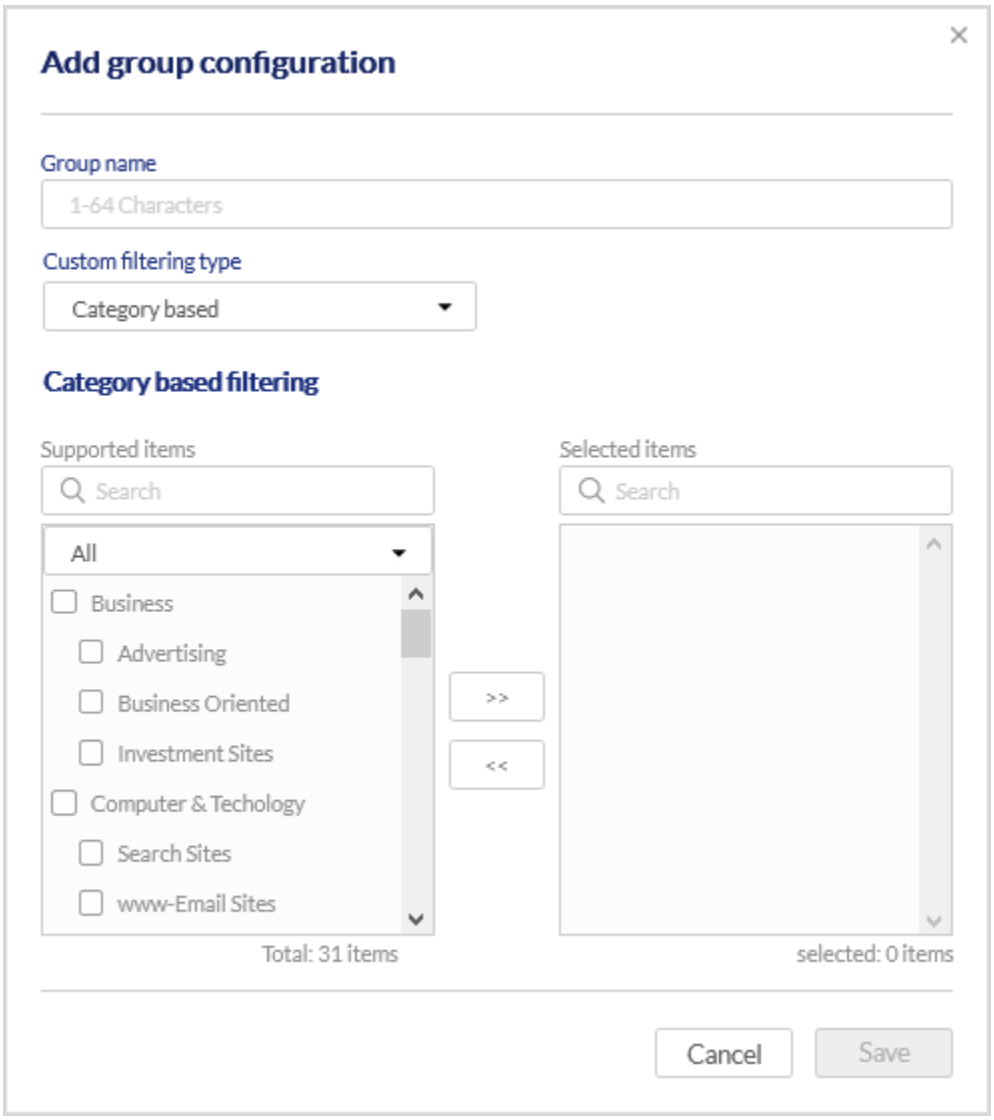
Les champs affichés dans le*Liste de groupes personnalisée*le tableau est le suivant :

Champ	Description
Nom	Il affiche le nom du groupe.
URL	Il affiche la liste des URL sélectionnées.
Filtrage par catégorie	Il affiche la catégorie à laquelle appartiennent ces URL.
Utilisé	Il indique si ce groupe personnalisé est utilisé ou non.
Actions	Vous pouvez modifier ou supprimer la liste des groupes. ***Note**: Ce champ est disponible uniquement lorsque le champ « Utiliser la configuration du profil » est désactivé.*

Cliquez sur**Ajouter**pour ajouter un nouveau groupe. Cela ouvre le*Ajouter une configuration de groupe*page.

Remarque : Vous pouvez ajouter ou supprimer une entrée uniquement lorsque le champ « Utiliser la configuration du profil » est désactivé.





Les champs disponibles sur cette page sont les suivants :

Champ	Description
Nom de groupe	Entrez un nom pour votre groupe.
Type de filtrage personnalisé	Sélectionnez l'un des types de filtrage suivants que vous souhaitez appliquer à votre groupe : • **URL**: Si vous sélectionnez cette option, le*Filtrage d'URL*La section sera disponible. • **Basé sur la catégorie**: Si vous sélectionnez cette option, le*Filtrage par catégorie*La section sera disponible. • **Basé sur une URL + une catégorie**: Si vous sélectionnez cette option, les deux sections ci-dessus seront disponibles. Clique le**Suivant**bouton situé dans le coin inférieur droit de la page pour accéder au*Filtrage par catégorie*section.
Ajouter une URL/un mot clé	Sélectionnez cette option pour ajouter une nouvelle URL. Entrez l'URL dans la case ; 1 à 64 caractères sont autorisés. Pour ajouter une nouvelle URL, cliquez sur le**+Ajouter**bouton.
Importation en masse	Pour importer des URL en masse, sélectionnez « Importation en masse ». Ensuite, cliquez sur**Parcourir**pour localiser le fichier sur votre système, puis importez-le dans***.CSV**format. Vous pouvez télécharger l'exemple de fichier de modèle ici. *Notez que le nombre d'entrées est limité à un maximum de 512 URL.*
Éléments pris en charge	Cochez une ou plusieurs cases des catégories que vous souhaitez filtrer. Ensuite, cliquez sur le**">>"** pour le déplacer vers la case de l'élément sélectionné. Ceci est disponible lorsque vous sélectionnez «**Basé sur une catégorie**" ou "**Basé sur une URL + une catégorie**"type de filtrage.

Articles sélectionnés	Cette boîte affiche les éléments sélectionnés dans la liste des éléments pris en charge. Pour supprimer l'élément de la liste sélectionnée, cliquez sur le bouton**"<<"**bouton. Ceci est disponible lorsque vous sélectionnez «**Basé sur une catégorie**" ou "**Basé sur une URL + une catégorie**"type de filtrage.
Suivant	Cliquez sur**Suivant**pour aller à la*Filtrage par catégorie*section. Ce bouton est disponible uniquement lorsque vous sélectionnez**Basé sur l'URL + par catégorie**type de filtrage.
Précédent	Cliquez sur**Précédent**revenir au*Filtrage d'URL*section. Ce bouton est disponible uniquement lorsque vous sélectionnez**Basé sur l'URL + par catégorie**type de filtrage.
Sauvegarder	Cliquez sur**Sauvegarder**pour enregistrer vos paramètres.
Annuler	Cliquez sur**Annuler**pour revenir aux paramètres précédents.

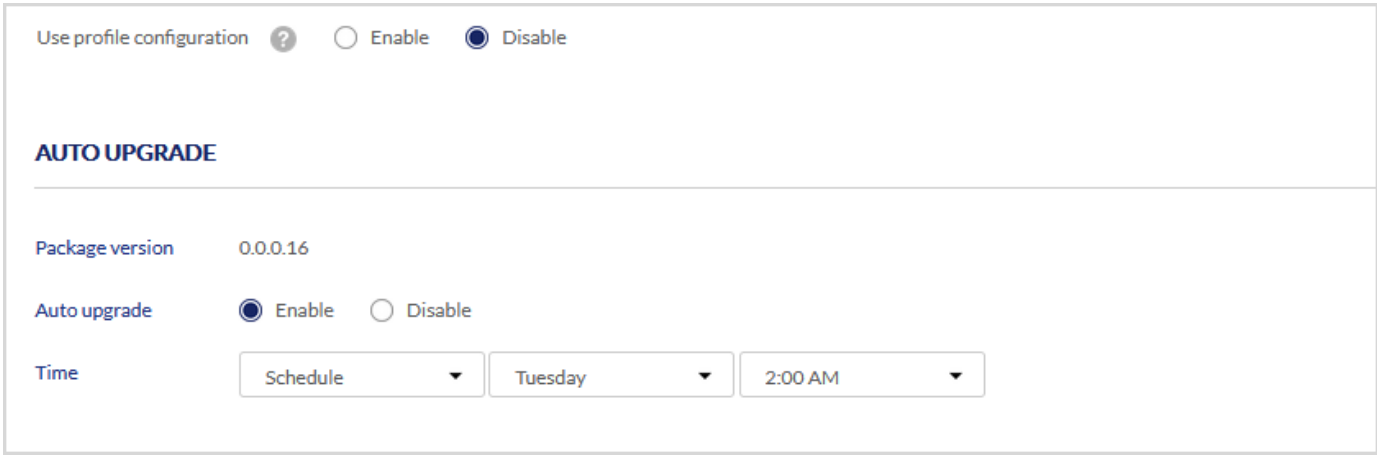
Application Control

Le contrôle des applications est une fonctionnalité qui permet aux administrateurs réseau d'autoriser, de bloquer ou de contrôler le trafic des applications qui traitent le trafic. Il vous permet de bloquer ou d'autoriser des applications spécifiques, comme Netflix, YouTube, Facebook, Twitter, etc.

Cette section couvre les sujets suivants :

Mise à niveau automatique

Cette section fournit la version actuelle du package exécuté sur l'appareil. Vous pouvez activer ou désactiver le*Mise à niveau automatique*fonctionnalité uniquement lorsque le*Utiliser la configuration du profil*le champ est désactivé. La fonction de mise à niveau automatique permet à l'utilisateur de définir un intervalle de temps ou un calendrier pour que l'appareil vérifie automatiquement les packages mis à jour sur le serveur. Quand le*Utiliser la configuration du profil*est activé, le*Mise à niveau automatique*La fonction est automatiquement activée et affiche les détails de l'heure.

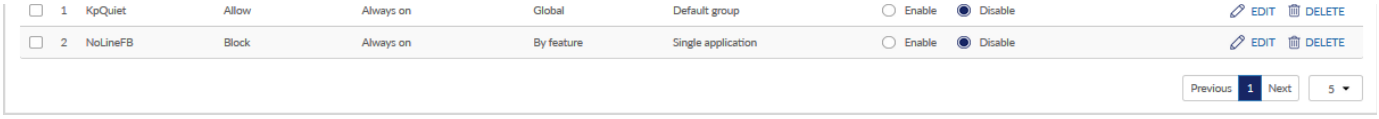


Les champs disponibles dans cette section sont les suivants :

Champ	Description
Version du paquet	Il fournit des détails sur la version du package en cours d'exécution.
Mise à niveau automatique	Activez ou désactivez l'option de mise à niveau automatique. ***Note**: Ce champ est disponible uniquement lorsque le champ « Utiliser la configuration du profil » est désactivé.*
Temps	Sélectionnez soit*Intervalle*ou*Calendrier*pour vérifier les packages mis à jour sur le serveur. Si vous sélectionnez*Intervalle*, saisissez le nombre de minutes après lesquelles l'appareil recherchera les mises à jour. Si vous sélectionnez*Calendrier*, choisis un**Jour**et**Temps**.

Liste de contrôle des applications

L'utilisateur peut sélectionner une application particulière ou sélectionner un groupe pour gérer les applications associées à ce groupe. Cela fournit à l'administrateur davantage d'options pour configurer des politiques permettant de contrôler l'accès aux applications pour les utilisateurs réseau, les adresses IP ou les segments de réseau sélectionnés. Vous pouvez configurer la liste de contrôle des applications uniquement lorsque le*Utiliser la configuration du profil*le champ est désactivé.

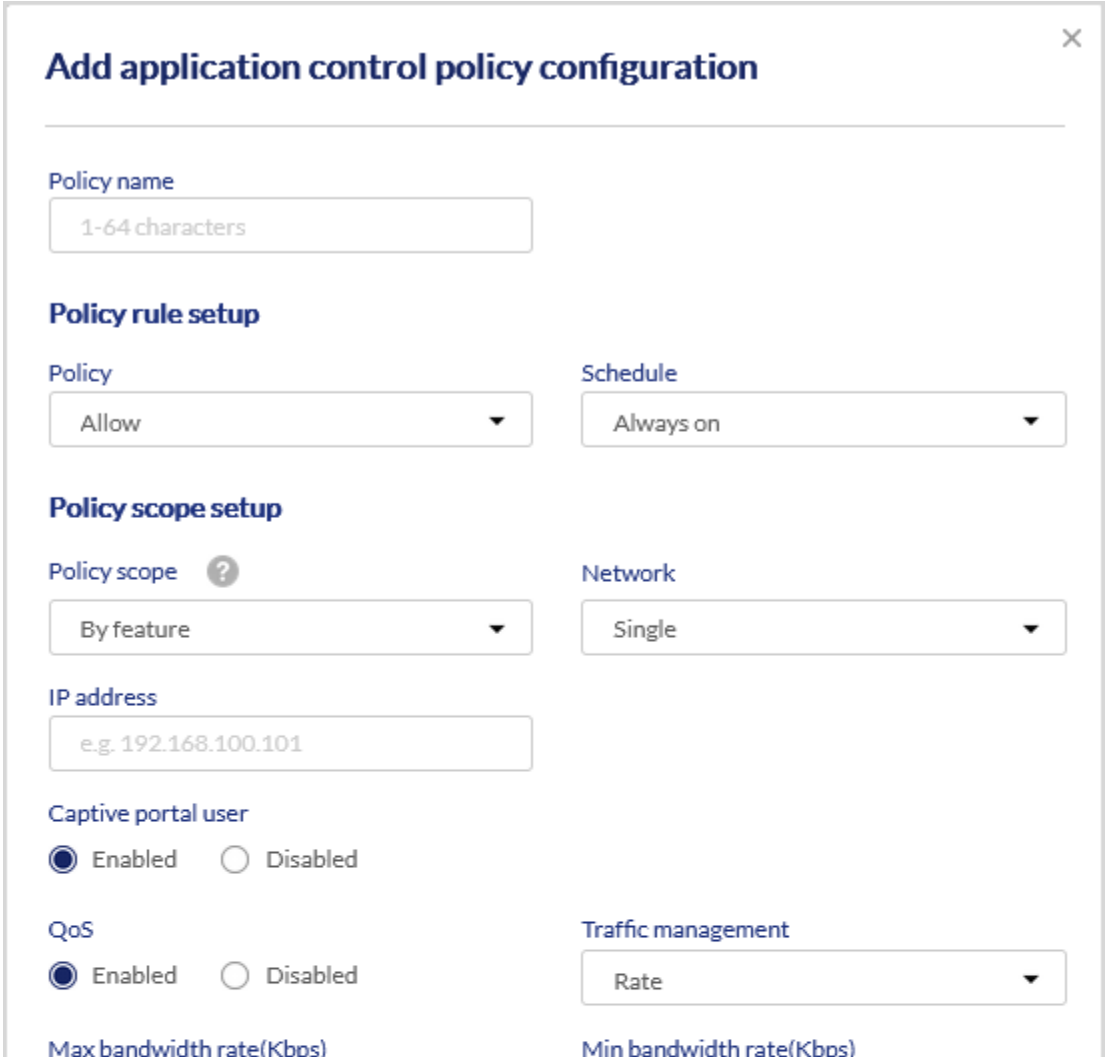


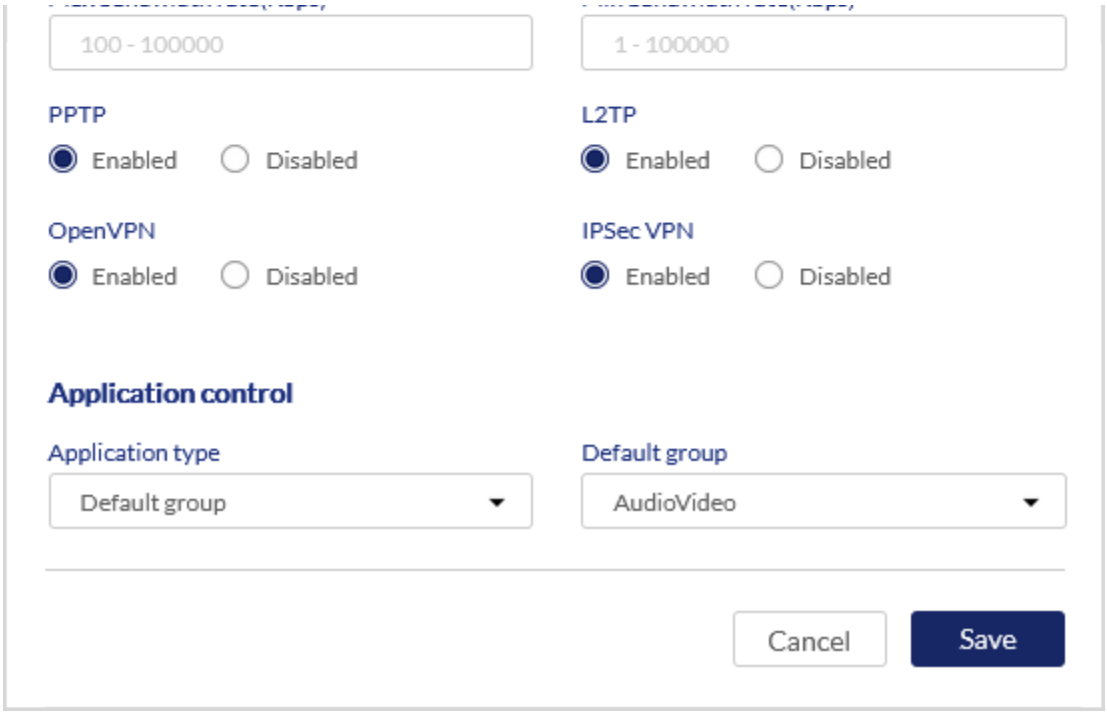
Les champs affichés dans le*Liste de contrôle des applications*sont les suivants:

Champ	Description
Nom	Il affiche le nom de la stratégie.
Politique	Il affiche la règle de la stratégie.
Calendrier	Il affiche le calendrier de votre police.
Portée	Il affiche la portée de la politique, c'est-à-dire si la politique est*Mondial*ou*Par fonctionnalité*.
Application	Il affiche le type d'application : groupe par défaut, application unique ou groupe personnalisé.
Actif	Vous pouvez activer ou désactiver la stratégie sélectionnée. ***Note**: Vous pouvez modifier ce champ uniquement lorsque l'option « Utiliser la configuration du profil » est désactivée.*
Actions	Vous pouvez modifier ou supprimer la stratégie sélectionnée. ***Note**: Ce champ est disponible uniquement lorsque l'option « Utiliser la configuration du profil » est désactivée.*

Cliquez sur**Ajouter**pour ajouter une nouvelle stratégie. Cela ouvre le*Ajouter la configuration de la stratégie de contrôle des applications*page. Pour supprimer plusieurs entrées, cochez les cases des stratégies de contrôle des applications que vous souhaitez supprimer, puis cliquez sur**Supprimer**.

***Note**: Le**Ajouter**et**Supprimer**les boutons situés au-dessus du tableau ne sont disponibles que lorsque le champ « Utiliser la configuration du profil » est désactivé.*





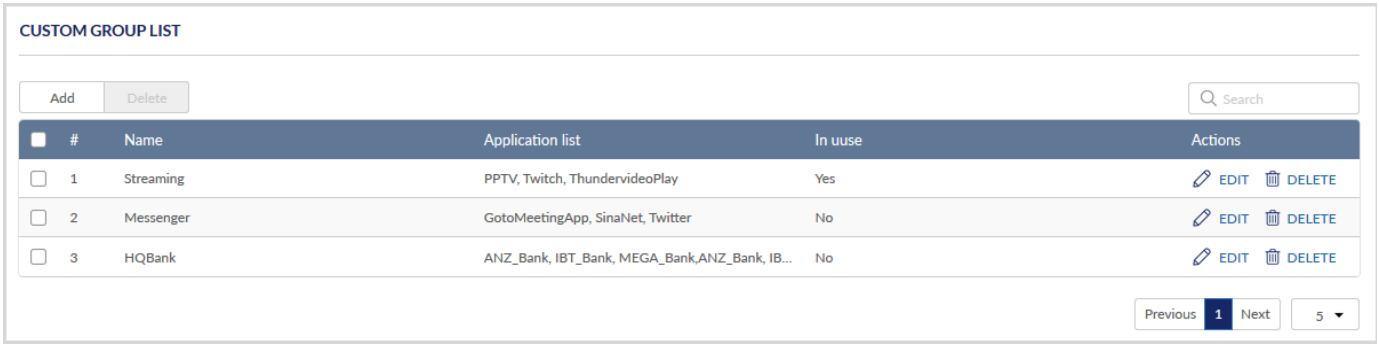
Les champs disponibles sur le*Ajouter la configuration de la stratégie de contrôle des applications*page sont les suivantes :

Champ	Description
Nom de la politique	Entrez un nom pour identifier la stratégie.
Configuration des règles de stratégie	
Politique	Sélectionnez la règle de stratégie. Cela pourrait être soit*permettre*ou*bloc*.
Calendrier	Il vous permet de définir un calendrier lorsque vous souhaitez appliquer la politique. Pour configurer un nouvel horaire, reportez-vous auPolitiques de planificationsection.
Configuration de la portée de la stratégie	
Portée de la politique	Sélectionnez soit*Mondial*ou*Par fonctionnalité*comme le champ d'application de la politique. La politique globale affecte tous les types de trafic correspondant à la ou aux applications sélectionnées. Si la*Par fonctionnalité*est sélectionné comme type de politique, les champs suivants seront disponibles.
Réseau	Sélectionnez l'un des réseaux suivants : • **Célibataire**: Si vous sélectionnez cette option, entrez l'adresse IP. • **Plage ip**: Si vous sélectionnez cette option, entrez l'adresse IP de début et l'adresse IP de fin. • **Interface**: Si vous sélectionnez cette option, sélectionnez l'interface dans la liste déroulante.
adresse IP	Entrez l'adresse IP. Ce champ est disponible lorsque le*Réseau*est**Célibataire**.
Adresse IP de départ	Saisissez l'adresse IP de départ de la plage IP. Ce champ est disponible lorsque le*Réseau*est**Plage ip**.
Adresse IP de fin	Saisissez l'adresse IP de fin de la plage IP. Ce champ est disponible lorsque le*Réseau*est**Plage ip**.
Interface	Sélectionnez l'interface dans la liste déroulante. Ce champ est disponible lorsque le*Réseau*est**Interface**.
Utilisateur du portail captif	Activez ou désactivez l'option Portail captif. L'activation de cette option permet à tous les clients du portail captif de suivre cette politique.
QoS	Activez ou désactivez l'option QoS pour sélectionner le débit de bande passante ou la priorité pour le trafic accédant via l'application sélectionnée.
Gestion du trafic	Sélectionner**Taux**ou**Priorité**pour le trafic accédant via l'application sélectionnée.

Priorité	Spécifiez la priorité comme*Faible*,*Moyen*, ou*Haut*.
Débit de bande passante maximum (Kbps)	Entrez le débit de bande passante maximum.
Débit de bande passante minimum (Kbps)	Entrez le débit de bande passante minimum.
PPTP	Activez ou désactivez le VPN PPTP. L'activation de cette option permet à tout le trafic PPTP de suivre cette politique.
L2TP	Activez ou désactivez le VPN L2TP. L'activation de cette option permet à tout le trafic L2TP de suivre cette politique.
OpenVPN	Activez ou désactivez OpenVPN. L'activation de cette option permet à tout le trafic OpenVPN de suivre cette politique.
VPN IPSec	Activez ou désactivez le VPN IPSec. L'activation de cette option permet à tout le trafic IPSec de suivre cette politique.
Contrôle des applications	
Type de demande	Sélectionnez le type d'application dans la liste déroulante. Les options sont Groupe par défaut, Application unique et Groupe personnalisé.
Catégorie	Ce champ est disponible lorsque vous sélectionnez l'option**Demande unique**comme le*Type de demande* . Sélectionnez la catégorie d'application dans la liste déroulante.
Application	Ce champ est disponible lorsque vous sélectionnez l'option**Demande unique**comme le*Type de demande*. Sélectionnez une application dans la liste déroulante disponible pour chaque catégorie.
Groupe par défaut	Ce champ est disponible lorsque vous sélectionnez**Groupe par défaut**comme le*Type de demande*.Sélectionnez un groupe par défaut dans la liste déroulante.
Groupe personnalisé	Ce champ est disponible lorsque vous sélectionnez le**Groupe personnalisé**comme le*Type de demande*. Sélectionnez le groupe configuré dans la liste déroulante. Si vous souhaitez créer un nouveau groupe, cliquez sur le**Ajouter un groupe personnalisé**bouton. Il vous redirigera vers le*Ajouter une configuration de groupe*page. Pour plus de détails, reportez-vous auListe de groupes personnalisée pour le contrôle des applicationssection.
Sauvegarder	Cliquez sur**Sauvegarder**pour enregistrer vos paramètres.
Annuler	Cliquez sur**Annuler**pour revenir aux paramètres précédents.

Liste de groupes personnalisée pour le contrôle des applications

Cette section permet de configurer des groupes et de leur associer des applications. Il affiche une liste des groupes configurés ainsi que la liste des applications qui leur sont associées.

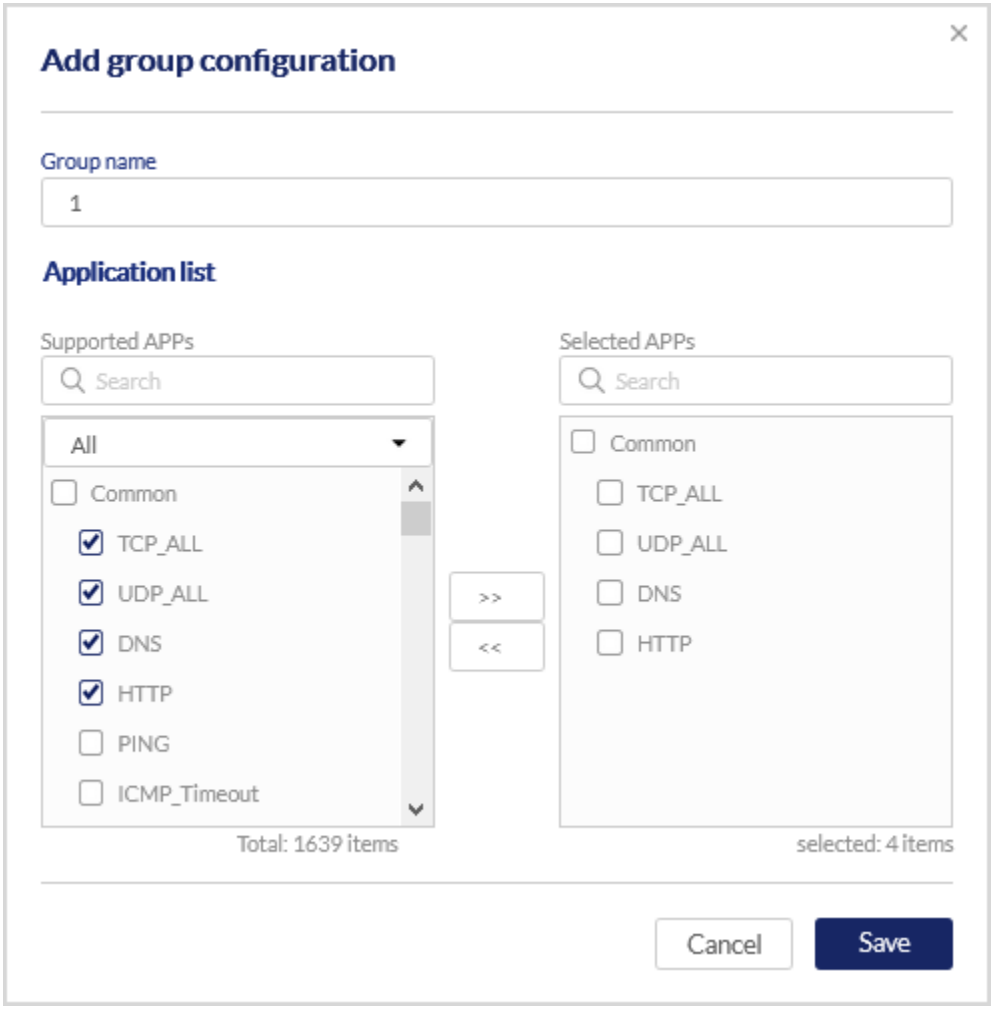


Les champs affichés dans le*Liste de groupes personnalisée*le tableau est le suivant :

Champ	Description
Nom	Il affiche le nom du groupe.
Liste des candidatures	Il affiche la liste des applications sélectionnées.
Utilisé	Il affiche l'état de l'application sélectionnée, c'est-à-dire si le groupe est utilisé ou non.
Actions	Vous pouvez modifier ou supprimer le groupe sélectionné. ***Note**: Ce champ est disponible uniquement lorsque le champ « Utiliser la configuration du profil » est désactivé.*

Cliquez sur**Ajouter**pour configurer un nouveau groupe. Cela ouvre le*Ajouter une configuration de groupe*page. Pour supprimer plusieurs groupes, cochez les cases correspondantes et cliquez sur**Supprimer**.

***Note:**Le**Ajouter**et**Supprimer**les boutons situés au-dessus du tableau ne sont disponibles que lorsque le champ « Utiliser la configuration du profil » est désactivé.*



Les champs disponibles sur le*Ajouter une configuration de groupe*page sont les suivantes :

Champ	Description
Nom de groupe	Entrez le nom du groupe. Il peut comporter de 1 à 64 caractères.
Liste des candidatures	Il comprend les deux cases suivantes : • **Applications prises en charge**: Il répertorie toutes les applications prises en charge par l'appareil. Cochez la case de l'application correspondante que vous souhaitez ajouter au groupe. Clique le **">>"**pour ajouter l'application à la liste des applications sélectionnées. • **Applications sélectionnées**: Il répertorie toutes les applications à ajouter au groupe. Cochez la case de l'application correspondante que vous souhaitez supprimer de la liste des applications sélectionnées. Clique le**« << »**pour supprimer l'application de la liste des applications sélectionnées.
Sauvegarder	Cliquez sur**Sauvegarder**pour enregistrer vos paramètres.
Annuler	Cliquez sur**Annuler**pour revenir aux paramètres précédents.

Chapitre 5VPN

Le VPN fournit un canal de communication sécurisé (« tunnel ») entre deux routeurs passerelles ou un client PC distant. La passerelle cloud Nuclias prend en charge les types de tunnels suivants :

- VPN passerelle à passerelle : pour connecter deux ou plusieurs routeurs afin de sécuriser le trafic entre les sites distants.

- Client distant (tunnel VPN client-passerelle) : un client distant initie un tunnel VPN car l'adresse IP du client PC distant n'est pas connue à l'avance. La passerelle, dans ce cas, joue le rôle de répondeur.
- Client distant derrière un routeur NAT : le client possède une adresse IP dynamique et se trouve derrière un routeur NAT. Le
  Le client PC distant sur le routeur NAT initie un tunnel VPN car l'adresse IP du routeur NAT distant n'est pas connue à l'avance. Le port WAN de la passerelle fait office de répondeur.
- Tunnel serveur PPTP pour les connexions client PPTP Tunnel
- serveur L2TP pour les connexions client L2TP Tunnel serveur
- OpenVPN pour les connexions client OpenVPN Tunnel GRE
-

Dans ce chapitre, vous apprendrez comment configurer les protocoles VPN pris en charge par la passerelle cloud.

Ce chapitre couvre les sujets suivants:

Site de Site VPN

Comme son nom l'indique, le VPN site à site est une technique qui permet la connectivité entre les bureaux situés à plusieurs endroits en mettant en place un tunnel IPSec sur Internet pour accéder à l'intranet. En bref, un VPN site à site crée un chemin sécurisé sur un chemin non sécurisé. La passerelle cloud Nuclias permet aux utilisateurs d'établir un tunnel VPN sans saisir manuellement les détails du point de terminaison du tunnel et les réseaux locaux/distants. Au lieu de cela, la passerelle cloud Nuclias conserve ces détails et les utilisateurs sélectionnent les réseaux en fonction de leurs besoins. La page VPN site à site comprend les deux sections suivantes :

1. Topologie VPN

La topologie VPN explique comment tous les clients et réseaux sont connectés via le tunnel IPSec. Le*VPN rapide*Le champ permet aux utilisateurs de créer des tunnels VPN entre les appareils DBG-2000 déployés dans la même organisation du cloud Nuclias. Il existe les trois modes suivants dans le*VPN rapide*champ:

- Désactiver (manuel)
- Site à site
- En étoile

Lorsque vous sélectionnez le mode Site-to-Site ou Hub-and-Spoke dans Quick VPN, chaque appareil DBG-2000 participant exécute automatiquement les fonctions suivantes :

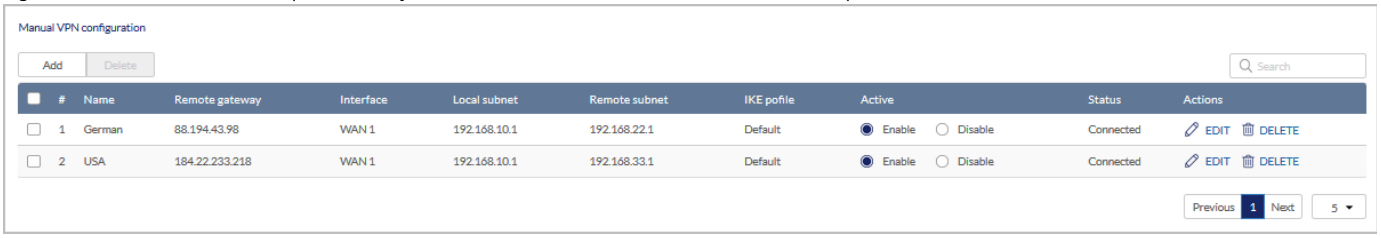
- Annonce ses sous-réseaux locaux qui participent au VPN Annonce
- ses adresses IP WAN sur les ports WAN disponibles Applique la
- table de routage VPN globale
- Applique la configuration nécessaire à l'établissement du tunnel VPN et au cryptage du trafic

Le résultat net est une solution VPN site à site automatique qui se configure en un seul clic.

2. Paramètres VPN

Désactiver (manuel)

Lorsque vous sélectionnez*Désactiver (manuel)*En mode VPN, DBG-2000 ne participe pas à la connexion VPN de site à site ou en étoile, et l'utilisateur ne pourra pas rejoindre automatiquement la connexion VPN de site à site ou en étoile. Au lieu de cela, l'utilisateur peut le configurer manuellement dans le*Configuration VPN manuelle*section et créez des tunnels VPN IPSec. Ce mode est utile lorsque vous essayez d'établir un tunnel entre deux appareils DBG-2000 déployés dans différentes organisations cloud Nuclias ou lorsque vous essayez d'établir un tunnel entre DBG-2000 et/ou avec une passerelle tierce.

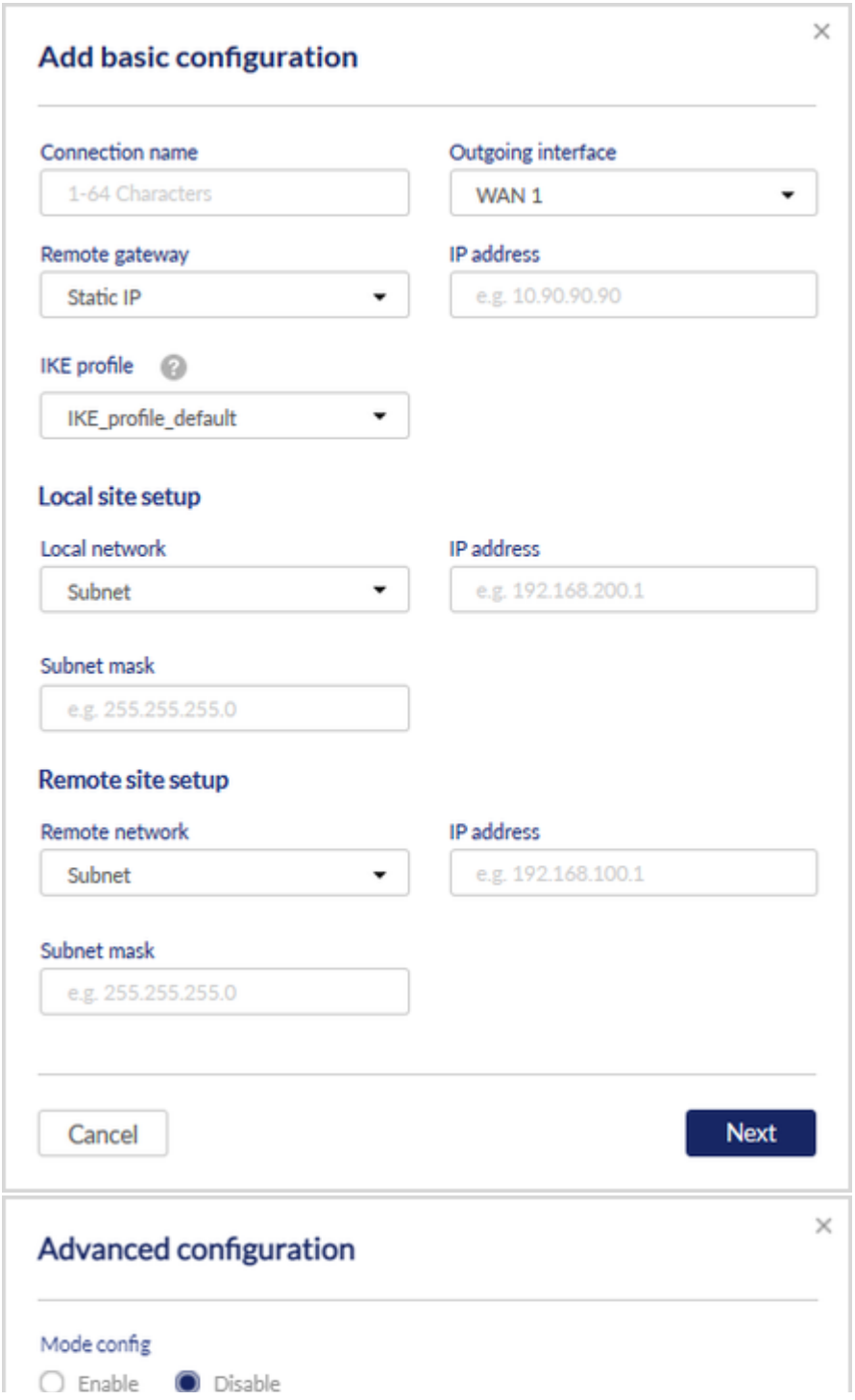


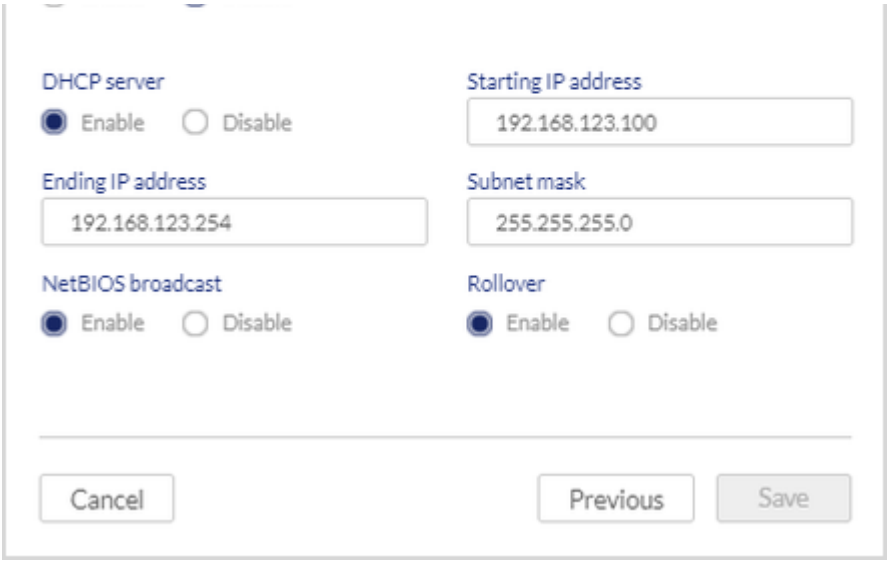
Les champs disponibles dans le*Configuration manuelle du VPN*le tableau est le suivant :

Champ	Description
Nom	Il affiche le nom du VPN.
Passerelle distante	Il affiche l'adresse IP distante sur laquelle le tunnel VPN est établi.

Interface	Il affiche l'interface utilisée pour la connexion VPN.
Sous-réseau local	Il affiche le sous-réseau local utilisé par cette connexion VPN.
Sous-réseau distant	Il affiche le sous-réseau distant utilisé par cette connexion VPN.
Profil IKE	Il affiche le profil IKE sélectionné pour la connexion VPN configurée.
Actif	Vous pouvez activer ou désactiver la connexion.
Statut	Il affiche si la connexion VPN est connectée ou déconnectée.
Actions	Vous pouvez modifier ou supprimer la configuration existante.

Cliquez sur**Ajouter**pour ajouter une nouvelle configuration VPN. Cela ouvre le*Ajouter une configuration de base*page. Pour supprimer une ou plusieurs entrées, cochez les cases correspondantes, puis cliquez sur**Supprimer**.





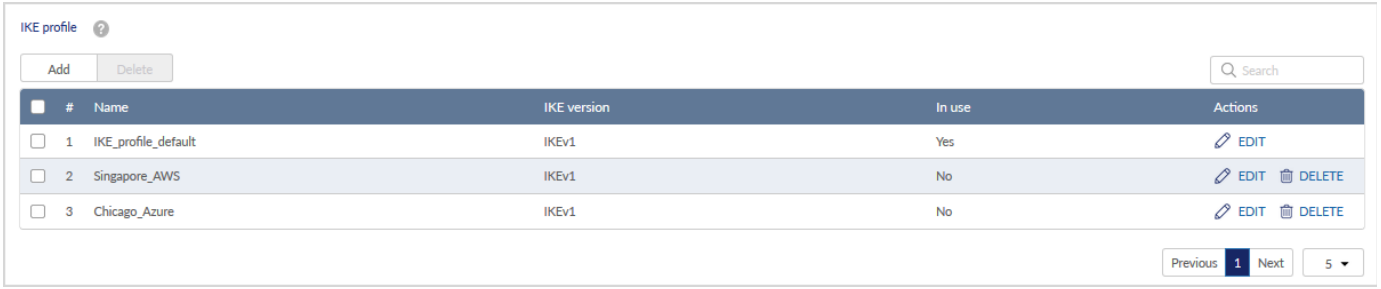
Les champs disponibles sur le*Ajouter une configuration de base*et*Configuration avancée*les pages sont les suivantes :

Champ	Description
Nom de la connexion	Saisissez un nom descriptif pour la connexion VPN.
Interface sortante	Spécifiez l'interface à utiliser pour les données sortantes.
Passerelle distante	Sélectionnez la passerelle que vous souhaitez utiliser pour la connexion. Les options sont*I.P statique*et*Nom de domaine complet*.
adresse IP	Si vous sélectionnez*I.P statique*comme passerelle distante, entrez l'adresse IP.
Nom de domaine	Si vous sélectionnez*Nom de domaine complet*comme passerelle distante, entrez le nom de domaine.
Profil IKE	Sélectionnez l'un des profils IKE configurés dans la liste déroulante.
Configuration du site local	
Réseau local	Sélectionnez le type d'accès réseau que vous souhaitez fournir via le tunnel IPSec. • **N'importe lequel** : il spécifie que la politique s'applique à tout trafic provenant du point de terminaison local donné. • **IP unique** : Il limite la politique à un seul hôte. Saisissez l'adresse IP de l'hôte qui fera partie du VPN. • **Sous-réseau**: Il permet à un sous-réseau entier de se connecter au VPN. Entrez l'adresse réseau et le masque de sous-réseau dans les champs fournis.
adresse IP	Entrez l'adresse IP pour vous connecter au VPN.
Masque de sous-réseau	Saisissez le masque de sous-réseau pour l'adresse réseau.
Configuration du site distant	
Réseau distant	Sélectionnez le type d'accès réseau que vous souhaitez fournir via le tunnel IPSec. • **N'importe lequel** : il spécifie que la stratégie s'applique à tout trafic provenant du point de terminaison distant donné. • **IP unique** : Il limite la politique à un seul hôte. Saisissez l'adresse IP de l'hôte qui fera partie du VPN. • **Sous-réseau**: Il permet à un sous-réseau entier de se connecter au VPN. Entrez l'adresse réseau et le masque de sous-réseau dans les champs fournis.
adresse IP	Entrez l'adresse IP pour vous connecter au VPN.
Masque de sous-réseau	Saisissez le masque de sous-réseau pour l'adresse réseau.
Suivant	Cliquez sur**Suivant**pour aller à la*Configuration avancée*page.
Configuration avancée	
Configuration des modes	

	Le mode Config est similaire à DHCP et est utilisé pour attribuer des adresses IP aux clients VPN distants. Vous pouvez activer ou désactiver cette fonctionnalité.
Mode tunnel	Sélectionnez soit *Tunnel complet* ou *Tunnel divisé*. • Tunnel complet : il fournit un accès client VPN à tous les services intranet et Internet. • Split Tunnel : il fournit un accès client VPN à tous les services intranet.
Adresse IP de départ	Saisissez l'adresse IP de départ de la plage IP attribuée aux clients VPN.
Adresse IP de fin	Entrez l'adresse IP de fin de la plage IP attribuée aux clients VPN.
DNS primaire	Saisissez l'adresse IP du DNS principal.
DNS secondaire (facultatif)	Saisissez l'adresse IP du DNS secondaire. C'est un champ facultatif.
Serveur DHCP	Activez-le pour permettre aux clients VPN connectés à votre routeur via IPsec de recevoir une adresse IP attribuée via DHCP.
Adresse IP de départ	Saisissez la première adresse IP de la plage IP DHCP.
Adresse IP de fin	Saisissez la dernière adresse IP de la plage IP DHCP.
Masque de sous-réseau	Entrez le masque de sous-réseau pour la plage IP.
Diffusion NetBIOS	Activez-le pour permettre à la diffusion NetBIOS de circuler via le tunnel VPN.
Rouler sur	Pour activer un rollover VPN, vous devez disposer du *Mode réseau étendu* mis à **Rouler sur**.
Précédent	Cliquez sur **Précédent** pour aller à la *Ajouter une configuration de base* page.
Sauvegarder	Cliquez sur **Sauvegarder** pour enregistrer vos paramètres.
Annuler	Cliquez sur **Annuler** pour revenir aux paramètres précédents.

Profil IKE

Le profil IKE est la configuration centrale d'IPSec qui définit la plupart des paramètres IPSec tels que le protocole, les algorithmes, la durée de vie de SA et le protocole de gestion des clés. De plus, il contient des informations relatives aux algorithmes tels que le cryptage, l'authentification et le groupe DH pour les négociations des phases I et II. Cette section répertorie tous les profils IKE configurés.



Les champs affichés sur le *Profil IKE* le tableau est le suivant :

Champ	Description
Nom	Il affiche le nom du profil IKE configuré.
Version IKE	Il affiche la version d'IKE qui a été utilisée.
Utilisé	Il indique si le profil IKE configuré est utilisé ou non.
Actions	Vous pouvez modifier ou supprimer le profil IKE sélectionné. *Remarque : Vous ne pouvez pas supprimer le profil IKE par défaut.*

Cliquez sur **Ajouter** pour ajouter une nouvelle entrée à la liste. Cela ouvre le *Ajouter des profils IKE* page. Pour supprimer plusieurs entrées, cochez les cases des profils IKE que vous souhaitez supprimer, puis cliquez sur **Supprimer**.

Profile name
1-64 Characters

IKE version
IKEv1 IKEv2

IKE phase-1 settings

Exchange mode
Main

Local identifer type
Local WAN IP

Remote identifer type
Remote WAN IP

DH group
Group 2 (1024 bit)

Encryption algorithm
Multiple select

Authentication algorithm
SHA-1

SA lifetime (sec.)
28800

Authentication method
Pre-shared key

Pre-shared key
••••••••

Dead peer detection
Enable Disable

Detection interval
10

Reconnect after failure
3

VPN tunnel backup
Enable Disable

Backup tunnel

Failure time to primary (seconds)
30

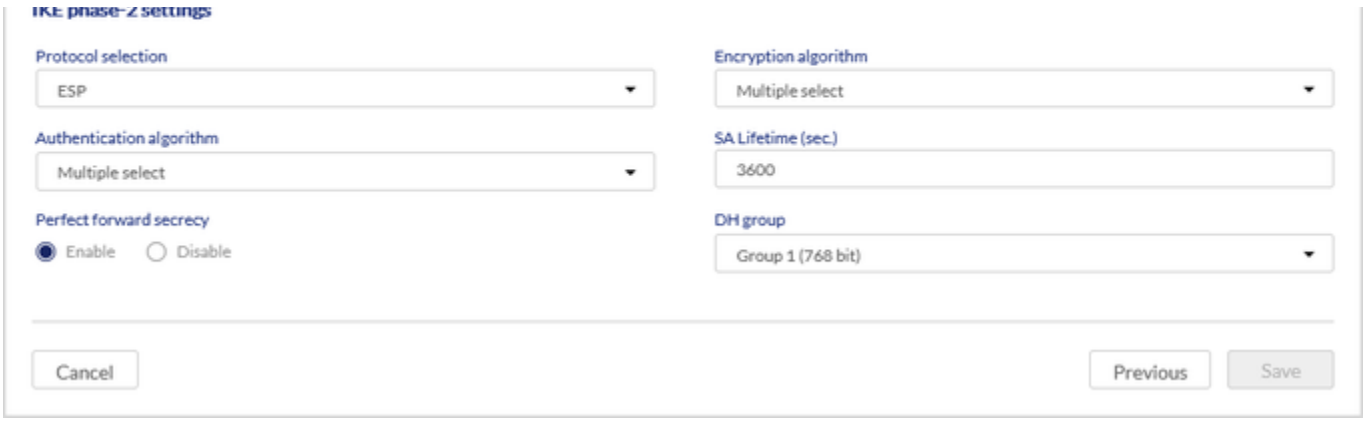
Extended authentication
Enable Disable

Extended authentication type
Local authentication

Local authentication
cp

Cancel Next

Add IKE profile



Les champs disponibles sur le*Ajouter des profils IKE*La page 1 et la page 2 sont les suivantes :

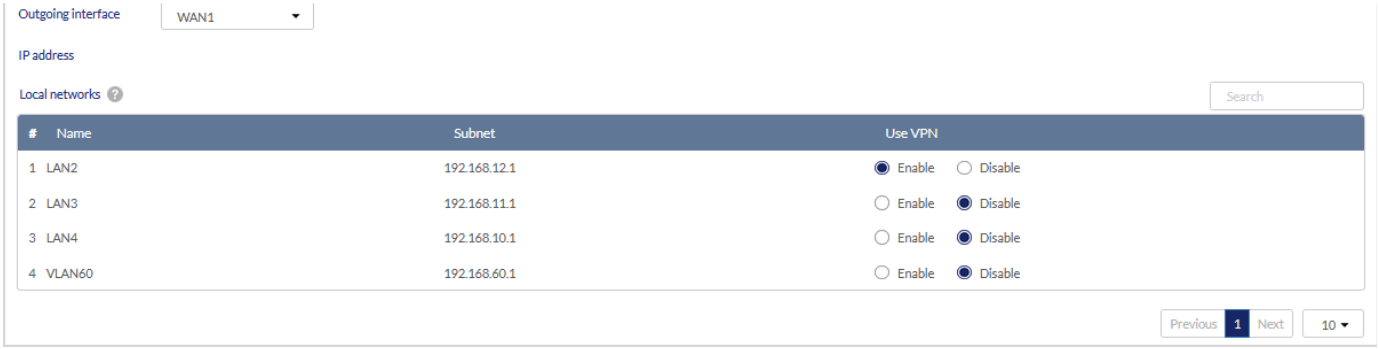
Champ	Description
Nom de profil	Entrez un nom unique pour le profil IKE.
Version IKE	Sélectionnez la version d'IKE.
Paramètres IKE phase 1	
Mode d'échange	Sélectionnez le mode d'échange :*Principal*ou*Agressif*.
Type d'identifiant local	Sélectionnez le type d'identifiant local. Les options sont Local WAN IP, FQDN et User-FQDN. Si vous sélectionnez **Nom de domaine complet de l'utilisateur**, saisissez le nom FQDN dans le champ*Identifiant local*champ. Lorsque vous sélectionnez **IP WAN locale**ou**Nom de domaine complet**, il utilise l'adresse IP locale de l'interface WAN et le nom FQDN du WAN configuré sur leDNS dynamiquepage.
Type d'identifiant distant	Sélectionnez le type d'identifiant distant. Les options sont IP WAN distant, FQDN et User-FQDN. Si vous sélectionnez**Nom de domaine complet**ou**Nom de domaine complet de l'utilisateur**, saisissez le nom FQDN dans le champ*Identifiant distant* champ. Lorsque vous sélectionnez**IP WAN distant**, il utilise l'adresse IP distante saisie dans la politique VPN.
Groupe DH	Sélectionnez le DH (**Diffie-Hellman**) groupe. Il définit la force de la clé utilisée dans le processus d'échange de clés.
Algorithme de cryptage	Sélectionnez l'algorithme de cryptage à suivre lors de l'échange de clés. Vous pouvez sélectionner plusieurs algorithmes.
Algorithme d'authentification	Sélectionnez l'algorithme d'authentification dans la liste déroulante. Vous pouvez sélectionner plusieurs algorithmes.
Durée de vie SA (sec.)	Il fait référence à la durée de vie de l'association de sécurité et la plage varie de 300 à 604 800 secondes.
Méthode d'authentification	Sélectionnez la méthode d'authentification. Les options sont la clé pré-partagée et la signature RSA (certificat).
Clé Pré-Partagée	Entrez la clé pré-partagée. Ce champ est disponible uniquement lorsque vous sélectionnez le**Clé Pré-Partagée** comme le *Méthode d'authentification*.
Certificat	Sélectionnez le certificat à utiliser pour l'authentification. Ce champ est disponible uniquement lorsque vous sélectionnez**Signature RSA (Certificat)**comme le*Méthode d'authentification*.
Détection des pairs morts	Vous pouvez activer ou désactiver le*Détection des pairs morts*fonctionnalité. S'il est activé, il vous permet de détecter si le homologue distant est accessible ou non. S'il n'est pas accessible, cette fonctionnalité fera descendre le tunnel.
Intervalle de détection	Entrez l'intervalle auquel vous souhaitez envoyer des paquets de détection d'homologue à l'homologue pour vérifier sa vivacité.
Se reconnecter après un échec	Il s'agit du nombre d'échecs, après quoi l'autre homologue est considéré comme étant en panne. Entrez le nombre d'échecs.
Sauvegarde du tunnel VPN	Vous pouvez activer ou désactiver le*Sauvegarde du tunnel VPN*fonctionnalité.
Tunnel de sauvegarde	

	Si*Sauvegarde du tunnel VPN*est activé, vous pouvez utiliser la sauvegarde VPN du profil sélectionné si le tunnel principal est en panne. Lorsque le tunnel principal est actif, le tunnel de sauvegarde sera désactivé.
Temps de défaillance vers le primaire (secondes)	Spécifiez le délai après lequel le tunnel de sauvegarde sera indisponible.
Authentification étendue	Activez ou désactivez la fonctionnalité d'authentification étendue.
Type d'authentification étendu	Sélectionnez le type d'authentification que vous souhaitez utiliser. Les options sont Authentification locale, Serveur d'authentification et Hôte IPSec (Initiateur).
Serveur d'authentification	Sélectionnez l'un des serveurs d'authentification externes dans la liste déroulante, puis sélectionnez le serveur correspondant.
Nom d'utilisateur	Entrez le nom d'utilisateur. Ce champ est disponible lorsque vous sélectionnez le**Hôte IPSec (initiateur)**comme le*Type d'authentification étendu*. La longueur du nom d'utilisateur peut varier de 1 à 64 caractères.
Mot de passe	Entrer le mot de passe. Ce champ est disponible lorsque vous sélectionnez le**Hôte IPSec (initiateur)** comme le*Type d'authentification étendu*. La longueur du mot de passe peut varier de 8 à 63 caractères.
Authentification locale	Vous pouvez sélectionner l'une des authentifications enregistrées sur le serveur local. Ce champ est disponible lorsque vous sélectionnez**Authentification locale**comme le*Type d'authentification étendu*.
Suivant	Cliquez sur**Suivant**pour accéder à la page IKE Phase-2.
Paramètres IKE phase 2	
Sélection du protocole	Sélectionnez le protocole pour IKE phase-2.
Algorithme de cryptage	Sélectionnez l'algorithme de cryptage à utiliser. Vous pouvez sélectionner plusieurs algorithmes.
Algorithme d'authentification	Sélectionnez l'algorithme d'authentification dans la liste déroulante. Vous pouvez sélectionner plusieurs algorithmes.
Durée de vie SA (sec.)	Il fait référence à la durée de vie de l'association de sécurité et la plage varie de 300 à 604 800 secondes.
Secret de transfert parfait	S'il est activé, il ne permet pas de générer la même clé, obligeant l'utilisateur à utiliser un nouvel échange de clé DH.
Groupe DH	Sélectionnez le groupe DH.
Précédent	Cliquez sur**Précédent**pour aller à la*Paramètres IKE Phase-1*page.
Sauvegarder	Cliquez sur**Sauvegarder**pour enregistrer vos paramètres.
Annuler	Cliquez sur**Annuler**pour revenir aux paramètres précédents.

Site à site

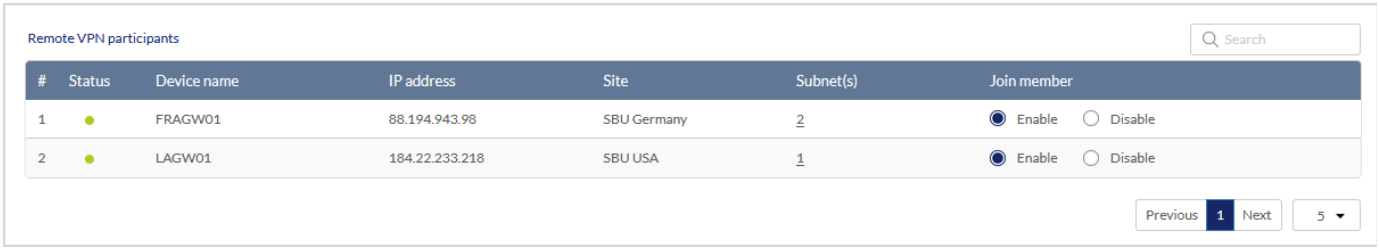
Le VPN site à site établit le tunnel IPsec passerelle à passerelle avec d'autres appareils DBG-2000 enregistrés sur le même site ou sur des sites différents de la même organisation. Une fois qu'un utilisateur sélectionne le type de VPN rapide Site à site, tous les autres participants DBG-2000 avec le même mode VPN rapide sont répertoriés. Pour établir un tunnel avec un périphérique distant particulier, activez l'option*Rejoindre un membre*champ. Une fois la configuration du tunnel transmise aux homologues distants, le trafic est initié par l'utilisateur et un tunnel est établi entre les homologues distants.

Dans le*Réseaux locaux*, si vous avez plusieurs sous-réseaux, vous pouvez spécifier quel sous-réseau participe au VPN, c'est-à-dire que le trafic du sous-réseau activé sera crypté par le VPN IPSec. Tous les sous-réseaux locaux doivent être uniques au sein de la topologie VPN.



Les champs affichés dans le*Réseaux locaux*le tableau est le suivant :

Champ	Description
Interface sortante	C'est l'interface WAN sur laquelle le tunnel sera établi.
adresse IP	Il affiche l'adresse IP WAN actuelle de l'appareil.
Nom	Il affiche le nom de l'interface LAN/VLAN du sous-réseau local.
Sous-réseau	Il affiche l'adresse IP du sous-réseau.
Utiliser un VPN	Activez le sous-réseau si vous souhaitez chiffrer son trafic par VPN IPSec.



Le*Participants VPN à distance*Le tableau répertorie tous les VPN distants et affiche les champs suivants :

Champ	Description
Statut	Il indique l'état de l'appareil distant, qu'il soit en ligne ou hors ligne. La couleur verte indique qu'il est en ligne et la couleur rouge indique qu'il est hors ligne.
Nom de l'appareil	Il affiche le nom de l'appareil distant avec lequel la connexion VPN est établie.
adresse IP	Il affiche l'adresse IP WAN des périphériques de passerelle distante.
Site	Il affiche le site des périphériques de passerelle distante.
Sous-réseau(s)	Il affiche les sous-réseaux des périphériques de passerelle distante. Il s'agit d'un lien hypertexte ; si vous passez votre souris dessus, vous pouvez afficher le sous-réseau et le masque de sous-réseau du périphérique distant.
Rejoindre un membre	Si cette option est activée, la configuration du tunnel nécessaire pour établir un tunnel est transmise aux homologues distants.

En étoile

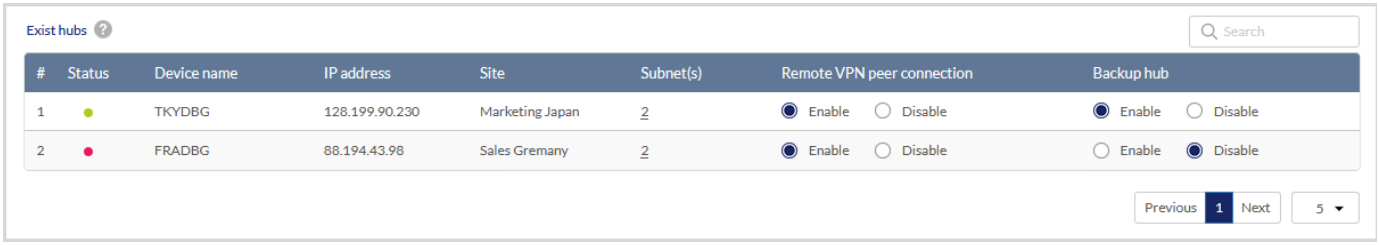
Les connexions VPN site à site entre les appareils DBG-2000 seront automatiquement établies entre tous les homologues activés site à site dans la même organisation. Cependant, cela est souvent indésirable car de telles connexions peuvent établir des tunnels IPSec inutiles entre des sites distants et créer une surcharge réseau dégradant les performances. Par conséquent, il est préférable de configurer Hub and Spoke dans de tels cas, ce qui désigne un périphérique DBG-2000 comme périphérique**Moyeu**et tous les sites distants comme le**Parlait**. De plus, le mode Hub-and-Spoke peut être utile dans les organisations où plusieurs sites auxiliaires nécessitent une connexion au siège.

Il existe deux options pour configurer le DBG-2000 en mode Hub-and-Spoke :

1. **Moyeu (maille)**: L'appareil DBG-2000 établira des tunnels VPN vers tous les homologues VPN distants également configurés dans ce mode. Si un autre DBG-2000 dans la même organisation est configuré comme hub, il peut être ajouté en tant que**Hub existant**. Si un appareil DBG-2000 est sélectionné comme

HUB, il sera annoncé sur la page SITE-SITE VPN de tous les appareils restants si le *Type de VPN rapide* est sélectionné comme Hub-and-Spoke. Si d'autres périphériques HUB existent dans l'organisation, ils seront affichés en tant que Hubs existants. Les utilisateurs peuvent utiliser ces HUB existants pour former un tunnel de site en activant *Connexion homologue VPN à distance*, ou ils peuvent l'utiliser comme hub de sauvegarde en activant le *Centre de sauvegarde* champ.

Lorsque vous sélectionnez **Moyeu** en tant que type Hub-and-Spoke, il répertorie les hubs existants.



Les champs affichés dans le *Il existe des hubs* le tableau est le suivant :

Champ	Description
Statut	Il affiche l'état actuel des périphériques hub distants, qu'ils soient en ligne ou hors ligne. La couleur verte indique qu'il est en ligne et la couleur rouge indique qu'il est hors ligne.
Nom de l'appareil	Il affiche le nom des appareils distants qui ont le type Quick VPN comme **En étoile** et le rôle de **MOYEU**.
adresse IP	Il affiche l'adresse IP WAN des périphériques de passerelle distante.
Site	Il affiche le nom du site des appareils « Exist Hub ».
Sous-réseau(s)	Il affiche le sous-réseau des appareils distants. Il s'agit d'un lien hypertexte ; si vous passez votre souris dessus, vous pouvez afficher le sous-réseau et le masque de sous-réseau du périphérique distant.
Connexion homologue VPN à distance	Vous pouvez activer ou désactiver un tunnel de site à site vers le hub existant.
Centre de sauvegarde	Vous pouvez sélectionner l'autre hub comme hub de sauvegarde pour le hub actuel.

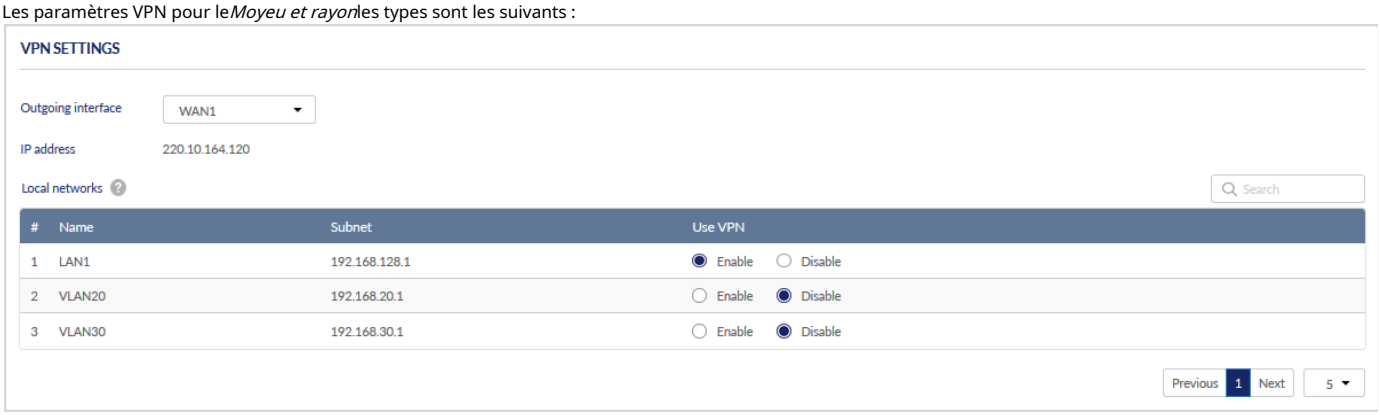
2. **Parlait:** Le périphérique DBG-2000 (Spoke) établit des tunnels directs uniquement vers les périphériques DBG-2000 distants spécifiés en tant que hubs. Lorsqu'un périphérique DBG-2000 est configuré en tant que Spoke, vous pouvez configurer plusieurs hubs VPN pour ce DBG-2000. Dans cette configuration, le Spoke DBG-2000 envoie tout le trafic de site à site vers ses hubs VPN configurés. Les rayons n'échangent pas de données directement entre eux.

Si vous sélectionnez le *Type en moyeu et rayons* comme **Parlait**, il affiche une liste de tous les hubs existants sous le *Topologie VPN* section. De plus, il répertorie les périphériques hub Exist disponibles avec une option de *Centre principal*. Si vous activez le *Centre principal* champ, le hub sélectionné sera le hub principal du satellite et pourra communiquer avec tous les périphériques satellite liés à ce hub. À la fois, vous ne pouvez activer qu'un seul hub principal à la fois.

Les champs affichés dans le *Il existe des hubs* le tableau est le suivant :

Champ	Description
Statut	Il affiche l'état des hubs existants disponibles. Si le hub est en ligne, un point vert s'affiche et si le hub est hors ligne, un point rouge s'affiche.
Nom de l'appareil	Il affiche le nom du périphérique hub avec lequel nous souhaitons établir le tunnel.
adresse IP	Il affiche l'adresse IP WAN du hub avec lequel le tunnel sera établi.
Site	Il fait référence au nom du site configuré pour identifier le périphérique hub.
Sous-réseau(s)	Il affiche le nombre de réseaux locaux/privés partagés par les appareils distants. Il s'agit d'un hyperlien ; si vous passez votre souris dessus, vous pouvez afficher le sous-réseau et le masque de sous-réseau du périphérique distant.
Centre principal	Activez cette option pour le sélectionner comme hub principal pour le périphérique de configuration.

Les paramètres VPN pour le*Moyeu et rayon*les types sont les suivants :



Les champs disponibles sur le*Paramètres VPN*La section pour le VPN Hub and Spoke est la suivante :

Champ	Description
Interface sortante	C'est l'interface WAN sur laquelle l'utilisateur souhaite établir un tunnel.
adresse IP	Il affiche l'adresse IP WAN actuelle de l'appareil.
Réseaux locaux	
Nom	Il affiche le nom de l'interface LAN/VLAN du sous-réseau local.
Sous-réseau	Il affiche le sous-réseau de l'interface ci-dessus.
Utiliser un VPN	Tu peux**activer**ou**désactiver**la fonctionnalité Utiliser VPN. Lorsqu'il est activé, les sous-réseaux sont sélectionnés pour les sélecteurs de trafic local pour la politique VPN.

PPTP/L2TP

Mode serveur

La passerelle cloud Nuclias peut établir un VPN PPTP/L2TP. Une fois activé, un serveur PPTP/L2TP est disponible sur la passerelle pour que les utilisateurs des clients PPTP/L2TP LAN et WAN puissent y accéder, c'est-à-dire que les clients PPTP/L2TP peuvent atteindre le serveur PPTP/L2TP de la passerelle. De plus, une fois authentifiés par le serveur PPTP/L2TP (point final du tunnel), les clients PPTP/L2TP peuvent accéder au réseau LAN géré par la passerelle.

La plage d'adresses IP allouée aux clients PPTP/L2TP ne doit pas coïncider avec le sous-réseau LAN. De plus, le serveur PPTP/L2TP utilisera par défaut l'authentification utilisateur PPTP/L2TP locale, mais peut être configuré pour utiliser un serveur d'authentification RADIUS externe si celui-ci est configuré.

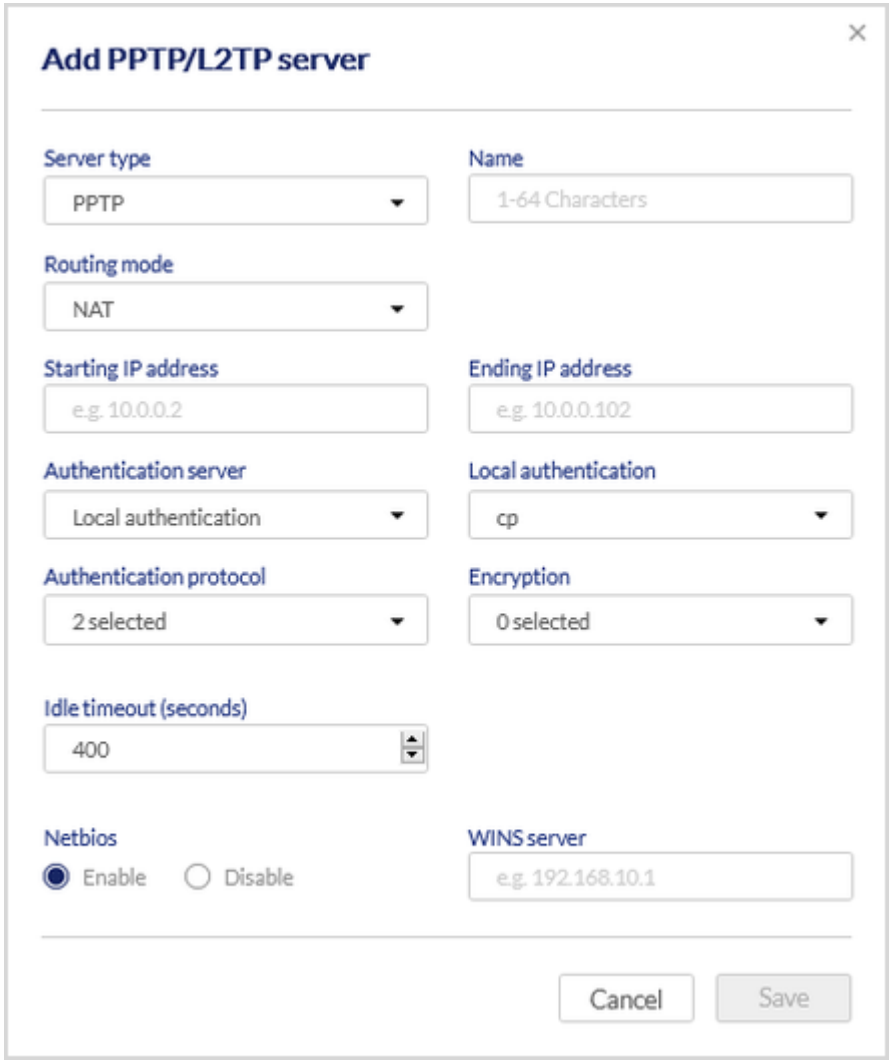
Les champs disponibles dans le*Mode serveur*le tableau est le suivant :

Champ	Description
Nom	Il affiche le nom du serveur PPTP/L2TP.
Type de serveur	Il affiche le type de serveur, c'est-à-dire PPTP ou L2TP.
L2TP sur IPsec	Il affiche si le*L2TP sur IPsec*est activé ou désactivé.
adresse IP	Il affiche la plage d'adresses IP allouée aux clients PPTP/L2TP.
Actif	Vous pouvez activer ou désactiver le serveur.

Actions	Vous pouvez modifier ou supprimer le serveur PPTP/L2TP configuré.

Cliquez sur**Ajouter**pour ajouter une nouvelle entrée à la liste. Cela ouvre le*Ajouter un serveur PPTP/L2TP*page. Pour supprimer une ou plusieurs entrées, cochez les cases correspondantes, puis cliquez sur**Supprimer**.

Ajout d'un serveur PPTP

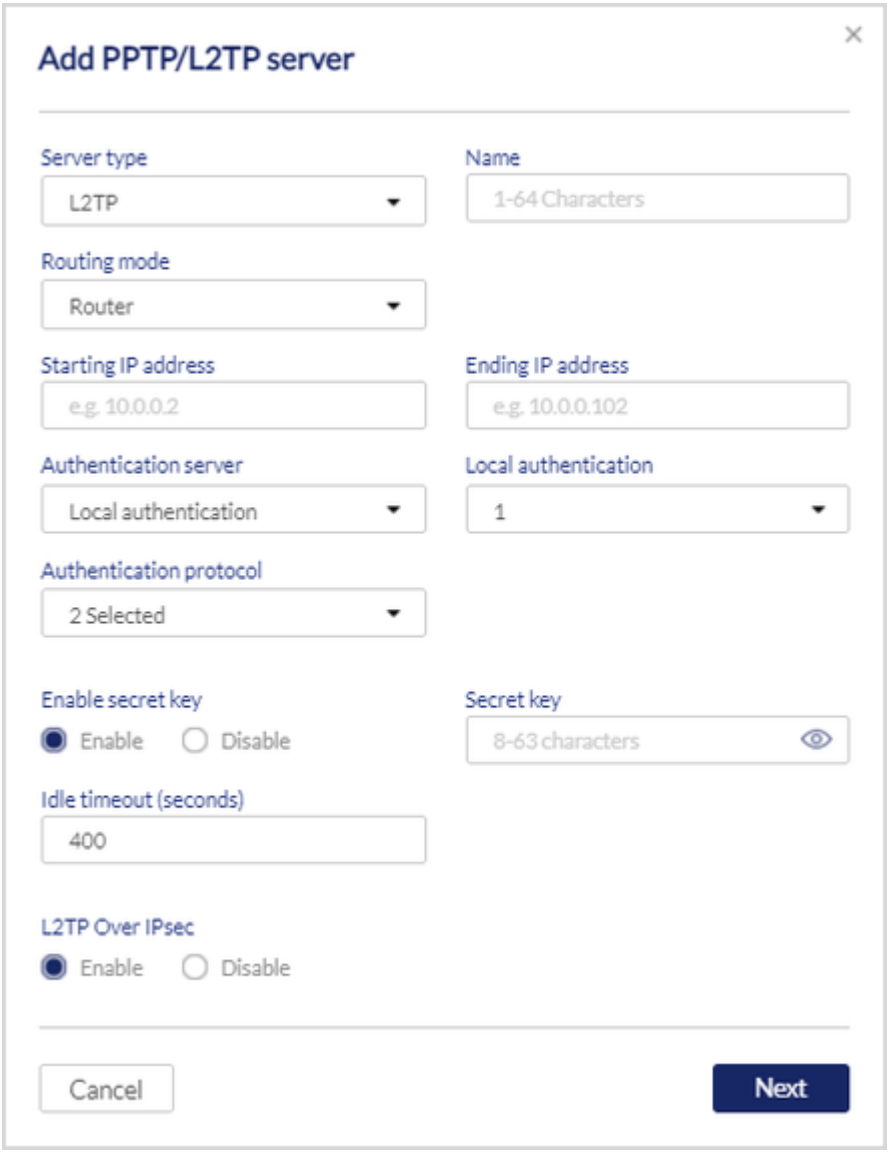


Les champs disponibles sur le*Ajouter un serveur PPTP/L2TP*page pour le**Serveur PPTP**type sont les suivants :

Champ	Description
Serveur PPTP	
Type de serveur	Sélectionner**PPTP**comme type de serveur.
Nom	Saisissez le nom du serveur PPTP.
Mode de routage	Sélectionnez le mode de routage, soit*NAT*ou*Routeur*.
Adresse IP de départ	Saisissez l'adresse IP de départ de la plage d'adresses IP à attribuer à vos clients PPTP.
Adresse IP de fin	Saisissez l'adresse IP de fin de la plage d'adresses IP à attribuer à vos clients PPTP.
Serveur d'authentification	Sélectionnez l'un des serveurs d'authentification disponibles. Les options sont*Authentification locale*, *RAYON*, et*Aucun*authentification.
Serveur RADIUS	Sélectionnez le serveur RADIUS. Il est disponible lorsque vous sélectionnez**Rayon**comme le*Serveur d'authentification*.
Authentification locale	Sélectionnez l'une des authentifications enregistrées sur le serveur local.

Protocole d'authentification	Sélectionnez un ou plusieurs types d'authentification dans la liste déroulante (*Tous/ BOUILLIE/ TYPE/ MS-CHAP/ MSCHAPv2*).
Chiffrement	Ce champ est disponible uniquement lorsque**MS-CHAP**ou**MS-CHAPv2**est sélectionné comme*Protocole d'authentification*. • **Tous**: Cochez la case pour sélectionner toutes les options de cryptage. • **Mppe 40 bits**: cochez la case pour activer le cryptage Mppe 40 bits. **MPPE** • **128 bits**: cochez la case pour activer le cryptage Mppe 128 bits. • **Mppe avec état**: cochez la case pour activer le chiffrement Stateful Mppe. Ce mode de cryptage Mppe est moins sécurisé et peut être utilisé pour des raisons de compatibilité.
Délai d'inactivité (secondes)	Entrez le temps en secondes après lequel la connexion sera déconnectée en cas d'inactivité.
Netbios	Activez-le pour permettre aux diffusions NetBIOS de circuler via le tunnel VPN.
Serveur WINS	Entrez l'adresse du serveur WINS pour Netbios. Ce champ est disponible lorsque vous activez Netbios.
Sauvegarder	Cliquez sur**Sauvegarder**pour enregistrer vos paramètres.
Annuler	Cliquez sur**Annuler**pour revenir aux paramètres précédents.

Ajout d'un serveur L2TP

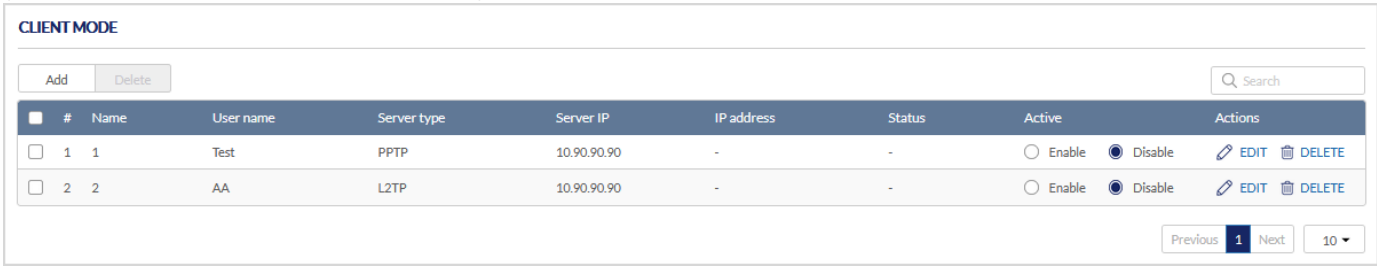


Les champs disponibles sur le*Ajouter un serveur PPTP/L2TP*page pour le**serveur L2TP**type sont les suivants :

Champ	Description
Serveur L2TP	
Type de serveur	Sélectionner**L2TP**comme type de serveur.
Nom	Saisissez le nom du serveur L2TP.
Mode de routage	Sélectionnez le mode de routage, soit*NAT*ou*Routeur*.
Adresse IP de départ	Saisissez l'adresse IP de départ de la plage d'adresses IP à attribuer à vos clients L2TP.
Adresse IP de fin	Saisissez l'adresse IP de fin de la plage d'adresses IP à attribuer à vos clients L2TP.
Serveur d'authentification	Sélectionnez le serveur d'authentification. Les options sont*Authentification locale*,*RAYON*, et*Aucun* authentification.
Authentification locale	Sélectionnez l'une des authentifications enregistrées sur le serveur local. Ce champ est disponible lorsque vous sélectionnez**Authentification locale**comme serveur d'authentification.
Serveur RADIUS	Sélectionnez le serveur Radius. Ce champ est disponible lorsque vous sélectionnez**Rayon**comme serveur d'authentification.
Protocole d'authentification	Sélectionnez n'importe quel type d'authentification dans le menu déroulant (*Tous*/ *BOUILLIE*/ *TYPE*/ *MS-CHAP*/ *MSCHAPv2*).
Chiffrement	Activez-le pour ajouter une clé secrète.
Activer la clé secrète	Si la*Chiffrement*est activé, entrez la clé secrète.
Délai d'inactivité (secondes)	Entrez la durée en secondes pendant laquelle la connexion se déconnectera en cas d'inactivité.
L2TP sur IPsec	Quand le*L2TP sur IPsec*configuration est activée, l'initiation du tunnel IPsec démarre automatiquement. Néanmoins, l'établissement du tunnel dépend de la configuration côté client et côté serveur et de la réponse du serveur. Cliquez sur**Suivant**pour configurer le*Profil IKE*pour IPsec. Pour plus de détails, reportez-vous àhttps://dlink-dbg.atlassian.net/wiki/spaces/CGD/pages /2687700/Site+to+Site+VPN#IKE-Profile.
Sauvegarder	Cliquez sur**Sauvegarder**pour enregistrer vos paramètres.
Annuler	Cliquez sur**Annuler**pour revenir aux paramètres précédents.

Mode client

La passerelle cloud Nuclias peut configurer le client VPN PPTP/L2TP. Grâce à ce client, nous pouvons accéder à un réseau distant local sur le serveur PPTP /L2TP. Une fois qu'un client est activé, il tentera de se connecter automatiquement au serveur.



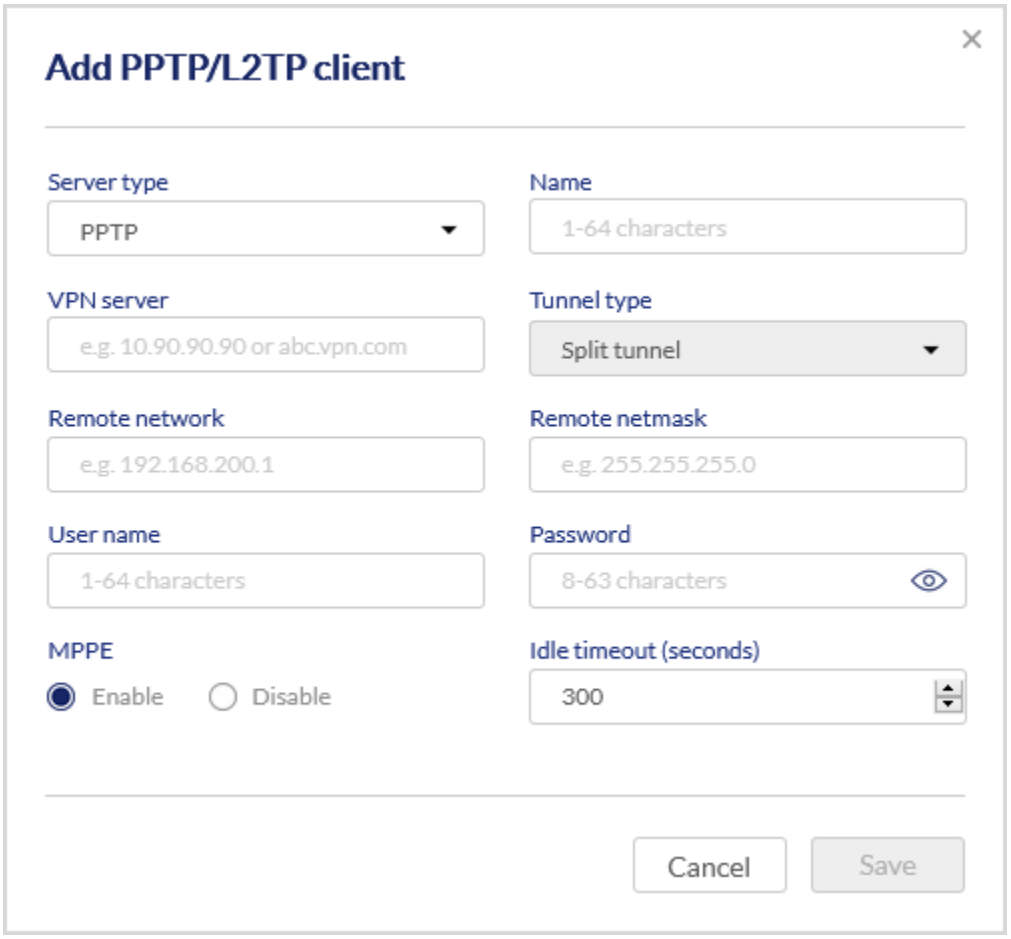
Les champs affichés dans le*Mode client*le tableau est le suivant :

Champ	Description
Nom	Il affiche le nom du client.
Nom d'utilisateur	Il affiche le nom d'utilisateur utilisé.
Type de serveur	Il affiche le serveur auquel le client est connecté.
IP du serveur	Il affiche l'adresse IP du serveur.

adresse IP	Il affiche l'adresse IP du client.
Statut	Il affiche l'état du client, qu'il soit connecté ou non.
Actif	Vous pouvez activer ou désactiver le client.
Actions	Vous pouvez modifier ou supprimer le client sélectionné de la liste.

Cliquez sur**Ajouter**pour ajouter une nouvelle entrée à la liste. Cela ouvre le*Ajouter un client PPTP/L2TP*page. Pour supprimer une ou plusieurs entrées, cochez les cases correspondantes, puis cliquez sur**Supprimer**.

Ajout d'un client PPTP

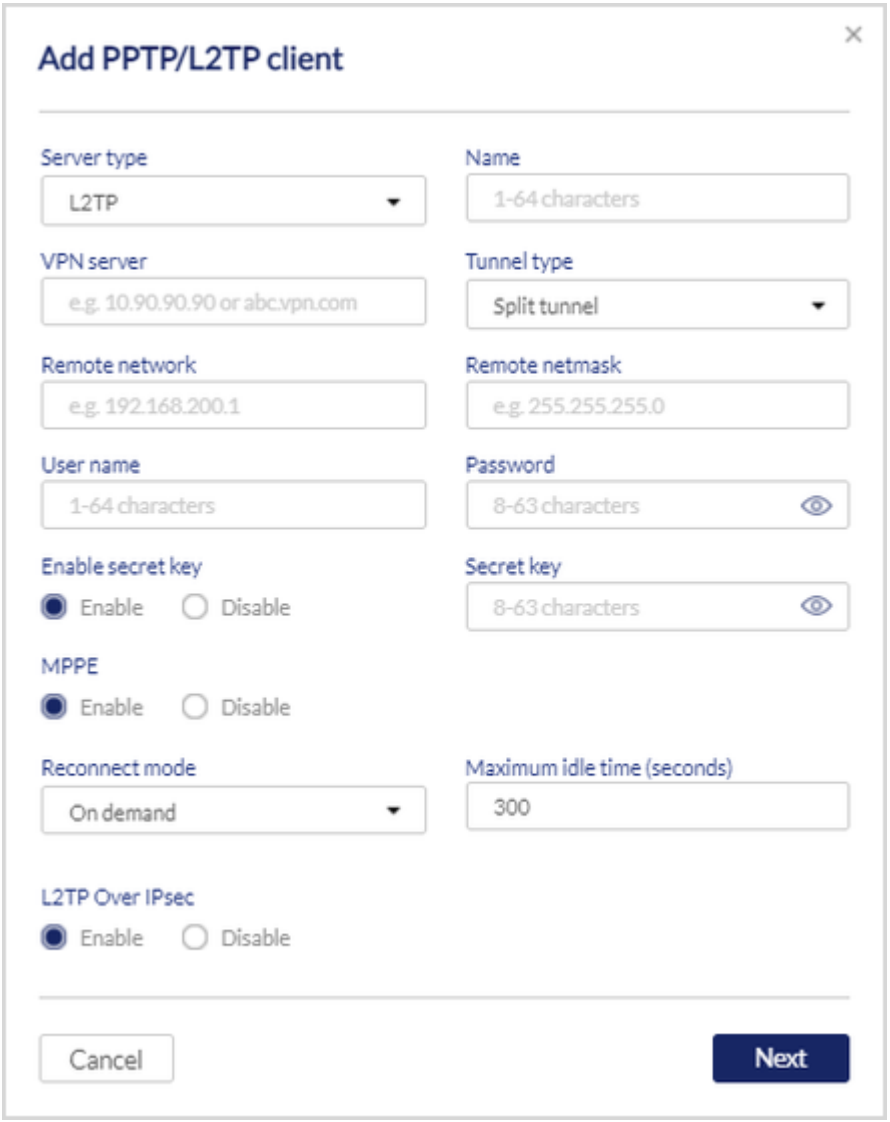


Les champs disponibles sur le*Ajouter un client PPTP/L2TP*page sont les suivantes :

Champ	Description
Type de serveur	Sélectionnez le type de serveur comme**PPTP**.
Nom	Entrez le nom.
serveur VPN	Saisissez l'adresse IP ou le nom de domaine du serveur PPTP auquel vous souhaitez vous connecter.
Type de tunnel	Sélectionnez le type de tunnel. • **Tunnel complet**: Si cette option est sélectionnée, il accédera à Internet et à l'hôte LAN connecté au périphérique serveur via le serveur PPTP une fois la connexion établie, • **Tunnel divisé**: Si cette option est sélectionnée, il accédera uniquement au réseau distant sélectionné.
Réseau distant	Entrez l'adresse du réseau distant. Cette adresse est locale pour le serveur PPTP.
Masque de réseau distant	Entrez le masque de sous-réseau du réseau distant.
Nom d'utilisateur	Entrez le nom d'utilisateur pour vous connecter au serveur.

Mot de passe	Entrez le mot de passe pour vous connecter au serveur.
MPPE	Activez ou désactivez le chiffrement point à point Microsoft (MPPE).
Délai d'inactivité (secondes)	Entrez la durée (en secondes) pendant laquelle vous vous déconnecterez du serveur PPTP en cas d'inactivité.
Sauvegarder	Cliquez sur**Sauvegarder**pour enregistrer vos paramètres.
Annuler	Cliquez sur**Annuler**pour revenir aux paramètres précédents.

Ajout d'un client L2TP



Les champs disponibles sur le*Ajouter un client PPTP/L2TP*page sont les suivantes :

Champ	Description
Type de serveur	Sélectionnez le type de serveur comme**L2TP**.
Nom	Entrez le nom.
serveur VPN	Saisissez l'adresse IP du serveur L2TP auquel vous souhaitez vous connecter.
Type de tunnel	Sélectionnez le type de tunnel. • **Tunnel complet**: Si cette option est sélectionnée, il accédera à Internet et à l'hôte LAN connecté au périphérique serveur via le serveur L2TP une fois la connexion établie.

	• **Tunnel divisé**: Si cette option est sélectionnée, il accédera uniquement au réseau distant sélectionné.
Réseau distant	Entrez l'adresse du réseau distant. Cette adresse est locale pour le serveur L2TP.
Masque de réseau distant	Entrez le masque de sous-réseau du réseau distant.
Nom d'utilisateur	Entrez le nom d'utilisateur pour vous connecter au serveur VPN.
Mot de passe	Entrez le mot de passe pour vous connecter au serveur VPN.
Activer la clé secrète	Vous pouvez activer ou désactiver la clé secrète.
Clef secrète	Si la clé secrète est activée, entrez la clé secrète.
MPPE	Activez ou désactivez le chiffrement point à point Microsoft (MPPE).
Mode reconnexion	Sélectionnez soit *Toujours activé* ou *Sur demande*.
Temps d'inactivité maximum (secondes)	Entrez le temps d'inactivité en secondes avant que la passerelle ne se déconnecte du serveur L2TP. Ce champ est disponible uniquement lorsque *Mode reconnexion* est **Sur demande**.
L2TP sur IPsec	Vous pouvez activer ou désactiver cette fonctionnalité. S'il est activé, il vous redirigera vers les paramètres IPsec. Cliquez sur **Suivant** pour configurer le *Profil IKE* pour IPsec. Pour plus de détails, reportez-vous à https://dlink-dbg.atlassian.net/wiki/spaces/CGD/pages/2687700/Site+to+Site+VPN#IKE-Profile.
Sauvegarder	Cliquez sur **Sauvegarder** pour enregistrer vos paramètres.
Annuler	Cliquez sur **Annuler** pour revenir aux paramètres précédents.

OpenVPN

La passerelle cloud Nuclias fournit la fonctionnalité OmniSSL, un OpenVPN personnalisé, similaire à la connectivité VPN SSL. OmniSSL fournit un fichier de configuration exécutable via une page de portail (*<https://<IP WAN de l'appareil>/omnissl>*) qui facilite l'installation du client à partir de l'appareil et constitue une amélioration de l'OpenVPN existant. De plus, cet outil VPN peut être utilisé via des appareils mobiles, éliminant ainsi les dépendances du navigateur et de Java typiques des solutions VPN SSL.

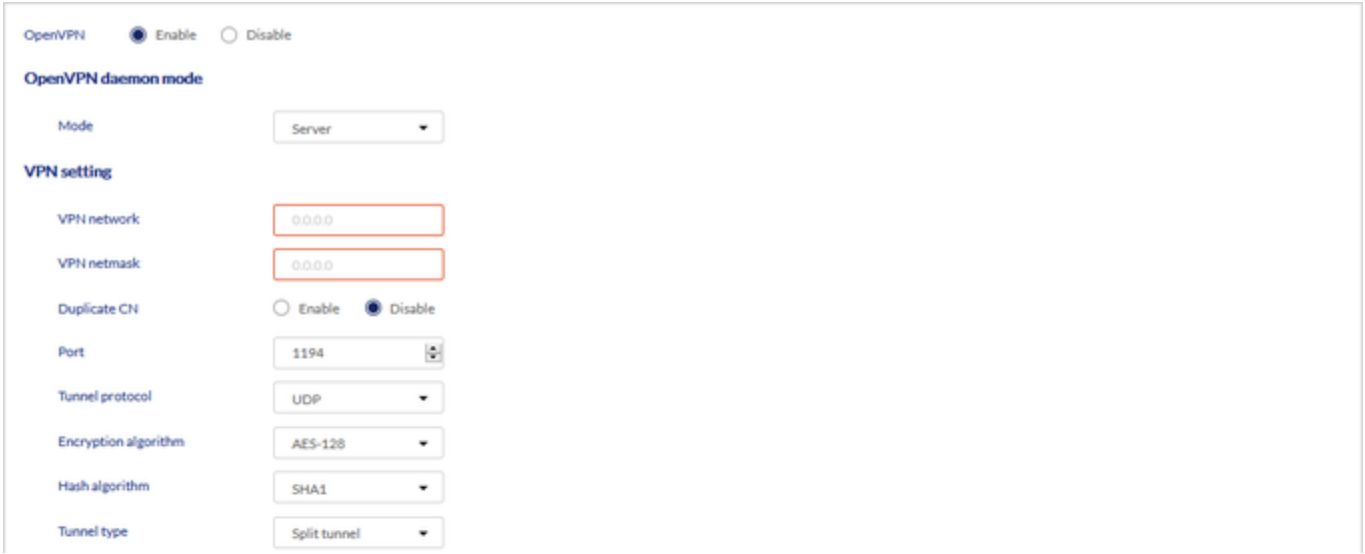
OpenVPN permet aux pairs de s'authentifier mutuellement à l'aide de certificats ou d'un nom d'utilisateur/mot de passe. Lorsqu'il est utilisé dans un configuration multi-client-serveur, elle permet au serveur de délivrer un certificat d'authentification pour chaque client, en utilisant la signature et l'autorité de certification. Un OpenVPN peut être établi via cette passerelle.

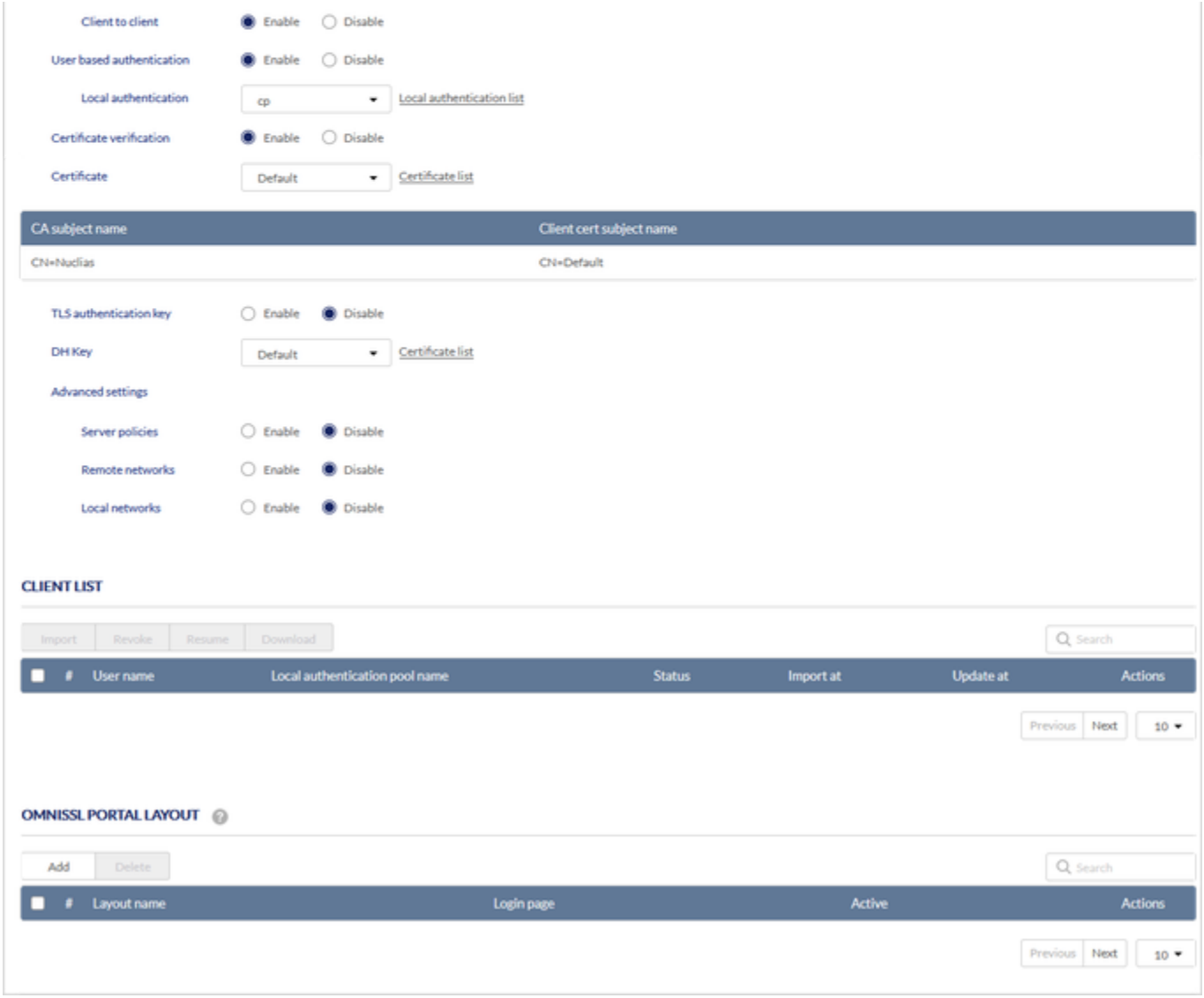
En mode serveur d'accès-client, l'utilisateur télécharge le profil de connexion automatique à partir du serveur d'accès OpenVPN et le télécharge pour se connecter. Vous pouvez sélectionner les modes suivants :

- Mode serveur
- Mode client
- Accéder au mode serveur-client

Mode serveur

Dans cette section, vous découvrirez la configuration d'OpenVPN dans le *Serveur* mode.





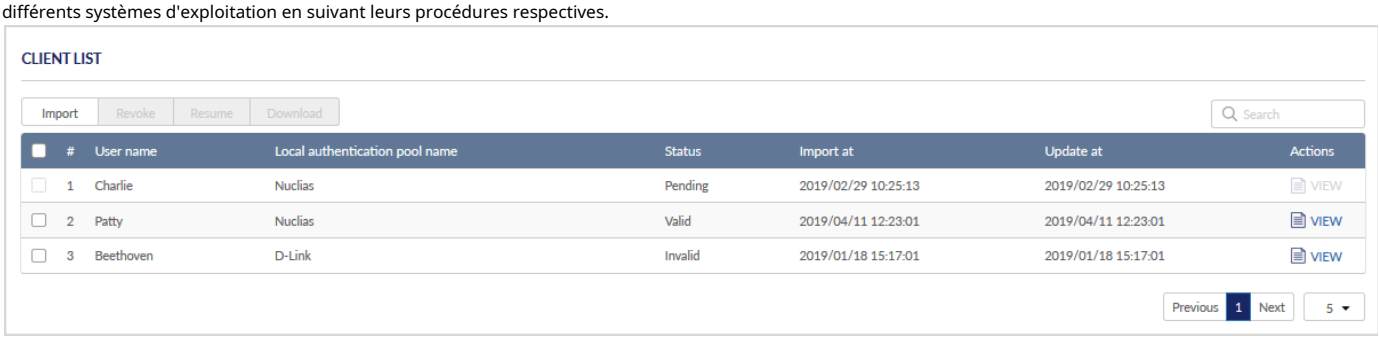
Les champs disponibles sur cette page sont les suivants :

Champ	Description
OpenVPN	Vous pouvez activer ou désactiver la fonctionnalité OpenVPN.
Mode démon OpenVPN	
Mode	Sélectionner**Serveur**.
Paramètre VPN	
Réseau VPN	Entrez le réseau IP du VPN.
Masque de réseau VPN	Entrez le masque de réseau.
CN en double	Activez-le pour permettre à l'utilisateur d'utiliser la même certification pour se connecter à plusieurs clients. L'authentification basée sur l'utilisateur est également requise pour cette fonctionnalité, et plusieurs clients doivent disposer de leurs noms d'utilisateur et mots de passe respectifs.
Port	Entrez le numéro de port sur lequel le serveur OpenVPN s'exécute. Le port par défaut est 1194.
Protocole de tunnel	Sélectionnez soit*TCP*ou*UDP*pour communiquer avec l'hôte distant.
Algorithme de cryptage	Sélectionnez l'algorithme de cryptage dans le menu déroulant. Les options sont*AES-128*, *BF-CBC*,*AES-192*, et*AES-256*.
Algorithme de hachage	

	Sélectionnez l'algorithme de hachage dans le menu déroulant. Les options sont*SHA1*,*SHA256*, et *SHA512*.
Type de tunnel	Sélectionnez soit**Tunnel complet**ou**Tunnel divisé**. Le mode Tunnel complet envoie tout le trafic du client via le tunnel VPN vers la passerelle. Le mode Split Tunnel envoie uniquement le trafic vers le réseau local privé en fonction de routes client prédéfinies. Si vous sélectionnez**Tunnel divisé**, faire référence àRéseaux locauxpour créer des réseaux locaux.
Client à client	Activez ce champ pour permettre aux clients OpenVPN de communiquer entre eux dans le cas du tunnel divisé. Par défaut, c'est désactivé.
Authentification basée sur l'utilisateur	Cette option fournit une méthode d'authentification supplémentaire. Vous pouvez activer ce champ pour sélectionner un serveur d'authentification.
Authentification locale	Sélectionnez une authentification locale configurée enregistrée sur le serveur local. Pour ajouter un nouveau serveur d'authentification local, cliquez sur le bouton*Liste d'authentification locale*lien. Pour plus de détails, reportez-vous auListe d'authentification localesection.
Vérification du certificat	Activez ou désactivez la vérification du certificat. Cette méthode ne nécessite pas le certificat client ; le client s'authentifie en utilisant uniquement le nom d'utilisateur/mot de passe. Il est activé par défaut.
Certificat	Sélectionnez le profil qui contient une liste de certificats téléchargés pour le mode serveur/client configuré.
Clé d'authentification TLS	L'activation de cette option ajoute l'authentification TLS, qui ajoute une couche d'authentification. Il ne peut être vérifié que lorsque la clé TLS est téléchargée. Il est désactivé par défaut.
Clé TLS	Sélectionnez le type de nom de certificat TLS.
Clé DH	Sélectionnez la clé DH dans la liste déroulante.
Réglages avancés	
Politiques du serveur	Activer ou désactiver le*Politiques du serveur*fonctionnalité; si activé, configurez les stratégies du serveur sous lePolitiques du serveursection.
Réseaux distants	Activer ou désactiver le*Réseaux distants*fonctionnalité; si elle est activée, configurez cette fonctionnalité dans le Réseaux distantssection.
Réseaux locaux	Activer ou désactiver le*Réseaux locaux*fonctionnalité; si elle est activée, configurez cette fonctionnalité dans leRéseaux locaux section. Cette section est disponible lorsque vous sélectionnez**Tunnel divisé**comme le*Type de tunnel*.

Liste des clients

Il permet à l'utilisateur de générer la configuration du client. De plus, OmniSSL est une fonctionnalité adaptable car elle prend en charge et s'installe sur différents systèmes d'exploitation en suivant leurs procédures respectives.

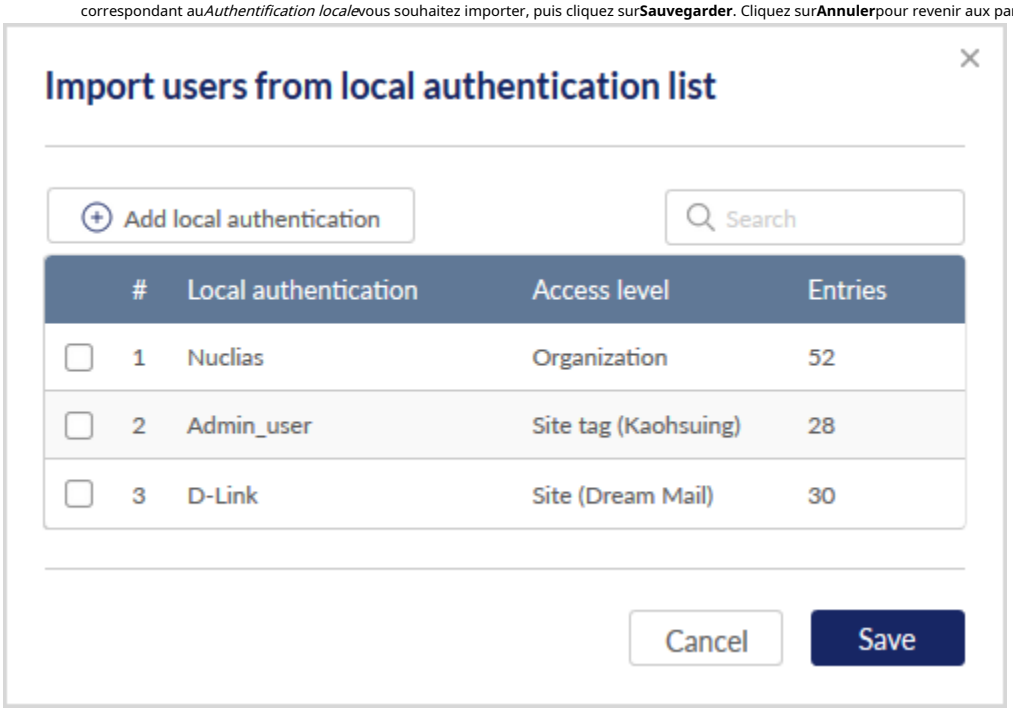


Les champs disponibles sur le*Liste des clients*le tableau est le suivant :

Champ	Description
Nom d'utilisateur	Il affiche le nom du client OmniSSL.
Nom du pool d'authentification local	Il affiche le nom du pool d'authentification local auquel appartiennent les clients.
Statut	Il affiche l'état des certificats.
Importer à	Il affiche la date et l'heure auxquelles les certificats de l'utilisateur ont été importés pour la première fois.
Mise à jour à	Il affiche la date et l'heure de la dernière mise à jour des certificats de l'utilisateur.

Actions	Il vous permet de visualiser les détails du client. ***Note:****Vous ne pouvez pas afficher les détails du client si le statut est En attente.*
Importer	Cliquez sur**Importer**pour importer la liste des clients OmniSSL.
Révoquer	Cliquez sur**Révoquer**pour valider le certificat client par rapport aux certificats révoqués.
CV	Lorsque le client est en statut de révocation, l'utilisateur peut cliquer sur**CV**pour reprendre le client, et le Cloud génère une nouvelle CRL.
Télécharger	Cliquez sur**Télécharger**pour télécharger le certificat sélectionné et l'utiliser si nécessaire.

- Cliquez sur**Importer**pour importer une liste de clients OmniSSL. Cela ouvre le*Importer des utilisateurs à partir de la liste d'authentification locale*page. Cochez la case correspondant au*Authentification locale*vous souhaitez importer, puis cliquez sur**Sauvegarder**. Cliquez sur**Annuler**pour revenir aux paramètres précédents.



Les champs disponibles sur cette page sont les suivants :

Champ	Description
Authentification locale	Il affiche le nom de l'authentification locale.
Niveau d'accès	Il affiche le niveau d'accès pour l'authentification locale.
Entrées	Il affiche le nombre d'identifiants de connexion enregistrés sur le serveur d'authentification local.
Ajouter une authentification locale	Cliquez sur ce bouton pour ajouter une authentification locale. Cela ouvre le*Ajouter une liste d'authentification locale*page âge. Pour plus de détails, reportez-vous auListe d'authentification locale.
Sauvegarder	Cliquez sur**Sauvegarder**pour enregistrer vos paramètres.
Annuler	Cliquez sur**Annuler**pour revenir aux paramètres précédents.

- Cliquez sur**Télécharger**pour télécharger la liste OmniSSL au format *.csv.

Disposition du portail OmniSSL

La passerelle cloud Nuclias prend en charge une page de portail statique pour activer ou désactiver l'authentification auprès des utilisateurs OmniSSL distants.

Les champs affichés dans le*Disposition du portail OmniSSL*le tableau est le suivant :

Champ	Description
Nom de la mise en page	Il affiche un nom pour la disposition du portail.
Page de connexion	Il affiche le lien de la page de connexion au portail.
Actif	Vous pouvez activer ou désactiver la disposition du portail. Lorsque vous l'activez, l'URL OmniSSL apparaîtra au-dessus du tableau dans le coin droit.

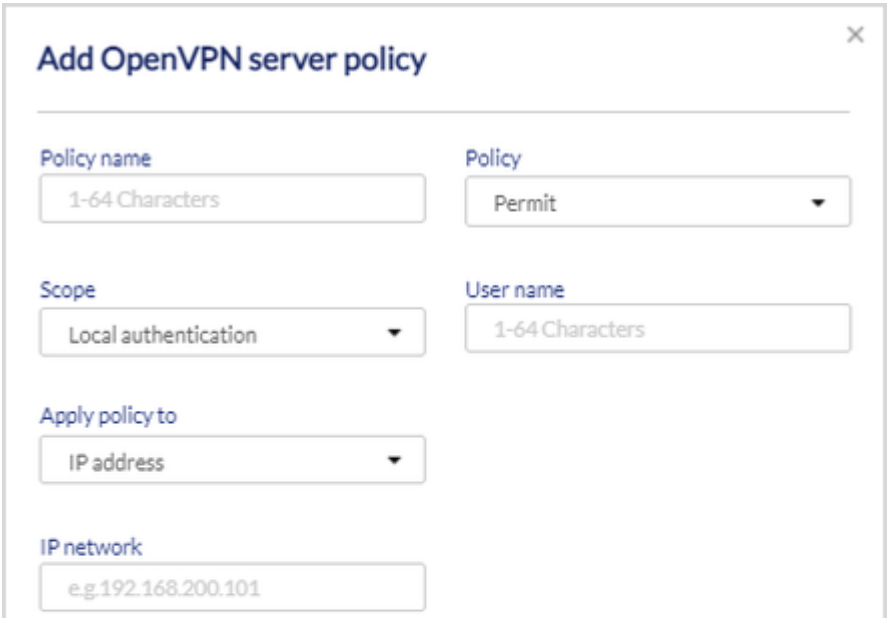
Politiques du serveur

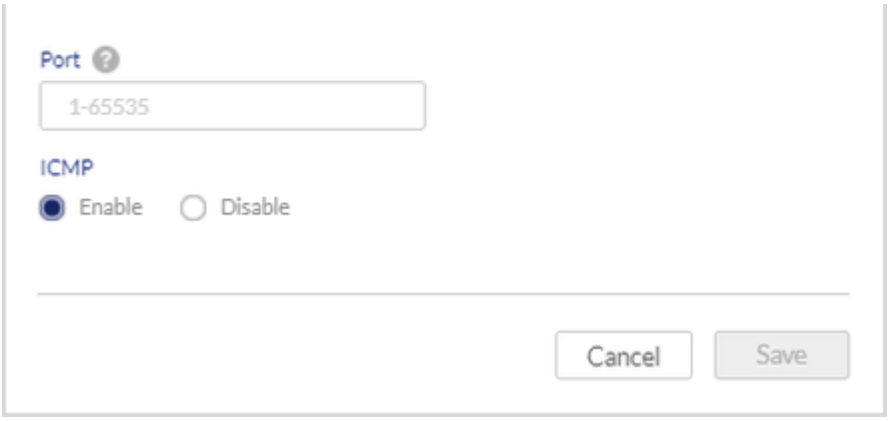
Les politiques du serveur OmniSSL sont utiles pour autoriser ou refuser l'accès à des adresses IP ou à des réseaux IP spécifiques. Ils peuvent être définis au niveau de l'utilisateur ou au niveau global.

Les champs affichés dans le*Politiques du serveur*le tableau est le suivant :

Champ	Description
Nom	Il affiche le nom de la stratégie du serveur.
Politique	Il affiche la politique appliquée à l'adresse IP.
Portée	Il affiche la portée. C'est soit*Mondial*ou*Authentification locale*.
Destination	Il affiche l'adresse IP à laquelle la politique OpenVPN est appliquée.
Port	Il affiche le numéro de port auquel la stratégie est appliquée.
Actions	Vous pouvez modifier ou supprimer la stratégie de serveur sélectionnée. Lorsque vous cliquez**Modifier**, il ouvre le*Modifier la politique du serveur OpenVPN*page.

Cliquez sur**Ajouter**pour ajouter une nouvelle entrée à la liste. Cela ouvre le*Ajouter une politique de serveur OpenVPN*page. Pour supprimer plusieurs entrées, cochez les cases correspondantes, puis cliquez sur**Supprimer**.



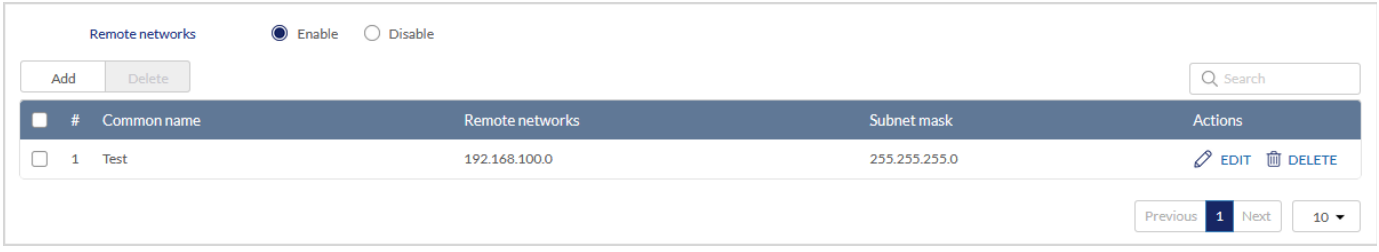


Les champs disponibles sur le*Ajouter une politique de serveur OpenVPN*page sont les suivantes :

Champ	Description
Nom de la politique	Entrez un nom pour la stratégie de serveur.
Politique	Sélectionnez la stratégie, s'il faut autoriser ou refuser l'accès à l'adresse IP ou au réseau IP spécifique.
Portée	Sélectionnez la portée dans le menu déroulant. C'est soit*Mondial*ou*Authentification locale*.
Authentification locale	Si**Authentification locale**est sélectionné comme*Portée*, spécifiez le nom d'utilisateur (client) auquel cette stratégie doit être appliquée.
Appliquer la politique à	Sélectionnez une adresse IP ou un réseau IP accessible auquel la stratégie est appliquée.
Réseau IP	Entrez le réseau IP auquel la politique OpenVPN doit être appliquée.
Masque de sous-réseau	Entrez le masque de sous-réseau pour le réseau IP ci-dessus.
adresse IP	Saisissez l'adresse IP à laquelle la politique OpenVPN doit être appliquée.
Port	Entrez la plage de numéros de port à laquelle la stratégie sera appliquée.
ICMP	Activez-le pour prendre en charge le trafic ICMP.
Sauvegarder	Cliquez sur**Sauvegarder**pour enregistrer vos paramètres.
Annuler	Cliquez sur**Annuler**pour revenir aux paramètres précédents.

Réseaux distants

Cette section affiche une liste des réseaux distants configurés. Les adresses IP configurées peuvent accéder à distance au serveur via un tunnel OpenVPN.

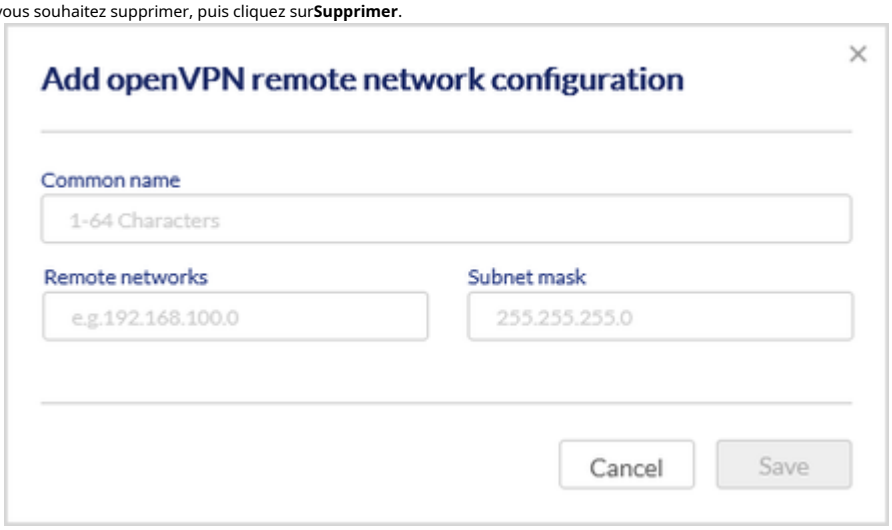


Les champs affichés sur le*Réseaux distants*le tableau est le suivant :

Champ	Description
Nom commun	Il affiche le nom du réseau distant.
Réseaux distants	Il affiche l'adresse IP des réseaux distants.
Masque de sous-réseau	Il affiche le masque de sous-réseau pour l'adresse IP du réseau distant.
Actions	

	Vous pouvez modifier ou supprimer le réseau distant correspondant. Lorsque vous cliquez**Modifier**, il ouvre le *Modifier la configuration du réseau distant OpenVPN*page.

Cliquez sur**Ajouter**pour ajouter une nouvelle entrée à la liste. Cela ouvre le*Ajouter la configuration du réseau distant OpenVPN*page. Pour supprimer plusieurs entrées, cochez les cases des réseaux distants que vous souhaitez supprimer, puis cliquez sur**Supprimer**.



Les champs disponibles sur le*Ajouter la configuration du réseau distant OpenVPN*page sont les suivantes :

Champ	Description
Nom commun	Entrez le nom du réseau distant.
Réseaux distants	Saisissez l'adresse IP des réseaux distants.
Masque de sous-réseau	Saisissez le masque de sous-réseau pour l'adresse IP du réseau distant.
Sauvegarder	Cliquez sur**Sauvegarder**pour enregistrer vos paramètres.
Annuler	Cliquez sur**Annuler**pour revenir aux paramètres précédents.

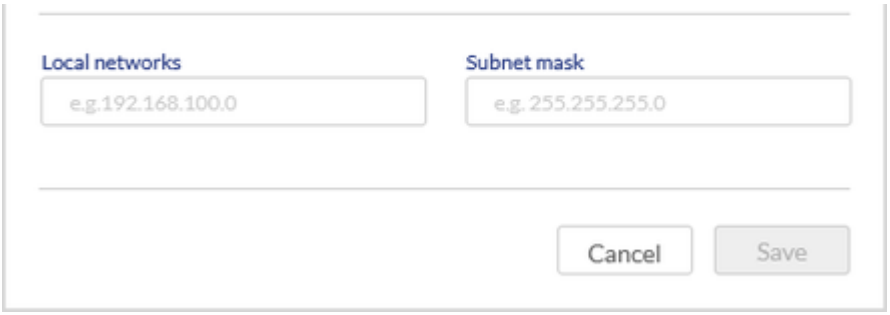
Réseaux locaux (tunnel divisé)

Cette section est disponible uniquement lorsque le**Tunnel divisé**est sélectionné comme*Type de tunnel*. Il affiche une liste des réseaux locaux OpenVPN configurés. Les clients ont accès uniquement à ces réseaux locaux configurés.

Les champs affichés sur le*Réseaux locaux*la liste est la suivante :

Champ	Description
Réseau local	Il affiche l'adresse IP du réseau local.
Masque de sous-réseau	Il affiche le masque de sous-réseau pour l'adresse IP du réseau local.
Actions	Vous pouvez modifier ou supprimer le réseau local correspondant. Lorsque vous cliquez**Modifier**, il ouvre le *Modifier la configuration du réseau local OpenVPN*fenêtre.

Cliquez sur**Ajouter**pour ajouter une nouvelle entrée à la liste. Cela ouvre le*Ajouter la configuration du réseau local OpenVPN*page. Pour supprimer plusieurs réseaux locaux, cochez les cases correspondant aux réseaux locaux que vous souhaitez supprimer, puis cliquez sur**Supprimer**.

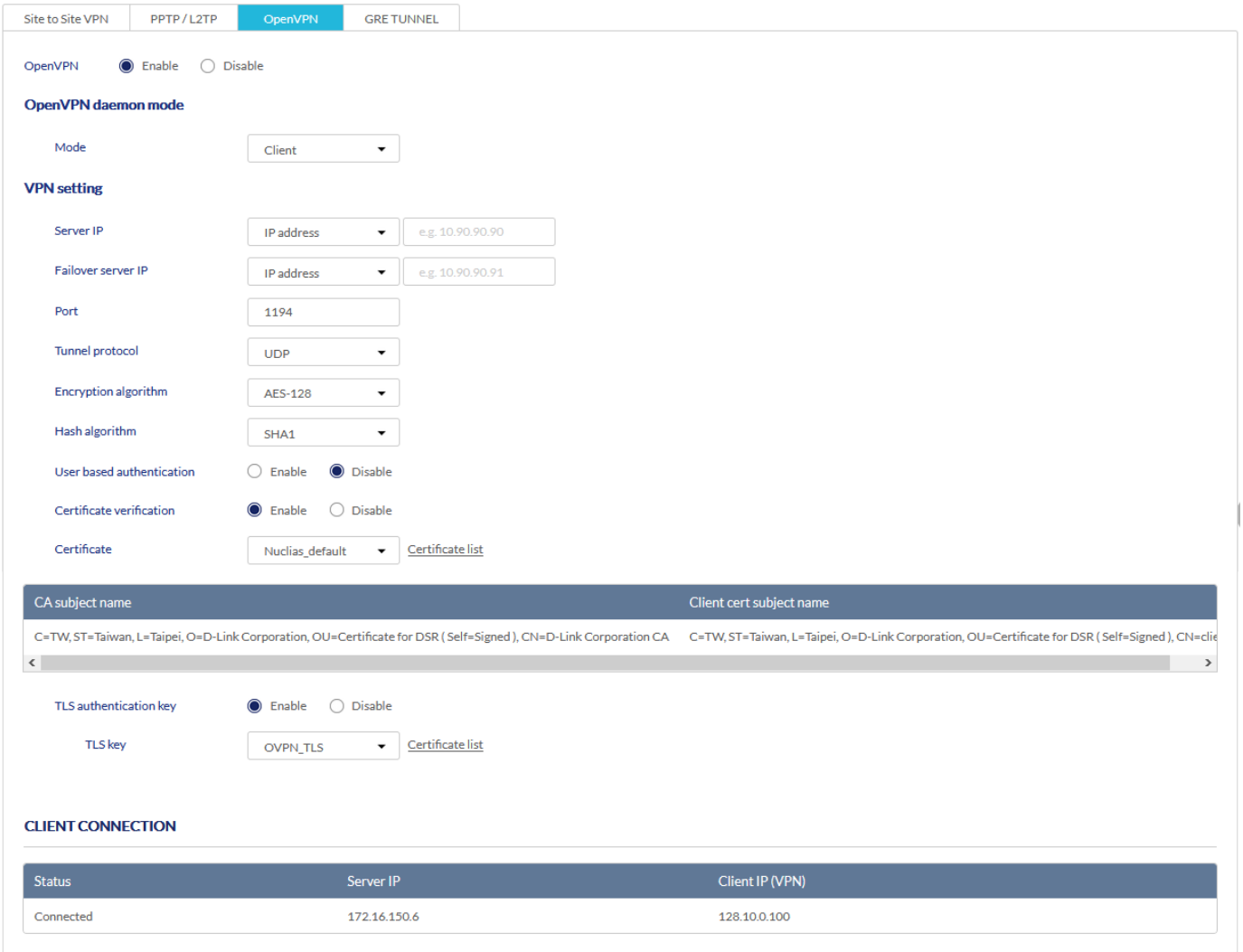


Les champs disponibles sur le*Ajouter la configuration du réseau local OpenVPN*page sont les suivantes :

Champ	Description
Réseaux locaux	Saisissez l'adresse IP du réseau local.
Masque de sous-réseau	Saisissez le masque de sous-réseau pour l'adresse IP du réseau local.
Sauvegarder	Cliquez sur**Sauvegarder**pour enregistrer vos paramètres.
Annuler	Cliquez sur**Annuler**pour revenir aux paramètres précédents.

Mode client

Dans cette section, vous découvrirez la configuration d'OpenVPN dans le*Client*mode.

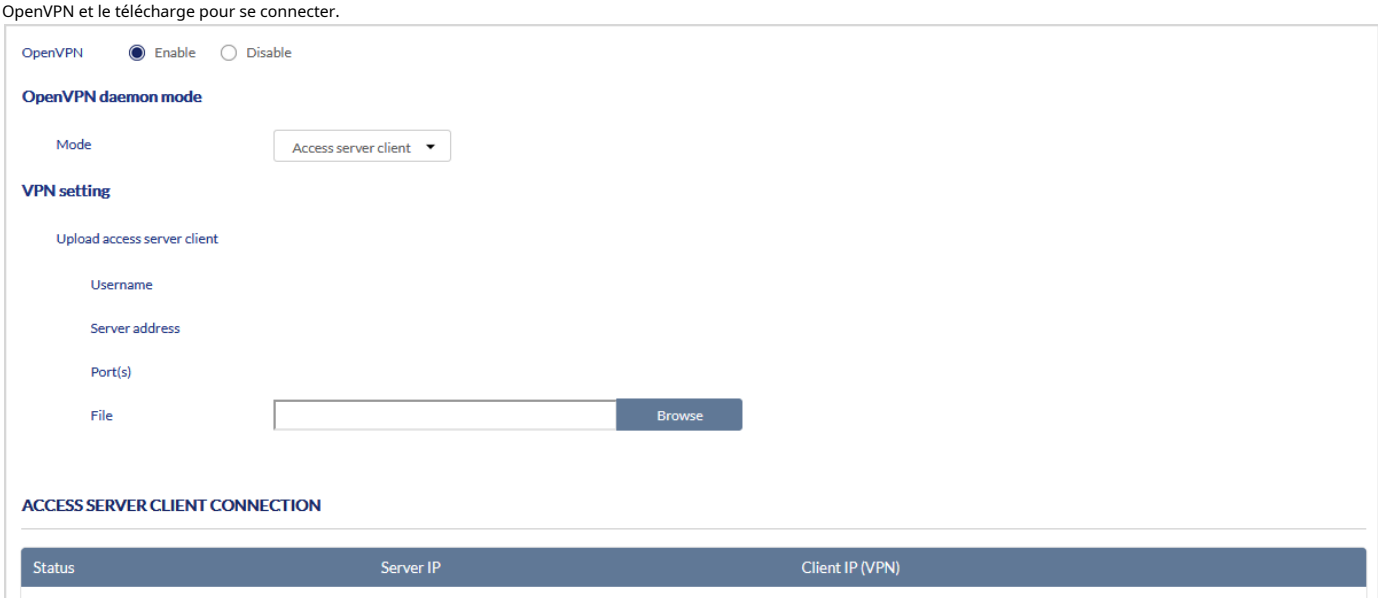


Les champs disponibles lorsque le*Mode client*est sélectionné sont les suivants :

Champ	Description
Mode	Sélectionner**Client**.
Paramètre VPN	
IP du serveur	Entrez l'adresse IP/FQDN du serveur OpenVPN.
IP du serveur de basculement	Sélectionnez le type d'identifiant que vous souhaitez fournir pour le mécanisme de basculement au niveau de l'adresse IP du serveur de basculement :**Adresse IP**ou**Nom de domaine complet**(Nom de domaine complet). Cette fonctionnalité permet de configurer un serveur OpenVPN supplémentaire pour le client, qui sera utilisé lorsque le serveur principal sera en panne. Ceci est applicable uniquement en mode client.
Port	Entrez le numéro de port sur lequel le serveur OpenVPN (ou le serveur d'accès) s'exécute.
Protocole de tunnel	Sélectionnez soit*TCP*ou*UDP*.
Algorithme de cryptage	Sélectionnez l'algorithme de cryptage dans le menu déroulant.
Algorithme de hachage	Sélectionnez l'algorithme de hachage dans le menu déroulant.
Authentification basée sur l'utilisateur	Cette option fournit une méthode d'authentification supplémentaire utilisant un nom d'utilisateur/mot de passe. Il est désactivé par défaut.
Nom d'utilisateur	Entrez le nom d'utilisateur. Ce champ est disponible lorsque*Authentification basée sur l'utilisateur*est autorisé.
Mot de passe	Entrer le mot de passe. Ce champ est disponible lorsque*Authentification basée sur l'utilisateur*est autorisé.
Vérification du certificat	Cette méthode permet d'effectuer une authentification par tunnel avec des certificats. Il est activé par défaut.
Certificat	Sélectionnez le profil pour lequel les certificats de liste ont été téléchargés pour le mode client configuré.
Clé d'authentification TLS	L'activation de cette option ajoute l'authentification TLS, qui ajoute une couche d'authentification. Il ne peut être activé que lorsque la clé TLS est téléchargée. Il est désactivé par défaut.
Clé TLS	Sélectionnez le type de nom de certificat TLS. Lorsque vous cliquez sur le*Liste des certificats*lien, il vous redirigera vers le*Gestion des certificats*page pour ajouter un nouveau certificat et une nouvelle clé.
Connexion client	
Statut	Il affiche l'état de la connexion du VPN.
IP du serveur	Il affiche l'adresse IP du serveur auquel le client est connecté.
IP client (VPN)	Il affiche l'adresse IP du client connecté.

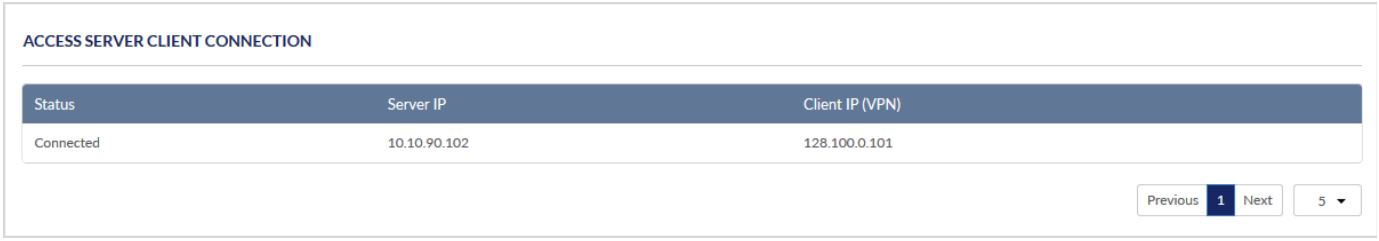
Accéder au mode serveur-client

Sélectionnez le mode d'accès au mode serveur-client. En mode serveur d'accès-client, l'utilisateur télécharge le profil de connexion automatique à partir du serveur d'accès OpenVPN et le télécharge pour se connecter.



Les champs disponibles lorsque le*Accéder au serveur-client*mode est sélectionné sont les suivants :

Champ	Description
Mode	Sélectionnez le**Accéder au serveur-client**mode.
Paramètre VPN	
Télécharger le client du serveur d'accès	
Nom d'utilisateur	Il affiche le nom d'utilisateur du client qui tente de se connecter au serveur.
Adresse du serveur	Il affiche l'adresse IP du serveur OpenVPN auquel le client tente de se connecter.
Port(s)	Il affiche les numéros de port sur lesquels le client se connectera au serveur OpenVPN (ou Access Server).
Déposer	Cliquez sur**Parcourir**et localisez le fichier de configuration. Cliquez sur**Ouvrir**, puis cliquez sur**Télécharger**.



Le tableau ci-dessus indique l'état du*Accéder à la connexion serveur-client,*et les champs affichés dans ce tableau sont les suivants :

Champ	Description
Statut	Il affiche l'état de la connexion VPN. Il indique si le client est connecté au serveur ou non.
IP du serveur	Il affiche l'adresse IP du serveur.
IP client (VPN)	Il affiche l'adresse IP du client.

GRE Tunnel

Les tunnels GRE permettent au trafic de diffusion LAN de la passerelle de passer sur Internet et de être reçu par les hôtes LAN distants. Lors de la création d'un tunnel GRE, une adresse IP unique doit identifier le point de terminaison du tunnel GRE. Elle sera référencée dans la route statique de l'autre passerelle en tant qu'adresse IP de la passerelle. L'adresse d'extrémité distante dans la page de configuration du tunnel GRE est l'adresse IP WAN de l'autre passerelle de point de terminaison.

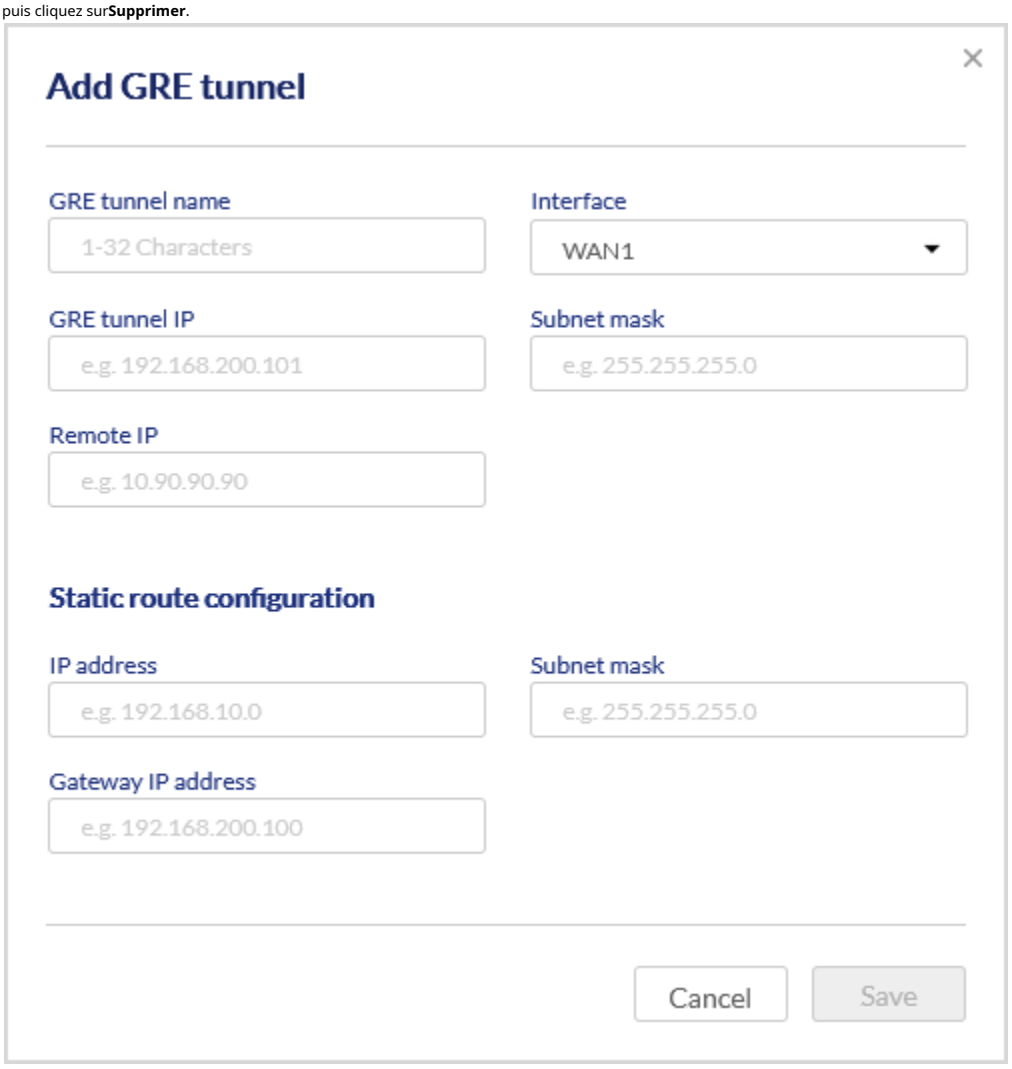
Une fois le tunnel établi, une route statique sur la passerelle peut être réalisée en utilisant l'interface du tunnel GRE configuré. L'adresse IP de destination de la route statique est le sous-réseau LAN distant. L'adresse IP de la passerelle de la route sera l'adresse IP du tunnel GRE de la passerelle de terminaison (la même passerelle qui gère le sous-réseau LAN distant). Une fois ces deux étapes terminées, le trafic peut circuler entre les sous-réseaux LAN distants configurés via le tunnel GRE.

Les champs affichés dans le*Configuration*le tableau est le suivant :

Champ	Description
Nom	Il affiche le nom du tunnel GRE.
Interface	Il affiche l'interface avec laquelle ce tunnel est créé.
IP du tunnel GRE	Il affiche l'adresse IP de ce point de terminaison.

IP distante	Il affiche l'adresse IP WAN de la passerelle du point de terminaison.
Actif	Vous pouvez activer ou désactiver le tunnel configuré.
Statut	Il affiche l'état du tunnel GRE, c'est-à-dire s'il est connecté ou déconnecté.
Actions	Vous pouvez modifier ou supprimer le tunnel GRE sélectionné. Lorsque vous cliquez**Modifier**, il ouvre le*Modifier le tunnel GRE*fenêtre.

Cliquez sur**Ajouter**pour ajouter une nouvelle entrée. Cela ouvre le*Ajouter un tunnel GRE*page. Pour supprimer plusieurs entrées, cochez les cases des tunnels GRE que vous souhaitez supprimer, puis cliquez sur**Supprimer**.



Les champs disponibles sur le*Ajouter un tunnel GRE*page sont données ci-dessous.

Champ	Description
Nom du tunnel GRE	Entrez un nom pour le tunnel GRE.
Interface	Sélectionnez l'interface pour créer ce tunnel.
IP du tunnel GRE	Entrez l'adresse IP de ce point de terminaison. Elle sera référencée dans la route statique de l'autre passerelle en tant qu'adresse IP de la passerelle.
Masque de sous-réseau	Entrez le masque de sous-réseau.
IP distante	Entrez l'adresse IP WAN de la passerelle du point de terminaison.
Configuration d'itinéraire statique	
adresse IP	Entrez l'adresse IP de destination de la route statique à partir du sous-réseau LAN distant.

Masque de sous-réseau	Entrez le masque de sous-réseau.
Adresse IP de la passerelle	Saisissez l'adresse IP de la passerelle de terminaison.
Sauvegarder	Cliquez sur**Sauvegarder**pour enregistrer vos paramètres.
Annuler	Cliquez sur**Annuler**pour revenir aux paramètres précédents.

Chapitre 6 Outils

Ce chapitre du guide de l'utilisateur vous fournit les informations et la configuration des outils de diagnostic pris en charge par la passerelle cloud Nuclias, comme ping et traceroute. Vous pouvez également connaître les performances de la connexion WAN. En cliquant sur un bouton, vous afficherez la vitesse de téléchargement et de téléchargement du port WAN. Vous pouvez utiliser ces outils pour détecter la connectivité et la dépanner si nécessaire.

Ce chapitre couvre les sujets suivants:

Ping

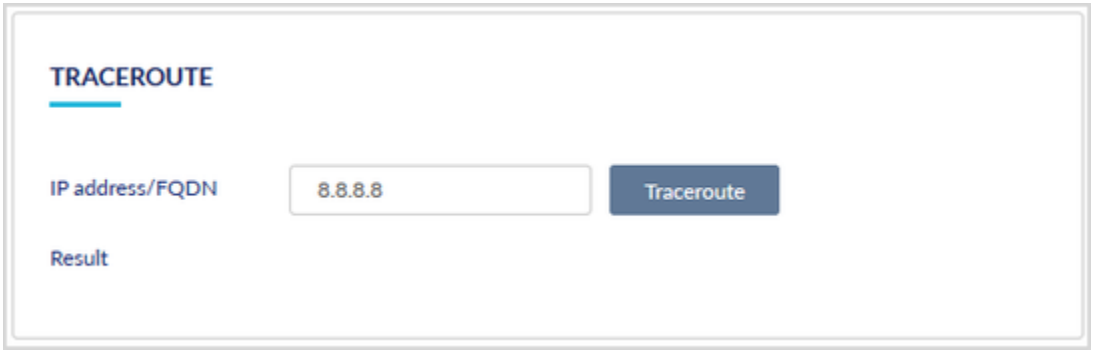
Dans le cadre des outils de diagnostic pris en charge par la passerelle cloud Nuclias, vous pouvez cingler une adresse IP ou un FQDN (Fully Qualified Domain Name). Vous pouvez utiliser cette fonctionnalité pour tester la connectivité entre la passerelle cloud Nuclias et un autre appareil du réseau connecté à la passerelle.

Les champs disponibles dans cette section sont les suivants :

Champ	Description
Adresse IP/FQDN	Saisissez l'adresse IP ou le FQDN.
Ping	Cliquez sur**Ping**pour envoyer un paquet de demande d'écho ICMP à la destination en utilisant le réseau IPv4.
Résultat	Il affiche le résultat de l'adresse IP. Si l'adresse IP de destination est active, vous pouvez voir une réponse. UN*réponse chronométrée-dehors*Le message indique que la destination n'est pas active ou bloque les requêtes ping.

Traceroute

La passerelle cloud Nuclias fournit un*Traceroute*fonction pour mapper le chemin réseau vers un hôte public. De plus, il affiche jusqu'à 30 « sauts » entre cette passerelle et la destination.



Les champs disponibles dans le*Traceroute*section sont les suivantes :

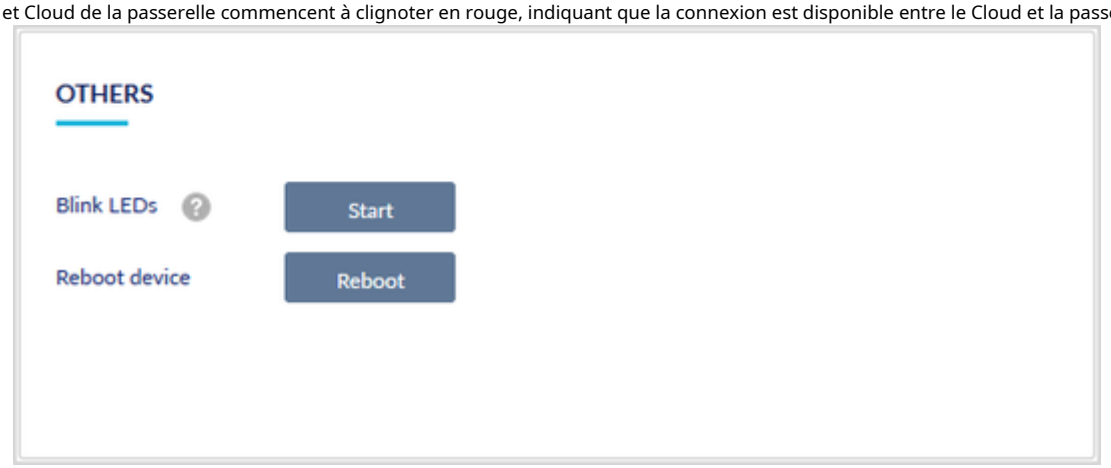
Champ	Description

Adresse IP/FQDN	Saisissez l'adresse IP ou le FQDN.
Traceroute	Cliquez sur**Traceroute**pour afficher tous les routeurs présents entre l'adresse IP de destination et cette passerelle.
Résultat	Cette section affiche les résultats de l'opération Traceroute.

Others

LED clignotantes

Le panneau avant de la passerelle cloud est composé de deux LED qui indiquent l'alimentation de la passerelle et l'état cloud de la passerelle. Le*LED clignotantes* La fonctionnalité vous aide à vérifier si la connexion a été établie entre la passerelle et le cloud. Après avoir cliqué sur le**Commencer**bouton, les voyants Power et Cloud de la passerelle commencent à clignoter en rouge, indiquant que la connexion est disponible entre le Cloud et la passerelle.



Voyant d'alimentation

Le voyant d'alimentation indique l'état d'alimentation de la passerelle.

DIRIGÉ	Couleur	Statut	Description
Pouvoir	Orange/Vert/Rouge	Orange uni	La mise sous tension est en cours.
		Orange clignotant	Mise à jour du micrologiciel en cours.
		Vert uni	Mise sous tension terminée.
		Rouge uni	Réinitialisation d'usine en cours.
		Rouge clignotant	Le**Commencer**bouton de*LED clignotantes*est cliqué.
		Désactivé	L'appareil est éteint.

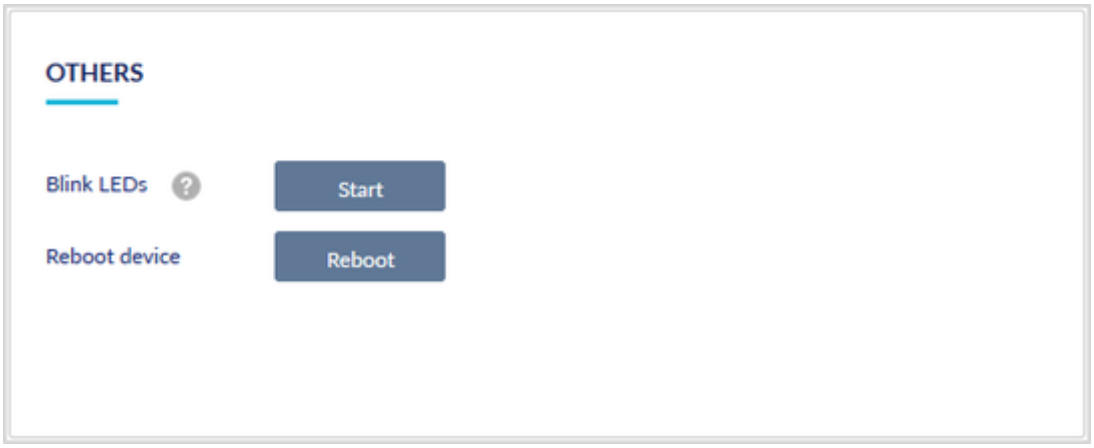
LED d'état du cloud

Le voyant d'état du cloud indique l'état de connexion au cloud Nuclias de l'appareil.

DIRIGÉ	Couleur	Statut	Description
Nuage	Orange/Vert/Rouge	Orange uni	Établir une connexion Cloud
		Vert uni	Connexion Cloud établie
		Rouge uni	Aucune connexion cloud établie
		Rouge clignotant	Le**Commencer**bouton de*LED clignotantes*est cliqué.
		Désactivé	L'appareil est éteint.

Redémarrer l'appareil

Clique le**Redémarrer**bouton pour effectuer le cycle d'alimentation.



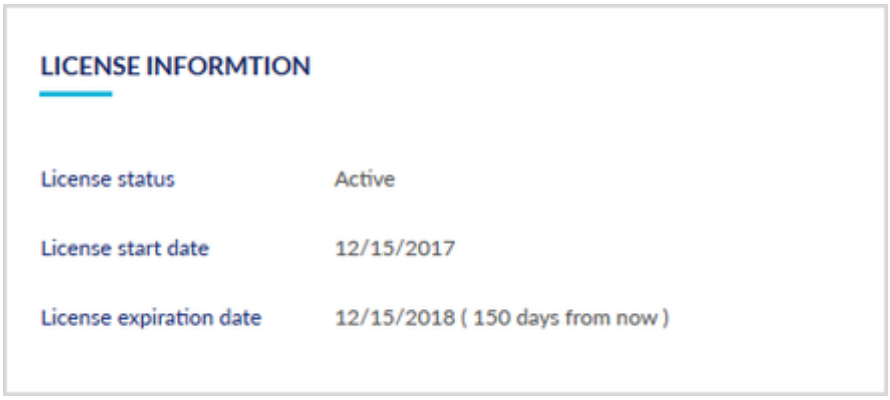
Chapitre 7 Licence

La passerelle cloud Nuclias prend en charge les fonctionnalités cloud, et ces fonctionnalités sont accompagnées d'une licence. Dans ce chapitre, vous découvrirez la licence active sur votre appareil. Il vous guidera également sur la façon d'ajouter une licence à votre appareil.

Ce chapitre couvre les sujets suivants:

License Information

Cette section du menu Licence fournit des détails sur la licence, comme la date d'activation, son statut actuel et sa date d'expiration.

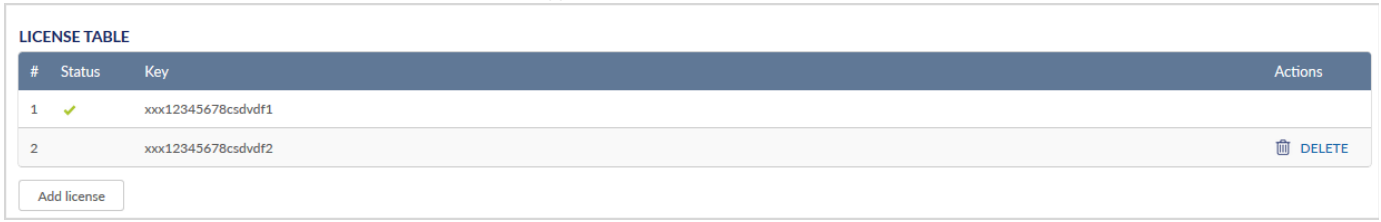


Les champs disponibles dans cette section sont les suivants :

Champ	Description
Statut de la licence	Il affiche l'état actuel de votre licence, c'est-à-dire si la licence est active ou non.
Date de début de licence	Il affiche la date à laquelle vous avez activé la licence.
Date d'expiration de la licence	Il affiche la date d'expiration de la licence et le nombre de jours restant pour l'expiration.

License Table

Le tableau des licences fournit une liste des licences activées sur l'appareil.



Les champs affichés sur cette page sont les suivants :

Champ	Description
Statut	Il affiche l'état de la licence, c'est-à-dire si la licence est active ou non. Si elle est active, une coche s'affiche.
Clé	Il affiche le code d'activation de la licence.
Actions	Vous pouvez supprimer la licence sélectionnée.

Pour ajouter une nouvelle licence, cliquez sur**Ajouter une licence**. Cela ouvre le*Ajouter une licence*page. Sélectionnez une clé de licence et cliquez sur**Sauvegarder**. Cliquez sur**Annuler**pour fermer la page.