



Citrix Secure Web Gateway 12.1

Machine translated content

Disclaimer

La version officielle de ce document est en anglais. Certains contenus de la documentation Cloud Software Group ont été traduits de façon automatique à des fins pratiques uniquement. Cloud Software Group n'exerce aucun contrôle sur le contenu traduit de façon automatique, qui peut contenir des erreurs, des imprécisions ou un langage inapproprié. Aucune garantie, explicite ou implicite, n'est fournie quant à l'exactitude, la fiabilité, la pertinence ou la justesse de toute traduction effectuée depuis l'anglais d'origine vers une autre langue, ou quant à la conformité de votre produit ou service Cloud Software Group à tout contenu traduit de façon automatique, et toute garantie fournie en vertu du contrat de licence de l'utilisateur final ou des conditions d'utilisation des services applicables, ou de tout autre accord avec Cloud Software Group, quant à la conformité du produit ou service à toute documentation ne s'applique pas dans la mesure où cette documentation a été traduite de façon automatique. Cloud Software Group ne pourra être tenu responsable de tout dommage ou problème dû à l'utilisation de contenu traduit de façon automatique.

Contents

Notes de publication	3
Plates-formes matérielles et logicielles prises	3
Exigence de	4
Installation	10
Prise en main d'une appliance Citrix ADC MPX et VPX SWG	10
Prise en main d'une instance SWG sur une appliance Citrix ADC SDX	13
Modes proxy	14
Interception SSL	17
Profil SSL	18
Infrastructure de stratégie SSL pour l'interception SSL	27
Magasin de certificats d'interception SSL	30
Apprentissage automatique des erreurs SSL	34
Gestion des identités utilisateur	36
Filtrage d'URL	40
Liste des URL	43
Sémantique des modèles d'URL	50
Catégories d'URL de mappage	50
Cas d'utilisation : filtrage d'URL à l'aide d'un jeu d'URL personnalisé	50
Catégorisation d'URL	53
Configuration de la sécurité	65
Score de réputation d'URL	66
Utilisation d'ICAP pour l'inspection du contenu à distance	68
Intégration avec IPS ou NGFW en tant que périphériques en ligne	80

Analytics	127
Cas d'utilisation : Rendre l'accès Internet d'entreprise conforme et sécurisé	128
Cas d'utilisation : sécuriser le réseau d'entreprise à l'aide d'ICAP pour l'inspection à distance des logiciels malveillants	143
Articles pratiques	157
Comment créer une stratégie de catégorisation d'URL	158
Comment créer une stratégie de liste d'URL	160
Comment placer sur liste verte une URL d'exception	163
Comment bloquer les sites Web de catégorie adulte	164
Systeme	166
Mise en réseau	167
AppExpert	168
SSL	169
Questions fréquentes	169

Notes de publication

April 27, 2021

Les notes de mise à jour du produit Citrix Secure Web Gateway sont capturées dans les notes de publication principales d'une appliance Citrix ADC. Consultez [Notes de mise à jour de Citrix ADC](#).

Plates-formes matérielles et logicielles prises

April 27, 2021

L'appliance Citrix Secure Web Gateway (SWG) est actuellement disponible en tant qu'appliance matérielle et en tant qu'appliance virtuelle. Les spécifications détaillées sont disponibles dans la fiche technique, disponible sur www.citrix.com. Placez le pointeur de la souris sur **Produits**, dans la liste **Mise en réseau**, sélectionnez **Citrix Secure Web Gateway**.

Avant d'installer votre appliance SWG, vérifiez que vous disposez de la ou des licences appropriées. Chaque appliance dans une configuration haute disponibilité nécessite sa propre licence. Pour plus d'informations sur les licences, reportez-vous à la section [Exigences relatives](#). Pour plus d'informations sur la haute disponibilité, reportez-vous à la rubrique [Introduction à la haute disponibilité](#).

Appareil matériel (MPX)

- Citrix SWG MPX 14020/14030/14040
- Citrix SWG MPX 14020-40G/14040-40G
- Citrix SWG MPX 14060-40S/14080-40S/14100-40S

Appliance virtuelle (VPX)

- Citrix SWG VPX 200
- Citrix SWG VPX 1000
- Citrix SWG VPX 3000
- Citrix SWG VPX 5000
- Citrix SWG VPX 8000
- Citrix SWG VPX 10G
- Citrix SWG VPX 15G
- Citrix SWG VPX 25G

Appliance matérielle (SDX)

Les instances SWG peuvent être provisionnées sur n'importe quelle plate-forme SDX en installant la licence « SDX 2-Instance Add-On Pack for Secure Web Gateway ». Avec une seule licence d'installation, vous pouvez provisionner deux instances SWG sur une appliance SDX. Vous pouvez provisionner davantage d'instances SWG sur votre appliance en ajoutant plus de licences. Pour plus d'informations sur le provisionnement d'une instance Citrix SWG, reportez-vous à la section [Provisionnement d'instances Citrix ADC](#).

Exigence de

April 27, 2021

Une licence vous donne accès à un ensemble de fonctionnalités sur une appliance Citrix Secure Web Gateway (SWG).

L'infrastructure de licences Citrix vous permet de vous concentrer sur la valorisation maximale des produits Citrix. Le processus d'attribution de vos licences est très simple. Dans l'utilitaire de configuration SWG (GUI), vous pouvez utiliser votre numéro de série matériel (HSN) ou votre code d'activation de licence (BAC) pour allouer vos licences. Si une licence est déjà présente sur votre ordinateur local, vous pouvez la télécharger sur l'appliance.

Pour toutes les autres fonctionnalités, telles que le retour ou la réaffectation de votre licence, vous devez utiliser le portail de licences (que vous pouvez également utiliser pour l'attribution initiale de la licence si vous préférez). Pour plus d'informations sur le portail de licences, reportez-vous à la section <http://support.citrix.com/article/CTX131110>.

Vous pouvez allouer partiellement des licences selon les besoins de votre déploiement. Par exemple, si votre fichier de licence contient dix licences, mais que votre exigence actuelle ne concerne que six licences, vous pouvez allouer six licences maintenant et allouer des licences supplémentaires ultérieurement. Vous ne pouvez pas allouer plus de licences que le nombre total de licences présentes dans votre fichier de licences.

Avant d'utiliser votre appliance SWG, vous devez installer les licences suivantes à l'aide de l'interface graphique ou de l'interface de ligne de commande :

- **Licence Citrix Secure Web Gateway**

- La licence Citrix SWG Platform est la condition minimale requise pour utiliser votre appliance MPX SWG et pour déployer votre instance VPX sur différents hyperviseurs, tels que XenServer, VMware ESX, Microsoft Hyper-V et Linux-KVM.

- Pour les plates-formes SDX, au moins une licence de pack complémentaire SWG pour les sessions simultanées SDX 10K est requise pour provisionner une instance Citrix SWG sur une appliance Citrix ADC SDX.
- **Licence de fonctionnalité URL Threat Intelligence** Cette licence est requise pour l'utilisation des fonctionnalités de filtrage d'URL, de catégorisation d'URL et de score de réputation d'URL.

Conditions préalables

Pour utiliser le numéro de série du matériel ou le code d'activation de licence pour allouer vos licences :

- Vous devez pouvoir accéder aux domaines publics via l'appliance. Par exemple, l'appliance doit pouvoir accéder à www.citrix.com. Le logiciel d'allocation de licence accède en interne au portail de licences Citrix pour votre licence. Pour accéder à un domaine public, vous pouvez utiliser un serveur proxy ou configurer un serveur DNS et, sur votre appliance Citrix ADC, configurer une adresse NSIP ou une adresse IP de sous-réseau (SNIP).
- Votre licence doit être liée à votre matériel, ou vous devez disposer d'un code d'activation de licence (BAC) valide. Citrix envoie votre BAC par e-mail lorsque vous achetez une licence.

Licences pour les appliances dans une configuration haute disponibilité

Vous devez acheter une licence distincte pour chaque appliance dans une paire haute disponibilité (HA). Assurez-vous que le même type de licence est installé sur les deux appliances.

Sur une appliance Citrix ADC SDX, vous pouvez configurer une configuration haute disponibilité (HA) entre deux instances SWG sur la même appliance. Toutefois, Citrix vous recommande de configurer une configuration HA entre deux instances SWG sur différentes appliances Citrix ADC SDX.

Allouer et installer vos licences

Vous pouvez allouer et installer vos licences à l'aide de l'interface graphique. L'installation de vos licences à l'aide de l'interface de ligne de commande nécessite de copier les licences dans le répertoire `/nsconfig/license/`.

Allouer vos licences à l'aide de l'interface graphique Citrix SWG

1. Dans un navigateur Web, tapez l'adresse IP de l'appliance Citrix SWG.
2. Dans **Nom d'utilisateur** et **Mot de passe**, tapez les informations d'identification de l'administrateur.

3. Sous l'onglet **Configuration**, accédez à **Système > Licences**.
 4. Dans le volet d'informations, cliquez sur **Gérer les licences**, cliquez sur **Ajouter une nouvelle licence**, puis sélectionnez l'une des options suivantes :
 - **Utilisez le numéro de série.** Le logiciel récupère en interne le numéro de série de votre appliance et utilise ce numéro pour afficher vos licences.
 - **Utilisez le code d'activation de licence.** Citrix envoie par e-mail le code d'activation de licence (BAC) pour la licence que vous avez achetée. Entrez le BAC dans la zone de texte.
- Si vous ne souhaitez pas configurer la connectivité Internet sur l'appliance Citrix ADC, vous pouvez utiliser un serveur proxy. Sélectionnez **Se connecter via le serveur proxy** et spécifiez l'adresse IP et le port de votre serveur proxy.
5. Cliquez sur **Obtenir les licences**.
 6. Sélectionnez le fichier de licences que vous souhaitez utiliser pour allouer vos licences.
 7. Dans la colonne **Allocation**, entrez le nombre de licences à allouer. Cliquez ensuite sur **Obtenir**.
 8. Cliquez sur **Reboot** pour que la licence prenne effet.
 9. Dans la boîte de dialogue **Redémarrer**, cliquez sur **OK**.

Installez vos licences à l'aide de l'interface graphique Citrix SWG

1. Dans un navigateur Web, tapez l'adresse IP de l'appliance Citrix SWG (par exemple <http://192.168.100.1>).
2. Dans **Nom d'utilisateur** et **Mot de passe**, tapez les informations d'identification de l'administrateur.
3. Sous l'onglet **Configuration**, accédez à **Système > Licences**.
4. Dans le volet d'informations, cliquez sur **Gérer les licences**.
5. Cliquez sur **Ajouter une nouvelle licence**, puis sélectionnez **Télécharger les fichiers de licence**.
6. Cliquez sur **Parcourir**. Accédez à l'emplacement des fichiers de licence, sélectionnez le fichier de licences, puis cliquez sur **Ouvrir**.
7. Cliquez sur **Reboot** pour appliquer la licence.
8. Dans la boîte de dialogue **Redémarrer**, cliquez sur **OK**.

Installez vos licences à l'aide de l'interface de ligne de commande Citrix SWG

1. Ouvrez une connexion SSH à l'appliance Citrix SWG à l'aide d'un client SSH, tel que PuTTY.

2. Connectez-vous à l'apppliance à l'aide des informations d'identification de l'administrateur.
3. Passez à l'invite shell et copiez le (s) nouveau (s) fichier (s) de licence dans le sous-répertoire de licence du répertoire nsconfig. Si le sous-répertoire n'existe pas, créez-le avant de copier le ou les fichiers.

Exemple :

```
1 login: nsroot
2
3 Password: nsroot
4
5 Last login: Mon Aug 4 03:37:27 2008 from 10.102.29.9
6
7 Done
8
9 > shell
10
11 Last login: Mon Aug 4 03:51:42 from 10.103.25.64
12
13 root@ns# mkdir /nsconfig/license
14
15 root@ns# cd /nsconfig/license
```

Copiez le (s) nouveau (s) fichier (s) de licence dans ce répertoire.

Remarque

L'interface de ligne de commande ne vous invite pas à redémarrer l'apppliance pour activer les licences. Exécutez la commande **reboot -w** pour redémarrer le système à chaud ou exécutez la commande **reboot** pour redémarrer le système normalement.

Vérifier les fonctionnalités sous licence

Avant d'utiliser une fonctionnalité, assurez-vous que votre licence prend en charge la fonctionnalité.

Vérifier les fonctionnalités sous licence à l'aide de l'interface graphique Citrix SWG

1. Dans un navigateur Web, tapez l'adresse IP de l'apppliance Citrix SWG (par exemple <http://192.168.100.1>).
2. Dans **Nom d'utilisateur** et **Mot de passe**, tapez les informations d'identification de l'administrateur.
3. Accédez à **Système > Licences**.
L'écran comporte une coche verte à côté de chaque fonction sous licence.

Vérifier les fonctionnalités sous licence à l'aide de l'interface de ligne de commande Citrix SWG

1. Ouvrez une connexion SSH à l'apppliance Citrix SWG à l'aide d'un client SSH, tel que PuTTY.
2. Connectez-vous à l'apppliance à l'aide des informations d'identification de l'administrateur.
3. À l'invite de commandes, entrez la commande `sh ns license` pour afficher les fonctionnalités prises en charge par la licence.

Exemple :

```
1 > sh license
2
3     License status:
4
5             Web Logging: NO
6
7             Surge Protection: NO
8
9             Load Balancing: YES
10
11             ...
12
13            Forward Proxy: YES
14
15            SSL Interception: YES
16
17            Model Number ID: 25000
18
19            Licensing mode: Local
20
21 Terminé
```

Activer ou désactiver une fonctionnalité

Lorsque vous utilisez l'apppliance Citrix Secure Web Gateway pour la première fois, vous devez activer une fonctionnalité avant de pouvoir l'utiliser. Si vous configurez une fonctionnalité avant qu'elle ne soit activée, un message d'avertissement s'affiche. La configuration est enregistrée, mais elle ne s'applique pas tant que la fonctionnalité n'est pas activée.

Activer une fonctionnalité à l'aide de l'interface graphique Citrix SWG

1. Dans un navigateur Web, tapez l'adresse IP de l'apppliance Citrix SWG (par exemple <http://192.168.100.1>).
2. Dans **Nom d'utilisateur** et **Mot de passe**, tapez les informations d'identification de l'administrateur.
3. Accédez à **Système > Paramètres > Configurer les fonctionnalités avancées**.

- Sélectionnez les fonctionnalités (par exemple, Proxy de transfert, Interception SSL et Filtrage d'URL) que vous souhaitez activer.

Activer une fonctionnalité à l'aide de l'interface de ligne de commande Citrix SWG

À l'invite de commandes, tapez les commandes suivantes pour activer une fonctionnalité et vérifier la configuration :

```
enable feature <FeatureName>
```

```
show feature
```

L'exemple suivant montre comment activer les fonctions d'interception SSL, de transfert de proxy et de filtrage d'URL.

```

1 > enable feature forwardProxy sslinterception urlfiltering
2
3 Done
4
5 >show feature
6
7     Feature                               Acronym           Status
8
9     -----                               -
10
11 1)    Web Logging                         WL                OFF
12
13 2)    Surge Protection                    SP                OFF
14
15 ...
16
17 ...
18
19 36)   URL Filtering                       URLFiltering      ON
20
21 37)   Video Optimization                  VideoOptimization OFF
22
23 38)   Forward Proxy                      ForwardProxy      ON
24
25 39)   SSL Interception                    SSLInterception   ON
26
27 Done

```

Remarque

Si la clé de licence n'est pas disponible pour une fonctionnalité, le message d'erreur suivant s'affiche pour cette fonctionnalité :

ERREUR : fonctionnalité non associée à une licence

Installation

April 27, 2021

Une appliance Citrix Secure Web Gateway (SWG) doit être correctement installée et accessible à Internet avant de pouvoir commencer à la configurer pour sécuriser votre entreprise.

Pour plus d'informations sur l'installation et la configuration initiale de votre appliance matérielle, reportez-vous à la section [Configuration du matériel SWG](#).

Une appliance virtuelle Citrix SWG (VPX) est prise en charge sur différentes plates-formes de virtualisation.

Pour plus d'informations sur les hyperviseurs pris en charge et sur les instructions de déploiement d'une appliance VPX, reportez-vous à la section [Déployer une instance de Citrix ADC VPX sur AWS](#).

Prise en main d'une appliance Citrix ADC MPX et VPX SWG

April 27, 2021

Après avoir installé votre matériel (MPX) ou logiciel (VPX) et effectué la configuration initiale, vous êtes prêt à le configurer en tant qu'appliance de passerelle Web sécurisée pour recevoir du trafic.

Important :

- La vérification OSCP nécessite une connexion Internet pour vérifier la validité des certificats. Si votre appliance n'est pas accessible depuis Internet à l'aide de l'adresse NSIP, ajoutez des listes de contrôle d'accès (ACL) pour effectuer NAT à partir de l'adresse NSIP à l'adresse SNIP du sous-réseau (SNIP). Le SNIP doit être accessible à partir d'Internet. Par exemple,

```
1  add ns acl a1 ALLOW -srcIP = <NSIP> -destIP "!="  
    10.0.0.0-10.255.255.255  
2  
3  set rnat a1 -natIP <SNIP>  
4  
5  apply acls
```

- Spécifiez un serveur de noms DNS pour résoudre les noms de domaine. Pour de plus amples informations, consultez la section [Configuration initiale](#).
- Assurez-vous que la date de l'appliance est synchronisée avec les serveurs NTP. Si la date n'est pas synchronisée, l'appliance ne peut pas vérifier efficacement si un certificat de serveur d'origine est expiré.

Pour utiliser l'appliance Citrix SWG, vous devez effectuer les tâches suivantes :

- Ajoutez un serveur proxy en mode explicite ou transparent.
- Activer l'interception SSL.
 - Configurez un profil SSL.
 - Ajouter et lier des stratégies SSL au serveur proxy.
 - Ajoutez et liez une paire de clés de certification CA pour l'interception SSL.

Remarque : une appliance Citrix SWG configurée en mode proxy transparent peut intercepter uniquement les protocoles HTTP et HTTPS. Pour contourner tout autre protocole, tel que telnet, vous devez ajouter la stratégie d'écoute suivante sur le serveur virtuel proxy.

Le serveur virtuel accepte désormais uniquement le trafic entrant HTTP et HTTPS.

```
1 set cs vserver transparent-pxy1 PROXY * * -cltTimeout 180 -Listenpolicy "CLIENT.TCP.DSTPORT.EQ(80) || CLIENT.TCP.DSTPORT.EQ(443)"`
```

Vous devrez peut-être configurer les fonctionnalités suivantes, en fonction de votre déploiement :

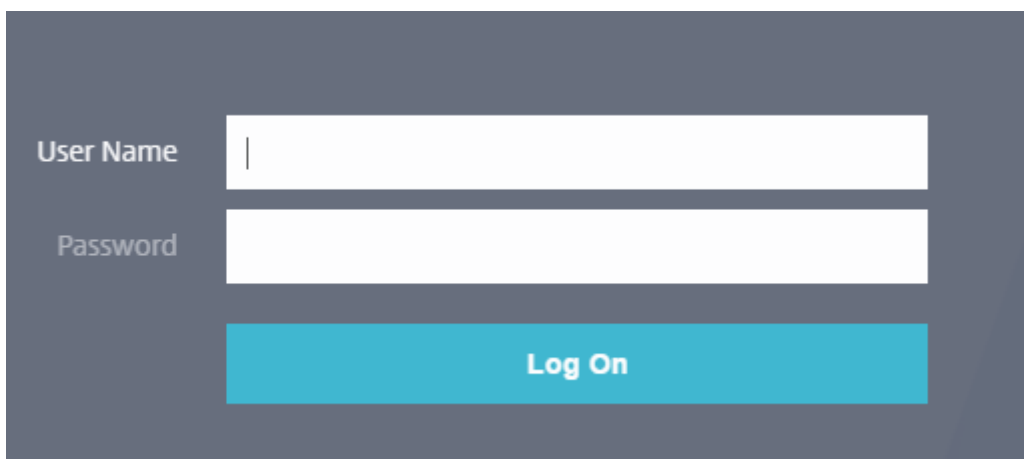
- Service d'authentification (recommandé) —pour authentifier les utilisateurs. Sans le service d'authentification, l'activité de l'utilisateur est basée sur l'adresse IP du client.
- Filtrage d'URL : pour filtrer les URL par catégories, score de réputation et listes d'URL.
- Analytics : permet d'afficher l'activité utilisateur, les indicateurs de risque utilisateur, la consommation de bande passante et les transactions dans Citrix Application Delivery Management (ADM).

Remarque : SWG implémente la majorité des normes HTTP et HTTPS typiques suivies par des produits similaires. Cette implémentation est faite sans navigateur spécifique à l'esprit et est compatible avec la plupart des navigateurs courants. SWG a été testé avec des navigateurs courants et des versions récentes de Google Chrome, Internet Explorer et Mozilla Firefox.

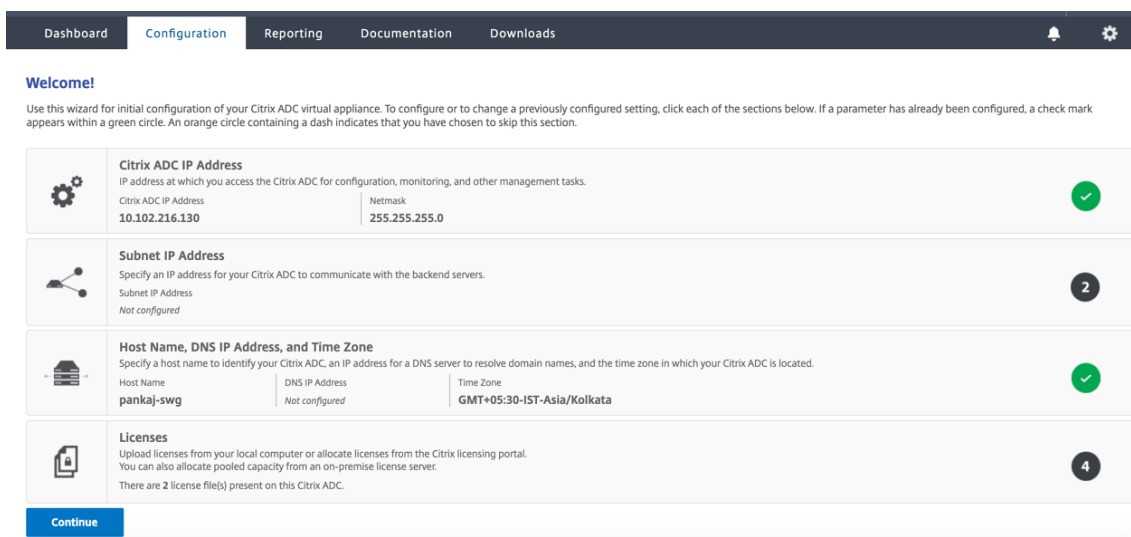
Assistant Passerelle Web sécurisée

L'assistant SWG fournit aux administrateurs un outil permettant de gérer l'ensemble du déploiement SWG à l'aide d'un navigateur Web. Il aide les clients à mettre en place rapidement un service SWG et simplifie la configuration en suivant une séquence d'étapes bien définies.

1. Ouvrez votre navigateur Web et entrez l'adresse NSIP que vous avez spécifiée lors de la configuration initiale. Pour plus d'informations sur la configuration initiale, reportez-vous à la section [Configuration initiale](#).
2. Saisissez votre nom d'utilisateur et votre mot de passe.

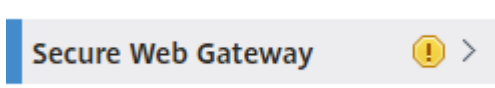


3. Si vous n'avez pas spécifié d'adresse IP de sous-réseau (SNIP), l'écran suivant s'affiche.

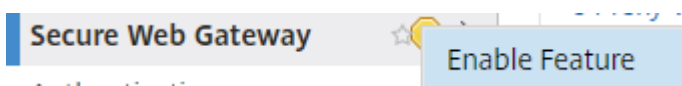


Dans Adresse IP du sous-réseau, entrez une adresse IP et un masque de sous-réseau. La coche dans un cercle vert indique que la valeur est configurée.

4. Dans **Nom d'hôte, Adresse IP DNS et Fuseau horaire**, ajoutez l'adresse IP d'un serveur DNS pour résoudre les noms de domaine et spécifiez votre fuseau horaire.
5. Cliquez sur **Continuer**.
6. (Facultatif) Vous pouvez voir un point d'exclamation, comme suit :



Cette marque indique que la fonction n'est pas activée. Pour activer l'entité, cliquez avec le bouton droit sur l'entité, puis cliquez sur **Activer la fonction**.



7. Dans le volet de navigation, cliquez sur **Secure Web Gateway**. Dans **Mise en route**, cliquez sur **Assistant Secure Web Gateway**.



8. Suivez les étapes de l'Assistant pour configurer votre déploiement.

Ajouter une stratégie d'écoute au serveur proxy transparent

1. Accédez à **Secure Web Gateway > Serveurs proxy**. Sélectionnez le serveur proxy transparent et cliquez sur **Modifier**.
2. Modifiez **les paramètres de base**, puis cliquez sur **Plus**.
3. Dans **Priorité d'écoute**, entrez 1.
4. Dans **Listen Policy Expression**, entrez l'expression suivante :

```
1 (CLIENT.TCP.DSTPORT.EQ(80) || CLIENT.TCP.DSTPORT.EQ(443))
```

Cette expression suppose des ports standard pour le trafic HTTP et HTTPS. Si vous avez configuré différents ports, par exemple 8080 pour HTTP ou 8443 pour HTTPS, modifiez l'expression pour refléter ces ports.

Limitations

SWG n'est pas pris en charge dans une configuration de cluster, dans les partitions d'administration et sur une appliance Citrix ADC FIPS.

Prise en main d'une instance SWG sur une appliance Citrix ADC SDX

April 27, 2021

L'appliance Citrix ADC SDX est une plate-forme multilocataire sur laquelle vous pouvez provisionner et gérer plusieurs instances virtuelles Citrix ADC. L'appliance SDX répond aux exigences de cloud computing et de multilocation en permettant à un administrateur unique de configurer et de gérer l'appliance et de déléguer l'administration de chaque instance hébergée aux locataires. L'appliance SDX

permet à l'administrateur du matériel de fournir à chaque locataire les avantages suivants. Ils sont donnés ci-dessous :

- Une instance complète. Chaque instance dispose des privilèges suivants :
 - Ressources dédiées pour CPU et mémoire
 - Un espace séparé pour les entités
 - L'indépendance pour gérer la libération et la construction de leur choix
 - Indépendance du cycle de vie
- Un réseau complètement isolé. Le trafic destiné à une instance particulière est envoyé uniquement à cette instance.

Si vous n'avez pas déjà installé votre appliance Citrix ADC SDX, reportez-vous à la section [Installation matérielle](#) pour plus d'informations sur l'installation de l'appliance.

Vous devez utiliser le service de gestion pour effectuer la configuration initiale de l'appliance Citrix ADC SDX. Pour de plus amples informations, consultez la section [Prise en main de l'interface utilisateur du service de gestion](#).

Vous pouvez provisionner des instances Citrix SWG sur l'appliance Citrix ADC SDX de la même manière que vous le souhaitez pour une instance Citrix ADC VPX. Pour provisionner une instance SWG sur une appliance SDX, vous devez installer une licence « SDX - 10K sessions simultanées SWG add-on pack ». Cette licence est similaire aux packs d'instances SDX pour VPX, mais elle est exclusive aux instances SWG. Pour plus d'informations sur le Provisioning des instances Citrix ADC, reportez-vous à la section [Provisionnement des instances Citrix ADC](#).

Pour configurer l'instance SWG Citrix pour recevoir du trafic, suivez les instructions de la section [Mise en route d'une appliance Citrix SWG](#).

Modes proxy

April 27, 2021

L'appliance Citrix Secure Web Gateway (SWG) agit comme proxy d'un client pour se connecter aux applications Internet et SaaS. En tant que proxy, il accepte tout le trafic et détermine le protocole du trafic. Sauf si le trafic est HTTP ou SSL, il est transféré à la destination telle quelle. Lorsque l'appliance reçoit une demande d'un client, elle l'intercepte et exécute certaines actions, telles que l'authentification utilisateur, la catégorisation du site et la redirection. Il utilise des stratégies pour déterminer le trafic à autoriser et le trafic à bloquer.

L'appliance gère deux sessions différentes, l'une entre le client et le proxy et l'autre entre le proxy et le serveur d'origine. Le proxy s'appuie sur des stratégies définies par le client pour autoriser ou

bloquer le trafic HTTP et HTTPS. Par conséquent, il est important que vous définissiez des stratégies pour contourner les données sensibles, telles que les informations financières. L'apppliance offre un ensemble complet d'attributs de trafic de couche 4 à couche 7 et d'attributs d'identité utilisateur pour créer des stratégies de gestion du trafic.

Pour le trafic SSL, le proxy vérifie le certificat du serveur d'origine et établit une connexion légitime avec le serveur. Il émule ensuite le certificat du serveur, le signe à l'aide d'un certificat d'autorité de certification installé sur Citrix SWG et présente le certificat de serveur créé au client. Vous devez ajouter le certificat de l'autorité de certification en tant que certificat approuvé au navigateur du client pour que la session SSL soit correctement établie.

L'apppliance prend en charge les modes proxy transparents et explicites. En mode proxy explicite, le client doit spécifier une adresse IP dans son navigateur, à moins que l'organisation n'envoie le paramètre sur le périphérique du client. Cette adresse est l'adresse IP d'un serveur proxy configuré sur l'apppliance SWG. Toutes les demandes client sont envoyées à cette adresse IP. Pour le proxy explicite, vous devez configurer un serveur virtuel de commutation de contenu de type PROXY et spécifier une adresse IP et un numéro de port valide.

Le proxy transparent, comme son nom l'indique, est transparent pour le client. En d'autres termes, les clients peuvent ne pas savoir qu'un serveur proxy effectue la médiation de leurs demandes. L'apppliance SWG est configurée dans un déploiement en ligne et accepte de manière transparente tout le trafic HTTP et HTTPS. Pour le proxy transparent, vous devez configurer un serveur virtuel de commutation de contenu de type PROXY, avec des astérisques (*) comme adresse IP et port. Lorsque vous utilisez l'assistant Secure Web Gateway dans l'interface graphique, vous n'avez pas besoin de spécifier une adresse IP et un port.

Remarque

Pour intercepter des protocoles autres que HTTP et HTTPS en mode proxy transparent, vous devez ajouter une stratégie d'écoute et la lier au serveur proxy.

Configurer le proxy de transfert SSL à l'aide de l'interface de ligne de commande Citrix SWG

À l'invite de commandes, tapez :

```
1 add cs vserver <name> PROXY <ipaddress> <port>
```

Arguments :

Nom :

Nom du serveur proxy. Doit commencer par un caractère alphanumérique ASCII ou un trait de soulignement (_), et ne doit contenir que des caractères alphanumériques ASCII, un trait de souligne-

ment, un hachage (#), un point (.), deux points (:), à (@), égal à (=) et un trait d'union (-). Impossible de modifier une fois le serveur virtuel CS créé.

L'exigence suivante s'applique uniquement à l'interface de ligne de commande :

Si le nom comprend un ou plusieurs espaces, placez le nom entre guillemets doubles ou simples (par exemple, « mon serveur » ou « mon serveur »).

Il s'agit d'un argument obligatoire. Longueur maximale : 127

Adresse IP :

Adresse IP du serveur proxy.

port :

Numéro de port du serveur proxy. Valeur minimale : 1

Exemple de proxy explicite :

```
1 add cs vserver swgVS PROXY 192.0.2.100 80
```

Exemple pour le proxy transparent :

```
1 add cs vserver swgVS PROXY * *
```

Ajouter une stratégie d'écoute au serveur proxy transparent à l'aide de l'interface graphique Citrix SWG

1. Accédez à **Secure Web Gateway > Serveurs proxy**. Sélectionnez le serveur proxy transparent et cliquez sur **Modifier**.
2. Modifiez **les paramètres de base**, puis cliquez sur **Plus**.
3. Dans **Priorité d'écoute**, entrez 1.
4. Dans **Listen Policy Expression**, entrez l'expression suivante :

```
1 (CLIENT.TCP.DSTPORT.EQ(80) || CLIENT.TCP.DSTPORT.EQ(443))
```

Remarque

Cette expression suppose des ports standard pour le trafic HTTP et HTTPS. Si vous avez configuré différents ports, par exemple 8080 pour HTTP ou 8443 pour HTTPS, modifiez l'expression ci-dessus pour spécifier ces ports.

Interception SSL

April 27, 2021

Une appliance Citrix Secure Web Gateway (SWG) configurée pour l'interception SSL agit comme un proxy. Il peut intercepter et déchiffrer le trafic SSL/TLS, inspecter la demande non chiffrée et permettre à un administrateur d'appliquer les règles de conformité et les contrôles de sécurité. SSL Interception utilise une stratégie qui spécifie le trafic à intercepter, bloquer ou autoriser. Par exemple, le trafic vers et en provenance de sites Web financiers, comme les banques, ne doit pas être intercepté, mais d'autres trafic peuvent être interceptés, et les sites sur liste rouge peuvent être identifiés et bloqués. Citrix vous recommande de configurer une stratégie générique pour intercepter le trafic et des stratégies plus spécifiques pour contourner un certain trafic.

Le client et le proxy Citrix SWG établissent une connexion HTTP/TLS. Le proxy SWG établit une autre connexion HTTPS/TLS avec le serveur et reçoit le certificat du serveur. Le proxy vérifie le certificat du serveur au nom du client et vérifie également la validité du certificat du serveur à l'aide du protocole OCSP (Online Certificate Status Protocol). Il régénère le certificat du serveur, le signe à l'aide de la clé du certificat de l'autorité de certification installée sur l'appliance et le présente au client. Par conséquent, un certificat est utilisé entre le client et le dispositif Citrix ADC, et un autre certificat entre l'appliance et le serveur principal.

Important

Le certificat d'autorité de certification utilisé pour signer le certificat de serveur doit être préinstallé sur tous les périphériques clients, de sorte que le certificat de serveur régénéré soit approuvé par le client.

Pour le trafic HTTPS intercepté, le serveur proxy SWG déchiffre le trafic sortant, accède à la requête HTTP en texte clair et peut utiliser n'importe quelle application de couche 7 pour traiter le trafic, par exemple en consultant l'URL de texte brut et en autorisant ou bloquant l'accès sur la base de la stratégie d'entreprise et de la réputation d'URL. Si la décision de stratégie est d'autoriser l'accès au serveur d'origine, le serveur proxy transmet la requête chiffrée au service de destination (sur le serveur d'origine). Le proxy déchiffre la réponse à partir du serveur d'origine, accède à la réponse HTTP en texte clair et applique éventuellement toutes les stratégies à la réponse. Le proxy recrypte ensuite la réponse et la transmet au client. Si la décision de stratégie consiste à bloquer la demande au serveur d'origine, le proxy peut envoyer une réponse d'erreur, telle que HTTP 403, au client.

Pour effectuer l'interception SSL, en plus du serveur proxy configuré précédemment, vous devez configurer les éléments suivants sur une appliance SWG :

- Profil SSL
- Stratégie SSL

- Magasin de certificats CA
- Apprentissage automatique des erreurs SSL et mise en cache

Profil SSL

April 27, 2021

Un profil SSL est un ensemble de paramètres SSL, tels que les chiffrements et les protocoles. Un profil est utile si vous avez des paramètres communs pour différents serveurs. Au lieu de spécifier les mêmes paramètres pour chaque serveur, vous pouvez créer un profil, spécifier les paramètres dans le profil, puis lier le profil à différents serveurs. Si aucun profil SSL frontal personnalisé n'est créé, le profil frontal par défaut est lié aux entités côté client. Ce profil vous permet de configurer les paramètres de gestion des connexions côté client. Pour l'interception SSL, vous devez créer un profil SSL et activer l'interception SSL (SSLi) dans le profil. Un groupe de chiffrement par défaut est lié à ce profil, mais vous pouvez configurer d'autres chiffrements en fonction de votre déploiement. Vous devez lier un certificat d'autorité de certification SSL à ce profil, puis lier le profil à un serveur proxy. Pour l'interception SSL, les paramètres essentiels d'un profil sont ceux utilisés pour vérifier l'état OCSP du certificat du serveur d'origine, déclencher la renégociation du client si le serveur d'origine demande une renégociation et vérifier le certificat du serveur d'origine avant de réutiliser la session SSL frontale. Vous devez utiliser le profil principal par défaut lorsque vous communiquez avec les serveurs d'origine. Définissez tous les paramètres côté serveur, tels que les suites de chiffrement, dans le profil principal par défaut. Un profil principal personnalisé n'est pas pris en charge.

Pour obtenir des exemples des paramètres SSL les plus couramment utilisés, consultez « Exemple de profil » à la fin de cette section.

La prise en charge du chiffre/protocole diffère sur le réseau interne et externe. Dans les tableaux suivants, la connexion entre les utilisateurs et une appliance SWG est le réseau interne. Le réseau externe se trouve entre l'appliance et Internet.

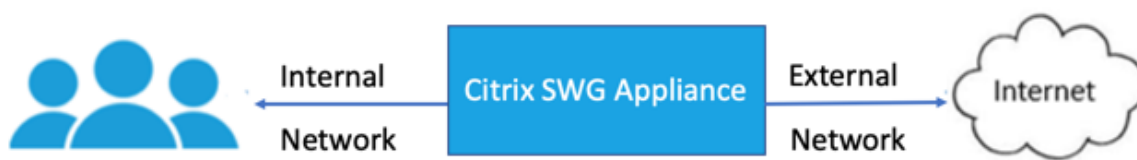


Tableau 1 : Matrice de prise en charge du chiffre/protocole pour le réseau interne

(Chiffrement/Protocole)/Plateforme	MPX (N3)*	VPX
TLS 1.1/1.2	12.1	12.1
ECDHE/DHE (Exemple TLS1-ECDHE-RSA-AES128-SHA)	12.1	12.1
AES-GCM (Exemple TLS1.2-AES128-GCM-SHA256)	12.1	12.1
Ciphers SHA-2 (Exemple TLS1.2-AES-128-SHA256)	12.1	12.1
ECDSA (Exemple TLS1-ECDHE- ECDSA-AES256-SHA)	12.1	12.1

Tableau 2 : Matrice de prise en charge du chiffre/protocole pour le réseau externe

(Chiffrement/Protocole)/Plateforme	MPX (N3)*	VPX
TLS 1.1/1.2	12.1	12.1
ECDHE/DHE (Exemple TLS1-ECDHE-RSA-AES128-SHA)	12.1	12.1
AES-GCM (Exemple TLS1.2-AES128-GCM-SHA256)	12.1	12.1
Ciphers SHA-2 (Exemple TLS1.2-AES-128-SHA256)	12.1	12.1
ECDSA (Exemple TLS1-ECDHE- ECDSA-AES256-SHA)	12.1	Non pris en charge

* Utilisez la commande **sh hardware** (show hardware) pour déterminer si votre appliance possède des puces N3.

Exemple :

```

1 sh hardware
2
3 Platform: NSMPX-22000 16\*CPU+24\*IX+12\*E1K+2\*E1K+4*CVM N3 2200100
4
5 Manufactured on: 8/19/2013
6
7 CPU: 2900MHZ
8
9 Host Id: 1006665862
10
11 Serial no: ENUK6298FT

```

```
12
13 Encoded serial no: ENUK6298FT
14
15 Done
```

Ajouter un profil SSL et activer l'interception SSL à l'aide de l'interface de ligne de commande Citrix SWG

À l'invite de commandes, tapez :

```
add ssl profile <name> -sslinterception ENABLED -ssliReneg ( ENABLED
| DISABLED )-ssliOCSPCheck ( ENABLED | DISABLED )-ssliMaxSessPerServer
<positive_integer>
```

Arguments :

sslInterception:

Activer ou désactiver l'interception des sessions SSL.

Valeurs possibles : ENABLED, DISABLED

Valeur par défaut : DISABLED

ssliReneg:

Activez ou désactivez le déclenchement de la renégociation client lorsqu'une demande de renégociation est reçue du serveur d'origine.

Valeurs possibles : ENABLED, DISABLED

Valeur par défaut : ENABLED

ssliOCSPCheck:

Activez ou désactivez la vérification OCSP pour un certificat de serveur d'origine.

Valeurs possibles : ENABLED, DISABLED

Valeur par défaut : ENABLED

ssliMaxSessPerServer:

Nombre maximal de sessions SSL à mettre en cache par serveur d'origine dynamique. Une session SSL unique est créée pour chaque extension SNI reçue du client dans un message de bonjour client. La session correspondante est utilisée pour la réutilisation de session serveur.

Valeur par défaut : 10

Valeur minimale : 1

Valeur maximale : 1000

Example :

```
1 add ssl profile swg_ssl_profile -sslinterception ENABLED
2
3 Done
4
5 sh ssl profile swg_ssl_profile
6
7 1) Name: swg_ssl_profile (Front-End)
8
9          SSLv3: DISABLED          TLSv1.0: ENABLED  TLSv1
          .1: ENABLED  TLSv1.2: ENABLED
10
11          Client Auth: DISABLED
12
13          Use only bound CA certificates: DISABLED
14
15          Strict CA checks:                      NO
16
17          Session Reuse: ENABLED
          Timeout: 120 seconds
18
19          DH: DISABLED
20
21          DH Private-Key Exponent Size Limit: DISABLED
          Ephemeral RSA: ENABLED
          Refresh Count: 0
22
23          Deny SSL Renegotiation
          ALL
24
25          Non FIPS Ciphers: DISABLED
26
27          Cipher Redirect: DISABLED
28
29          SSL Redirect: DISABLED
30
31          Send Close-Notify: YES
32
33          Strict Sig-Digest Check: DISABLED
34
35          Push Encryption Trigger: Always
36
37          PUSH encryption trigger timeout:          1 ms
38
39          SNI: DISABLED
40
41          OCSP Stapling: DISABLED
42
43          Strict Host Header check for SNI enabled SSL sessions:
          NO
44
45          Push flag:          0x0 (Auto)
46
```

```
47      SSL quantum size:                               8 kB
48
49      Encryption trigger timeout                       100 mS
50
51      Encryption trigger packet count:                 45
52
53      Subject/Issuer Name Insertion Format: Unicode
54
55      SSL Interception: ENABLED
56
57      SSL Interception OCSP Check: ENABLED
58
59      SSL Interception End to End Renegotiation: ENABLED
60
61      SSL Interception Server Cert Verification for Client
        Reuse: ENABLED
62
63      SSL Interception Maximum Reuse Sessions per Server: 10
64
65      Session Ticket: DISABLED                          Session Ticket
        Lifetime: 300 (secs)
66
67      HSTS: DISABLED
68
69      HSTS IncludeSubDomains: NO
70
71      HSTS Max-Age: 0
72
73      ECC Curve: P_256, P_384, P_224, P_521
74
75 1)      Cipher Name: DEFAULT Priority :1
76
77          Description: Predefined Cipher Alias
78
79 Done
```

Lier un certificat d'autorité de certification d'interception SSL à un profile SSL à l'aide de l'interface de ligne de commande Citrix SWG

À l'invite de commandes, tapez :

```
bind ssl profile <name> -ssliCACertkey <ssli-ca-cert >
```

Exemple :

```
1 bind ssl profile swg_ssl_profile -ssliCACertkey swg_ca_cert
2
3 Done
4
5 sh ssl profile swg_ssl_profile
6
```

```
7 1) Name: swg_ssl_profile (Front-End)
8
9     SSLv3: DISABLED           TLSv1.0: ENABLED  TLSv1
    .1: ENABLED  TLSv1.2: ENABLED
10
11     Client Auth: DISABLED
12
13     Use only bound CA certificates: DISABLED
14
15     Strict CA checks:                               NO
16
17     Session Reuse: ENABLED
    Timeout: 120 seconds
18
19     DH: DISABLED
20
21     DH Private-Key Exponent Size Limit: DISABLED
    Ephemeral RSA: ENABLED
    Refresh Count: 0
22
23     Deny SSL Renegotiation
    ALL
24
25     Non FIPS Ciphers: DISABLED
26
27     Cipher Redirect: DISABLED
28
29     SSL Redirect: DISABLED
30
31     Send Close-Notify: YES
32
33     Strict Sig-Digest Check: DISABLED
34
35     Push Encryption Trigger: Always
36
37     PUSH encryption trigger timeout:                 1 ms
38
39     SNI: DISABLED
40
41     OCSP Stapling: DISABLED
42
43     Strict Host Header check for SNI enabled SSL sessions:
    NO
44
45     Push flag:           0x0 (Auto)
46
47     SSL quantum size:           8 kB
48
49     Encryption trigger timeout           100 mS
50
51     Encryption trigger packet count:           45
52
53     Subject/Issuer Name Insertion Format: Unicode
```



```
54
55         SSL Interception: ENABLED
56
57         SSL Interception OCSP Check: ENABLED
58
59         SSL Interception End to End Renegotiation: ENABLED
60
61         SSL Interception Server Cert Verification for Client
62             Reuse: ENABLED
63
64         SSL Interception Maximum Reuse Sessions per Server: 10
65
66         Session Ticket: DISABLED           Session Ticket
67             Lifetime: 300 (secs)
68
69         HSTS: DISABLED
70
71         HSTS IncludeSubDomains: NO
72
73         HSTS Max-Age: 0
74
75         ECC Curve: P_256, P_384, P_224, P_521
76
77         1) Cipher Name: DEFAULT Priority :1
78             Description: Predefined Cipher Alias
79
80         1) SSL Interception CA CertKey Name: swg_ca_cert
81 Done
```

Lier un certificat d'autorité de certification d'interception SSL à un profile SSL à l'aide de l'interface graphique Citrix SWG

1. Accédez à **Système > Profils > Profil SSL**.
2. Cliquez sur **Ajouter**.
3. Spécifiez un nom pour le profil.
4. Activer l'**interception des sessions SSL**.
5. Cliquez sur **OK**.
6. Dans **Paramètres avancés**, cliquez sur **Clé de certificat**.
7. Spécifiez une clé de certificat SSLi CA à lier au profil.
8. Cliquez sur **Sélectionner**, puis sur **Lier**.
9. Vous pouvez également configurer les chiffrements en fonction de votre déploiement.

- Cliquez sur l'icône Modifier, puis cliquez sur **Ajouter**.
- Sélectionnez un ou plusieurs groupes de chiffrement, puis cliquez sur la flèche droite.
- Cliquez sur **OK**.

10. Cliquez sur **Terminé**.

Liez un profil SSL à un serveur proxy à l'aide de l'interface graphique Citrix SWG

1. Accédez à **Secure Web Gateway > Serveurs proxy**, puis ajoutez un nouveau serveur ou sélectionnez un serveur à modifier.
2. Dans **Profil SSL**, cliquez sur l'icône Modifier.
3. Dans la liste **Profil SSL**, sélectionnez le profil SSL que vous avez créé précédemment.
4. Cliquez sur **OK**.
5. Cliquez sur **Terminé**.

Exemple de profil :

```

1 Name: swg_ssl_profile (Front-End)
2
3         SSLv3: DISABLED           TLSv1.0: ENABLED  TLSv1
         .1: ENABLED  TLSv1.2: ENABLED
4
5         Client Auth: DISABLED
6
7         Use only bound CA certificates: DISABLED
8
9         Strict CA checks:                               NO
10
11        Session Reuse: ENABLED
         Timeout: 120 seconds
12
13        DH: DISABLED
14
15        DH Private-Key Exponent Size Limit: DISABLED
         Ephemeral RSA: ENABLED
         Refresh Count: 0
16
17        Deny SSL Renegotiation
         ALL
18
19        Non FIPS Ciphers: DISABLED
20
21        Cipher Redirect: DISABLED
22
23        SSL Redirect: DISABLED
24
25        Send Close-Notify: YES
26
27        Strict Sig-Digest Check: DISABLED

```

```
28
29     Push Encryption Trigger: Always
30
31     PUSH encryption trigger timeout:           1 ms
32
33     SNI: DISABLED
34
35     OCSP Stapling: DISABLED
36
37     Strict Host Header check for SNI enabled SSL sessions:
38         NO
39
40     Push flag:           0x0 (Auto)
41
42     SSL quantum size:           8 kB
43
44     Encryption trigger timeout           100 mS
45
46     Encryption trigger packet count:           45
47
48     Subject/Issuer Name Insertion Format: Unicode
49
50     SSL Interception: ENABLED
51
52     SSL Interception OCSP Check: ENABLED
53
54     SSL Interception End to End Renegotiation: ENABLED
55
56     SSL Interception Maximum Reuse Sessions per Server: 10
57
58     Session Ticket: DISABLED           Session Ticket
59         Lifetime: 300 (secs)
60
61     HSTS: DISABLED
62
63     HSTS IncludeSubDomains: NO
64
65     HSTS Max-Age: 0
66
67     ECC Curve: P_256, P_384, P_224, P_521
68
69     1) Cipher Name: DEFAULT Priority :1
70         Description: Predefined Cipher Alias
71
72     1) SSL Interception CA CertKey Name: swg_ca_cert
```

Infrastructure de stratégie SSL pour l'interception SSL

April 27, 2021

Une stratégie agit comme un filtre sur le trafic entrant. Les stratégies de l'appliance Citrix Secure Web Gateway (SWG) permettent de définir comment gérer les connexions et les demandes par proxy. Le traitement est basé sur les actions configurées pour cette stratégie. Autrement dit, les données des demandes de connexion sont comparées à une règle spécifiée dans la stratégie et l'action est appliquée aux connexions qui correspondent à la règle (expression). Après avoir défini une action pour la stratégie et créé la stratégie, liez-la à un serveur proxy, de sorte qu'elle s'applique au trafic circulant à travers ce serveur proxy.

Une stratégie SSL pour l'interception SSL évalue le trafic entrant et applique une action prédéfinie aux requêtes qui correspondent à une règle (expression). La décision d'intercepter, de contourner ou de réinitialiser une connexion est prise en fonction de la stratégie SSL définie. Vous pouvez configurer l'une des trois actions d'une stratégie : Intercept, BYPASS ou RESET. Spécifiez une action lorsque vous créez une stratégie. Pour appliquer une stratégie, vous devez la lier à un serveur proxy de l'appliance. Pour spécifier qu'une stratégie est destinée à l'interception SSL, vous devez spécifier le type (point de liaison) comme INTERCEPT_REQ lorsque vous liez la stratégie à un serveur proxy. Lorsque vous dissociez une stratégie, vous devez spécifier le type INTERCEPT_REQ.

Note :

Le serveur proxy ne peut décider d'intercepter que si vous spécifiez une stratégie.

L'interception du trafic peut être basée sur n'importe quel attribut de poignée de main SSL. Le plus couramment utilisé est le domaine SSL. Le domaine SSL est généralement indiqué par les attributs de la poignée de main SSL. Il peut s'agir de la valeur de l'indicateur de nom de serveur extraite du message Hello client SSL, le cas échéant, ou de la valeur de nom alternatif de serveur (SAN) extraite du certificat du serveur d'origine. La stratégie SSLi sur Citrix SWG présente un attribut spécial nommé DETECTED_DOMAIN, qui facilite la création de stratégies d'interception basées sur le domaine SSL à partir du certificat du serveur d'origine. Le client peut faire correspondre le nom de domaine avec une chaîne, une liste d'URL (jeu d'URL ou [patset](#)) ou une catégorie d'URL dérivée du domaine.

Créer une stratégie SSL à l'aide de l'interface de ligne de commande Citrix SWG

À l'invite de commandes, tapez :

```
1 add ssl policy <name> -rule <expression> -action <string>
```

Exemples :

Les exemples suivants concernent les stratégies avec des expressions qui utilisent l'attribut `detected_domain` pour rechercher un nom de domaine.

Ne pas intercepter le trafic vers une institution financière, telle que XYZBANK

```
1 add ssl policy pol1 -rule client.ssl.detected_domain.contains("XYZBANK") -action BYPASS
```

Ne permettez pas à un utilisateur de se connecter à YouTube à partir du réseau d'entreprise.

```
1 add ssl policy pol2 -rule client.ssl.client.ssl.detected_domain.url_categorize(0,0).category.eq("YouTube") -action RESET
```

Intercepter tout le trafic utilisateur.

```
1 add ssl policy pol3 -rule true -action INTERCEPT
```

Si le client ne souhaite pas utiliser le domaine `detected_domain`, il peut utiliser l'un des attributs de handshake SSL pour extraire et déduire le domaine.

Par exemple, un nom de domaine est introuvable dans l'extension SNI du message client Hello. Le nom de domaine doit être extrait du certificat du serveur d'origine. Les exemples suivants concernent les stratégies avec des expressions qui vérifient la présence d'un nom de domaine dans le nom de sujet du certificat du serveur d'origine.

Interceptez tout le trafic utilisateur vers n'importe quel domaine Yahoo.

```
1 add ssl policy pol4 -rule client.ssl.origin_server_cert.subject.contains("yahoo") -action INTERCEPT
```

Intercepter tout le trafic utilisateur pour la catégorie « Shopping/Retail ».

```
1 add ssl policy pol_url_category -rule client.ssl.origin_server_cert.subject.URL_CATEGORIZE(0,0).CATEGORY.eq("Shopping/Retail") -action INTERCEPT
```

Interceptez tout le trafic utilisateur vers une URL non catégorisée.

```
1 add ssl policy pol_url_category -rule client.ssl.origin_server_cert.subject.url_categorize(0,0).category.eq("Uncategorized") -action INTERCEPT
```

Les exemples suivants concernent les stratégies qui correspondent au domaine par rapport à une entrée d'un jeu d'URL.

Interceptez tout le trafic utilisateur si le nom de domaine dans SNI correspond à une entrée du jeu d'URL « top100 ».

```
1 add ssl policy pol_url_set -rule client.ssl.client_hello.SNI.URLSET_MATCHES_ANY("top100") -action INTERCEPT
```

Interceptez tout le trafic utilisateur du nom de domaine si le certificat du serveur d'origine correspond à une entrée du jeu d'URL « top100 ».

```
1 add ssl policy pol_url_set -rule client.ssl.origin_server_cert.subject
   .URLSET_MATCHES_ANY("top100") -action INTERCEPT
```

Créer une stratégie SSL sur un serveur proxy à l'aide de l'interface graphique SWG

1. Accédez à **Secure Web Gateway > SSL > Stratégies**.
2. Sous l'onglet **Stratégies SSL**, cliquez sur **Ajouter** et spécifiez les paramètres suivants :
 - Nom de la stratégie
 - Action de stratégie : sélectionnez l'interception, le contournement ou la réinitialisation.
 - Expression.
3. Cliquez sur **Créer**.

Liez une stratégie SSL à un serveur proxy à l'aide de l'interface de ligne de commande SWG

À l'invite de commandes, tapez :

```
1 bind ssl vserver <vServerName> -policyName <string> -priority <
   positive_integer> -type INTERCEPT_REQ
```

Exemple :

```
1 bind ssl vserver <name> -policyName pol1 -priority 10 -type
   INTERCEPT_REQ
```

Liez une stratégie SSL à un serveur proxy à l'aide de l'interface graphique Citrix SWG

1. Accédez à **Secure Web Gateway > Serveurs virtuels proxy**.
2. Sélectionnez un serveur virtuel et cliquez sur **Modifier**.
3. Dans **Paramètres avancés**, cliquez sur **Stratégies SSL**.
4. Cliquez dans la zone **Stratégie SSL**.
5. Dans **Sélectionner une stratégie**, sélectionnez une stratégie à lier.
6. Dans **Type**, sélectionnez **INTERCEPT_REQ**.
7. Cliquez sur **Lier**, puis sur **OK**.

Délier une stratégie SSL à un serveur proxy à l'aide de la ligne de commande

À l'invite de commandes, tapez :

```
1 unbind ssl vserver <vServerName> -policyName <string> -type
  INTERCEPT_REQ
```

Expressions SSL utilisées dans les stratégies SSL pour SWG

Expression.	Description
<code>CLIENT.SSL.CLIENT_HELLO.SNI.*</code>	Renvoie l'extension SNI dans un format de chaîne. Évaluez la chaîne pour voir si elle contient le texte spécifié. Exemple : client.ssl.client_hello.sni.contains ("xyz.com")
<code>CLIENT.SSL.ORIGIN_SERVER_CERT.*</code>	Renvoie un certificat, reçu d'un serveur principal, au format chaîne. Évaluez la chaîne pour voir si elle contient le texte spécifié. Exemple : client.ssl.origin_server_cert.subject.contains ("xyz.com")
<code>CLIENT.SSL.DETECTED_DOMAIN.*</code>	Renvoie un domaine, à partir de l'extension SNI ou du certificat du serveur d'origine, au format chaîne. Évaluez la chaîne pour voir si elle contient le texte spécifié. Exemple : client.ssl.detected_domain.contains ("xyz.com")

Magasin de certificats d'interception SSL

April 27, 2021

Un certificat SSL, qui fait partie intégrante de toute transaction SSL, est un formulaire de données numériques (X509) qui identifie une entreprise (domaine) ou un individu. Un certificat SSL est délivré par une autorité de certification (CA). Une AC peut être privée ou publique. Les certificats émis par des autorités de certification publiques, telles que Verisign, sont approuvés par les applications qui effectuent des transactions SSL. Ces applications tiennent à jour une liste d'autorités de certification qu'elles ont confiance.

En tant que proxy de transfert, une appliance Citrix Secure Web Gateway (SWG) effectue le chiffrement et le déchiffrement du trafic entre un client et un serveur. Il agit comme un serveur pour le client (utilisateur) et comme un client pour le serveur. Pour qu'une appliance puisse traiter le trafic HTTPS, elle doit valider l'identité d'un serveur afin d'éviter toute transaction frauduleuse. Par conséquent, en tant que client du serveur d'origine, l'appliance doit vérifier le certificat du serveur d'origine avant de l'accepter. Pour vérifier le certificat d'un serveur, tous les certificats (par exemple, certificats racine et intermédiaire) utilisés pour signer et émettre le certificat de serveur doivent être présents sur l'appliance. Un ensemble de certificats d'autorité de certification par défaut est préinstallé sur une appliance. Le Citrix SWG peut utiliser ces certificats pour vérifier presque tous les certificats d'origine et de serveur courants. Ce jeu par défaut ne peut pas être modifié. Toutefois, si votre déploiement nécessite plus de certificats d'autorité de certification, vous pouvez créer un ensemble de ces certificats et importer le bundle dans l'appliance. Un bundle peut également contenir un seul certificat.

Lorsque vous importez un bundle de certificats sur l'appliance, celle-ci télécharge le bundle à partir de l'emplacement distant et, après avoir vérifié que le bundle contient uniquement des certificats, l'installe sur l'appliance. Vous devez appliquer un ensemble de certificats avant de pouvoir l'utiliser pour valider un certificat de serveur. Vous pouvez également exporter un ensemble de certificats pour modification ou le stocker dans un emplacement hors connexion en tant que sauvegarde.

Importer et appliquer un ensemble de certificats d'autorité de certification sur l'appliance à l'aide de l'interface de ligne de commande Citrix SWG

À l'invite de commandes, tapez :

```
1 import ssl certBundle <name> <src>
```

```
1 apply ssl certBundle <name>
```

```
1 show ssl certBundle
```

ARGUMENTS :

Nom :

Nom à affecter à l'ensemble de certificats importé. Doit commencer par un caractère alphanumérique ASCII ou un trait de soulignement (_), et ne doit contenir que des caractères alphanumériques ASCII, un trait de soulignement, un hachage (#), un point (.), deux points (:), à (@), égal à (=) et un trait d'union (-). L'exigence suivante s'applique uniquement à l'interface de ligne de commande :

Si le nom comprend un ou plusieurs espaces, placez le nom entre guillemets doubles ou simples (par exemple, "mon fichier" ou 'mon fichier').

Longueur maximale : 31

src :

URL spécifiant le protocole, l'hôte et le chemin d'accès, y compris le nom du fichier, au bundle de certificats à importer ou à exporter. Par exemple, `http://www.example.com/cert_bundle_file`.

REMARQUE : L'importation échoue si l'objet à importer se trouve sur un serveur HTTPS qui nécessite l'authentification de certificat client pour l'accès.

Longueur maximale : 2047

Exemple :

```
1 import ssl certbundle swg-certbundle http://www.example.com/cert_bundle
```

```
1 apply ssl certBundle swg-certbundle
```

```
1 show ssl certbundle
2
3     Name : swg-certbundle(Inuse)
4
5     URL  : http://www.example.com/cert_bundle
6
7     Done
```

Importez et appliquez un ensemble de certificats d'autorité de certification sur l'appliance à l'aide de l'interface graphique de Citrix SWG

1. Accédez à **Secure Web Gateway > Mise en route > Bundles de certificats**.
2. Procédez comme suit :
 - Sélectionnez un ensemble de certificats dans la liste.
 - Pour ajouter un nouveau paquet de certificats, cliquez sur « + » et indiquez un nom et une URL source. Cliquez sur **OK**.
3. Cliquez sur **OK**.

Supprimez un ensemble de certificats d'autorité de certification de l'appliance à l'aide de l'interface de ligne de commande

À l'invite de commandes, tapez :

```
1 remove certBundle <cert bundle name>
```

Exemple :

```
1 remove certBundle mytest-cacert
```

Exporter un ensemble de certificats d'autorité de certification à partir de l'appliance à l'aide de l'interface de ligne de commande Citrix SWG

À l'invite de commandes, tapez :

```
1 export certBundle <cert bundle name> <Path to export>
```

ARGUMENTS :

Nom :

Nom à affecter à l'ensemble de certificats importé. Doit commencer par un caractère alphanumérique ASCII ou un trait de soulignement (_), et ne doit contenir que des caractères alphanumériques ASCII, un trait de soulignement, un hachage (#), un point (.), deux points (:), à (@), égal à (=) et un trait d'union (-). L'exigence suivante s'applique uniquement à l'interface de ligne de commande :

Si le nom comprend un ou plusieurs espaces, placez le nom entre guillemets doubles ou simples (par exemple, "mon fichier" ou 'mon fichier').

Longueur maximale : 31

src :

URL spécifiant le protocole, l'hôte et le chemin d'accès, y compris le nom du fichier, au bundle de certificats à importer ou à exporter. Par exemple, http://www.example.com/cert_bundle_file.

REMARQUE : L'importation échoue si l'objet à importer se trouve sur un serveur HTTPS qui nécessite l'authentification de certificat client pour l'accès.

Longueur maximale : 2047

Exemple :

```
1 export certBundle mytest-cacert http://192.0.2.20/
```

Importer, appliquer et vérifier un ensemble de certificats de l'autorité de certification à partir du magasin de certificats de l'autorité de certification Mozilla CA

À l'invite de commandes, tapez :

```
1 > import certbundle mozilla_public_ca https://curl.haxx.se/ca/cacert.  
pem  
2 Done
```

Pour appliquer le bundle, tapez :

```
1 > apply certbundle mozilla_public_ca  
2 Done
```

Pour vérifier l'ensemble de certificats en cours d'utilisation, tapez :

```
1 > sh certbundle | grep mozilla
2     Name : mozilla_public_ca (Inuse)
```

Limitation

Les lots de certificats ne sont pas pris en charge dans une configuration de cluster ou sur une appliance partitionnée.

Apprentissage automatique des erreurs SSL

April 27, 2021

L'appliance Citrix SWG ajoute un domaine à la liste de contournement SSL si le mode d'apprentissage est activé. Le mode d'apprentissage est basé sur le message d'alerte SSL reçu d'un client ou d'un serveur d'origine. C'est-à-dire que l'apprentissage dépend de l'envoi d'un message d'alerte par le client ou le serveur. Il n'y a pas d'apprentissage si un message d'alerte n'est pas envoyé. L'appliance apprend si l'une des conditions suivantes est remplie :

1. Une demande de certificat client est reçue du serveur.
2. L'une des alertes suivantes est reçue dans le cadre de la poignée de main :
 - BAD_CERTIFICATE
 - UNSUPPORTED_CERTIFICATE
 - CERTIFICATE_REVOKED
 - CERTIFICATE_EXPIRED
 - CERTIFICATE_UNKNOWN
 - UNKNOWN_CA (Si un client utilise l'épinglage, il envoie ce message d'alerte s'il reçoit un certificat de serveur.)
 - HANDSHAKE_FAILURE

Pour activer l'apprentissage, vous devez activer le cache d'erreurs et spécifier la mémoire réservée pour cela.

Activer l'apprentissage à l'aide de l'interface graphique Citrix SWG

1. Accédez à **Secure Web Gateway > SSL**.
2. Dans **Paramètres**, cliquez sur **Modifier les paramètres SSL avancés**.

3. Dans **Interception SSL**, sélectionnez **SSL Interception Error Cache**.
4. Dans **SSL Interception Max Error Cache Memory**, spécifiez la mémoire (en octets) à réserver.

The screenshot shows a dialog box titled "SSL Interception". It contains a checked checkbox for "SSL Interception Error Cache". Below it is a text input field for "SSL Interception Max Error Cache Memory" with the value "1048576". At the bottom, there are two buttons: "OK" and "Close".

5. Cliquez sur **OK**.

Activer l'apprentissage à l'aide de l'interface de ligne de commande Citrix SWG

À l'invite de commandes, tapez :

```
set ssl parameter -ssliErrorCache ( ENABLED | DISABLED )-ssliMaxErrorCacheMem
<positive_integer>
```

Arguments :

SSLierrorCache :

```
1      Activez ou désactivez l'apprentissage dynamique et mettez en
      cache les informations apprises pour prendre les décisions
      suivantes d'intercepter ou de contourner les demandes.
      Lorsqu'elle est activée, l'appliance effectue une
      recherche de cache pour décider s'il faut contourner la
      demande.
2
3      Valeurs possibles : `ENABLED, DISABLED`
4
5      Valeur par défaut : `DISABLED`
```

SSLIMaxErrorCacheMem :

```
1      Spécifiez la mémoire maximale, en octets, qui peut être
      utilisée pour mettre en cache les données apprises. Cette
      mémoire est utilisée comme cache LRU de sorte que les
      anciennes entrées sont remplacées par de nouvelles entrées
      après épuisement de la limite de mémoire définie. La
      valeur 0 détermine automatiquement la limite.
2
3      Valeur par défaut : 0
4
5      Valeur minimale : 0
6
```

Gestion des identités utilisateur

April 27, 2021

Un nombre croissant de violations de la sécurité et la popularité croissante des appareils mobiles ont souligné la nécessité de veiller à ce que l'utilisation de l'Internet externe soit conforme aux politiques de l'entreprise et que seuls les utilisateurs autorisés accèdent aux ressources externes fournies par le personnel de l'entreprise. La gestion des identités permet de vérifier l'identité d'une personne ou d'un appareil. Il ne détermine pas les tâches que l'individu peut effectuer ni les fichiers qu'il peut voir.

Un déploiement de Secure Web Gateway (SWG) identifie l'utilisateur avant d'autoriser l'accès à Internet. Toutes les demandes et réponses de l'utilisateur sont inspectées. L'activité de l'utilisateur est consignée et les enregistrements sont exportés vers Citrix Application Delivery Management (ADM) à des fins de création de rapports. Dans Citrix ADM, vous pouvez afficher les statistiques sur les activités utilisateur, les transactions et la consommation de bande passante.

Par défaut, seule l'adresse IP de l'utilisateur est enregistrée, mais vous pouvez configurer l'appliance Citrix SWG pour enregistrer plus de détails sur l'utilisateur et utiliser ces informations d'identité pour créer des stratégies d'utilisation Internet plus riches pour des utilisateurs spécifiques.

L'appliance Citrix ADC prend en charge les modes d'authentification suivants pour une configuration de proxy explicite.

- **LDAP (Lightweight Directory Access Protocol)**. Authentifie l'utilisateur via un serveur d'authentification LDAP externe. Pour de plus amples informations, consultez la section [Stratégies d'authentification LDAP](#).
- **RAYON**. Authentifie l'utilisateur via un serveur RADIUS externe. Pour de plus amples informations, consultez la section [Stratégies d'authentification RADIUS](#).
- **TACACS+**. Authentifie l'utilisateur via un serveur d'authentification TACACS (Terminal Access Controller Access-Control System) externe. Pour de plus amples informations, consultez la section [Stratégies d'authentification](#).
- **Negotiate**. Authentifie l'utilisateur via un serveur d'authentification Kerberos. En cas d'erreur dans l'authentification Kerberos, l'appliance utilise l'authentification NTLM. Pour de plus amples informations, consultez la section [Négocier des stratégies d'authentification](#).

Pour le proxy transparent, seule l'authentification LDAP basée sur IP est actuellement prise en charge. Lorsqu'une demande client est reçue, le proxy authentifie l'utilisateur en vérifiant une entrée pour l'adresse IP du client dans l'annuaire actif et crée une session basée sur l'adresse IP de l'utilisateur.

Toutefois, si vous configurez l'attribut `SsonameAttribute` dans une action LDAP, une session est créée à l'aide du nom d'utilisateur au lieu de l'adresse IP. Les stratégies classiques ne sont pas prises en charge pour l'authentification dans une configuration de proxy transparente.

Remarque

Pour le proxy explicite, vous devez définir le nom de connexion LDAP sur `sAMAccountName`. Pour le proxy transparent, vous devez définir le nom de connexion LDAP sur `networkAddress` et `attribute1` sur `sAMAccountName`.

Exemple de proxy explicite :

```
1 add authentication ldapAction swg-auth-action-explicit -serverIP
  10.105.157.116 -ldapBase "CN=Users,DC=CTXNSSFB,DC=COM" -ldapBindDn "
  CN=Administrator,CN=Users,DC=CTXNSSFB,DC=COM" -ldapBindDnPassword
  freebsd123$ -ldapLoginName sAMAccountName
```

Exemple pour le proxy transparent :

```
1 add authentication ldapAction swg-auth-action-explicit -serverIP
  10.105.157.116 -ldapBase "CN=Users,DC=CTXNSSFB,DC=COM" -ldapBindDn "
  CN=Administrator,CN=Users,DC=CTXNSSFB,DC=COM" -ldapBindDnPassword
  freebsd123$ -ldapLoginName networkAddress -authentication disable -
  Attribute1 sAMAccountName
```

Configurer l'authentification utilisateur à l'aide de l'interface de ligne de commande Citrix SWG

À l'invite de commandes, tapez :

```
1 add authentication vsServer <vsServer name> SSL
2
3 bind ssl vsServer <vsServer name> -certKeyName <certkey name>
4
5 add authentication ldapAction <action name> -serverIP <ip_addr> -
  ldapBase <string> -ldapBindDn <string> -ldapBindDnPassword -
  ldapLoginName <string>
6
7 add authentication Policy <policy name> -rule <expression> -action <
  string>
8
9 bind authentication vsServer <vsServer name> -policy <string> -priority <
  positive_integer>
10
11 set cs vsServer <name> -authn401 ON -authnVsName <string>
```

Arguments :

Nom du serveur :

Nom du serveur virtuel d'authentification auquel lier la stratégie.

Longueur maximale : 127

Type de service :

Type de protocole du serveur virtuel d'authentification. Toujours SSL.

Valeurs possibles : SSL

Valeur par défaut : SSL

Nom de l'action :

Nom de la nouvelle action LDAP. Doit commencer par une lettre, un chiffre ou le caractère de soulignement (_) et ne contenir que des lettres, des chiffres et des traits d'union (-), point (.) dièse (#), espace (), arobase (@), égal (=), deux-points (:) et trait de soulignement. Impossible de modifier une fois l'action LDAP ajoutée. L'exigence suivante s'applique uniquement à l'interface de ligne de commande :

Si le nom inclut un ou plusieurs espaces, placez le nom entre guillemets doubles ou simples (par exemple, « mon action d'authentification » ou « mon action d'authentification »).

Longueur maximale : 127

serverIP:

Adresse IP attribuée au serveur LDAP.

ldapBase:

Base (nœud) à partir de laquelle démarrer les recherches LDAP. Si le serveur LDAP s'exécute localement, la valeur par défaut de base est dc = netscaler, dc = com. Longueur maximale : 127

ldapBindDn:

Nom unique complet (DN) utilisé pour lier au serveur LDAP.

Valeur par défaut : `cn=Manager,dc=netscaler,dc=com`

Longueur maximale : 127

ldapBindDnPassword:

Mot de passe utilisé pour se lier au serveur LDAP.

Longueur maximale : 127

ldapLoginName:

Attribut de nom de connexion LDAP. L'appliance Citrix ADC utilise le nom de connexion LDAP pour interroger les serveurs LDAP externes ou Active Directory. Longueur maximale : 127

Nom de la stratégie :

Nom de la stratégie d'authentification avancée. Doit commencer par une lettre, un chiffre ou le caractère de soulignement (_) et ne contenir que des lettres, des chiffres et des traits d'union (-), point (.) dièse (#), espace (), arobase (@), égal (=), deux-points (:) et trait de soulignement. Impossible de modifier une fois la stratégie AUTHENTICATION créée. L'exigence suivante s'applique uniquement à l'interface de ligne de commande :

Si le nom comporte un ou plusieurs espaces, placez le nom entre guillemets doubles ou simples (par exemple, « ma politique d'authentification » ou « ma politique d'authentification »).

Longueur maximale : 127

règle :

Nom de la règle, ou d'une expression de syntaxe par défaut, utilisée par la stratégie pour déterminer s'il faut tenter d'authentifier l'utilisateur auprès du serveur AUTHENTICATION.

Longueur maximale : 1499

action :

Nom de l'action d'authentification à effectuer si la stratégie correspond.

Longueur maximale : 127

priorité :

Entier positif spécifiant la priorité de la stratégie. Un nombre inférieur spécifie une priorité plus élevée. Les stratégies sont évaluées dans l'ordre de leurs priorités et la première stratégie qui correspond à la demande est appliquée. Doit être unique dans la liste des stratégies liées au serveur virtuel d'authentification.

Valeur minimale : 0

Valeur maximale : 4294967295

Exemple :

```
1 add authentication vserver swg-auth-vs SSL
2
3 Done
4
5 bind ssl vserver explicit-auth-vs -certkeyName ns-swg-ca-certkey
6
7 Done
8
9 add authentication ldapAction swg-auth-action-explicit -serverIP
   192.0.2.116 -ldapBase "CN=Users,DC=CTXNSSFB,DC=COM" -ldapBindDn "CN=
   Administrator,CN=Users,DC=CTXNSSFB,DC=COM" -ldapBindDnPassword zzzzz
   -ldapLoginName sAMAccountName
10
11 Done
12
```



```
13 add authenticationpolicy swg-auth-policy -rule true -action swg-auth-  
    action-explicit  
    Done  
14  
15 bind authentication vserver swg-auth-vs -policy swg-auth-policy -  
    priority 1  
16  
17 Done  
18  
19 set cs vserver testswg -authn401 ON -authnVsName swg-auth-vs  
20  
21 Done
```

Activer la journalisation des noms d'utilisateur à l'aide de l'interface de ligne de commande Citrix SWG

À l'invite de commandes, tapez :

```
1 set appflow param -AAAUserName ENABLED
```

Arguments :

AAAUserName

Activez la journalisation des noms d'utilisateur AAA AppFlow.

Valeurs possibles : **ENABLED**, **DISABLED**

Valeur par défaut : **DISABLED**

Exemple :

```
1 set appflow param -AAAUserName ENABLED
```

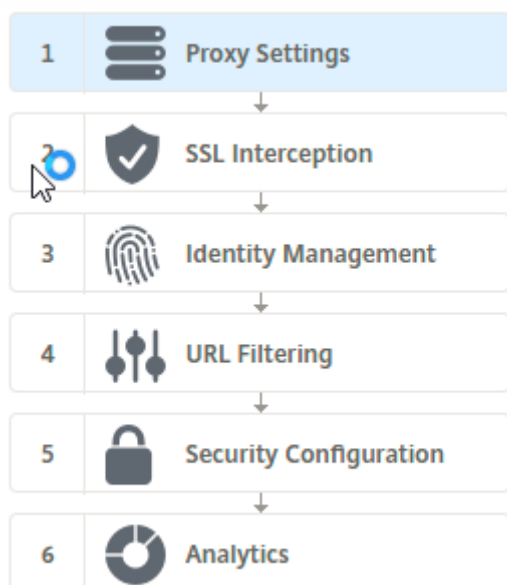
Filtrage d'URL

April 27, 2021

Le filtrage d'URL fournit un contrôle basé sur des stratégies des sites Web à l'aide des informations contenues dans les URL. Cette fonctionnalité permet aux administrateurs réseau de surveiller et de contrôler l'accès des utilisateurs aux sites Web malveillants sur le réseau.

Mise en route

Si vous êtes un nouvel utilisateur et que vous souhaitez configurer le filtrage d'URL, vous devez terminer la configuration SWG initiale. Pour commencer à utiliser le filtrage d'URL, vous devez d'abord vous connecter à l'Assistant Citrix SWG. L'Assistant vous aide à suivre une série d'étapes de configuration avant d'appliquer les stratégies de filtrage d'URL.



Remarque

Avant de commencer, assurez-vous que vous disposez d'une licence de fonctionnalité URL Threat Intelligence valide installée sur votre appliance. Si vous utilisez une version d'évaluation, assurez-vous d'acheter une licence valide pour continuer à utiliser cette fonctionnalité sur l'appliance SWG.

Connexion à l'assistant SWG

L'assistant Citrix SWG vous guide à travers une série de tâches de configuration simplifiées et le volet droit affiche la séquence de flux correspondante. Vous pouvez utiliser cet Assistant pour appliquer des stratégies de filtrage d'URL à une liste d'URL ou à une liste prédéfinie de catégories.

Étape 1 : Configurer les paramètres de proxy

Vous devez d'abord configurer un serveur proxy via lequel le client accède à la passerelle SWG. Ce serveur est de type SSL et fonctionne en mode explicite ou transparent. Pour plus d'informations sur la configuration du serveur proxy, reportez-vous à la section [Modes Proxy](#).

Étape 2 : Configurer l'interception SSL

Après avoir configuré le serveur proxy, vous devez configurer le proxy d'interception SSL pour intercepter le trafic chiffré sur le dispositif Citrix SWG. Dans le cas du filtrage d'URL, le proxy SSL intercepte le trafic et bloque les URL sur liste rouge tandis que tout autre trafic peut être contourné. Pour plus d'informations sur la configuration de l'interception SSL, reportez-vous à la section [Interception SSL](#).

Étape 3 : Configurer la gestion des identités

Un utilisateur est authentifié avant d'être autorisé à se connecter au réseau d'entreprise. L'authentification offre la flexibilité nécessaire pour définir des stratégies spécifiques pour un utilisateur ou un groupe d'utilisateurs, en fonction de leurs rôles. Pour plus d'informations sur l'authentification des utilisateurs, voir [Gestion de l'identification de l'utilisateur](#)

Étape 4 : Configurer le filtrage des URL

L'administrateur peut appliquer une stratégie de filtrage d'URL à l'aide de la fonctionnalité Catégorisation d'URL ou à l'aide de la fonctionnalité Liste d'URL.

[Catégorisation d'URL](#). Contrôle l'accès aux sites Web et aux pages Web en filtrant le trafic sur la base d'une liste prédéfinie de catégories.

[Liste d'URL](#). Contrôle l'accès aux sites Web et aux pages Web répertoriés sur la liste rouge en refusant l'accès aux URL figurant dans un jeu d'URL importé dans l'appliance.

Étape 5 : Configurer la configuration de la sécurité

Cette étape vous permet de configurer un score de réputation et de permettre aux utilisateurs de contrôler l'accès aux sites Web en refusant l'accès si le score est trop faible. Votre score de réputation peut varier de un à quatre, et vous pouvez configurer le seuil auquel le score devient inacceptable. Pour les scores qui dépassent le seuil, vous pouvez sélectionner une action de stratégie pour autoriser, bloquer ou rediriger le trafic. Pour de plus amples informations, consultez la section [Configuration de la sécurité](#).

Étape 6 : Configurer l'analyse SWG

Cette étape vous permet d'activer SWG Analytics pour catégoriser le trafic Web, enregistrer la catégorie d'URL dans les journaux de transactions utilisateur et afficher les analyses de trafic. Pour plus d'informations sur SWG Analytics, reportez-vous à la section [Analytics](#).

Étape 7 : Cliquez sur **Terminé** pour terminer la configuration initiale et continuer à gérer la configuration du filtrage d'URL

Liste des URL

April 27, 2021

La fonctionnalité Liste d'URL permet aux clients d'entreprise de contrôler l'accès à des sites Web et à des catégories de sites Web spécifiques. La fonctionnalité filtre les sites Web en appliquant une stratégie de répondeur liée à un algorithme de correspondance d'URL. L'algorithme correspond à l'URL entrante par rapport à un ensemble d'URL comprenant jusqu'à un million (1 000 000) entrées. Si la requête d'URL entrante correspond à une entrée de l'ensemble, l'appliance utilise la stratégie du répondeur pour évaluer la demande (HTTP/HTTPS) et en contrôler l'accès.

Types de jeux d'URL

Chaque entrée d'un jeu d'URL peut inclure une URL et, éventuellement, ses métadonnées (catégorie d'URL, groupes de catégories ou toute autre donnée connexe). Pour les URL avec métadonnées, l'appliance utilise une expression de stratégie qui évalue les métadonnées. Pour de plus amples informations, consultez la section [Jeu d'URL](#).

Citrix SWG prend en charge les ensembles d'URL personnalisés. Vous pouvez également utiliser des jeux de motifs pour filtrer les URL.

Jeu d'URL personnalisé. Vous pouvez créer un ensemble d'URL personnalisé avec jusqu'à 1 000 000 entrées d'URL et l'importer en tant que fichier texte dans votre appliance.

Jeu de motifs. Une appliance SWG peut utiliser des jeux de modèles pour filtrer les URL avant d'accorder l'accès aux sites Web. Un jeu de motifs est un algorithme de correspondance de chaînes qui recherche une correspondance exacte entre une URL entrante et jusqu'à 5000 entrées. Pour de plus amples informations, consultez la section [Jeu de motifs](#).

Chaque URL d'un ensemble d'URL importé peut avoir une catégorie personnalisée sous la forme de métadonnées d'URL. Votre organisation peut héberger le jeu et configurer l'appliance SWG pour mettre à jour périodiquement le jeu sans intervention manuelle.

Une fois l'ensemble mis à jour, l'appliance Citrix ADC détecte automatiquement les métadonnées et la catégorie est disponible en tant qu'expression de stratégie pour évaluer l'URL et appliquer une action telle que permettre, bloquer, rediriger ou notifier l'utilisateur.

Expressions de stratégie avancées utilisées avec les jeux d'URL

Le tableau suivant décrit les expressions de base que vous pouvez utiliser pour évaluer le trafic entrant.

1. `.URLSET_MATCHES_ANY` - Évalue sur `TRUE` si l'URL correspond exactement à n'importe quelle entrée de l'ensemble d'URL.
2. `.GET_URLSET_METADATA()` - L'expression `GET_URLSET_METADATA()` renvoie les métadonnées associées si l'URL correspond exactement à un motif dans l'ensemble d'URL. Une chaîne vide est renvoyée s'il n'y a pas de correspondance.
3. `.GET_URLSET_METADATA().EQ(<METADATA>)` - `.GET_URLSET_METADATA().EQ(<METADATA>)`
4. `.GET_URLSET_METADATA().TYPECAST_LIST_T('','').GET(0).EQ()` - Évalue sur `TRUE` si les métadonnées appariées sont au début de la catégorie. Ce modèle peut être utilisé pour encoder des champs distincts dans les métadonnées, mais correspondre uniquement au premier champ.
5. `HTTP.REQ.HOSTNAME.APPEND(HTTP.REQ.URL)` - Joint les paramètres hôte et URL, qui peuvent ensuite être utilisés comme un pour la correspondance.

Types d'action du répondeur

Note : Dans le tableau, `HTTP.REQ.URL` est généralisé comme `<URL expression>`.

Le tableau suivant décrit les actions qui peuvent être appliquées au trafic Internet entrant.

Action du répondeur	Description
Autoriser	Autoriser la demande à accéder à l'URL cible.
Rediriger	Rediriger la demande vers l'URL spécifiée comme cible.
Bloquer	Refuser la demande.

Conditions préalables

Vous devez configurer un serveur DNS si vous importez un jeu d'URL à partir d'une URL de nom d'hôte. Cela n'est pas nécessaire si vous utilisez une adresse IP.

À l'invite de commandes, tapez :

```
add dns nameServer ((<IP> [-local]) | <dnsVserverName>) [-state (
ENABLED | DISABLED )] [-type <type>] [-dnsProfileName <string>]
```

Exemple :

```
1 ajouter le serveur de noms dns 10.140.50.5
```

Configurer une liste d'URL

Pour configurer une liste d'URL, vous pouvez utiliser l'assistant Citrix SWG ou l'interface de ligne de commande (CLI) de Citrix ADC. Sur l'appliance Citrix SWG, vous devez d'abord configurer la stratégie de répondeur, puis lier la stratégie à un jeu d'URL.

Citrix vous recommande d'utiliser l'Assistant SWG Citrix comme option préférée pour configurer une liste d'URL. Utilisez l'Assistant pour lier une stratégie de répondeur à un jeu d'URL. Vous pouvez également lier la stratégie à un jeu de motifs.

Configurer une liste d'URL à l'aide de l'assistant Citrix SWG

Pour configurer la liste d'URL pour le trafic HTTPS à l'aide de l'interface utilisateur graphique Citrix SWG :

1. Ouvrez une session sur le dispositif Citrix SWG et accédez à la page **Secured Web Gateway** .
2. Dans le volet d'informations, effectuez l'une des opérations suivantes :
 - a) Cliquez sur **Secured Web Gateway Wizard** pour créer une nouvelle configuration SWG avec la fonctionnalité Liste d'URL.
 - b) Sélectionnez une configuration existante et cliquez sur **Modifier**.
3. Dans la section **Filtrage d'URL**, cliquez sur **Modifier**.
4. Activez la case à cocher **Liste d'URL** pour activer la fonctionnalité.
5. Sélectionnez une stratégie de **liste d'URL** et cliquez sur **Lier** .
6. Cliquez sur **Continuer**, puis **Terminé**.

Pour de plus amples informations, consultez la section [Procédure de création d'une stratégie de liste d'URL](#).

Configurer une liste d'URL à l'aide de l'interface de ligne de commande Citrix SWG

Pour configurer une liste d'URL, procédez comme suit.

1. Configurez un serveur virtuel proxy pour le trafic HTTP et HTTPS.
2. Configurez l'interception SSL pour intercepter le trafic HTTPS.
3. Configurez une liste d'URL contenant un jeu d'URL pour le trafic HTTP.
4. Configurez la liste d'URL contenant le jeu d'URL pour le trafic HTTPS.
5. Configurez un jeu d'URL privé.

Remarque

Si vous avez déjà configuré une appliance SWG, vous pouvez ignorer les étapes 1 et 2 et la configurer à l'étape 3.

Configuration d'un serveur virtuel proxy pour le trafic Internet L'appliance Citrix SWG prend en charge les serveurs virtuels proxy transparents et explicites. Pour configurer un serveur virtuel proxy pour le trafic Internet en mode explicite, procédez comme suit :

1. Ajouter un serveur virtuel SSL proxy.
2. Liez une stratégie de répondeur au serveur virtuel proxy.

Pour ajouter un serveur virtuel proxy à l'aide de l'interface de ligne de commande Citrix SWG :

À l'invite de commandes, tapez :

```
1 add cs vserver <name> <serviceType> <IPAddress> <port>
```

Exemple :

```
1 add cs vserver starcs PROXY 10.102.107.121 80 -cltTimeout 180
```

Pour lier une stratégie de répondeur à un serveur virtuel proxy à l'aide de l'interface de ligne de commande Citrix SWG :

```
1 bind ssl vserver <vServerName> -policyName <string> [-priority <positive_integer>]
```

Remarque

Si vous avez déjà configuré l'intercepteur SSL dans le cadre de la configuration de Citrix SWG, vous pouvez ignorer la procédure suivante.

Configurer l'interception SSL pour le trafic HTTPS Pour configurer l'interception SSL pour le trafic HTTPS, procédez comme suit :

1. Liez une paire de clés de certificat de l'autorité de certification au serveur virtuel proxy.
2. Activez le profil SSL par défaut.
3. Créez un profil SSL frontal et liez-le au serveur virtuel proxy et activez l'interception SSL dans le profil SSL frontal.

Pour lier une paire de clés de certificat de l'autorité de certification au serveur virtuel proxy à l'aide de l'interface de ligne de commande Citrix SWG :

À l'invite de commandes, tapez :

```
1 bind ssl vserver <vServerName> -certkeyName <certificate-KeyPairName>
```

Pour configurer un profil SSL frontal à l'aide de l'interface de ligne de commande Citrix SWG :

À l'invite de commandes, tapez :

```
1 set ssl parameter -defaultProfile ENABLED
2
3 add ssl profile <name> -sslInterception ENABLED -ssliMaxSessPerServer <
  positive_integer>
```

Pour lier un profil SSL frontal à un serveur virtuel proxy à l'aide de l'interface de ligne de commande Citrix SWG

À l'invite de commandes, tapez :

```
1 set ssl vserver <vServer name> -sslProfile <name>
```

Configurer une liste d'URL en important un jeu d'URL pour le trafic HTTP Pour plus d'informations sur la configuration d'un jeu d'URL pour le trafic HTTP, reportez-vous à la section [Jeu d'URL](#).

Effectuer une correspondance de sous-domaine explicite Vous pouvez maintenant effectuer une correspondance de sous-domaine explicite pour un jeu d'URL importé. Pour ce faire, un nouveau paramètre, "SubDomainExactMatch" est ajouté à la `import policy URLset` commande.

Lorsque vous activez le paramètre, l'algorithme de filtrage d'URL effectue une correspondance de sous-domaine explicite. Par exemple, si l'URL entrante est `news.example.com` et si l'entrée de l'ensemble d'URL est `example.com`, l'algorithme ne correspond pas aux URL.

À l'invite de commandes, tapez :

```
import policy urlset <name> [-overwrite] [-delimiter <character>] [-
rowSeparator <character>] -url [-interval <secs>] [-privateSet] [-
subdomainExactMatch] [-canaryUrl <URL>]
```

Exemple

```
import policy urlset test -url http://10.78.79.80/top-1k.csv -privateSet
-subdomainExactMatch -interval 900
```

Configurer un jeu d'URL pour le trafic HTTPS Pour configurer un jeu d'URL pour le trafic HTTPS à l'aide de l'interface de ligne de commande Citrix SWG

À l'invite de commandes, tapez :

```
1 add ssl policy <name> -rule <expression> -action <string> [-undefAction
  <string>] [-comment <string>]
```

Exemple :


```
1 add ssl policy pol1 -rule "client.ssl.client_hello.SNI.
  URLSET_MATCHES_ANY("top1m") -action INTERCEPT
```

Pour configurer un jeu d'URL pour le trafic HTTPS à l'aide de l'assistant Citrix SWG Citrix vous recommande d'utiliser l'assistant Citrix SWG comme option préférée pour configurer une liste d'URL. Utilisez l'Assistant pour importer un jeu d'URL personnalisé et lier à une stratégie de répondeur.

1. Ouvrez une session sur l'apppliance **Citrix SWG** et accédez à **Secured Web Gateway > Filtrage d'URL > Listes d'URL**.
2. Dans le volet d'informations, cliquez sur **Ajouter**.
3. Dans la page **Stratégie de liste d'URL**, spécifiez le nom de la stratégie.
4. Sélectionnez une option pour importer un jeu d'URL.
5. Dans la page de l'onglet **Stratégie de liste d'URL**, activez la case à cocher **Importer le jeu d'URL** et spécifiez les paramètres de jeu d'URL suivants.
 - a) Nom du jeu d'URL : nom du jeu d'URL personnalisé.
 - b) URL—Adresse Web de l'emplacement où accéder à l'ensemble d'URL.
 - c) Remplacer : écrase un jeu d'URL précédemment importé.
 - d) Delimiter—Séquence de caractères qui délimite un enregistrement de fichier CSV.
 - e) Séparateur de lignes —Séparateur de lignes utilisé dans le fichier CSV.
 - f) Intervalle (Intervalle) : intervalle en secondes arrondi au nombre de secondes le plus proche égal à 15 minutes au cours duquel le jeu d'URL est mis à jour.
 - g) Private Set—Option pour empêcher l'exportation du jeu d'URL.
 - h) URL Canary : URL interne permettant de vérifier si le contenu de l'ensemble d'URL doit rester confidentiel. La longueur maximale de l'URL est de 2047 caractères.
6. Sélectionnez une action du répondeur dans la liste déroulante.
7. Cliquez sur **Créer** et **Fermer**.

Configurer un jeu d'URL privé Si vous configurez un jeu d'URL privé et que son contenu reste confidentiel, l'administrateur réseau peut ne pas connaître les URL répertoriées sur la liste rouge de l'ensemble. Dans de tels cas, vous pouvez configurer une URL Canary et l'ajouter à l'ensemble d'URL. À l'aide de l'URL Canary, l'administrateur peut demander que le jeu d'URL privé soit utilisé pour chaque requête de recherche. Vous pouvez vous référer à la section Assistant pour obtenir la description de chaque paramètre.

Pour importer un jeu d'URL à l'aide de l'interface de ligne de commande Citrix SWG :

À l'invite de commandes, tapez :

```
1 import policy urlset <name> [-overwrite] [-delimiter <character>] [-
  rowSeparator <character>] -url <URL> [-interval <secs>] [-privateSet
  ] [-canaryUrl <URL>]
```

Exemple :

```
1 import policy urlset test1 -url http://10.78.79.80/alytra/top-1k.csv -  
private -canaryUrl http://www.in.gr
```

Afficher le jeu d'URL importé

Vous pouvez désormais afficher des jeux d'URL importés en plus des jeux d'URL ajoutés. Pour ce faire, un nouveau paramètre 'imported' est ajouté à la commande 'show urlset'. Si vous activez cette option, l'appliance affiche tous les jeux d'URL importés et les distingue des jeux d'URL ajoutés.

À l'invite de commandes, tapez :

```
show policy urlset [<name>] [-imported]
```

Exemple

```
show policy urlset -imported
```

Configurer la messagerie du journal d'audit

La journalisation d'audit vous permet de consulter une condition ou une situation dans n'importe quelle phase du processus de liste d'URL. Lorsqu'une appliance Citrix ADC reçoit une URL entrante, si la stratégie du répondeur possède une expression de stratégie avancée de jeu d'URL, la fonctionnalité de journal d'audit collecte les informations d'ensemble d'URL dans l'URL et stocke les détails sous forme de message de journal pour toute cible autorisée par la journalisation d'audit.

1. Le message de journal contient les informations suivantes :
2. Horodatage.
3. Type de message de journal.
4. Les niveaux de journalisation prédéfinis (Critique, Erreur, Avis, Avertissement, Informations, Débogage, Alerte et Urgence).
5. Consigner les informations du message, telles que le nom du jeu d'URL, l'action de stratégie, l'URL.

Pour configurer la journalisation d'audit pour la fonctionnalité Liste d'URL, vous devez effectuer les tâches suivantes :

1. Activer le journal d'audit :
2. Action Créer un message journal d'audit.
3. Définissez la stratégie de répondeur de liste d'URL avec l'action de message Journal d'audit.

Pour plus d'informations, reportez-vous à la rubrique [Journalisation de l'audit](#).

Sémantique des modèles d'URL

April 27, 2021

Le tableau suivant présente les modèles d'URL utilisés pour spécifier la liste des pages que vous souhaitez filtrer. Par exemple, le modèle, `www.example.com/bar`, ne correspond qu'à une page sur `www.example.com/bar`. Pour faire correspondre toutes les pages dont l'URL commence par '`www.example.com/bar`', vous ajoutez un astérisque (*) à la fin de l'URL.

Sémantique pour le modèle d'URL pour correspondre au mappage des métadonnées

La sémantique de correspondance des motifs est disponible sous forme de tableau. Pour plus d'informations, consultez le pdf [Sémantique des motifs](#).

Catégories d'URL de mappage

April 27, 2021

Liste des catégories et groupes de catégories de tiers. Pour plus d'informations, reportez-vous à la page [Mappage des catégories d'URL](#).

Cas d'utilisation : filtrage d'URL à l'aide d'un jeu d'URL personnalisé

April 27, 2021

Si vous êtes un client d'entreprise à la recherche d'un moyen de contrôler l'accès à des sites Web et à des catégories de sites Web spécifiques, vous pouvez le faire en utilisant un jeu d'URL personnalisé lié à une stratégie de répondeur. L'infrastructure réseau de votre organisation peut utiliser un filtre d'URL pour bloquer l'accès à des sites Web malveillants ou dangereux tels que des sites Web présentant des adultes, des violences, des jeux, des drogues, des politiques ou des portails d'emploi. Outre le filtrage des URL, vous pouvez créer une liste personnalisée d'URL et l'importer dans l'appliance SWG. Par exemple, les stratégies de votre organisation peuvent exiger le blocage de l'accès à certains sites Web tels que les réseaux sociaux, les portails commerciaux et les portails d'emplois.

Chaque URL de la liste peut avoir une catégorie personnalisée sous forme de métadonnées. L'organisation peut héberger la liste des URL sous la forme d'une URL définie sur le dispositif Citrix SWG

et configurer l'apppliance pour qu'elle mette à jour périodiquement l'ensemble sans intervention manuelle.

Une fois l'ensemble mis à jour, l'apppliance Citrix ADC détecte automatiquement les métadonnées et la stratégie de répondeur utilise les métadonnées d'URL (détails de catégorie) pour évaluer l'URL entrante et appliquer une action telle que permettre, bloquer, rediriger ou notifier l'utilisateur.

Pour implémenter cette configuration dans votre réseau, vous pouvez effectuer les tâches suivantes :

1. Importer un ensemble d'URL personnalisé
2. Ajouter un ensemble d'URL personnalisé
3. Configurer une liste d'URL personnalisée dans l'Assistant Citrix SWG

Pour importer un ensemble d'URL personnalisé à l'aide de l'interface de ligne de commande Citrix SWG :

À l'invite de commandes, tapez :

```
import policy urlset <name> [-overwrite] [-delimiter <character>] [-rowSeparator <character>] -  
url <URL> [-interval <secs>] [-privateSet] [-canaryUrl <URL>]
```

```
1 import policy urlset test1 -url http://10.78.79.80/alytra/top-1k.csv
```

Pour ajouter un ensemble d'URL personnalisé à l'aide de l'interface de ligne de commande Citrix SWG :

À l'invite de commandes, tapez :

```
add urlset <urlset_name>
```

```
1 Add urlset test1
```

Configurer une liste d'URL à l'aide de l'assistant Citrix SWG

Citrix vous recommande d'utiliser l'Assistant SWG Citrix comme option préférée pour configurer une liste d'URL. Utilisez l'Assistant pour importer un ensemble d'URL personnalisé et le lier à une stratégie de répondeur.

1. Ouvrez une session sur l'apppliance **Citrix SWG** et accédez à **Secured Web Gateway > Filtrage d'URL > Listes d'URL**.
2. Dans le volet d'informations, cliquez sur **Ajouter**.
3. Dans la page **Stratégie de liste d'URL**, spécifiez le nom de la stratégie.
4. Sélectionnez une option pour importer un jeu d'URL.
5. Dans la page de l'onglet **Stratégie de liste d'URL**, activez la case à cocher **Importer le jeu d'URL** et spécifiez les paramètres de jeu d'URL suivants.

- a) Nom du jeu d'URL : nom du jeu d'URL personnalisé.
 - b) URL—Adresse Web de l'emplacement où accéder à l'ensemble d'URL.
 - c) Remplacer : écrase un jeu d'URL précédemment importé.
 - d) Delimiter—Séquence de caractères qui délimite un enregistrement de fichier CSV.
 - e) Séparateur de lignes —Séparateur de lignes utilisé dans le fichier CSV.
 - f) Intervalle—Intervalle en secondes, arrondi à 15 minutes près, au cours duquel le jeu d'URL est mis à jour.
 - g) Private Set—Option pour empêcher l'exportation du jeu d'URL.
 - h) URL Canary —URL interne permettant de tester si le contenu de l'ensemble d'URL doit rester confidentiel. La longueur maximale de l'URL est de 2047 caractères.
6. Sélectionnez une action du répondeur dans la liste déroulante.
 7. Cliquez sur **Créer** et **Fermer**.

The screenshot shows the 'URL List Policy' configuration page. At the top, there are tabs for 'URL List Policies' and 'URL List Policy'. The main heading is 'URL List Policy'. Below this, there are several input fields and checkboxes:

- URL***: A text input field containing 'http://10.78.79.80/alytra/top-1k.csv'.
- Overwrite**: A checkbox that is currently unchecked.
- Delimiter**: A text input field containing '4'.
- Row Separator**: A text input field containing '10'.
- Interval**: A text input field containing '15'.
- Private Set**: A checkbox that is currently unchecked.
- Canary URL**: An empty text input field.

Below these fields, there is an **Action*** dropdown menu with 'Allow' selected. At the bottom of the form, there are two buttons: 'Create' (highlighted in blue) and 'Close'.

Sémantique de métadonnées pour les jeux d'URL personnalisés

Pour importer un ensemble d'URL personnalisé, ajoutez les URL à un fichier texte et liez-le à une stratégie de répondeur pour bloquer les URL de réseaux sociaux.

Voici des exemples d'URL que vous pouvez ajouter au fichier texte :

cnn.com, Actualités

bbc.com, Actualités

google.com, moteur de recherche

yahoo.com, moteur de recherche

facebook.com, Médias sociaux

twitter.com, Médias sociaux

Configurer une stratégie de répondeur pour bloquer les URL des médias sociaux à l'aide de l'interface de ligne de commande Citrix ADC

add responder action act_url_unauthorized respondwith “HTTP/1.1 451 Unavailable For Legal Reasons\r\n\r\nURL is NOT authorized\r\n”

add responder policy pol_url_meta_match ‘HTTP.REQ.HOSTNAME.APPEND(HTTP.REQ.URL).GET_URLSET_META(“u1”).EQ(“Social Media”)’act_url_meta_match

Catégorisation d'URL

April 27, 2021

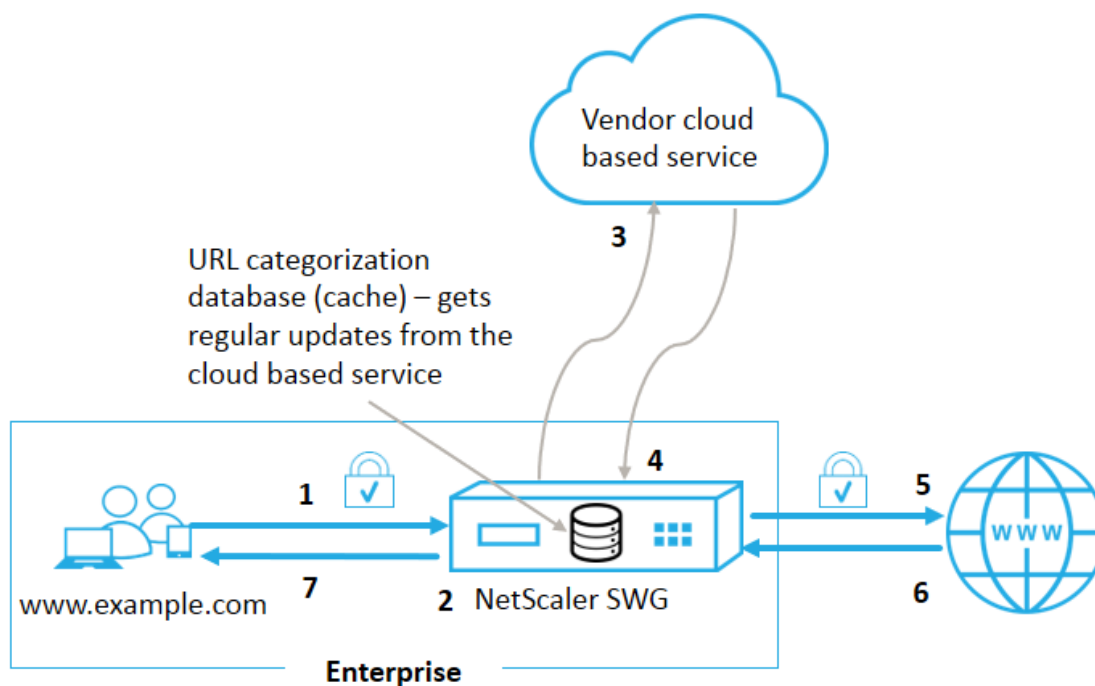
La catégorisation des URL limite l'accès des utilisateurs à des sites Web et à des catégories de sites Web spécifiques. En tant que service abonné offert par Citrix Secure Web Gateway (SWG), cette fonctionnalité permet aux clients d'entreprise de filtrer le trafic Web à l'aide d'une base de données de catégorisation commerciale. La base de données contient un grand nombre (milliards) d'URL classées en différentes catégories, telles que les réseaux sociaux, les jeux d'argent, le contenu pour adultes, les nouveaux médias et les achats. En plus de la catégorisation, chaque URL a un score de réputation tenu à jour en fonction du profil de risque historique du site. Pour filtrer votre trafic, vous pouvez configurer des stratégies avancées basées sur des catégories, des groupes de catégories (tels que Terrorisme, Drogues illégales) ou des scores de réputation de site.

Par exemple, vous pouvez bloquer l'accès à des sites dangereux, tels que des sites connus pour être infectés par des logiciels malveillants, et restreindre sélectivement l'accès au contenu tel que du contenu pour adultes ou des médias de divertissement en continu pour les utilisateurs d'entreprise. Vous pouvez également capturer les détails transactionnels de l'utilisateur et les détails du trafic sortant pour surveiller l'analyse du trafic Web sur le serveur Citrix ADM.

Citrix ADC télécharge ou télécharge des données à partir du [NetSTAR](https://nsv10.netstar-inc.com) périphérique préconfiguré nsv10.netstar-inc.com et incompasshybridpc.netstar-inc.com est utilisé comme hôte de nuage par défaut pour les demandes de catégorisation de nuage. L'appliance utilise son adresse NSIP comme adresse IP source et 443 comme port de destination pour la communication.

Fonctionnement de la catégorisation des URL

La figure suivante montre comment le service de catégorisation d'URL Citrix SWG est intégré à une base de données de catégorisation d'URL commerciale et aux services cloud pour les mises à jour fréquentes.



Les composants interagissent comme suit :

1. Un client envoie une demande d'URL liée à Internet.
2. Le proxy Citrix SWG applique une application de stratégie à la demande en fonction des détails de catégorie (tels que la catégorie, le groupe de catégories et le score de réputation de site) récupérés à partir de la base de données de catégorisation des URL. Si la base de données renvoie les détails de la catégorie, le processus passe à l'étape 5.
3. Si la base de données manque les détails de catégorisation, la demande est envoyée à un service de recherche basé sur un cloud géré par un fournisseur de catégorisation d'URL. Toutefois, l'appliance n'attend pas de réponse, mais l'URL est marquée comme non classée et une application de stratégie est exécutée (passez à l'étape 5). L'appliance continue de surveiller les retours de requête dans le cloud et met à jour le cache afin que les demandes futures puissent bénéficier de la recherche dans le cloud.
4. L'appliance SWG reçoit les détails de catégorie d'URL (catégorie, groupe de catégories et score de réputation) du service basé sur un cloud et les stocke dans la base de données de catégorisation.

5. La stratégie autorise l'URL et la demande est envoyée au serveur d'origine. Sinon, l'appliance supprime, redirige ou répond avec une page HTML personnalisée.
6. Le serveur d'origine répond avec les données demandées à l'appliance SWG.
7. L'appliance envoie la réponse au client.

Cas d'utilisation : utilisation d'Internet dans le cadre de la conformité des entreprises

Vous pouvez utiliser la fonctionnalité de filtrage d'URL pour détecter et mettre en œuvre des stratégies de conformité afin de bloquer les sites qui enfreignent la conformité de l'entreprise. Il peut s'agir de sites tels que les adultes, les médias en streaming, les réseaux sociaux qui peuvent être considérés comme non productifs ou consomment une bande passante Internet excédentaire dans un réseau d'entreprise. Le blocage de l'accès à ces sites Web peut améliorer la productivité des employés, réduire les coûts d'exploitation liés à l'utilisation de la bande passante et réduire les frais généraux liés à la consommation réseau.

Conditions préalables

La fonctionnalité de catégorisation des URL ne fonctionne sur une plate-forme Citrix SWG que si elle dispose d'un service d'abonnement facultatif avec des fonctionnalités de filtrage d'URL et une veille sur les menaces pour Citrix Secure Web Gateway. L'abonnement permet aux clients de télécharger les dernières catégories de menaces pour les sites Web, puis d'appliquer ces catégories sur Secure Web Gateway. L'abonnement est disponible pour les versions matérielles et logicielles (VPX) de Secure Web Gateway.

Avant d'activer et de configurer la fonctionnalité, vous devez installer les licences suivantes :

CNS_Webf_sServer_Retail.lic

CNS_XXXXX_SERVER_SWG_Retail.lic.

Où, XXXXX est le type de plate-forme, par exemple : V25000

Expressions de stratégie du répondeur

Le tableau suivant répertorie les différentes expressions de stratégie que vous pouvez utiliser pour vérifier si une URL entrante doit être autorisée, redirigée ou bloquée.

1. `<text>. URL_CATEGORIZE (<min_reputation>, <max_reputation>)` - Retourne un `URL_CATEGORY` objet. Si la valeur `<min_reputation>` est supérieure à 0, l'objet renvoyé ne contient pas de catégorie dont la réputation est inférieure à `<min_reputation>`.

Si la valeur `<max_reputation>` est supérieure à 0, l'objet renvoyé ne contient pas de catégorie dont la réputation est supérieure à `<max_reputation>`. Si la catégorie ne parvient pas à résoudre en temps opportun, la valeur `undef` est renvoyée.

2. `<url_category>`. `CATEGORY()` - Retourne la chaîne de catégorie de cet objet. Si l'URL n'a pas de catégorie, ou si l'URL est mal formée, la valeur renvoyée est « Unknown. »
3. `<url_category>`. `CATEGORY_GROUP()` - Retourne une chaîne identifiant le groupe de catégories de l'objet. Il s'agit d'un regroupement de catégories de niveau supérieur, ce qui est utile dans les opérations qui nécessitent des informations moins détaillées sur la catégorie d'URL. Si l'URL n'a pas de catégorie, ou si l'URL est mal formée, la valeur renvoyée est « Unknown. »
4. `<url_category>`. `REPUTATION()` - Retourne le score de réputation sous la forme d'un nombre compris entre 0 et 5, où 5 indique la réputation la plus risquée. S'il y a la catégorie « Inconnu », la valeur de réputation est 1.

Types de stratégie :

1. Stratégie pour sélectionner les demandes d'URL qui se trouvent dans la catégorie Moteur de recherche `-add responder policy p1 'HTTP.REQ.HOSTNAME.APPEND(HTTP.REQ.URL).URL_CATEGORIZE(0,0).CATEGORY().EQ("Search Engine")`
2. Stratégie pour sélectionner les demandes d'URL qui se trouvent dans le groupe de catégorie Adulte `-add responder policy p1 'HTTP.REQ.HOSTNAME.APPEND(HTTP.REQ.URL).URL_CATEGORIZE(0,0).CATEGORY_GROUP().EQ("Adult")'`
3. Stratégie pour sélectionner les demandes d'URL du moteur de recherche dont le score de réputation est inférieur à 4 `-add responder policy p2 'HTTP.REQ.HOSTNAME.APPEND(HTTP.REQ.URL).URL_CATEGORIZE(4,0).HAS_CATEGORY("Search Engine")`
4. Stratégie de sélection des demandes d'URL des moteurs de recherche et de shopping `-add responder policy p3 'HTTP.REQ.HOSTNAME.APPEND(HTTP.REQ.URL).URL_CATEGORIZE(0,0).CATEGORY().EQ("good_categories")`
5. Stratégie pour sélectionner les demandes d'URL du moteur de recherche avec un score de réputation égal ou supérieur à 4 `-add responder policy p5 'CLIENT.SSL.DETECTED_DOMAIN.URL_CATEGORIZE(4,0).CATEGORY().EQ("Search Engines")`
6. Stratégie pour sélectionner les demandes d'URL qui se trouvent dans la catégorie Moteur de recherche et les comparer avec un jeu d'URL `- 'HTTP.REQ.HOSTNAME.APPEND(HTTP.REQ.URL).URL_CATEGORIZE(0,0).CATEGORY().EQ("Search Engine")&&HTTP.REQ.HOSTNAME.APPEND(HTTP.REQ.URL).URLSET_MATCHES_ANY("u1")'`

Types de stratégie du répondeur

Il existe deux types de stratégies utilisées dans la fonction de catégorisation des URL et chacun de ces types de stratégie est expliqué ci-dessous :

Type de stratégie	Description
Catégorie d'URL	Catégorisez le trafic Web et, en fonction des résultats de l'évaluation, bloquez, autorisez ou redirigez le trafic.
Score de réputation d'URL	Déterminez le score de réputation du site Web et vous permet de contrôler l'accès en fonction du seuil de notation de réputation défini par l'administrateur.

Configurer la catégorisation d'URL

Pour configurer la catégorisation des URL sur une appliance Citrix SWG, procédez comme suit :

1. Activer le filtrage des URL.
2. Configurez un serveur proxy pour le trafic Web.
3. Configurez l'interception SSL pour le trafic Web en mode explicite.
4. Configurez la mémoire partagée pour limiter la mémoire cache.
5. Configurez les paramètres de catégorisation d'URL.
6. Configurez la catégorisation des URL à l'aide de l'assistant Citrix SWG.
7. Configurez les paramètres de catégorisation des URL à l'aide de l'assistant SWG.
8. Configurer le chemin de la base de données initiale et le nom du serveur de nuage

Étape 1 : Activation du filtrage d'URL

Pour activer la catégorisation d'URL, activez la fonction de filtrage d'URL et activez les modes de catégorisation d'URL.

Pour activer la catégorisation des URL à l'aide du Citrix SWG : CLI

À l'invite de commandes, tapez :

```
enable ns feature URLFiltering
```

```
disable ns feature URLFiltering
```

Étape 2 : Configurer un serveur proxy pour le trafic Web en mode explicite

L'apppliance Citrix SWG prend en charge les serveurs virtuels proxy transparents et explicites. Pour configurer un serveur virtuel proxy pour le trafic SSL en mode explicite, procédez comme suit :

1. Ajoutez un serveur proxy.
2. Liez une stratégie SSL au serveur proxy.

Pour ajouter un serveur proxy à l'aide de l'interface de ligne de commande Citrix SWG

À l'invite de commandes, tapez :

```
1 add cs vserver <name> [-td <positive_integer>] <serviceType> [-cltTimeout <secs>]
```

Exemple :

```
1 add cs vserver starcs PROXY 10.102.107.121 80 -cltTimeout 180
```

Liez une stratégie SSL à un serveur virtuel proxy à l'aide de l'interface de ligne de commande Citrix SWG

```
1 bind ssl vserver <vServerName> -policyName <string> [-priority <positive_integer>]
```

Étape 3 : Configurer l'interception SSL pour le trafic HTTPS

Pour configurer l'interception SSL pour le trafic HTTPS, procédez comme suit :

1. Liez une paire de clés de certificat de l'autorité de certification au serveur virtuel proxy.
2. Configurez le profil SSL par défaut avec les paramètres SSL.
3. Liez un profil SSL frontal au serveur virtuel proxy et activez l'interception SSL dans le profil SSL frontal.

Pour lier une paire de clés de certificat d'autorité de certification au serveur virtuel proxy à l'aide de l'interface de ligne de commande Citrix SWG

À l'invite de commandes, tapez :

```
1 bind ssl vserver <vServerName> -certkeyName <certificate-KeyPairName> -CA -skipCAName
```

Pour configurer le profil SSL par défaut à l'aide de l'interface de ligne de commande Citrix SWG

À l'invite de commandes, tapez :

```
1 set ssl profile <name> -denySSLReneg <denySSLReneg> -sslInterception (
  ENABLED | DISABLED) -sslMaxSessPerServer positive_integer>
```

Lier un profil SSL frontal à un serveur virtuel proxy à l'aide de l'interface de ligne de commande Citrix SWG

À l'invite de commandes, tapez :

```
1 set ssl vserver <vServer name> -sslProfile ssl_profile_interception
```

Étape 4 : Configurer la mémoire partagée pour limiter la mémoire cache

Pour configurer la mémoire partagée afin de limiter la mémoire cache à l'aide de l'interface de ligne de commande Citrix SWG

À l'invite de commandes, tapez :

```
1 set cache parameter [-memLimit <megaBytes>]
```

Où, la limite de mémoire configurée pour la mise en cache est définie sur 10 Mo.

Étape 5 : Configurer les paramètres de catégorisation d'URL

Pour configurer les paramètres de catégorisation d'URL à l'aide de l'interface de ligne de commande Citrix SWG

À l'invite de commandes, tapez :

```
1 set urlfiltering parameter [-HoursBetweenDBUpdates <positive_integer>]
  [-TimeOfDayToUpdateDB <HH:MM>]
```

Exemple :

```
1 Set urlfiltering parameter -urlfilt_hours_betweenDB_updates 20
```

Étape 6 : Configurer la catégorisation des URL à l'aide de l'Assistant Citrix SWG

Pour configurer la catégorisation des URL à l'aide de l'interface graphique Citrix SWG

1. Ouvrez une session sur le dispositif Citrix SWG et accédez à la page **Secured Web Gateway**.
2. Dans le volet d'informations, effectuez l'une des opérations suivantes :
 - a) Cliquez sur **Assistant Passerelle Web sécurisée** pour créer une nouvelle configuration.

- b) Sélectionnez une configuration existante et cliquez sur **Modifier**.
3. Dans la section **Filtrage d'URL**, cliquez sur **Modifier**.
4. Activez la case à cocher **Catégorisation d'URL** pour activer la fonction.
5. Sélectionnez une stratégie de **catégorisation d'URL** et cliquez sur **Lier**.
6. Cliquez sur **Continuer**, puis **Terminé**.

Pour plus d'informations sur la stratégie de catégorisation d'URL, reportez-vous à la section [Procédure de création d'une stratégie de catégorisation d'URL](#).

Étape 7 : Configuration des paramètres de catégorisation d'URL à l'aide de l'Assistant SWG

Pour configurer les paramètres de catégorisation d'URL à l'aide de l'interface graphique Citrix SWG

1. Connectez-vous à l'appliance **Citrix SWG** et accédez à **Secured Web Gateway > Filtrage d'URL**.
2. Dans la page **Filtrage d'URL**, cliquez sur **Modifier les paramètres de filtrage d'URL** lien.
3. Dans la page **Configuration des paramètres de filtrage d'URL**, spécifiez les paramètres suivants.
 - a) Heures entre les mises à jour de base de données. Heures de filtrage d'URL entre les mises à jour de la base de données. Valeur minimale : 0 et Valeur maximale : 720.
 - b) Heure de la journée pour mettre à jour la base de données. URL Filtrage heure de la journée pour mettre à jour la base de données.
 - c) Hôte du nuage. Chemin d'accès URL du serveur cloud.
 - d) Chemin de base de données de départ. Chemin d'URL du serveur de recherche de base de données d'origine.
4. Cliquez sur **OK** et **Fermer**.

Exemple de configuration :

```

1 enable ns feature LB CS SSL IC RESPONDER AppFlow URLFiltering
2
3 enable ns mode FR L3 Edge USNIP PMTUD
4
5 set ssl profile ns_default_ssl_profile_frontend -denySSLReneg NONSECURE
   -sslInterception ENABLED -ssliMaxSessPerServer 100
6
7 add ssl certKey swg_ca_cert -cert ns_swg_ca.crt -key ns_swg_ca.key
8
9 set cache parameter -memLimit 100
10
11 add cs vserver starcs PROXY 10.102.107.121 80 -cltTimeout 180
12
13 add responder action act1 respondwith "HTTP/1.1 200 OK\r\n\r\n" + http
   .req.url.url_categorize(0,0).reputation + "\n"
14

```

```

15 add responder policy p1 "HTTP.REQ.URL.URL_CATEGORIZE(0,0).CATEGORY.eq("
    Shopping/Retail") || HTTP.REQ.URL.URL_CATEGORIZE(0,0).CATEGORY.eq("
    Search Engines & Portals
16
17 ")" act1
18
19 bind cs vserver starcs_PROXY -policyName p1 -priority 10 -
    gotoPriorityExpression END -type REQUEST
20
21 add dns nameServer 10.140.50.5
22
23 set ssl parameter -denySSLReneg NONSECURE -defaultProfile ENABLED -
    sigDigestType RSA-MD5 RSA-SHA1 RSA-SHA224 RSA-SHA256 RSA-SHA384 RSA-
    SHA512 -ssliErrorCache ENABLED
24
25 -ssliMaxErrorCacheMem 100000000
26
27 add ssl policy pol1 -rule "client.ssl.origin_server_cert.subject.
    URL_CATEGORIZE(0,0).CATEGORY.eq("Search Engines & Portals")" -
    action INTERCEPT
28
29 add ssl policy pol3 -rule "client.ssl.origin_server_cert.subject.ne("
    citrix)" -action INTERCEPT
30
31 add ssl policy swg_pol -rule "client.ssl.client_hello.SNI.
    URL_CATEGORIZE(0,0).CATEGORY.ne("Uncategorized")" -action INTERCEPT
32
33 set urlfiltering parameter -HoursBetweenDBUpdates 3 -
    TimeOfDayToUpdateDB 03:00

```

Configurer le chemin de la base de données initiale et le nom du serveur de nuage

Vous pouvez maintenant configurer le chemin de la base de données d'origine et le nom du serveur de recherche de cloud pour définir manuellement le nom du serveur de recherche de cloud et le chemin de la base de données d'origine. Pour ce faire, deux nouveaux paramètres, « CloudHost » et « Seed-DBPath », sont ajoutés à la commande de paramètre de filtrage d'URL.

À l'invite de commandes, tapez :

```

set urlfiltering parameter [-HoursBetweenDBUpdates <positive_integer
>] [-TimeOfDayToUpdateDB <HH:MM>] [-LocalDatabaseThreads <positive_integer
>] [-CloudHost <string>] [-SeedDBPath <string>]

```

Exemple

```

set urlfiltering parameter -HoursBetweenDBUpdates 3 -TimeOfDayToUpdateDB
03:00 -CloudHost localhost -SeedDBPath /mypath

```

Communication entre une appliance Citrix ADC et NetSTAR peut nécessiter un serveur de noms de domaine. Vous pouvez tester à l'aide d'une simple console ou d'une connexion telnet de l'appliance.

Exemple :

```
1 root@ns# telnet nsv10.netstar-inc.com 443
2 Trying 1.1.1.1...
3 Connected to nsv10.netstar-inc.com.
4 Escape character is '^]'.
5
6 root@ns# telnet incompasshybridpc.netstar-inc.com 443
7 Trying 10.10.10.10...
8 Connected to incompasshybridpc.netstar-inc.com.
9 Escape character is '^]'.

```

Configurer la messagerie du journal d'audit

La journalisation d'audit vous permet d'examiner une condition ou une situation dans n'importe quelle phase du processus de catégorisation d'URL. Lorsqu'une appliance Citrix ADC reçoit une URL entrante, si la stratégie de répondeur possède une expression de filtrage d'URL, la fonctionnalité de journal d'audit collecte les informations relatives au jeu d'URL dans l'URL et les stocke en tant que messages de journal pour toute cible autorisée par la journalisation d'audit.

- Adresse IP source (adresse IP du client qui a fait la demande).
- Adresse IP de destination (adresse IP du serveur demandé).
- URL demandée contenant le schéma, l'hôte et le nom de domaine (<http://www.example.com>).
- Catégorie d'URL renvoyée par le cadre de filtrage d'URL.
- groupe de catégories d'URL renvoyé par le cadre de filtrage d'URL.
- Numéro de réputation d'URL renvoyé par le cadre de filtrage d'URL.
- Action du journal d'audit effectuée par la stratégie.

Pour configurer la journalisation d'audit pour la fonctionnalité Liste d'URL, vous devez effectuer les tâches suivantes :

1. Activer le journal d'audit :
2. Action Créer un message journal d'audit.
3. Définissez la stratégie de répondeur de liste d'URL avec l'action de message Journal d'audit.

Pour plus d'informations, reportez-vous à la rubrique [Journalisation de l'audit](#).

Stockage des erreurs d'échec à l'aide de la messagerie SYSLOG

À n'importe quelle étape du processus de filtrage d'URL, en cas de défaillance au niveau du système, l'appliance Citrix ADC utilise le mécanisme du journal d'audit pour stocker les journaux dans le fichier ns.log. Les erreurs sont stockées sous forme de messages texte au format SYSLOG de sorte qu'un administrateur puisse les afficher plus tard dans un ordre chronologique d'occurrence d'événement.

Ces journaux sont également envoyés à un serveur SYSLOG externe pour archivage. Pour de plus amples informations, consultez la section [article CTX229399](#).

Par exemple, si un échec se produit lorsque vous initialisez le SDK de filtrage d'URL, le message d'erreur est stocké dans le format de messagerie suivant.

```
Oct 3 15:43:40 <local0.err> ns URLFiltering[1349]: Error initializing NetStar SDK (SDK error=-1). (status=1).
```

L'apppliance Citrix ADC stocke les messages d'erreur sous quatre catégories de défaillance différentes :

- **Échec du téléchargement.** Si une erreur se produit lorsque vous essayez de télécharger la base de données de catégorisation.
- **Échec de l'intégration.** Si une erreur se produit lorsque vous intégrez une mise à jour dans la base de données de catégorisation existante.
- **Échec de l'initialisation.** Si une erreur se produit lorsque vous initialisez la fonction de catégorisation d'URL, définissez des paramètres de catégorisation ou terminez un service de catégorisation.
- **Échec de la récupération.** Si une erreur se produit lorsque l'apppliance récupère les détails de catégorisation de la demande.

Afficher le résultat de catégorisation d'URL via l'interface de commande

La catégorisation des URL vous permet d'entrer une URL et d'extraire les résultats de catégorisation (par exemple, catégorie, groupe et score de réputation) à partir de la base de données de catégorisation d'URL tierce NetStar.

Lorsque vous entrez une URL, la fonction de filtrage d'URL récupère et affiche le résultat de catégorisation sur l'interface de commande. Lorsque vous entrez d'autres URL, l'apppliance exclut les anciennes URL de la liste et affiche le résultat des trois URL les plus récentes.

Pour afficher le résultat de catégorie d'URL jusqu'à trois URL, procédez comme suit :

1. Ajouter une URL de catégorisation d'URL
2. Afficher les détails de catégorisation d'URL jusqu'à trois URL
3. Effacer les données de catégorisation des URL.

Pour ajouter une URL de catégorisation de filtrage d'URL

Pour ajouter une URL et récupérer ses détails de catégorisation, procédez comme suit :

À l'invite de commandes, tapez :

```
add urlfiltering categorization -Url <string>
```


Exemple :

```
add urlfiltering categorization -Url www.facebook.com
```

Pour afficher les détails de catégorisation d'URL jusqu'à trois URL

À l'invite de commandes, tapez :

```
> show urlfiltering categorization
```

Exemple :

```
1 show urlfiltering categorization
2 Url: http://www.facebook.com    Categorization: Facebook,Social
   Networking,1
3 Url: http://www.google.com      Categorization: Search Engines &
   Portals,Search,1
4 Url: http://www.citrix.com      Categorization: Computing & Internet,
   Computing & Internet,1
5 Done
```

Exemple de configuration :

```
1 add urlfiltering categorization -url www.facebook.com
2 Done
3 show urlfiltering categorization
4 Url: http://www.facebook.com    Categorization: Facebook,Social
   Networking,1
5 Done
6
7 add urlfiltering categorization -url www.google.com
8 Done
9 show urlfiltering categorization
10 Url: http://www.facebook.com   Categorization: Facebook,Social
   Networking,1
11 Url: http://www.google.com     Categorization: Search Engines &
   Portals,Search,1
12 Done
13
14 add urlfiltering categorization -url www.citrix.com
15 Done
16 show urlfiltering categorization
17 Url: http://www.facebook.com   Categorization: Facebook,Social
   Networking,1
18 Url: http://www.google.com     Categorization: Search Engines &
   Portals,Search,1
19 Url: http://www.citrix.com     Categorization: Computing & Internet,
   Computing & Internet,1
20 Done
21
22 add urlfiltering categorization -url www.in.gr
23 Done
```

```

24 show urlfiltering categorization
25 Url: http://www.google.com      Categorization: Search Engines &
    Portals,Search,1
26 Url: http://www.citrix.com      Categorization: Computing & Internet,
    Computing & Internet,1
27 Url: http://www.in.gr           Categorization: Search Engines & Portals,Search
    ,1 Done

```

Pour effacer le résultat de la catégorisation d'URL

À l'invite de commandes, tapez :

```

1 clear urlfiltering categorization
2 done
3
4 show urlfiltering categorization
5 done

```

Afficher le résultat de catégorisation d'URL via l'interface graphique

1. Dans le volet de navigation, développez **Secure Web Gateway > Filtrage d'URL**.
2. Dans le volet d'informations, cliquez sur le lien **Filtrage d'URL** dans la section **Outils**.
3. Dans la page **Catégorisation de recherche de filtrage d'URL**, entrez une demande d'URL et cliquez sur **Rechercher**.

URL	URL Category	URL Category Group	Reputation Score
http://www.google.com	Search Engines & Portals	Search	1
http://www.citrix.com	Computing & Internet	Computing & Internet	1
http://www.twitter.com	Twitter	Social Networking	1

4. L'apppliance affiche le résultat de la catégorie pour l'URL demandée et pour les deux demandes d'URL précédentes.

Configuration de la sécurité

April 27, 2021

La fonctionnalité Configuration de la sécurité vous permet de configurer la stratégie de sécurité pour le filtrage des URL. La rubrique Score de réputation d'URL fournit des détails conceptuels et de configuration pour le filtrage des URL en fonction de son score de réputation.

Vous pouvez utiliser ICAP pour l'inspection de contenu à distance.

Score de réputation d'URL

La fonctionnalité de catégorisation des URL utilise le score de réputation d'URL pour fournir un contrôle basé sur des règles afin de bloquer les sites Web à haut risque. Pour de plus amples informations, consultez la section [Score de réputation d'URL](#).

Utilisation d'ICAP pour l'inspection du contenu à distance

Le trafic HTTPS est intercepté, déchiffré et envoyé aux serveurs ICAP pour inspection du contenu pour les contrôles anti-programmes malveillants et la prévention des fuites de données.

Score de réputation d'URL

April 27, 2021

La fonction de catégorisation d'URL fournit un contrôle basé sur des stratégies pour restreindre les URL sur la liste rouge. Vous pouvez contrôler l'accès aux sites Web en fonction de la catégorie d'URL, du score de réputation ou de la catégorie d'URL et du score de réputation. Si un administrateur réseau surveille un utilisateur accédant à des sites Web à risque élevé, il peut utiliser une stratégie de réponse liée au score de réputation d'URL pour bloquer ces sites Web à risque.

À la réception d'une demande d'URL entrante, l'appliance récupère la catégorie et le score de réputation de la base de données de catégorisation d'URL. En fonction du score de réputation renvoyé par la base de données, l'appliance attribue une cote de réputation aux sites Web. La valeur peut varier de 1 à 4, où 4 est le type de sites Web le plus risqué, comme indiqué dans le tableau suivant.

Classement de la réputation d'URL	Commentaire de réputation
1	Nettoyer le site
2	Site inconnu
3	Potentiellement dangereux ou affilié à un site dangereux

Classement de la réputation d'URL	Commentaire de réputation
4	Site malveillant

Cas d'utilisation : Filtrage par score de réputation d'URL

Envisagez une organisation d'entreprise avec un administrateur réseau qui surveille les transactions utilisateur et la consommation de bande passante réseau. Si un logiciel malveillant peut entrer sur le réseau, l'administrateur doit améliorer la sécurité des données et contrôler l'accès aux sites Web malveillants et dangereux qui accèdent au réseau. Pour protéger le réseau contre de telles menaces, l'administrateur peut configurer la fonctionnalité de filtrage d'URL pour autoriser ou refuser l'accès par score de réputation d'URL.

Pour plus d'informations sur la surveillance du trafic sortant et des activités des utilisateurs sur le réseau, reportez-vous à la section [Analytics](#).

Si un employé de l'organisation tente d'accéder à un site Web de réseau social, l'appliance SWG reçoit une demande d'URL et interroge la base de données de catégorisation des URL pour récupérer la catégorie URL en tant que réseau social et un score de réputation 3, ce qui indique un site Web potentiellement dangereux. L'appliance vérifie ensuite la stratégie de sécurité configurée par l'administrateur, par exemple l'accès en bloc aux sites dont la cote de réputation est de 3 ou plus. Il applique ensuite la stratégie pour contrôler l'accès au site Web.

Pour implémenter cette fonctionnalité, vous devez configurer le score de réputation d'URL et les niveaux de seuil de sécurité à l'aide de l'Assistant Citrix SWG.

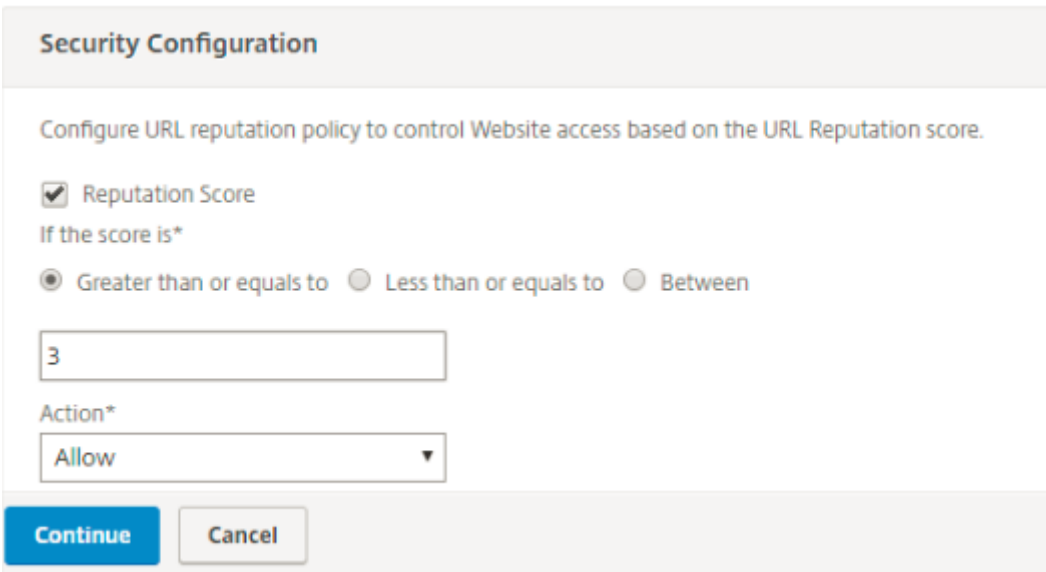
Configuration du score de réputation à l'aide de l'interface graphique Citrix SWG :

Citrix vous recommande d'utiliser l'Assistant Citrix SWG pour configurer le score de réputation et les niveaux de sécurité. En fonction du seuil configuré, vous pouvez sélectionner une action de stratégie pour autoriser, bloquer ou rediriger le trafic.

1. Connectez-vous à l'appliance **Citrix SWG** et accédez à **Secure Web Gateway**.
2. Dans le volet d'informations, cliquez sur **Assistant Secured Web Gateway**.
3. Dans la page **Configuration de Secure Web Gateway**, spécifiez les paramètres du serveur proxy SWG.
4. Cliquez sur **Continuer** pour spécifier d'autres paramètres tels que l'interception SSL et l'identification de la gestion.
5. Cliquez sur **Continuer** pour accéder à la section **Configuration de la sécurité**.
6. Dans la section **Configuration de la sécurité**, cochez la case **Score de réputation** pour contrôler l'accès en fonction du score de réputation d'URL.
7. Sélectionnez le niveau de sécurité et spécifiez la valeur de seuil de score de réputation :

- a) Supérieur ou égal à : autorise ou bloque un site Web si la valeur de seuil est supérieure ou égale à N, où N varie de un à quatre.
 - b) Inférieur ou égal à —Autoriser ou bloquer un site Web si la valeur de seuil est inférieure ou égale à N, où N varie de un à quatre.
 - c) Entre : permet ou bloque un site Web si la valeur de seuil est comprise entre N1 et N2 et que la plage est comprise entre un et quatre.
8. Sélectionnez une action du répondeur dans la liste déroulante.
9. Cliquez sur **Continuer** et fermer.

L'image suivante montre la section Configuration de la sécurité de l'Assistant Citrix SWG. Activez l'option Score de réputation d'URL pour configurer les paramètres de stratégie.



Security Configuration

Configure URL reputation policy to control Website access based on the URL Reputation score.

Reputation Score

If the score is*

Greater than or equals to Less than or equals to Between

3

Action*

Allow

Continue Cancel

Utilisation d'ICAP pour l'inspection du contenu à distance

April 27, 2021

Internet Content Adaptation Protocol (ICAP) est un protocole ouvert simple et léger. Il est généralement utilisé pour transporter des messages HTTP entre le proxy et les périphériques qui fournissent la prise en charge des programmes malveillants et des services de prévention des fuites de données. ICAP a créé une interface standard pour l'adaptation du contenu afin de permettre une plus grande flexibilité dans la distribution de contenu et de fournir un service à valeur ajoutée. Un client ICAP transfère les requêtes HTTP et les réponses à un serveur ICAP pour traitement. Le serveur ICAP effectue une certaine transformation sur les demandes et renvoie les réponses au client ICAP, avec l'action appropriée sur la demande ou la réponse.

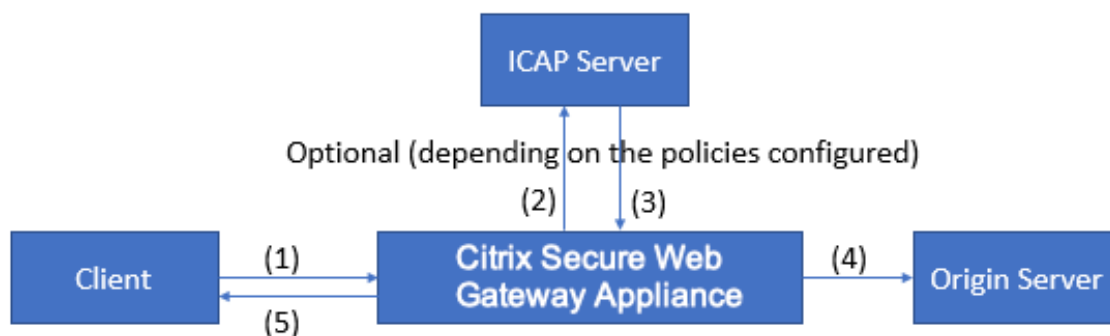
Utilisation d'ICAP sur l'appliance Citrix Secure Web Gateway

Remarque

La fonctionnalité d'inspection du contenu nécessite une licence SWG Edition.

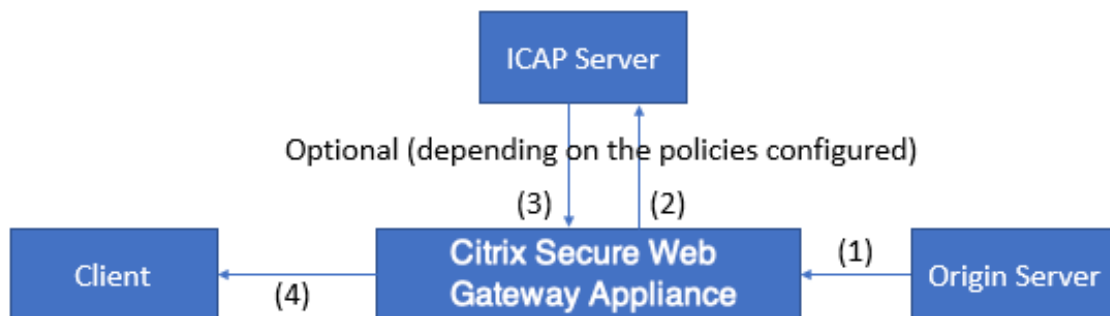
L'appliance Citrix Secure Web Gateway (SWG) agit en tant que client ICAP et utilise des stratégies pour interagir avec les serveurs ICAP. L'appliance communique avec des serveurs ICAP tiers spécialisés dans des fonctions telles que la lutte contre les programmes malveillants et la prévention des fuites de données (DLP). Lorsque vous utilisez ICAP sur une appliance SWG, les fichiers chiffrés sont également analysés. Les fournisseurs de sécurité ont auparavant contourné ces fichiers. L'appliance effectue une interception SSL, déchiffre le trafic client et l'envoie au serveur ICAP. Le serveur ICAP vérifie la détection de virus, de logiciels malveillants ou de logiciels espions, l'inspection des fuites de données ou tout autre service d'adaptation de contenu. L'appliance agit en tant que proxy, décrypte la réponse du serveur d'origine et l'envoie en texte brut au serveur ICAP pour inspection. Configurez des stratégies pour sélectionner le trafic envoyé aux serveurs ICAP.

Le flux de mode de requête fonctionne comme suit :



(1) L'appliance Citrix SWG intercepte les demandes du client. (2) L'appliance transmet ces demandes au serveur ICAP, en fonction des stratégies configurées sur l'appliance. (3) Le serveur ICAP répond par un message indiquant « Aucune adaptation requise », une erreur ou une demande modifiée. L'appliance (4) transmet le contenu au serveur d'origine demandé par le client ou (5) renvoie un message approprié au client.

Le flux en mode réponse fonctionne comme suit :



(1) Le serveur d'origine répond à l'apppliance Citrix SWG. (2) L'apppliance transmet la réponse au serveur ICAP, en fonction des stratégies configurées sur l'apppliance. (3) Le serveur ICAP répond par un message indiquant « Aucune adaptation requise », ou une erreur ou une demande modifiée. (4) En fonction du paramètre du serveur ICAP, l'apppliance transfère le contenu demandé au client ou envoie un message approprié.

Configuration d'ICAP sur l'apppliance Citrix Secure Web Gateway

Les étapes suivantes expliquent comment configurer ICAP sur l'apppliance Citrix SWG.

1. Activez la fonction d'inspection du contenu.
2. Configurez un serveur proxy.
3. Configurez un service TCP qui représente le serveur ICAP. Pour établir une connexion sécurisée entre l'apppliance SWG et le service ICAP, spécifiez le type de service SSL_TCP. Pour plus d'informations sur l'ICAP sécurisé, consultez la section « Secure ICAP » plus loin dans cette page.
4. Vous pouvez également ajouter un serveur virtuel d'équilibrage de charge pour équilibrer la charge des serveurs ICAP et lier le service ICAP à ce serveur virtuel.
5. Configurez un profil ICAP personnalisé. Le profil doit inclure l'URI ou le chemin d'accès du service ICAP et le mode ICAP (demande ou réponse). Il n'existe aucun profil par défaut ICAP similaire aux profils par défaut HTTP et TCP.
6. Configurez une action d'inspection de contenu et spécifiez le nom du profil ICAP. Spécifiez le nom du serveur virtuel d'équilibrage de charge ou le nom du service TCP/SSL_TCP dans le paramètre nom du serveur.
7. Configurez une stratégie d'inspection de contenu pour évaluer le trafic client et la lier au serveur proxy. Spécifiez l'action d'inspection du contenu dans cette stratégie.

Configurer ICAP en utilisant l'interface de ligne de commande

Configurez les entités suivantes :

1. Activez la fonctionnalité.

```
enable ns feature contentInspection
```

2. Configurez un serveur proxy.

```
add cs vserver <name> PROXY <IPAddress>
```

Exemple :

```
add cs vserver explicitSWG PROXY 192.0.2.100 80
```

3. Configurez un service TCP pour représenter les serveurs ICAP.

```
add service <name> <IP> <serviceType> <port>
```

Spécifiez le type de service SSL_TCP pour une connexion sécurisée avec le serveur ICAP.

Exemple :

```
add service icap_svc1 203.0.113.100 TCP 1344
```

```
add service icap_svc 203.0.113.200 SSL_TCP 11344
```

4. Configurez un serveur virtuel d'équilibrage de charge.

```
add lb vserver <name> <serviceType> <IPAddress> <port>
```

Exemple :

```
add lbvserver lbicap TCP 0.0.0.0 0
```

Liez le service ICAP au serveur virtuel d'équilibrage de charge.

```
bind lb vserver <name> <serviceName>
```

Exemple :

```
bind lb vserver lbicap icap_svc
```

5. Ajoutez un profil ICAP personnalisé.

```
add ns icapProfile <name> -uri <string> -Mode ( REQMOD | RESPMOD )
```

Exemple :

```
add icaprofile icaprofile1 -uri /example.com -Mode REQMOD
```

Paramètres**nom**

Nom d'un profil ICAP. Doit commencer par un caractère alphanumérique ASCII ou un trait de soulignement (_), et ne doit contenir que des caractères alphanumériques ASCII, un trait de soulignement, un hachage (#), un point (.), un espace, deux points (:), un signe arobase (@), un signe égal (=) et un trait d'union (-).

Utilisateurs CLI : si le nom comprend un ou plusieurs espaces, placez le nom entre guillemets doubles ou simples (par exemple, « mon profil icap » ou « mon profil icap »).

Longueur maximale : 127

uri

URI représentant le chemin du service ICAP.

Longueur maximale : 511 caractères

Mode

Mode ICAP. Les paramètres disponibles fonctionnent comme suit :

- REQMOD : En mode de modification de requête, le client ICAP transmet une requête HTTP au serveur ICAP.
- RESPMOD : En mode de modification de réponse, le serveur ICAP transmet une réponse HTTP du serveur d'origine au serveur ICAP.

Valeurs possibles : REQMOD, RESPMOD

6. Configurez une action à exécuter si la stratégie renvoie true.

```
add contentInspection action <name> -type ICAP -serverName <string> -icapProfileName <string>
```

Exemple :

```
add contentInspection action CiRemoteAction -type ICAP -serverName lbicap -icapProfileName icaprofile1
```

7. Configurez une stratégie pour évaluer le trafic.

```
add contentInspection policy <name> -rule <expression> -action <string>
```

Exemple :

```
add contentInspection policy CiPolicy -rule true -action CiRemoteAction
```

8. Liez la stratégie au serveur proxy.

```
bind cs vserver <vServerName> -policyName <string> -priority <positive_integer> -type [REQUEST | RESPONSE]
```

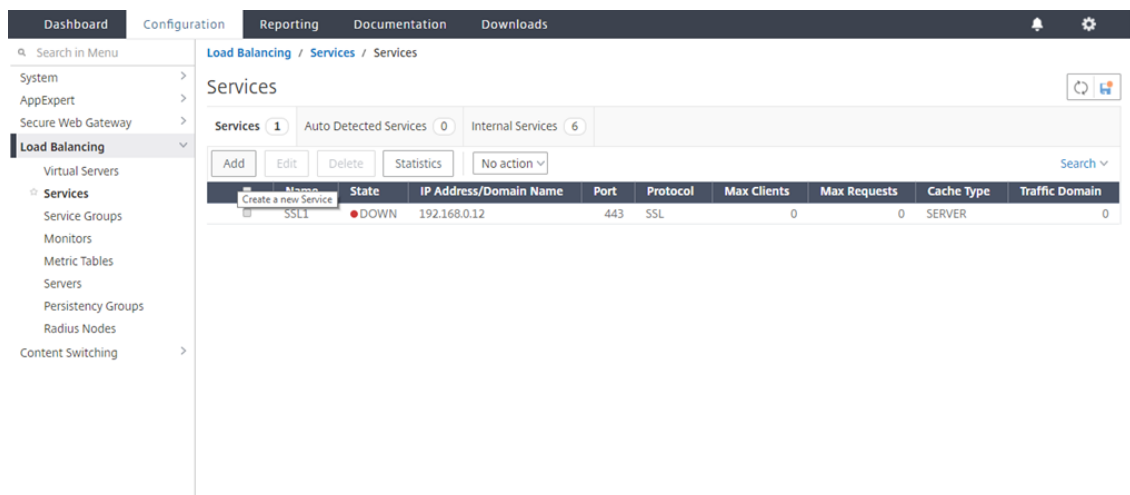
Exemple :

```
bind cs vserver explicitSWG -policyName CiPolicy -priority 200 -type REQUEST
```

Configurer ICAP à l'aide de l'interface graphique

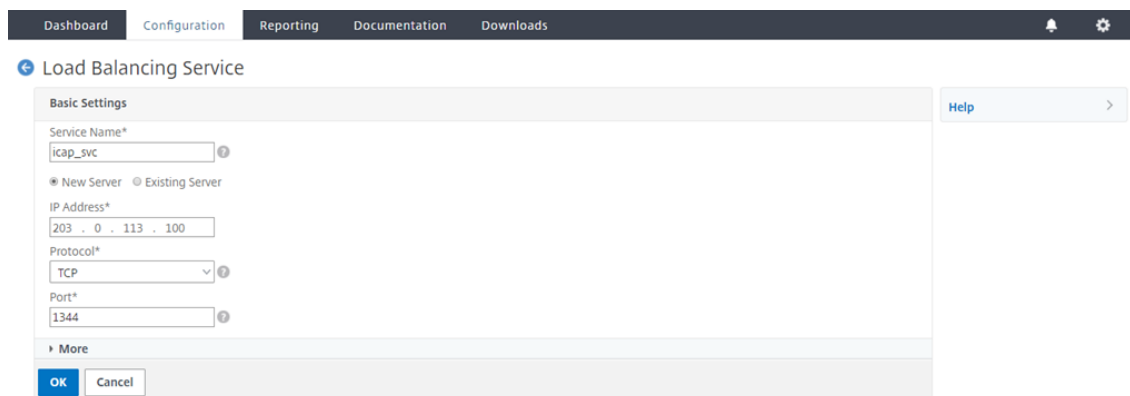
Procédez comme suit :

1. Accédez à **Équilibrage de charge** > **Services**, puis cliquez sur **Ajouter**.

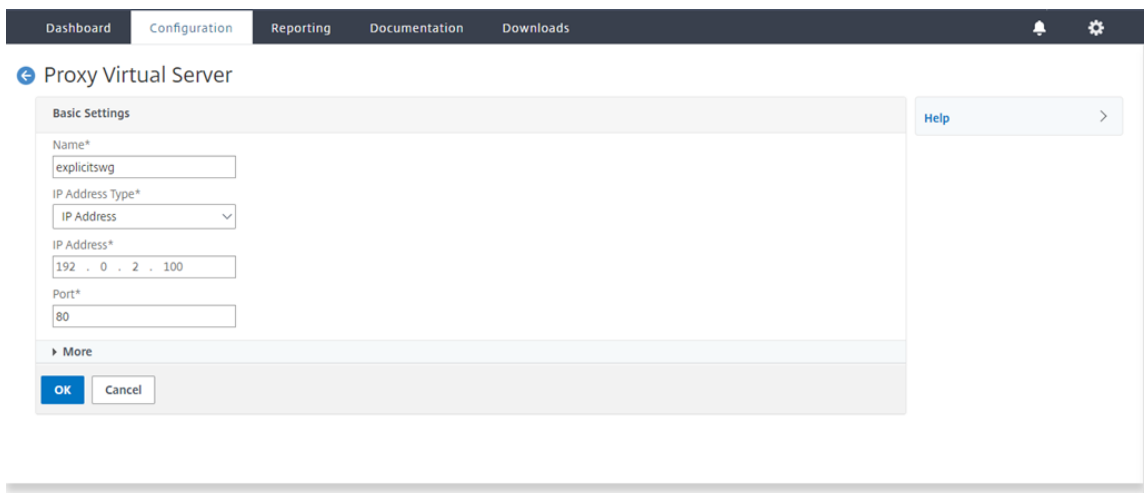


2. Tapez un nom et une adresse IP. Dans **Protocole**, sélectionnez **TCP**. Dans **Port**, tapez **1344**. Cliquez sur **OK**.

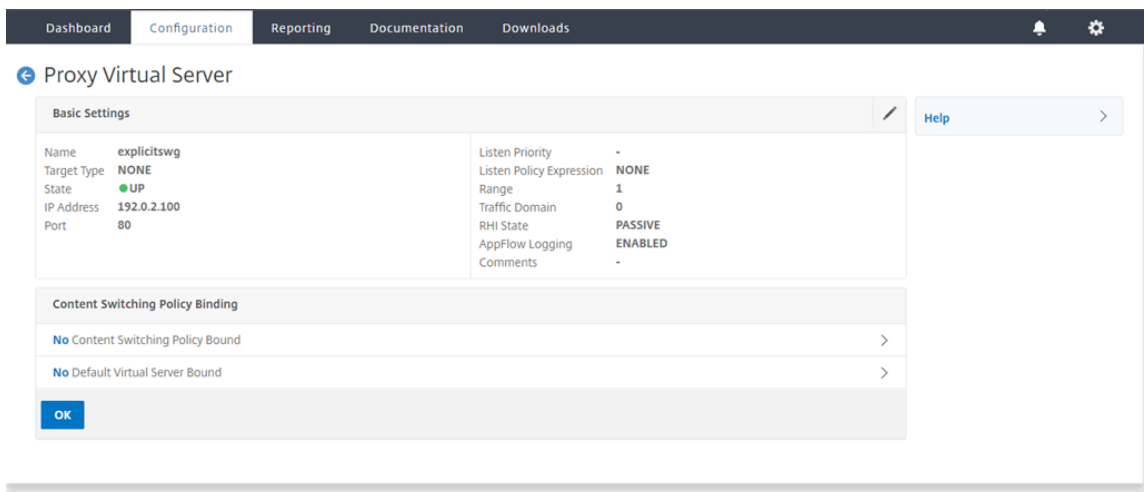
Pour une connexion sécurisée aux serveurs ICAP, sélectionnez protocole TCP_SSL et spécifiez le port en tant que 11344.



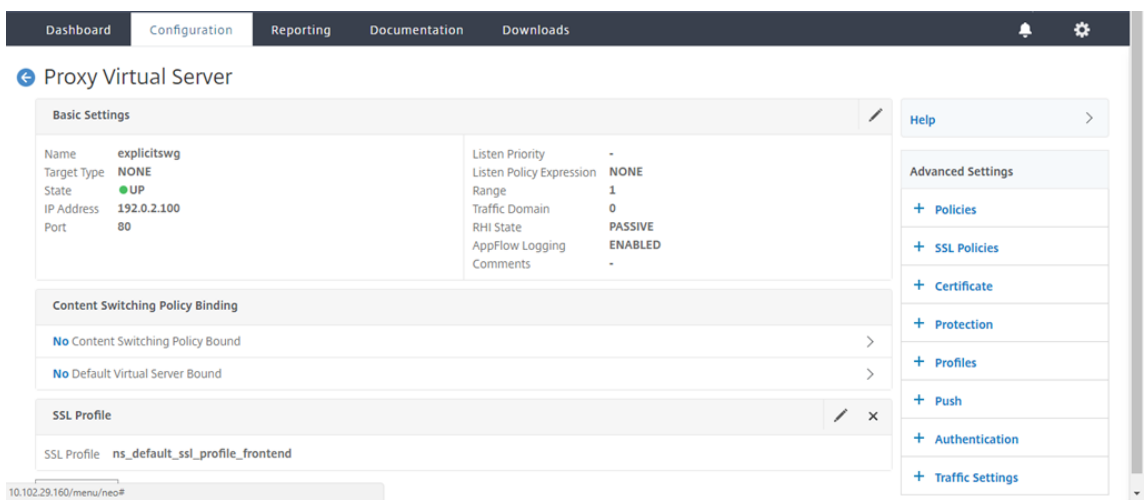
3. Accédez à **Secure Web Gateway** > **Serveurs virtuels proxy**. Ajoutez un serveur virtuel proxy ou sélectionnez un serveur virtuel et cliquez sur **Modifier**. Après avoir entré les détails, cliquez sur **OK**.



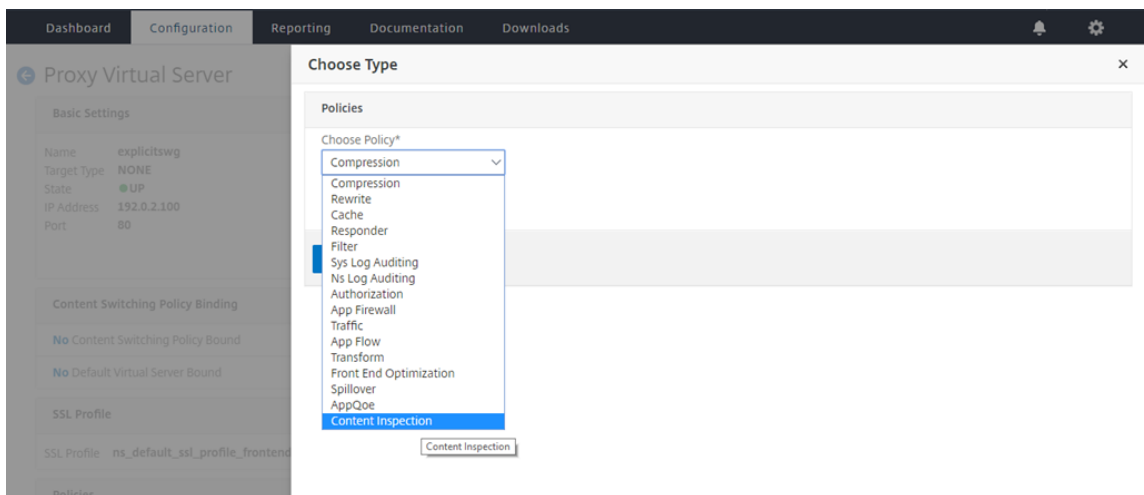
Cliquez à nouveau sur **OK**.



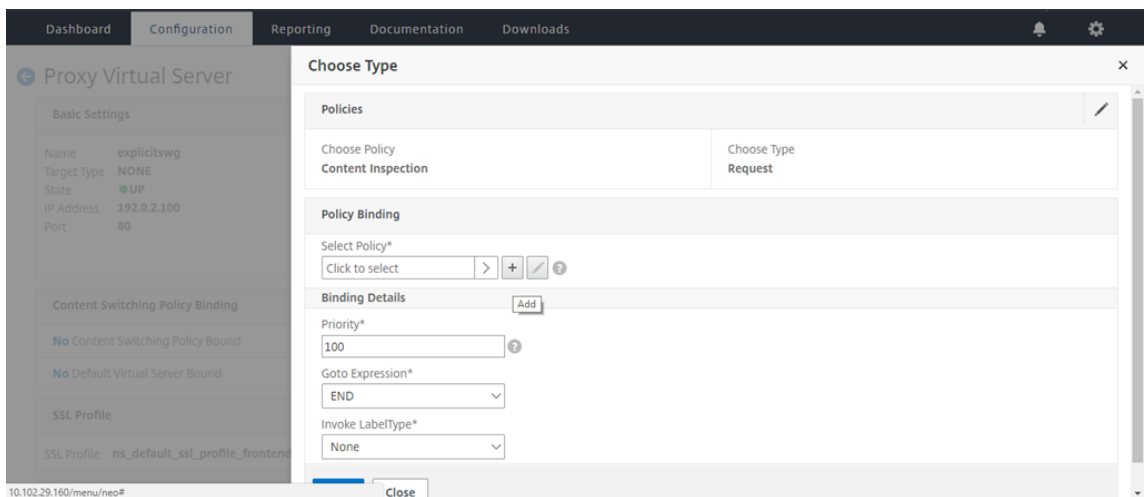
4. Dans **Paramètres avancés**, cliquez sur **Stratégies**.



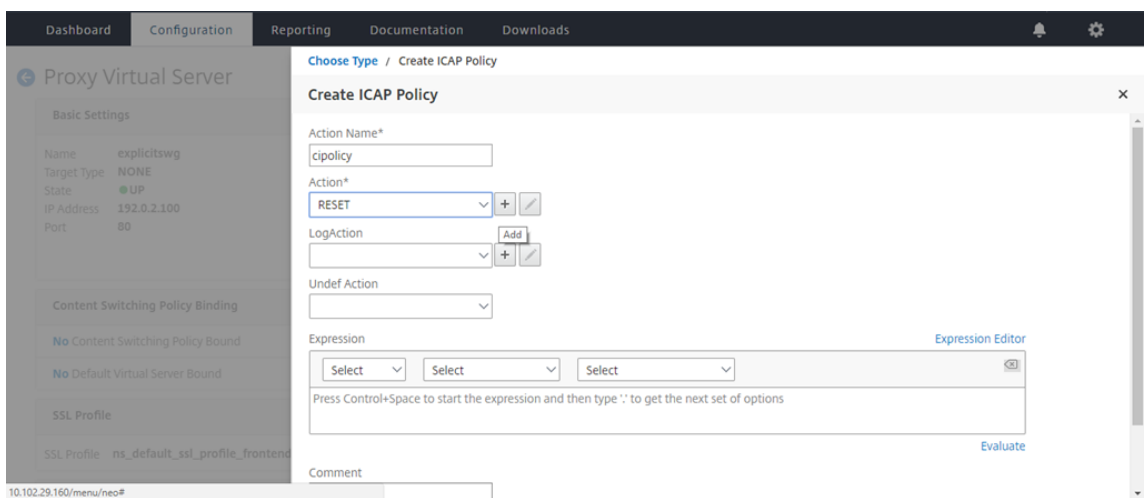
5. Dans **Choisir une stratégie**, sélectionnez **Contrôle du contenu**. Cliquez sur **Continuer**.



6. Dans **Sélectionner une stratégie**, cliquez sur le signe « + » pour ajouter une stratégie.

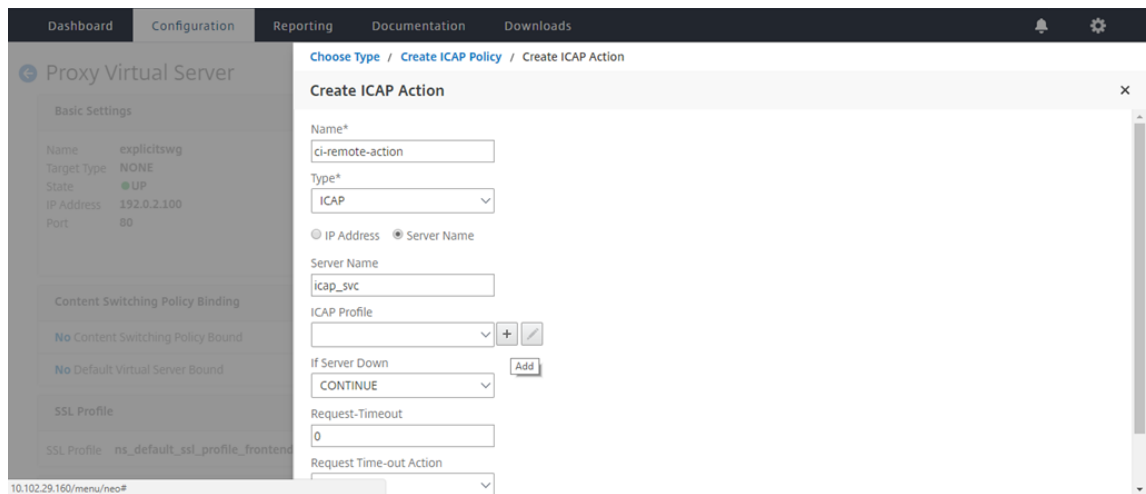


7. Entrez un nom pour la stratégie. Dans **Action**, cliquez sur le signe « + » pour ajouter une action.

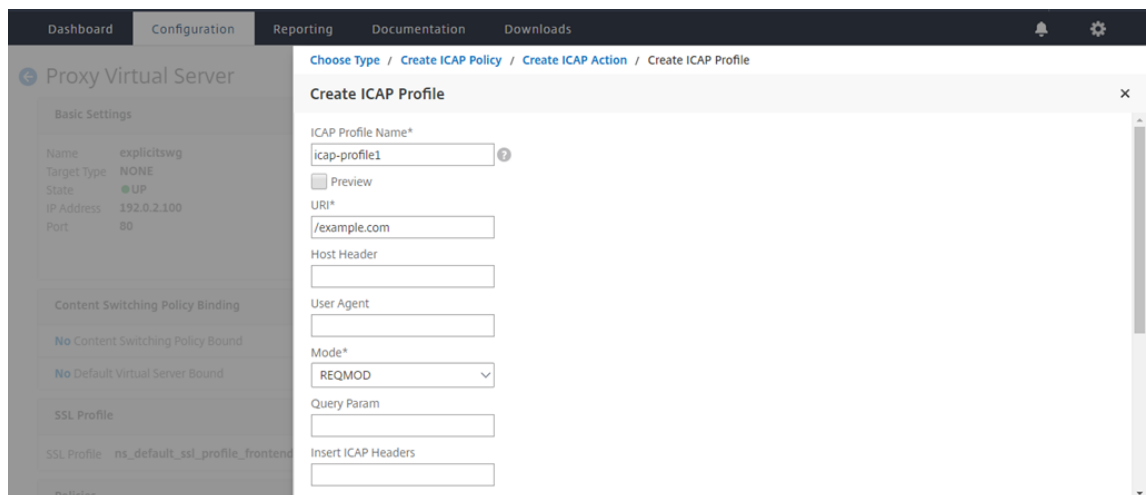


8. Tapez un nom pour l'action. Dans **Nom du serveur**, tapez le nom du service TCP créé précédem-

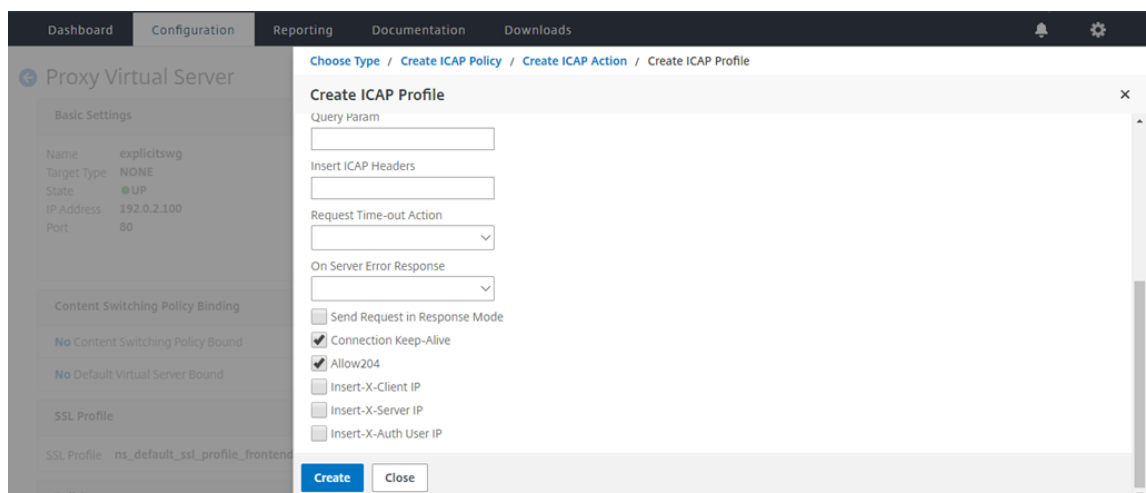
ment. Dans **Profil ICAP**, cliquez sur le signe « + » pour ajouter un profil ICAP.



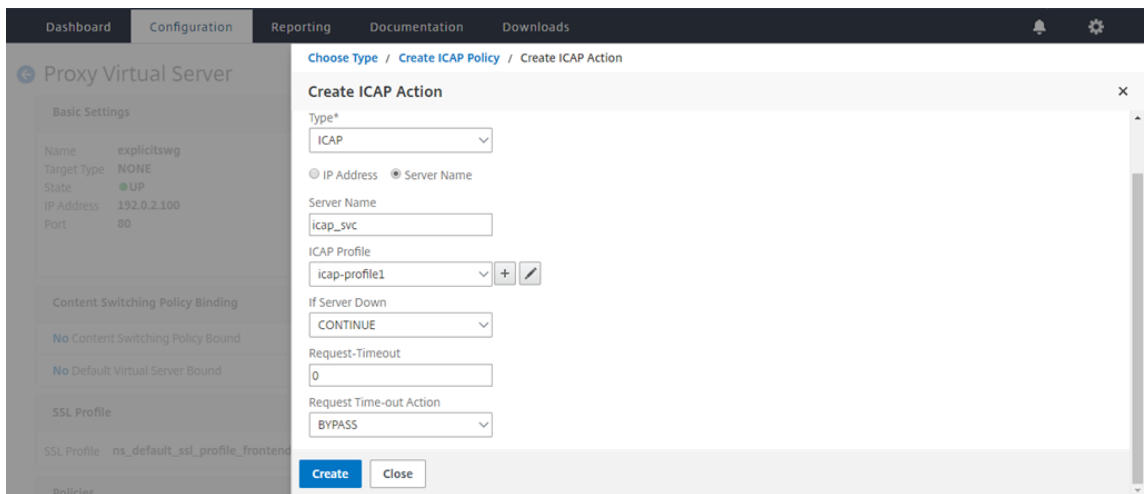
9. Tapez un nom de profil, URI. Dans **Mode**, sélectionnez **REQMOD**.



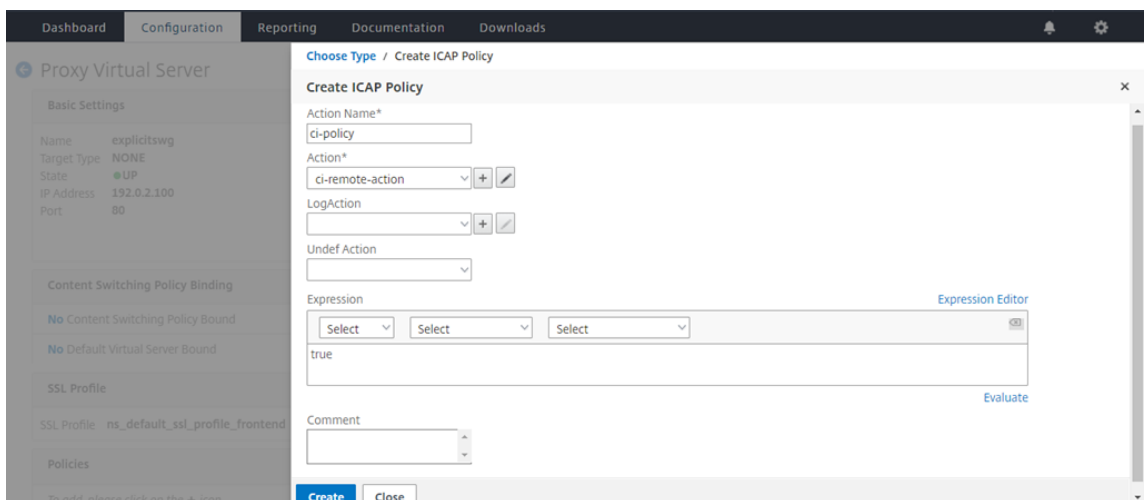
10. Cliquez sur **Créer**.



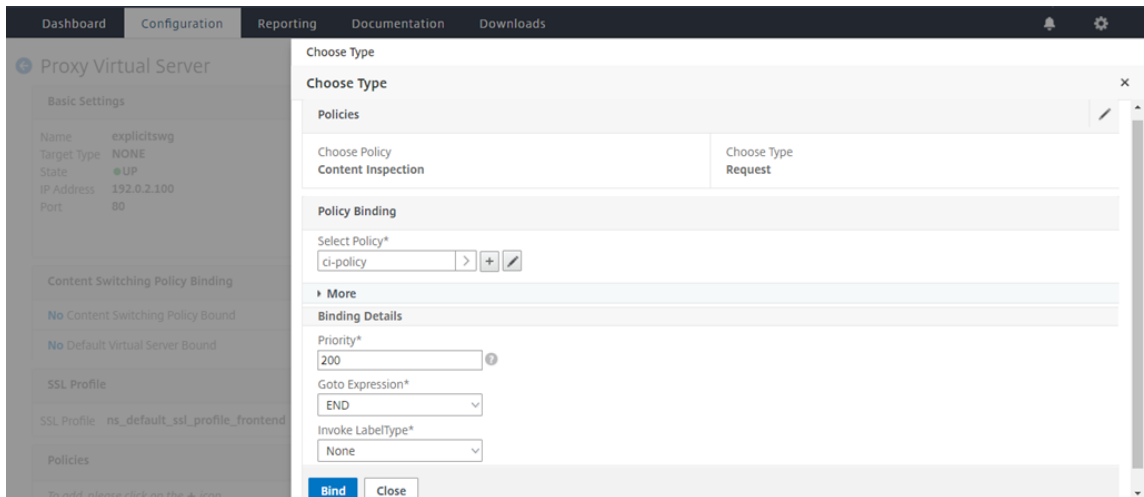
11. Dans la page **Créer une action ICAP**, cliquez sur **Créer**.



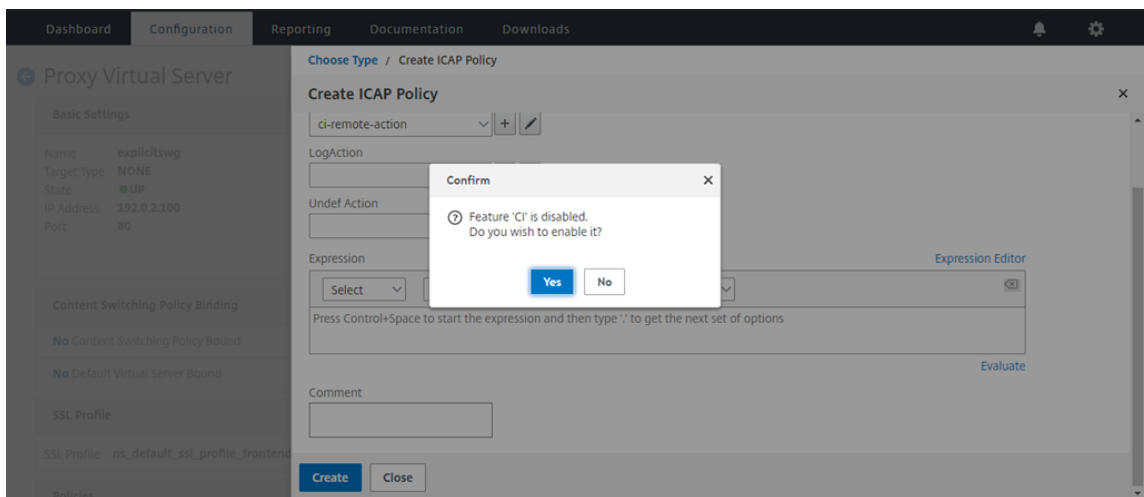
12. Dans la page **Créer une stratégie ICAP**, entrez true dans l'**éditeur d'expressions**. Cliquez ensuite sur **Créer**.



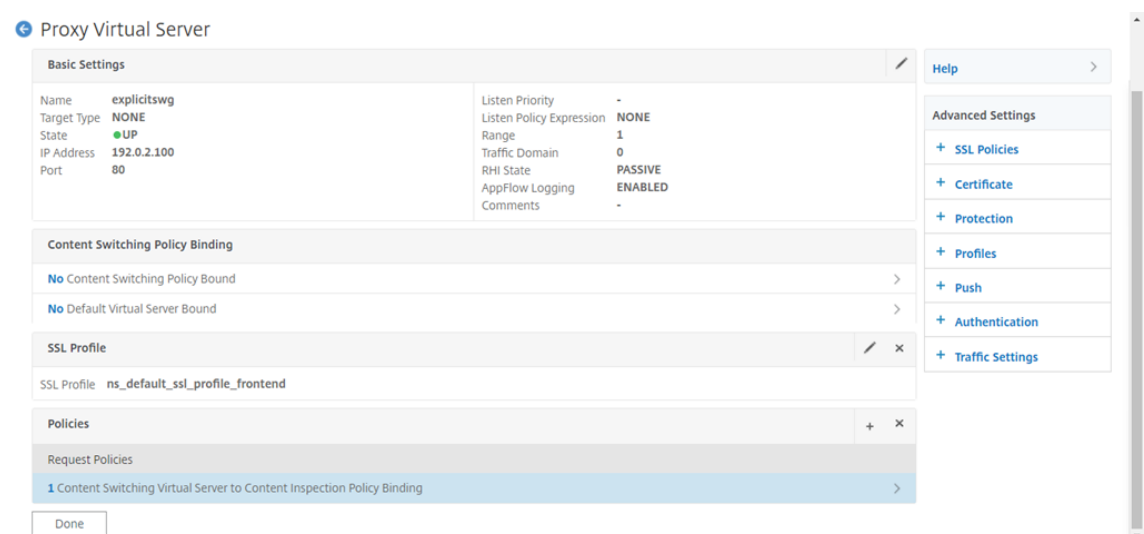
13. Cliquez sur **Bind**.



14. Lorsque vous êtes invité à activer la fonction d'inspection du contenu, sélectionnez **Oui**.



15. Cliquez sur **Terminé**.



ICAP sécurisé

Vous pouvez établir une connexion sécurisée entre l'apppliance SWG et les serveurs ICAP. Pour ce faire, créez un service SSL_TCP au lieu d'un service TCP. Configurez un serveur virtuel d'équilibrage de charge de type SSL_TCP. Liez le service ICAP au serveur virtuel d'équilibrage de charge.

Configurer ICAP sécurisé à l'aide de l'interface de ligne de commande

À l'invite de commandes, tapez :

- `add service <name> <IP> SSL_TCP <port>`
- `add lb vserver <name> <serviceType> <IPAddress> <port>`
- `bind lb vserver <name> <serviceName>`

Exemple :

```
1 add service icap_svc 203.0.113.100 SSL_TCP 1344
2
3 add lbvserver lbicap SSL_TCP 0.0.0.0 0
4
5 bind lb vserver lbicap icap_svc
```

Configurer ICAP sécurisé à l'aide de l'interface graphique

1. Accédez à **Équilibrage de charge** > **Serveurs virtuels**, puis cliquez sur **Ajouter**.
2. Spécifiez un nom pour le serveur virtuel, l'adresse IP et le port. Spécifiez le protocole SSL_TCP.
3. Cliquez sur **OK**.
4. Cliquez dans la section **Liaison de service serveur virtuel d'équilibrage** de charge pour ajouter un service ICAP.
5. Cliquez sur « + » pour ajouter un service.
6. Spécifiez un nom de service, une adresse IP, un protocole (SSL_TCP) et un port (le port par défaut pour ICAP sécurisé est 11344).
7. Cliquez sur **OK**.
8. Cliquez sur **Terminé**.
9. Cliquez sur **Bind**.
10. Cliquez deux fois sur **Continuer**.
11. Cliquez sur **Terminé**.

Limitations

Les fonctionnalités suivantes ne sont pas prises en charge :

- Mise en cache des réponses ICAP.
- Insertion de l'en-tête X-auth-User-URI.
- Insertion de la requête HTTP dans la requête ICAP dans RESPMOD.

Intégration avec IPS ou NGFW en tant que périphériques en ligne

April 27, 2021

Les dispositifs de sécurité tels que le système de prévention des intrusions (IPS) et le pare-feu de nouvelle génération (NGFW) protègent les serveurs contre les attaques réseau. Ces périphériques peuvent inspecter le trafic en direct et sont généralement déployés en mode Inline de couche 2. Citrix Secure Web Gateway (SWG) assure la sécurité des utilisateurs et du réseau d'entreprise lors de l'accès aux ressources sur Internet.

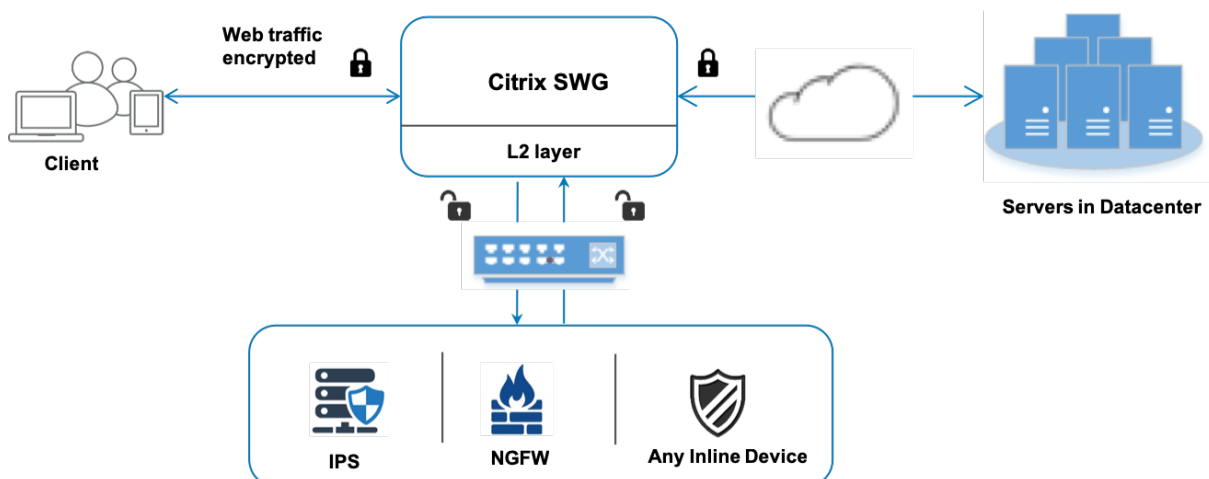
Une appliance Citrix SWG peut être intégrée à un ou plusieurs périphériques en ligne pour prévenir les menaces et fournir une protection de sécurité avancée. Les périphériques en ligne peuvent être n'importe quel périphérique de sécurité, tel que IPS et NGFW.

Voici quelques cas d'utilisation où vous pouvez bénéficier de l'utilisation de l'appliance Citrix SWG et de l'intégration de périphériques en ligne :

- **Inspection du trafic chiffré** : la plupart des appliances IPS et NGFW contournent le trafic chiffré, ce qui peut rendre les serveurs vulnérables aux attaques. Une appliance Citrix SWG peut déchiffrer le trafic et l'envoyer aux périphériques en ligne pour inspection. Cette intégration améliore la sécurité réseau du client.
- **Déchargement des périphériques en ligne du traitement TLS/SSL : le traitement TLS/SSL** est coûteux, ce qui peut entraîner une utilisation élevée du processeur dans les appliances IPS ou NGFW s'ils décryptent également le trafic. Une appliance Citrix SWG aide à décharger le traitement TLS/SSL des périphériques en ligne. Par conséquent, les appareils en ligne peuvent inspecter un volume plus élevé de trafic.
- **Chargement des périphériques en ligne d'équilibrage** : si vous avez configuré plusieurs périphériques en ligne pour gérer le trafic lourd, une appliance Citrix SWG peut équilibrer la charge et répartir le trafic uniformément vers ces périphériques.
- **Sélection intelligente du trafic** : au lieu d'envoyer tout le trafic au périphérique en ligne pour inspection, l'appliance effectue une sélection intelligente du trafic. Par exemple, il ignore l'envoi de fichiers texte pour inspection aux périphériques en ligne.

Intégration de Citrix SWG avec les périphériques en ligne

Le diagramme suivant montre comment un Citrix SWG est intégré aux périphériques de sécurité en ligne.



Lorsque vous intégrez des périphériques en ligne avec l'appliance Citrix SWG, les composants interagissent comme suit :

1. Un client envoie une demande à une appliance Citrix SWG.
2. L'appliance envoie les données au périphérique en ligne pour inspection du contenu en fonction de l'évaluation de la stratégie. Pour le trafic HTTPS, l'appliance déchiffre les données et les envoie en texte brut au périphérique en ligne pour inspection du contenu.

Remarque :

S'il y a au moins deux périphériques en ligne, la charge de l'appliance équilibre les périphériques et envoie le trafic.

3. Le périphérique en ligne inspecte les données à la recherche de menaces et décide de supprimer, de réinitialiser ou de renvoyer les données à l'appliance.
4. S'il existe des menaces de sécurité, le périphérique modifie les données et les envoie à l'appliance.
5. Pour le trafic HTTPS, l'appliance recrypte les données et transmet la demande au serveur principal.
6. Le serveur principal envoie la réponse à l'appliance.
7. L'appliance déchiffre à nouveau les données et les envoie au périphérique en ligne pour inspection.
8. Le périphérique en ligne inspecte les données. S'il existe des menaces de sécurité, le périphérique modifie les données et les envoie à l'appliance.

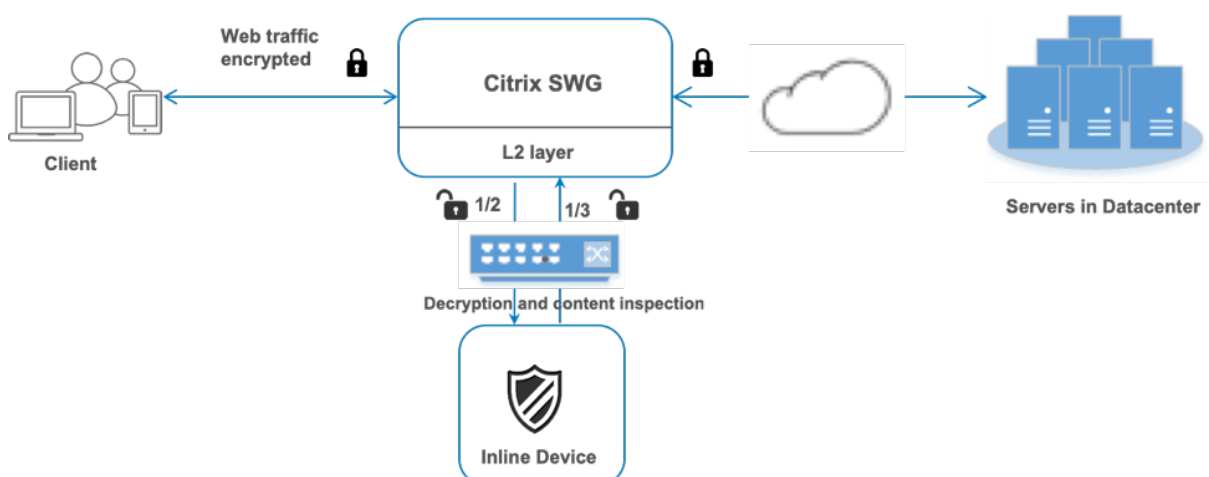
9. L'appareil recrypte les données et envoie la réponse au client.

Configuration de l'intégration de périphériques en ligne

Vous pouvez configurer une appliance Citrix SWG avec un périphérique en ligne de trois manières différentes, comme suit :

Scénario 1 : Utilisation d'un seul périphérique en ligne

Pour intégrer un périphérique de sécurité (IPS ou NGFW) en mode intégré, vous devez activer l'inspection de contenu et le transfert basé sur Mac (MBF) en mode global sur l'appareil SWG. Ensuite, ajoutez un profil d'inspection de contenu, un service TCP, une action d'inspection de contenu pour les périphériques en ligne pour réinitialiser, bloquer ou supprimer le trafic basé sur l'inspection. Ajoutez également une stratégie d'inspection du contenu utilisée par l'appareil pour décider du sous-ensemble de trafic à envoyer aux périphériques en ligne. Enfin, configurez le serveur virtuel proxy avec la connexion de couche 2 activée sur le serveur et liez la stratégie d'inspection de contenu à ce serveur virtuel proxy.



Procédez comme suit :

1. Activer le mode de transfert basé sur Mac (MPF).
2. Activez la fonction d'inspection du contenu.
3. Ajoutez un profil d'inspection de contenu pour le service. Le profil d'inspection de contenu contient les paramètres de périphérique en ligne qui intègrent l'appareil SWG à un périphérique en ligne.
4. (Facultatif) Ajoutez un moniteur TCP.

Remarque :

Les périphériques transparents n'ont pas d'adresse IP. Par conséquent, pour effectuer des vérifications de l'état, vous devez lier explicitement un moniteur.

5. Ajoutez un service. Un service représente un périphérique en ligne.
6. (Facultatif) Liez le service au moniteur TCP.
7. Ajoutez une action d'inspection du contenu pour le service.
8. Ajoutez une stratégie d'inspection du contenu et spécifiez l'action.
9. Ajoutez un serveur virtuel proxy HTTP ou HTTPS (commutation de contenu).
10. Liez la stratégie d'inspection de contenu au serveur virtuel.

Configuration à l'aide de l'interface de ligne de commande Tapez les commandes suivantes à l'invite de commandes. Des exemples sont donnés après la plupart des commandes.

1. Activez MBF.

```
1 enable ns mode mbf
```

2. Activez la fonctionnalité.

```
1 enable ns feature contentInspection
```

3. Ajouter un profil d'inspection de contenu.

```
1 add contentInspection profile <name> -type InlineInspection -
  egressInterface <interface_name> -ingressInterface <
  interface_name>[-egressVlan <positive_integer>] [-ingressVlan <
  positive_integer>]
```

Exemple :

```
1 add contentInspection profile ipsprof -type InlineInspection -
  ingressinterface "1/2" -egressInterface "1/3"
```

4. Ajoutez un service. Spécifiez une adresse IP fictive qui n'appartient à aucun des périphériques, y compris les périphériques en ligne. Définissez `use source IP address` (USIP) sur YES. Définissez `useproxyport` sur NO. Éteignez le moniteur d'intégrité. Activez la surveillance de l'intégrité uniquement si vous liez ce service à un moniteur TCP. Si vous liez un moniteur à un service, définissez l'option TRANSPARENT du moniteur sur ON.

```
1 add service <service_name> <IP> TCP <Port> -
  contentinspectionProfileName <Name> -healthMonitor NO -usip
  YES - useproxyport NO
```

Exemple :

```
1 add service ips_service 198.51.100.2 TCP * -healthMonitor YES -
  usip YES -useproxyport NO -contentInspectionProfileName ipsprof
```

5. Ajoutez une action d'inspection du contenu.

```
1 add contentInspection action <name> -type INLINEINSPECTION -
  serverName <string>
```

Exemple :

```
1 add contentInspection action ips_action -type INLINEINSPECTION -
  serverName ips_service
```

6. Ajoutez une stratégie d'inspection du contenu.

```
1 add contentInspection policy <name> -rule <expression> -action <
  string>
```

Exemple :

```
1 add contentInspection policy ips_pol -rule "HTTP.REQ.METHOD.NE("
  CONNECT")" -action ips_action
```

7. Ajoutez un serveur virtuel proxy.

```
1 add cs vserver <name> PROXY <IPAddress> <port> -cltTimeout <secs>
  -Listenpolicy <expression> -authn401 ( ON | OFF ) -authnVsName
  <string> -l2Conn ON
```

Exemple :

```
1 add cs vserver transparentcs PROXY * * -cltTimeout 180 -
  Listenpolicy exp1 -authn401 on -authnVsName swg-auth-vs-trans-
  http -l2Conn ON
```

8. Liez la stratégie au serveur virtuel.

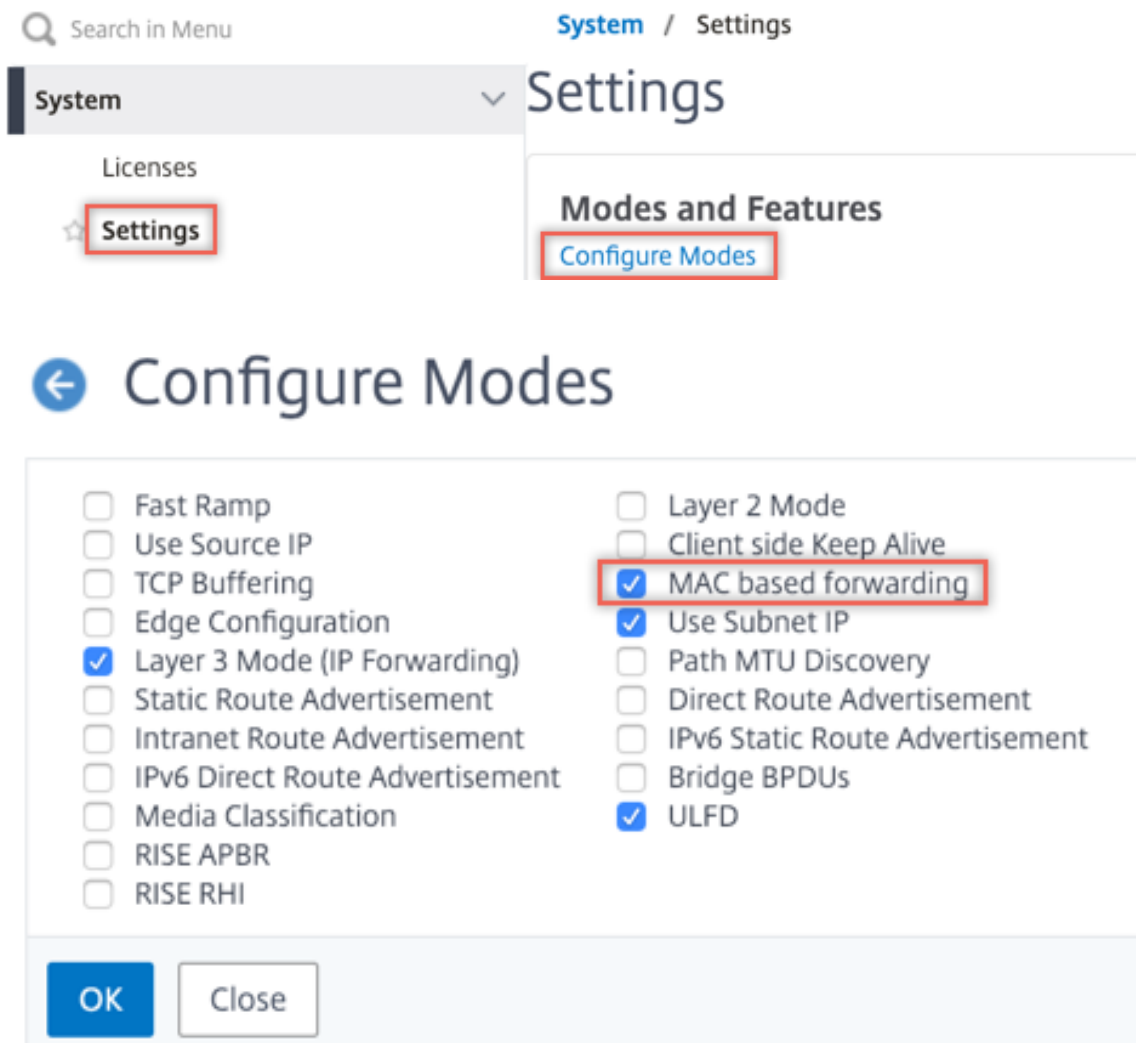
```
1 bind cs vserver <name> -policyName <string> -priority <
  positive_integer> -gotoPriorityExpression <expression> -type
  REQUEST
```

Exemple :

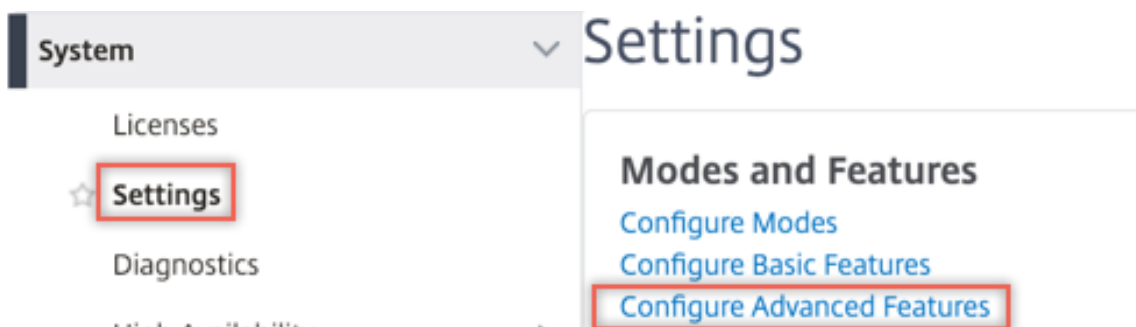
```
1 bind cs vserver explicitcs -policyName ips_pol -priority 1 -
  gotoPriorityExpression END -type REQUEST
```

Configuration à l'aide de l'interface graphique

1. Accédez à **Système > Paramètres**. Dans **Modes et fonctionnalités**, cliquez sur **Configurer les modes**.



2. Accédez à **Système > Paramètres**. Dans **Modes et fonctionnalités**, cliquez sur **Configurer les fonctionnalités avancées**.

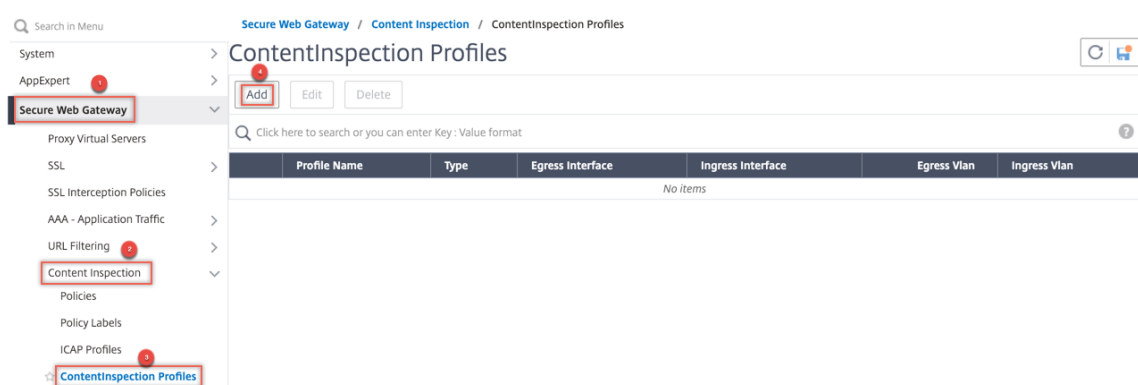


← Configure Advanced Features

<input type="checkbox"/> Surge Protection	<input type="checkbox"/> Sure Connect
<input type="checkbox"/> Priority Queuing	<input type="checkbox"/> Http Dos Protection
<input type="checkbox"/> Cache Redirection	<input type="checkbox"/> Global Server Load Balancing
<input type="checkbox"/> Web Logging	<input type="checkbox"/> OSPF Routing
<input type="checkbox"/> RIP Routing	<input type="checkbox"/> BGP Routing
<input type="checkbox"/> IPv6 Protocol Translation	<input checked="" type="checkbox"/> Responder
<input type="checkbox"/> EdgeSight Monitoring (HTML Injection)	<input type="checkbox"/> Citrix ADC Push
<input checked="" type="checkbox"/> AppFlow	<input type="checkbox"/> Cloud Bridge
<input type="checkbox"/> ISIS Routing	<input type="checkbox"/> Callhome
<input type="checkbox"/> AppQoE	<input type="checkbox"/> Front End Optimization
<input type="checkbox"/> Video Optimization	<input type="checkbox"/> Content Accelerator
<input type="checkbox"/> Large Scale NAT	<input type="checkbox"/> vPath
<input type="checkbox"/> RDP Proxy	<input type="checkbox"/> Reputation
<input checked="" type="checkbox"/> URL Filtering	<input checked="" type="checkbox"/> Forward Proxy
<input checked="" type="checkbox"/> SSL Interception	<input type="checkbox"/> Adaptive TCP
<input type="checkbox"/> Connection Quality Analytics	<input checked="" type="checkbox"/> Content Inspection
<input type="checkbox"/> RISE	

OK Close

3. Accédez à **Secure Web Gateway > Inspection du contenu > Profils d'inspection du contenu**. Cliquez sur **Ajouter**.



4. Accédez à **Équilibrage de charge > Services > Ajouter** et ajouter un service. Dans **Paramètres avancés**, cliquez sur **Profils**. Dans la liste **Nom du profil CI**, sélectionnez le profil d'inspection du contenu créé précédemment. Dans **Paramètres de service**, définissez **Utiliser l'adresse IP sourcesur YES** et **Utiliser le port proxysur Non**. Dans **Paramètres de base**, définissez le **contrôle de l'intégrité** sur NO. Activez la surveillance de l'intégrité uniquement si vous liez ce

service à un moniteur TCP. Si vous liez un moniteur à un service, définissez l'option TRANSPARENT dans le moniteur sur ON.

The screenshot displays the configuration interface for Citrix Secure Web Gateway, divided into three main sections:

- Profiles:** This section contains five dropdown menus, each with an 'Add' button and a help icon. The 'CI Profile Name' dropdown is selected and contains the text 'ipsprof'.
- Service Settings:** This section contains two columns of settings. The 'Use Proxy Port' setting is highlighted with a red box and set to 'NO'. The 'Use Source IP Address' setting is also highlighted with a red box and set to 'YES'. Other settings include 'Client Keep-Alive' (NO), 'TCP Buffering' (NO), 'Insert Client IP Address' (DISABLED), and 'Header' (client-ip).
- Basic Settings:** This section displays a table of configuration parameters for the service. The 'Health Monitoring' setting is highlighted with a red box and set to 'NO'. Other settings include 'Service Name' (ips_service), 'Server Name' (198.51.100.2), 'IP Address' (198.51.100.2), 'Server State' (UP), 'Protocol' (TCP), 'Port' (*), 'Traffic Domain' (0), 'Number of Active Connections' (-), 'Hash ID' (-), 'Server ID' (None), 'Cache Type' (SERVER), 'Cacheable' (NO), and 'AppFlow Logging' (ENABLED).

5. Accédez à **Secure Web Gateway > Servers virtuels Proxy > Ajouter**. Spécifiez un nom, une adresse IP et un port. Dans **Paramètres avancés**, sélectionnez **Stratégies**. Cliquez sur le signe « + ».

Proxy Virtual Server

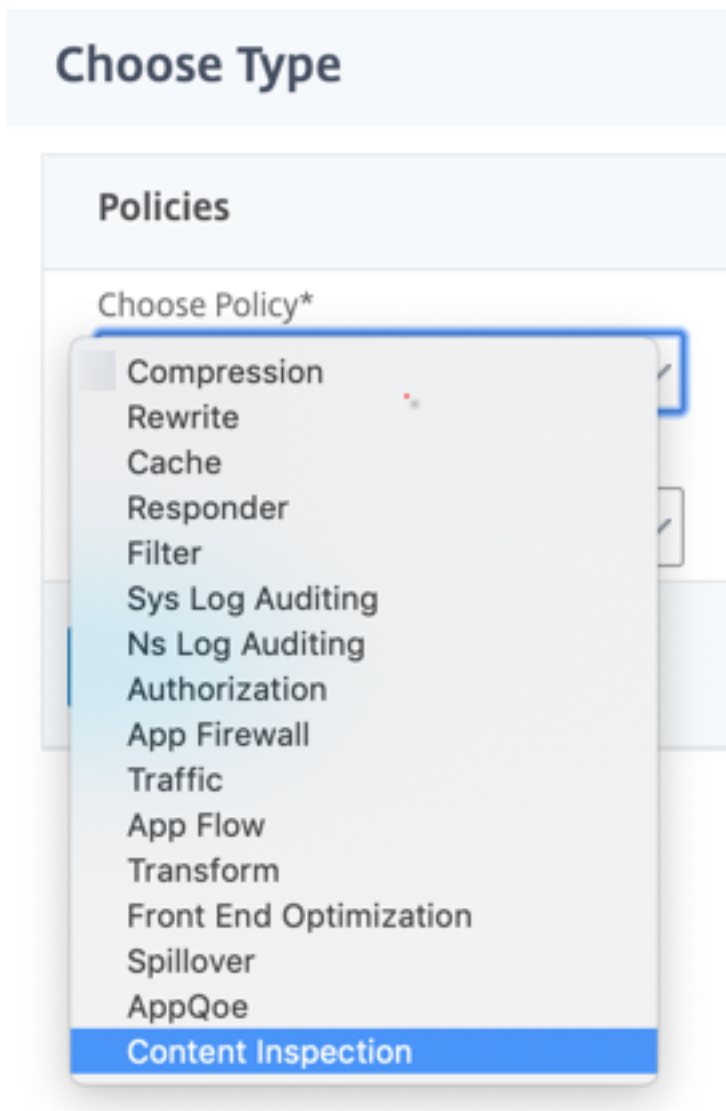
Basic Settings	
Name	proxyvsvr
State	● UP
IP Address	198.51.200.2
Port	80
Listen Priority	-
Listen Policy Expression	NONE
Range	1
IPset	-
Traffic Domain	0
RHI State	PASSIVE
AppFlow Logging	ENABLED
Comments	-

Content Switching Policy Binding	
No Content Switching Policy Bound	>
No Default Virtual Server Bound	>

Certificate	
No Server Certificate	>
No CA Certificate	>

Policies	
	+ x

6. Dans **Choisir une stratégie**, sélectionnez **Inspection du contenu**. Cliquez sur **Continuer**.



7. Cliquez sur **Ajouter**. Spécifiez un nom. Dans **Action**, cliquez sur **Ajouter**.

[Choose Type](#) / Create ContentInspection Policy

Create ContentInspection Policy

Policy Name*

Action*

Log Action

UNDEF Action

8. Spécifiez un nom. Dans **Type**, sélectionnez **INLINEINSPECTION**. Dans **Nom du serveur**, sélectionnez le service TCP créé précédemment.

← Create ContentInspection Action

Name*

Type*

Server Name*

If Server Down

Request-Timeout

Request timeout action

9. Cliquez sur **Créer**. Spécifiez la règle et cliquez sur **Créer**.

Configure ContentInspection Policy

Policy Name
ips_pol

Action*
ips_action Add Edit

Log Action
Add Edit

UNDEF Action

Expression* [Expression Editor](#)
Select Select Select
HTTP.REQ.METHOD.NE("CONNECT") [Evaluate](#)

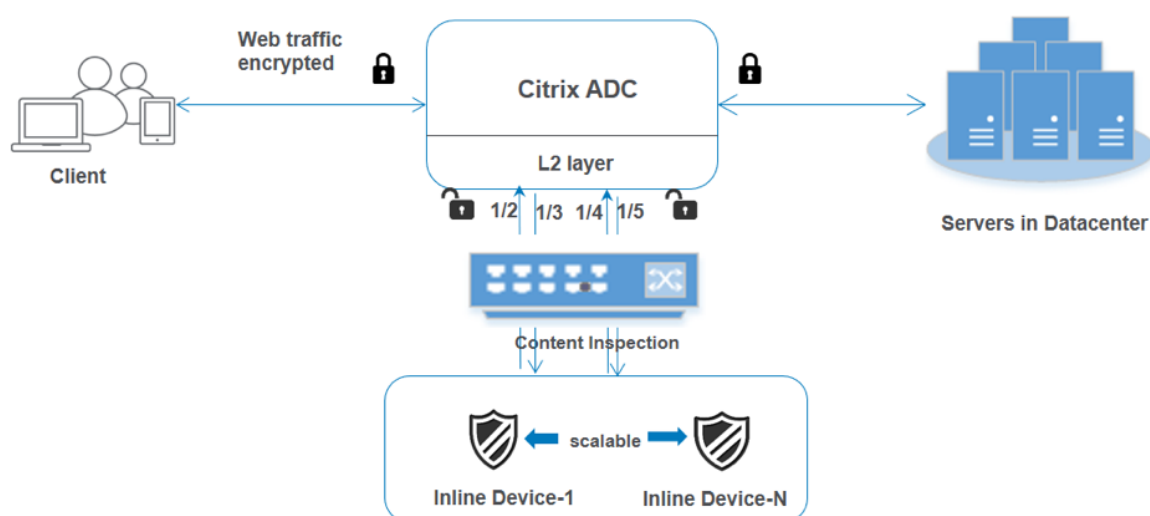
Comment

OK Close

10. Cliquez sur **Bind**.
11. Cliquez sur **Terminé**.

Scénario 2 : équilibrage de la charge de plusieurs périphériques en ligne avec interfaces dédiées

Si vous utilisez au moins deux périphériques en ligne, vous pouvez équilibrer la charge des périphériques à l'aide de différents services d'inspection de contenu avec des interfaces dédiées. Dans ce cas, la charge de l'apppliance Citrix SWG équilibre le sous-ensemble du trafic envoyé à chaque périphérique via une interface dédiée. Le sous-ensemble est décidé en fonction des stratégies configurées. Par exemple, les fichiers TXT ou image peuvent ne pas être envoyés pour inspection aux périphériques en ligne.



La configuration de base reste la même que dans le scénario 1. Toutefois, vous devez créer un profil d'inspection de contenu pour chaque périphérique en ligne et spécifier l'interface d'entrée et de sortie dans chaque profil. Ajoutez un service pour chaque périphérique en ligne. Ajoutez un serveur virtuel d'équilibrage de charge et spécifiez-le dans l'action d'inspection du contenu. Effectuez les étapes supplémentaires suivantes :

1. Ajoutez des profils d'inspection de contenu pour chaque service.
2. Ajoutez un service pour chaque périphérique.
3. Ajoutez un serveur virtuel d'équilibrage de charge.
4. Spécifiez le serveur virtuel d'équilibrage de charge dans l'action d'inspection du contenu.

Configuration à l'aide de l'interface de ligne de commande Tapez les commandes suivantes à l'invite de commandes. Des exemples sont donnés après chaque commande.

1. Activez MBF.

```
1 enable ns mode mbf
```

2. Activez la fonctionnalité.

```
1 enable ns feature contentInspection
```

3. Ajouter le profil 1 pour le service 1.

```
1 add contentInspection profile <name> -type InlineInspection -
  egressInterface <interface_name> -ingressInterface <
  interface_name>[-egressVlan <positive_integer>] [-ingressVlan <
  positive_integer>]
```

Exemple :

```
1 add contentInspection profile ipsprof1 -type InlineInspection -
  ingressInterface "1/2" -egressInterface "1/3"
```

4. Ajouter le profil 2 pour le service 2.

```
1 add contentInspection profile <name> -type InlineInspection -
  egressInterface <interface_name> -ingressInterface <
  interface_name>[-egressVlan <positive_integer>] [-ingressVlan <
  positive_integer>]
```

Exemple :

```
1 add contentInspection profile ipsprof2 -type InlineInspection -
  ingressInterface "1/4" -egressInterface "1/5"
```

5. Ajouter le service 1. Spécifiez une adresse IP fictive qui n'appartient à aucun des périphériques, y compris les périphériques en ligne. Définissez `use source IP address` (USIP) sur YES. Définissez `useproxyport` sur NO. Éteignez le moniteur d'intégrité. Activez la surveillance de l'intégrité uniquement si vous liez ce service à un moniteur TCP. Si vous liez un moniteur à un service, définissez l'option TRANSPARENT du moniteur sur ON.

```
1 add service <service_name> <IP> TCP <Port> -
  contentinspectionProfileName <Name> -healthMonitor NO -usip
  YES -useproxyport NO
```

Exemple :

```
1 add service ips_service1 192.168.10.2 TCP * -healthMonitor NO -
  usip YES -useproxyport NO -contentInspectionProfileName
  ipsprof1
```

6. Ajouter le service 2. Spécifiez une adresse IP fictive qui n'appartient à aucun des périphériques, y compris les périphériques en ligne. Définissez `use source IP address` (USIP) sur YES. Définissez `useproxyport` sur NO. Éteignez le moniteur d'intégrité. Activez la surveillance de l'intégrité uniquement si vous liez ce service à un moniteur TCP. Si vous liez un moniteur à un service, définissez l'option TRANSPARENT du moniteur sur ON.

```
1 add service <service_name> <IP> TCP <Port> -
  contentinspectionProfileName <Name> -healthMonitor NO -usip
  YES -useproxyport NO
```

Exemple :

```
1 add service ips_service2 192.168.10.3 TCP * -healthMonitor NO -
  usip YES -useproxyport NO -contentInspectionProfileName
  ipsprof2
```

7. Ajoutez un serveur virtuel d'équilibrage de charge.
-

```
1 add lb vserver <LB_VSERVER_NAME> TCP <IP> <port>
```

Exemple :

```
1 add lb vserver lb_inline_vserver TCP 192.0.2.100 *
```

8. Liez les services au serveur virtuel d'équilibrage de charge.

```
1 bind lb vserver <LB_VSERVER_NAME> <service_name>
2 bind lb vserver <LB_VSERVER_NAME> <service_name>
```

Exemple :

```
1 bind lb vserver lb_inline_vserver ips_service1
2 bind lb vserver lb_inline_vserver ips_service2
```

9. Spécifiez le serveur virtuel d'équilibrage de charge dans l'action d'inspection du contenu.

```
1 add contentInspection action <name> -type INLINEINSPECTION -
  serverName <string>
```

Exemple :

```
1 add contentInspection action ips_action -type INLINEINSPECTION -
  serverName lb_inline_vserver
```

10. Ajoutez une stratégie d'inspection du contenu. Spécifiez l'action d'inspection du contenu dans la stratégie.

```
1 add contentInspection policy <name> -rule <expression> -action <
  string>
```

Exemple :

```
1 add contentInspection policy ips_pol -rule "HTTP.REQ.METHOD.NE("
  CONNECT")" -action ips_action
```

11. Ajoutez un serveur virtuel proxy.

```
1 add cs vserver <name> PROXY <IPAddress> <port> -l2Conn ON
```

Exemple :

```
1 add cs vserver transparentcs PROXY * * -l2Conn ON
```

12. Liez la stratégie d'inspection de contenu au serveur virtuel.

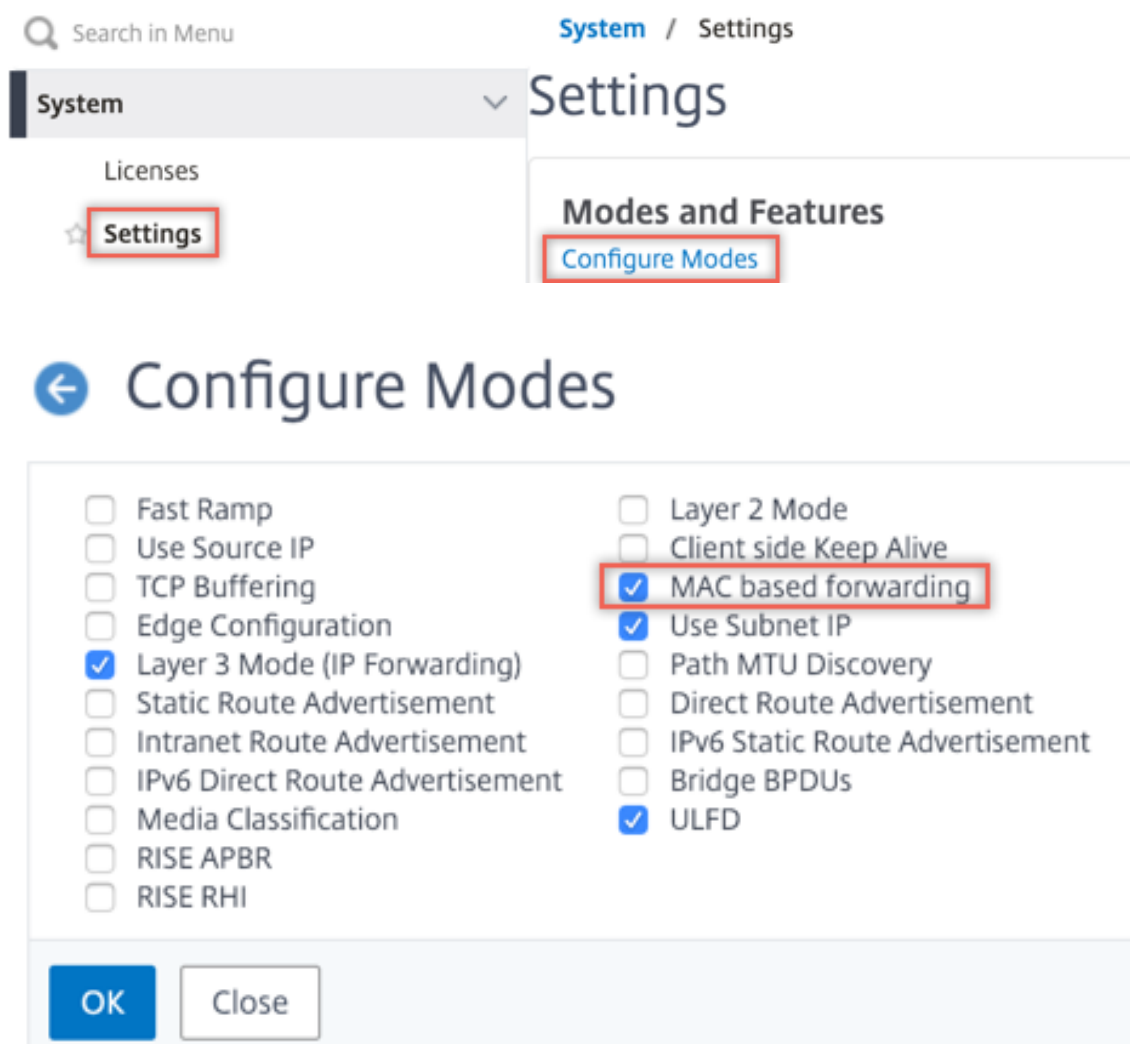
```
1 bind cs vserver <name> -policyName <string> -priority <
  positive_integer> -gotoPriorityExpression <expression> -type
  REQUEST
```

Exemple :

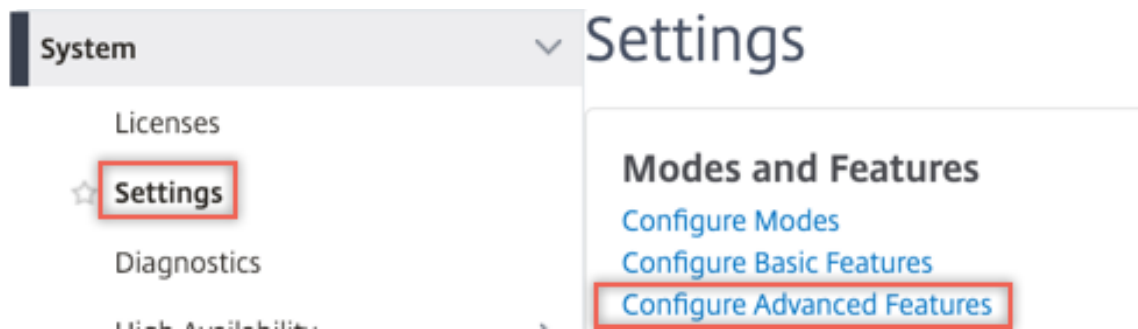

```
1 bind cs vserver explicitcs -policyName ips_pol -priority 1 -
gotoPriorityExpression END -type REQUEST
```

Configuration à l'aide de l'interface graphique

1. Accédez à **Système > Paramètres**. Dans **Modes et fonctionnalités**, cliquez sur **Configurer les modes**.



2. Accédez à **Système > Paramètres**. Dans **Modes et fonctionnalités**, cliquez sur **Configurer les fonctionnalités avancées**.

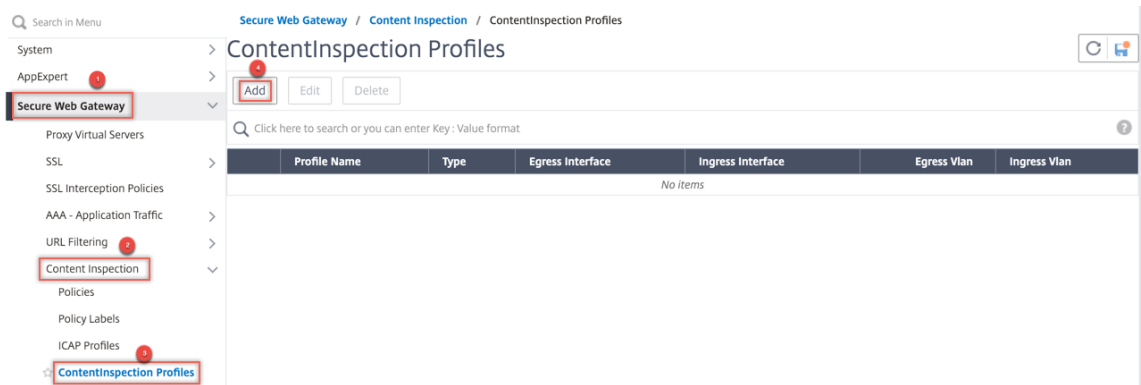


← Configure Advanced Features

<input type="checkbox"/> Surge Protection	<input type="checkbox"/> Sure Connect
<input type="checkbox"/> Priority Queuing	<input type="checkbox"/> Http Dos Protection
<input type="checkbox"/> Cache Redirection	<input type="checkbox"/> Global Server Load Balancing
<input type="checkbox"/> Web Logging	<input type="checkbox"/> OSPF Routing
<input type="checkbox"/> RIP Routing	<input type="checkbox"/> BGP Routing
<input type="checkbox"/> IPv6 Protocol Translation	<input checked="" type="checkbox"/> Responder
<input type="checkbox"/> EdgeSight Monitoring (HTML Injection)	<input type="checkbox"/> Citrix ADC Push
<input checked="" type="checkbox"/> AppFlow	<input type="checkbox"/> Cloud Bridge
<input type="checkbox"/> ISIS Routing	<input type="checkbox"/> Callhome
<input type="checkbox"/> AppQoS	<input type="checkbox"/> Front End Optimization
<input type="checkbox"/> Video Optimization	<input type="checkbox"/> Content Accelerator
<input type="checkbox"/> Large Scale NAT	<input type="checkbox"/> vPath
<input type="checkbox"/> RDP Proxy	<input type="checkbox"/> Reputation
<input checked="" type="checkbox"/> URL Filtering	<input checked="" type="checkbox"/> Forward Proxy
<input checked="" type="checkbox"/> SSL Interception	<input type="checkbox"/> Adaptive TCP
<input type="checkbox"/> Connection Quality Analytics	<input checked="" type="checkbox"/> Content Inspection
<input type="checkbox"/> RISE	

OK Close

3. Accédez à **Secure Web Gateway > Inspection du contenu > Profils d'inspection du contenu**. Cliquez sur **Ajouter**.



Spécifiez les interfaces d'entrée et de sortie.

← Create ContentInspectionProfile

Profile Name*

Type*

Egress Interface*

Ingress Interface*

Egress Vlan

Ingress Vlan

Créez deux profils. Spécifiez une interface d'entrée et de sortie différente dans le second profil.

- Accédez à **Équilibrage de charge > Services > Ajouter** et ajoutez un service. Dans **Paramètres avancés**, cliquez sur **Profils**. Dans la liste **Nom du profil CI**, sélectionnez le profil d'inspection du contenu créé précédemment. Dans **Paramètres de service**, définissez **Utiliser l'adresse IP source** sur YES et **Utiliser le port proxy** sur Non. Dans **Paramètres de base**, définissez le **contrôle de l'intégrité** sur NO. Activez la surveillance de l'intégrité uniquement si vous liez ce service à un moniteur TCP. Si vous liez un moniteur à un service, définissez l'option TRANSPARENT dans le moniteur sur ON.

Profiles

Net Profile

▼

?

TCP Profile

▼

HTTP Profile

▼

DNS Profile Name

▼

CI Profile Name

▼

?

Service Settings

Sure Connect		Use Source IP Address	YES
Surge Protection	OFF	Client Keep-Alive	NO
Use Proxy Port	NO	TCP Buffering	NO
Down State Flush	ENABLED	Insert Client IP Address	DISABLED
Access Down	NO	Header	client-ip

Basic Settings	
Service Name	ips_service
Server Name	198.51.100.2
IP Address	198.51.100.2
Server State	● UP
Protocol	TCP
Port	*
Comments	
Monitoring Connection Close Bit	NONE
Traffic Domain	0
Number of Active Connections	-
Hash ID	-
Server ID	None
Cache Type	SERVER
Cacheable	NO
Health Monitoring	NO
AppFlow Logging	ENABLED

Créez deux services. Spécifiez les adresses IP factices qui ne sont la propriété d'aucun des périphériques, y compris les périphériques en ligne.

5. Accédez à **Équilibrage de charge > Serveurs virtuels > Ajouter**. Créez un serveur virtuel d'équilibrage de charge TCP.

Load Balancing Virtual Server

Basic Settings
Create a virtual server by specifying a name, an IP address, a port, and a protocol type. If an application is accessible from the Internet, the virtual server IP (VIP) address is a public IP address. If the application is accessible only from the local area network (LAN) or wide area network (WAN), the VIP is usually a private (ICANN non-routable) IP address. You can configure multiple virtual servers to receive client requests, thereby increasing the availability of resources to process client requests.
Name*
<input type="text" value="lb_inline_server"/>
Protocol*
<input type="text" value="TCP"/>
IP Address Type*
<input type="text" value="IP Address"/>
IP Address*
<input type="text" value="192 . 0 . 2 . 100"/>
Port*
<input type="text" value="80"/>
More
<input type="button" value="OK"/> <input type="button" value="Cancel"/>

Cliquez sur **OK**.

6. Cliquez dans la section **Load Balancing Virtual Server Service Liaison**. Dans **Liaison de service**, cliquez sur la flèche dans **Sélectionner un service**. Sélectionnez les deux services créés précédemment, puis cliquez sur **Sélectionner**. Cliquez sur **Bind**.

Service Binding

Select Service*

Click to select



Add

Edit

Binding Details

Weight

1

Bind

Close

Service Binding / Service

Service

Select Add Edi

🔍 Click here to search or you can en

<input type="checkbox"/>	Name
<input type="checkbox"/>	icap_svc
<input type="checkbox"/>	icap_domain1
<input type="checkbox"/>	ssltcp_svc1
<input type="checkbox"/>	s1
<input type="checkbox"/>	ips_service
<input checked="" type="checkbox"/>	ips_service1
<input checked="" type="checkbox"/>	ips_service2

Service Binding

Service Binding

Select Service*

ips_service1, ips_service2 > Add Edit ?

Binding Details

Weight

1

Bind Close

7. Accédez à **Secure Web Gateway > Servers virtuels Proxy > Ajouter**. Spécifiez un nom, une adresse IP et un port. Dans **Paramètres avancés**, sélectionnez **Stratégies**. Cliquez sur le signe « + ».

← Proxy Virtual Server

Basic Settings	
Name	proxysvr
State	● UP
IP Address	198.51.200.2
Port	80
Listen Priority	-
Listen Policy Expression	NONE
Range	1
IPset	-
Traffic Domain	0
RHI State	PASSIVE
AppFlow Logging	ENABLED
Comments	-

Content Switching Policy Binding

No Content Switching Policy Bound >

No Default Virtual Server Bound >

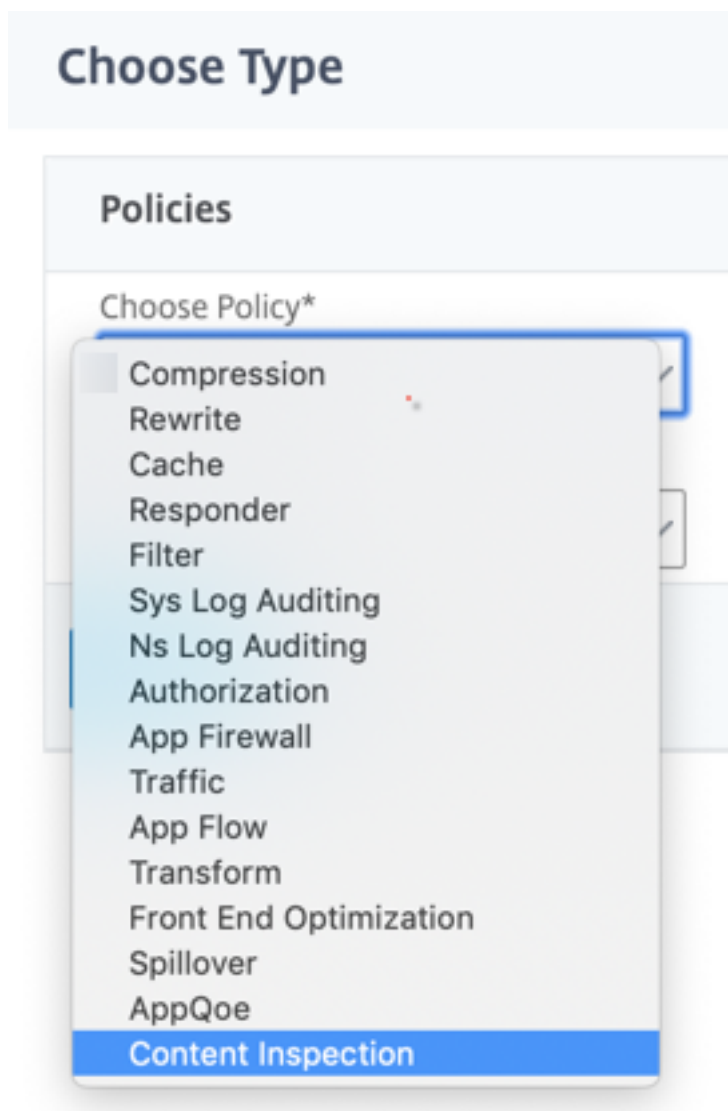
Certificate

No Server Certificate >

No CA Certificate >

Policies + x

8. Dans **Choisir une stratégie**, sélectionnez **Inspection du contenu**. Cliquez sur **Continuer**.



9. Cliquez sur **Ajouter**. Spécifiez un nom. Dans **Action**, cliquez sur **Ajouter**.

[Choose Type](#) / Create ContentInspection Policy

Create ContentInspection Policy

Policy Name*

Action*

Log Action

UNDEF Action

10. Spécifiez un nom. Dans **Type**, sélectionnez **INLINEINSPECTION**. Dans **Nom du serveur**, sélectionnez le serveur virtuel d'équilibrage de charge créé précédemment.

← Create ContentInspection Action

Name*

Type*

Server Name*

If Server Down

Request-Timeout

Request timeout action

11. Cliquez sur **Créer**. Spécifiez la règle et cliquez sur **Créer**.

Configure ContentInspection Policy

Policy Name
ips_pol

Action*
ips_action Add Edit

Log Action
Add Edit

UNDEF Action

Expression* [Expression Editor](#)
Select Select Select
HTTP.REQ.METHOD.NE("CONNECT") Evaluate

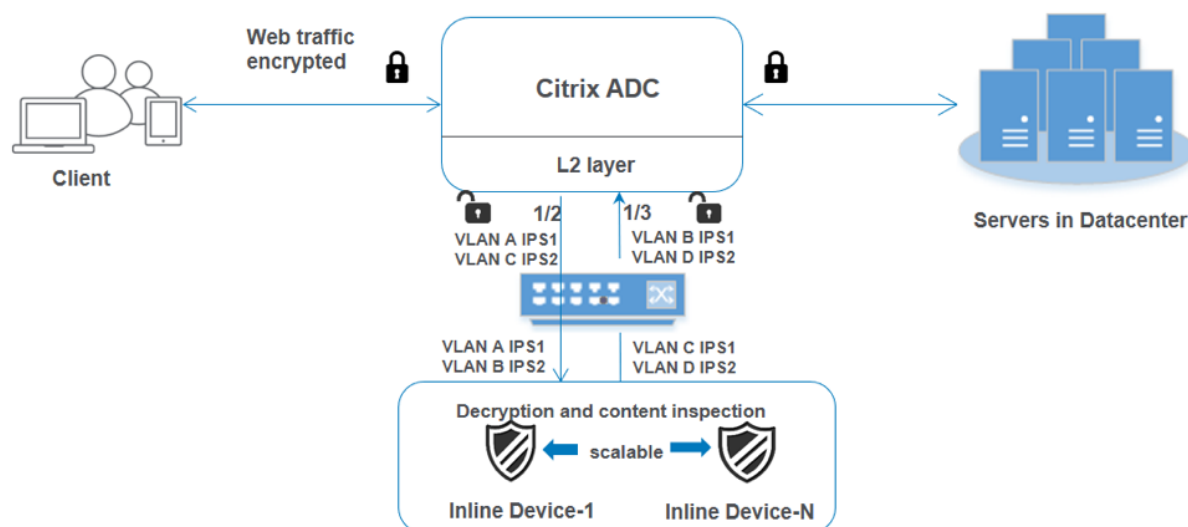
Comment

OK Close

12. Cliquez sur **Bind**.
13. Cliquez sur **Terminé**.

Scénario 3 : équilibrage de la charge de plusieurs périphériques en ligne avec des interfaces partagées

Si vous utilisez au moins deux périphériques en ligne, vous pouvez équilibrer la charge des périphériques à l'aide de différents services d'inspection de contenu avec des interfaces partagées. Dans ce cas, la charge de l'apppliance Citrix SWG équilibre le sous-ensemble du trafic envoyé à chaque périphérique via une interface partagée. Le sous-ensemble est décidé en fonction des stratégies configurées. Par exemple, les fichiers TXT ou image peuvent ne pas être envoyés pour inspection aux périphériques en ligne.



La configuration de base reste la même que dans le scénario 2. Pour ce scénario, liez les interfaces à différents VLAN pour séparer le trafic de chaque périphérique en ligne. Spécifiez les VLAN dans les profils d'inspection de contenu. Effectuez les étapes supplémentaires suivantes :

1. Liez les interfaces partagées à différents VLAN.
2. Spécifiez les VLAN d'entrée et de sortie dans les profils d'inspection de contenu.

Configuration à l'aide de l'interface de ligne de commande Tapez les commandes suivantes à l'invite de commandes. Des exemples sont donnés après chaque commande.

1. Activez MBF.

```
1 enable ns mode mbf
```

2. Activez la fonctionnalité.

```
1 enable ns feature contentInspection
```

3. Liez les interfaces partagées à différents VLAN.

```
1 bind vlan <id> -ifnum <interface> -tagged
```

Exemple :

```
1 bind vlan 100 -ifnum 1/2 tagged
2 bind vlan 200 -ifnum 1/3 tagged
3 bind vlan 300 -ifnum 1/2 tagged
4 bind vlan 400 -ifnum 1/3 tagged
```

4. Ajouter le profil 1 pour le service 1. Spécifiez les VLAN d'entrée et de sortie dans le profil.

```
1 add contentInspection profile <name> -type InlineInspection -
  egressInterface <interface_name> -ingressInterface <
  interface_name>[-egressVlan <positive_integer>] [-ingressVlan <
  positive_integer>]
```

Exemple :

```
1 add contentInspection profile ipsprof1 -type InlineInspection -
  egressInterface "1/3" -ingressinterface "1/2" - egressVlan 100
  -ingressVlan 300
```

5. Ajouter le profil 2 pour le service 2. Spécifiez les VLAN d'entrée et de sortie dans le profil.

```
1 add contentInspection profile <name> -type InlineInspection -
  egressInterface <interface_name> -ingressInterface <
  interface_name>[-egressVlan <positive_integer>] [-ingressVlan <
  positive_integer>]
```

Exemple :

```
1 add contentInspection profile ipsprof2 -type InlineInspection -
  egressInterface "1/3" -ingressinterface "1/2" - egressVlan 200
  -ingressVlan 400
```

6. Ajouter le service 1.

```
1 add service <service_name> <IP> TCP <Port> -
  contentinspectionProfileName <Name> -healthMonitor NO -usip
  YES - useproxyport NO
```

Exemple :

```
1 add service ips_service1 192.168.10.2 TCP * -healthMonitor NO -
  usip YES -useproxyport NO -contentInspectionProfileName
  ipsprof1
```

7. Ajouter le service 2.

```
1 add service <service_name> <IP> TCP <Port> -
  contentinspectionProfileName <Name> -healthMonitor NO -usip
  YES - useproxyport NO
```

Exemple :

```
1 add service ips_service2 192.168.10.3 TCP * -healthMonitor NO -
  usip YES -useproxyport NO -contentInspectionProfileName
  ipsprof2
```

8. Ajoutez un serveur virtuel d'équilibrage de charge.

```
1 add lb vserver <LB_VSERVER_NAME> TCP <IP> <port>
```

Exemple :

```
1 add lb vserver lb_inline_vserver TCP 192.0.2.100 *
```

9. Liez les services au serveur virtuel d'équilibrage de charge.

```
1 bind lb vserver <LB_VSERVER_NAME> <service_name>
2 bind lb vserver <LB_VSERVER_NAME> <service_name>
```

Exemple :

```
1 bind lb vserver lb_inline_vserver ips_service1
2 bind lb vserver lb_inline_vserver ips_service2
```

10. Spécifiez le serveur virtuel d'équilibrage de charge dans l'action d'inspection du contenu.

```
1 add contentInspection action <name> -type INLINEINSPECTION -
  serverName <string>
```

Exemple :

```
1 add contentInspection action ips_action -type INLINEINSPECTION -
  serverName lb_inline_vserver
```

11. Ajoutez une stratégie d'inspection du contenu. Spécifiez l'action d'inspection du contenu dans la stratégie.

```
1 add contentInspection policy <name> -rule <expression> -action <
  string>
```

Exemple :

```
1 add contentInspection policy ips_pol -rule "HTTP.REQ.METHOD.NE("
  CONNECT")" -action ips_action
```

12. Ajoutez un serveur virtuel proxy.

```
1 add cs vserver <name> PROXY <IPAddress> <port> -l2Conn ON
```

Exemple :

```
1 add cs vserver transparentcs PROXY * * -l2Conn ON
```

13. Liez la stratégie d'inspection de contenu au serveur virtuel.

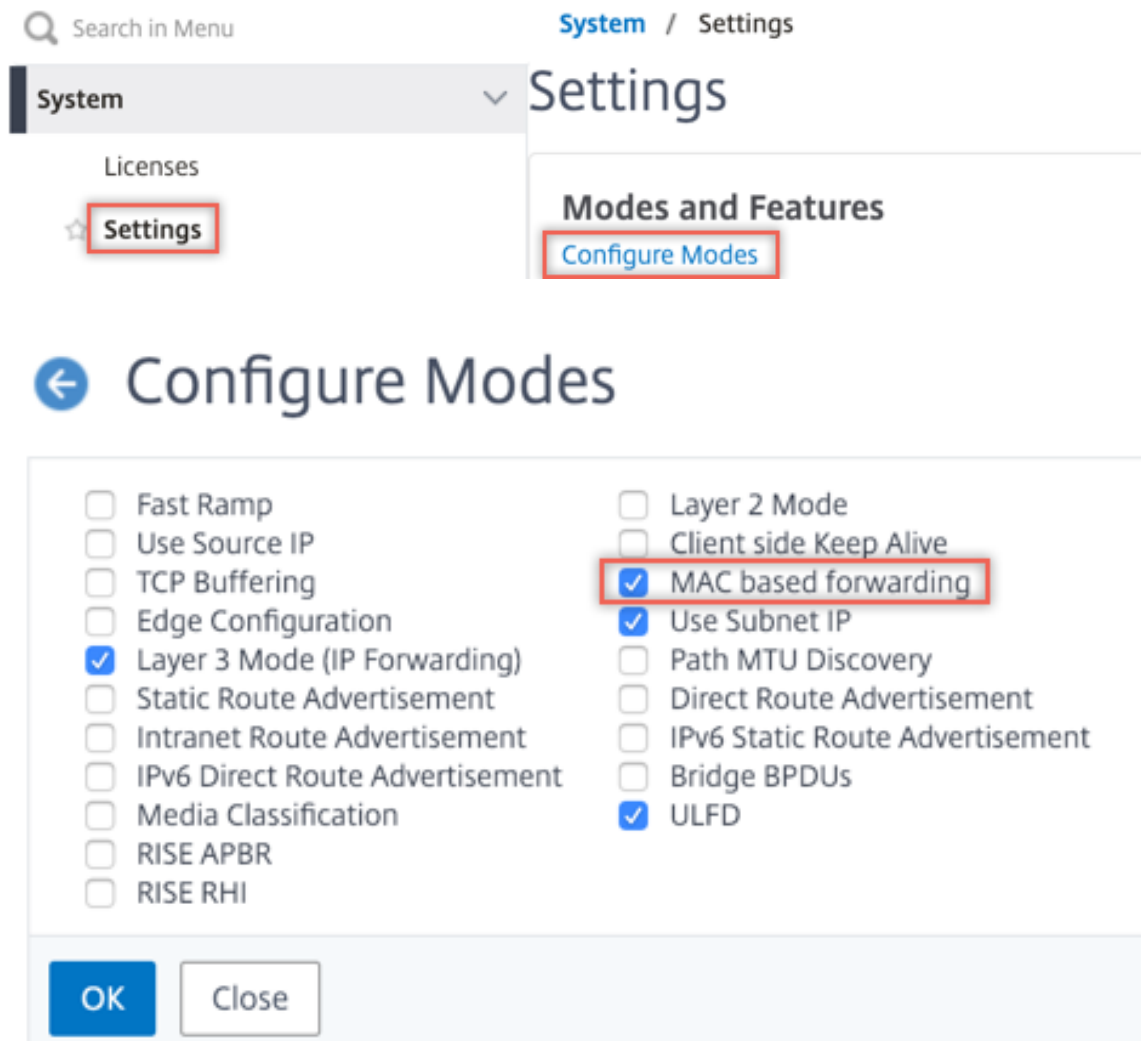
```
1 bind cs vserver <name> -policyName <string> -priority <
  positive_integer> -gotoPriorityExpression <expression> -type
  REQUEST
```

Exemple :

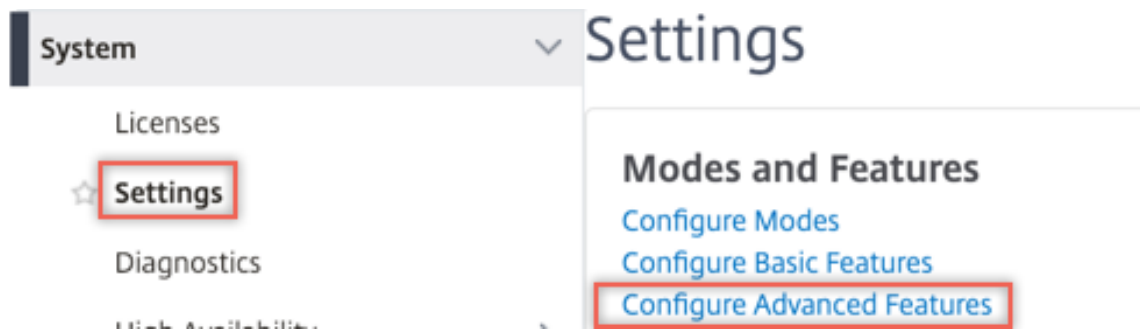
```
1 bind cs vserver explicitcs -policyName ips_pol -priority 1 -  
gotoPriorityExpression END -type REQUEST
```

Configuration à l'aide de l'interface graphique

1. Accédez à **Système > Paramètres**. Dans **Modes et fonctionnalités**, cliquez sur **Configurer les modes**.



2. Accédez à **Système > Paramètres**. Dans **Modes et fonctionnalités**, cliquez sur **Configurer les fonctionnalités avancées**.



← Configure Advanced Features

<input type="checkbox"/> Surge Protection	<input type="checkbox"/> Sure Connect
<input type="checkbox"/> Priority Queuing	<input type="checkbox"/> Http Dos Protection
<input type="checkbox"/> Cache Redirection	<input type="checkbox"/> Global Server Load Balancing
<input type="checkbox"/> Web Logging	<input type="checkbox"/> OSPF Routing
<input type="checkbox"/> RIP Routing	<input type="checkbox"/> BGP Routing
<input type="checkbox"/> IPv6 Protocol Translation	<input checked="" type="checkbox"/> Responder
<input type="checkbox"/> EdgeSight Monitoring (HTML Injection)	<input type="checkbox"/> Citrix ADC Push
<input checked="" type="checkbox"/> AppFlow	<input type="checkbox"/> Cloud Bridge
<input type="checkbox"/> ISIS Routing	<input type="checkbox"/> Callhome
<input type="checkbox"/> AppQoS	<input type="checkbox"/> Front End Optimization
<input type="checkbox"/> Video Optimization	<input type="checkbox"/> Content Accelerator
<input type="checkbox"/> Large Scale NAT	<input type="checkbox"/> vPath
<input type="checkbox"/> RDP Proxy	<input type="checkbox"/> Reputation
<input checked="" type="checkbox"/> URL Filtering	<input checked="" type="checkbox"/> Forward Proxy
<input checked="" type="checkbox"/> SSL Interception	<input type="checkbox"/> Adaptive TCP
<input type="checkbox"/> Connection Quality Analytics	<input checked="" type="checkbox"/> Content Inspection
<input type="checkbox"/> RISE	

OK Close

3. Accédez à **Système > Réseau > VLAN > Ajouter**. Ajoutez quatre VLAN et marquez-les sur les interfaces.

← Create VLAN

VLAN ID*

100



Alias Name

Maximum Transmission Unit

- Dynamic Routing
- IPv6 Dynamic Routing
- Partitions Sharing

Interface Bindings

IP Bindings

<input type="checkbox"/>	Name	Tagged
<input type="checkbox"/>	1/1	<input type="checkbox"/>
<input checked="" type="checkbox"/>	1/2	<input checked="" type="checkbox"/>
<input type="checkbox"/>	1/3	<input type="checkbox"/>

← Create VLAN

VLAN ID*

200



Alias Name

Maximum Transmission Unit

- Dynamic Routing
- IPv6 Dynamic Routing
- Partitions Sharing

Interface Bindings

IP Bindings

<input type="checkbox"/>	Name	Tagged
<input type="checkbox"/>	1/1	<input type="checkbox"/>
<input type="checkbox"/>	1/2	<input type="checkbox"/>
<input checked="" type="checkbox"/>	1/3	<input checked="" type="checkbox"/>

← Create VLAN

VLAN ID*

300



Alias Name

Maximum Transmission Unit

- Dynamic Routing
- IPv6 Dynamic Routing
- Partitions Sharing

Interface Bindings

IP Bindings

<input type="checkbox"/>	Name	Tagged
<input type="checkbox"/>	1/1	<input type="checkbox"/>
<input checked="" type="checkbox"/>	1/2	<input checked="" type="checkbox"/>
<input type="checkbox"/>	1/3	<input type="checkbox"/>

← Create VLAN

VLAN ID*

 ?

Alias Name

Maximum Transmission Unit

Dynamic Routing

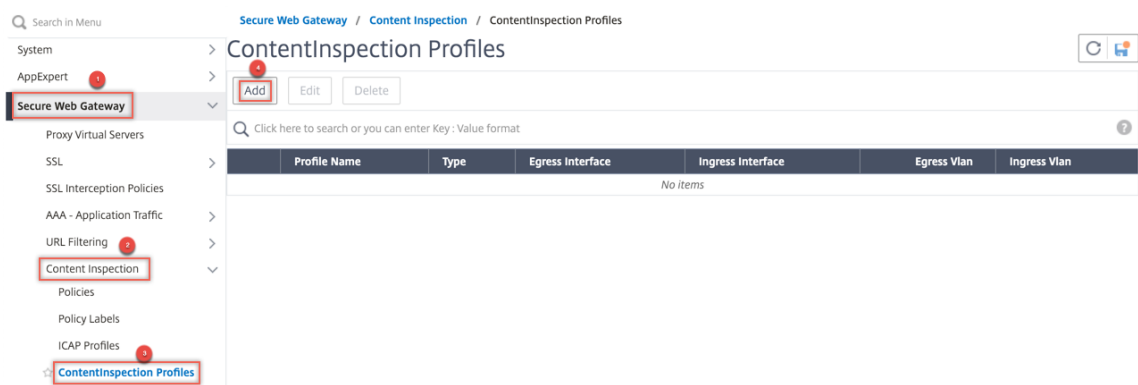
IPv6 Dynamic Routing

Partitions Sharing

Interface Bindings IP Bindings

<input type="checkbox"/>	Name	Tagged
<input type="checkbox"/>	1/1	<input type="checkbox"/>
<input type="checkbox"/>	1/2	<input type="checkbox"/>
<input checked="" type="checkbox"/>	1/3	<input checked="" type="checkbox"/>

4. Accédez à **Secure Web Gateway > Inspection du contenu > Profils d'inspection du contenu**. Cliquez sur **Ajouter**.



Spécifiez les VLAN d'entrée et de sortie.

← Create ContentInspectionProfile

Profile Name*

Type*

Egress Interface*

Ingress Interface*

Egress Vlan

Ingress Vlan

Créez d'autres profils. Spécifiez un VLAN d'entrée et de sortie différent dans le second profil.

← Create ContentInspectionProfile

Profile Name*

Type*

Egress Interface*

Ingress Interface*

Egress Vlan

Ingress Vlan

5. Accédez à **Équilibrage de charge > Services > Ajouter** et ajouter un service. Dans **Paramètres avancés**, cliquez sur **Profils**. Dans la liste **Nom du profil CI**, sélectionnez le profil d'inspection du contenu créé précédemment. Dans **Paramètres de service**, définissez **Utiliser l'adresse IP source** sur YES et **Utiliser le port proxy** sur Non. Dans **Paramètres de base**, définissez le **contrôle de l'intégrité** sur NO.

Créez deux services. Spécifiez les adresses IP factices qui ne sont la propriété d'aucun des périphériques, y compris les périphériques en ligne. Spécifiez le profil 1 dans le service 1 et le profil 2 dans le service 2.

Profiles

Net Profile

 ?

TCP Profile

HTTP Profile

DNS Profile Name

CI Profile Name

 ?

Profiles

Net Profile
 ▼ Add ?

TCP Profile
 ▼ Add

HTTP Profile
 ▼ Add

DNS Profile Name
 ▼ Add

CI Profile Name
 ▼ Add ?

OK

Service Settings

Sure Connect		Use Source IP Address	YES
Surge Protection	OFF	Client Keep-Alive	NO
Use Proxy Port	NO	TCP Buffering	NO
Down State Flush	ENABLED	Insert Client IP Address	DISABLED
Access Down	NO	Header	client-ip

Basic Settings

Service Name	ips_service	Traffic Domain	0
Server Name	198.51.100.2	Number of Active Connections	-
IP Address	198.51.100.2	Hash ID	-
Server State	● UP	Server ID	None
Protocol	TCP	Cache Type	SERVER
Port	*	Cacheable	NO
Comments		Health Monitoring	NO
		AppFlow Logging	ENABLED
Monitoring Connection Close Bit	NONE		

- Accédez à **Équilibrage de charge > Serveurs virtuels > Ajouter**. Créez un serveur virtuel d'équilibrage de charge TCP.

Load Balancing Virtual Server

Basic Settings

Create a virtual server by specifying a name, an IP address, a port, and a protocol type. If an application is accessible from the Internet, the virtual server IP (VIP) address is a public IP address. If the application is accessible only from the local area network (LAN) or wide area network (WAN), the VIP is usually a private (ICANN non-routable) IP address.
You can configure multiple virtual servers to receive client requests, thereby increasing the availability of resources to process client requests.

Name*

Protocol*

IP Address Type*

IP Address*

Port*

► More

Cliquez sur **OK**.

7. Cliquez dans la section **Load Balancing Virtual Server Service Liaison**. Dans **Liaison de service**, cliquez sur la flèche dans **Sélectionner un service**. Sélectionnez les deux services créés précédemment, puis cliquez sur **Sélectionner**. Cliquez sur **Bind**.

Service Binding

Select Service*

Binding Details

Weight

Service Binding / Service

Service

Select Add Edit

🔍 Click here to search or you can enter

<input type="checkbox"/>	Name
<input type="checkbox"/>	icap_svc
<input type="checkbox"/>	icap_domain1
<input type="checkbox"/>	ssltcp_svc1
<input type="checkbox"/>	s1
<input type="checkbox"/>	ips_service
<input checked="" type="checkbox"/>	ips_service1
<input checked="" type="checkbox"/>	ips_service2

Service Binding

Service Binding

Select Service*

ips_service1, ips_service2 > Add Edit ?

Binding Details

Weight

1

Bind Close

- Accédez à **Secure Web Gateway > Servers virtuels Proxy > Ajouter**. Spécifiez un nom, une adresse IP et un port. Dans **Paramètres avancés**, sélectionnez **Stratégies**. Cliquez sur le signe « + ».

← Proxy Virtual Server

Basic Settings

Name	proxysvr	Listen Priority	-
State	● UP	Listen Policy Expression	NONE
IP Address	198.51.200.2	Range	1
Port	80	IPset	-
		Traffic Domain	0
		RHI State	PASSIVE
		AppFlow Logging	ENABLED
		Comments	-

Content Switching Policy Binding

No Content Switching Policy Bound >

No Default Virtual Server Bound >

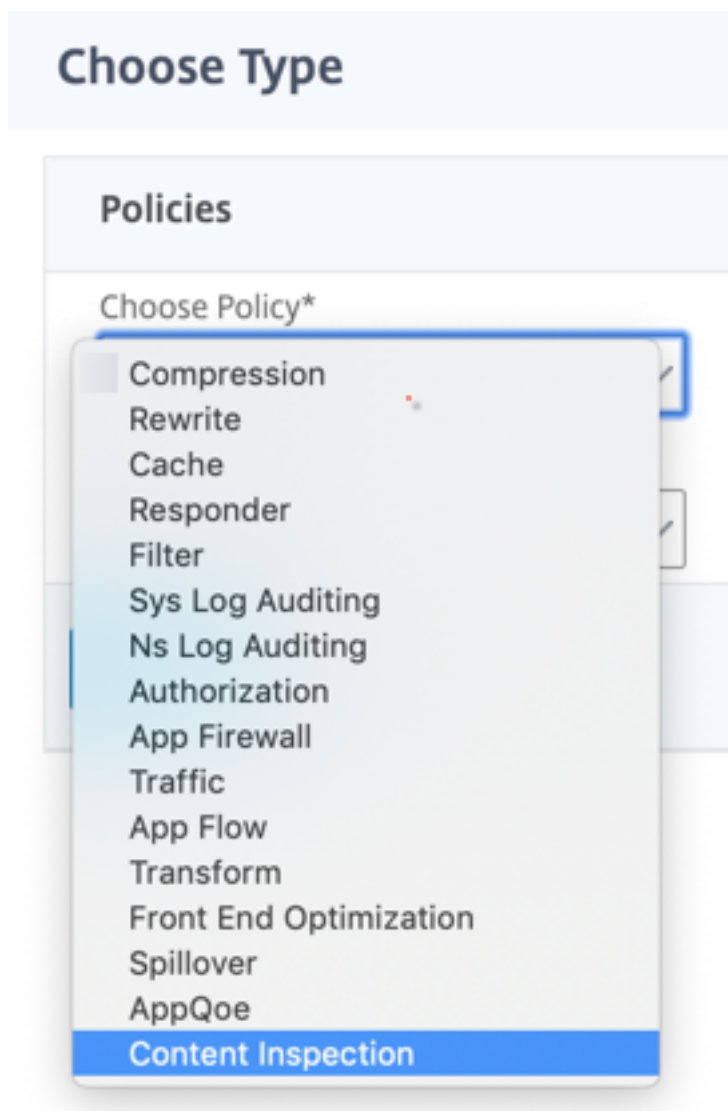
Certificate

No Server Certificate >

No CA Certificate >

Policies + x

- Dans **Choisir une stratégie**, sélectionnez **Inspection du contenu**. Cliquez sur **Continuer**.



10. Cliquez sur **Ajouter**. Spécifiez un nom. Dans **Action**, cliquez sur **Ajouter**.

[Choose Type](#) / Create ContentInspection Policy

Create ContentInspection Policy

Policy Name*

Action*

Log Action

UNDEF Action

11. Spécifiez un nom. Dans **Type**, sélectionnez **INLINEINSPECTION**. Dans **Nom du serveur**, sélectionnez le serveur virtuel d'équilibrage de charge créé précédemment.

← Create ContentInspection Action

Name*

Type*

Server Name*

If Server Down

Request-Timeout

Request timeout action

12. Cliquez sur **Créer**. Spécifiez la règle et cliquez sur **Créer**.

Configure ContentInspection Policy

Policy Name
ips_pol

Action*
ips_action Add Edit

Log Action
Add Edit

UNDEF Action

Expression* [Expression Editor](#)
Select Select Select
HTTP.REQ.METHOD.NE("CONNECT") Evaluate

Comment

OK Close

13. Cliquez sur **Bind**.

14. Cliquez sur **Terminé**.

Analytics

April 27, 2021

Dans l'apppliance Citrix SWG, tous les enregistrements utilisateur et les enregistrements suivants sont consignés. Lorsque vous intégrez Citrix Application Delivery Management (ADM) à l'apppliance Citrix SWG, l'activité utilisateur consignée et les enregistrements suivants de l'apppliance sont exportés vers Citrix ADM à l'aide du flux de journalisation.

Citrix ADM rassemble et présente des informations sur les activités des utilisateurs, telles que les sites Web visités et la bande passante dépensée. Il signale également l'utilisation de la bande passante et les menaces détectées, telles que les logiciels malveillants et les sites de phishing. Vous pouvez utiliser ces mesures clés pour surveiller votre réseau et prendre des mesures correctives avec l'apppliance Citrix SWG. Pour de plus amples informations, consultez la section [Analyses Citrix Secure Web Gateway](#).

Pour intégrer l'apppliance Citrix SWG à Citrix ADM :

1. Dans l'apppliance Citrix SWG, lors de la configuration de Secure Web Gateway, activez Analytics et fournissez les détails de l'instance Citrix ADM que vous souhaitez utiliser pour l'analyse.
2. Dans Citrix ADM, ajoutez l'apppliance Citrix SWG en tant qu'instance à Citrix ADM. Pour plus d'informations, consultez [Ajouter de nouvelles instances à Citrix ADM](#).

Cas d'utilisation : Rendre l'accès Internet d'entreprise conforme et sécurisé

April 27, 2021

Le directeur de la sécurité réseau dans une organisation financière veut protéger le réseau d'entreprise contre toute menace externe provenant du Web sous la forme de logiciels malveillants. Pour ce faire, le directeur doit gagner en visibilité pour contourner autrement le trafic crypté et contrôler l'accès aux sites Web malveillants. Le directeur est tenu de faire ce qui suit :

- Interceptez et examinez tout le trafic, y compris SSL/TLS (trafic crypté), entrant et sortant du réseau d'entreprise.
- Contournez l'interception des demandes vers des sites Web contenant des informations sensibles, telles que des informations financières de l'utilisateur ou des courriels.
- Bloquer l'accès aux URL nuisibles identifiées comme servant du contenu nuisible ou pour adultes.
- Identifiez les utilisateurs finaux (employés) de l'entreprise qui accèdent à des sites Web malveillants et bloquent l'accès à Internet pour ces utilisateurs ou bloquent les URL nuisibles.

Pour réaliser tout ce qui précède, le directeur peut configurer un proxy sur tous les périphériques de l'organisation et le pointer vers Citrix Secure Web Gateway (SWG), qui agit comme un serveur proxy dans le réseau. Le serveur proxy intercepte tout le trafic chiffré et non chiffré passant par le réseau de l'entreprise. Il demande l'authentification de l'utilisateur et associe le trafic à un utilisateur. Les catégories d'URL peuvent être spécifiées pour bloquer l'accès aux sites Web illégaux/nuisibles, adultes, malveillants et pourriels.

Pour atteindre ce qui précède, configurez les entités suivantes :

- Serveur de noms DNS pour résoudre les noms d'hôtes.
- Adresse IP de sous-réseau (SNIP) pour établir une connexion avec les serveurs d'origine. L'adresse SNIP doit avoir accès à Internet.
- Serveur proxy en mode explicite pour intercepter tout le trafic HTTP et HTTPS sortant.
- Profil SSL pour définir les paramètres SSL, tels que les chiffrements et les paramètres, pour les connexions.
- Paire de clé de certificat CA pour signer le certificat du serveur pour l'interception SSL.

- Stratégie SSL pour définir les sites Web à intercepter et à contourner.
- Authentification du serveur virtuel, de la stratégie et de l'action pour garantir que seuls les utilisateurs valides ont accès.
- Collecteur Appflow pour envoyer des données à Citrix Application Delivery Management (ADM).

Les procédures CLI et GUI sont répertoriées pour cet exemple de configuration. Les valeurs d'exemple suivantes sont utilisées. Remplacez-les par des données valides pour les adresses IP, le certificat et la clé SSL et les paramètres LDAP.

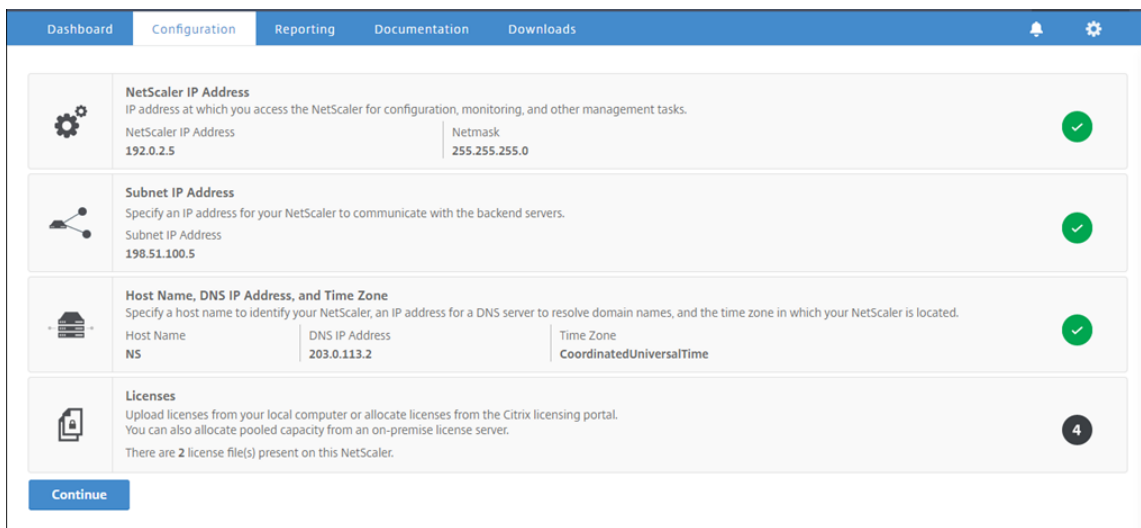
Nom	Valeurs utilisées dans l'exemple de configuration
Adresse du NSIP	192.0.2.5
Adresse IP du sous-réseau	198.51.100.5
Adresse IP du serveur virtuel LDAP	192.0.2.116
Adresse IP du serveur de noms DNS	203.0.113.2
Adresse IP du serveur proxy	192.0.2.100
Adresse IP MAS	192.0.2.41
Certificat d'autorité de certification pour l'interception SSL	ns-swg-ca-certkey (certificat : ns_swg_ca.crt et clé : ns_swg_ca.key)
DN de base LDAP	CN = utilisateurs, DC = CTXNSSFB, DC = COM
DN de liaison LDAP	CN=Administrateur, CN=Utilisateurs, DC=CTXNSSFB, DC=COM
Mot de passe DN de liaison LDAP	zzzzz

Utilisation de l'assistant de passerelle Web sécurisée pour configurer l'interception et l'examen du trafic à destination et en provenance du réseau d'entreprise

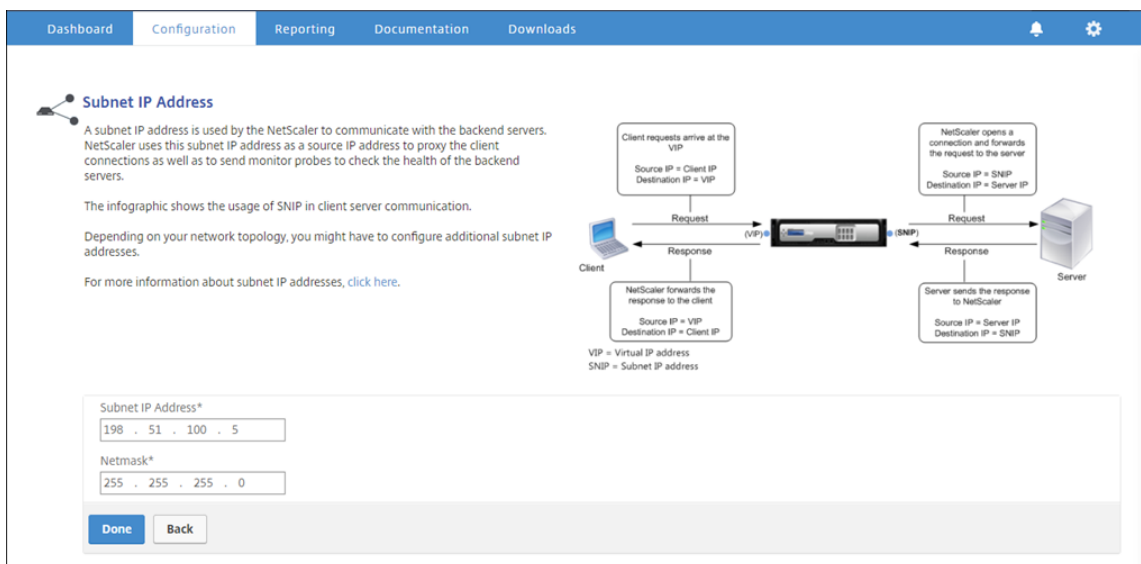
La création d'une configuration pour intercepter et examiner le trafic chiffré en plus de l'autre trafic à destination et en provenance d'un réseau nécessite la configuration des paramètres proxy, SSLi, des paramètres d'authentification utilisateur et des paramètres de filtrage d'URL. Les procédures suivantes incluent des exemples de valeurs saisies.

Configurer l'adresse SNIP et le serveur de noms DNS

1. Dans un navigateur Web, tapez l'adresse NSIP. Par exemple, <http://192.0.2.5>.
2. Dans **Nom d'utilisateur** et **Mot de passe**, tapez les informations d'identification de l'administrateur. L'écran suivant s'affiche.

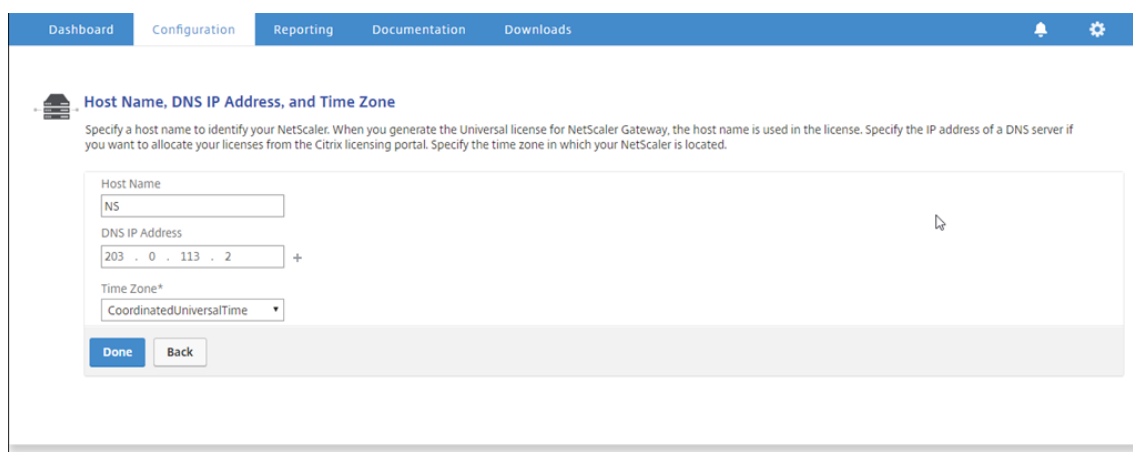


3. Cliquez dans la section **Adresse IP du sous-réseau**, puis entrez une adresse IP.



4. Cliquez sur **Terminé**.

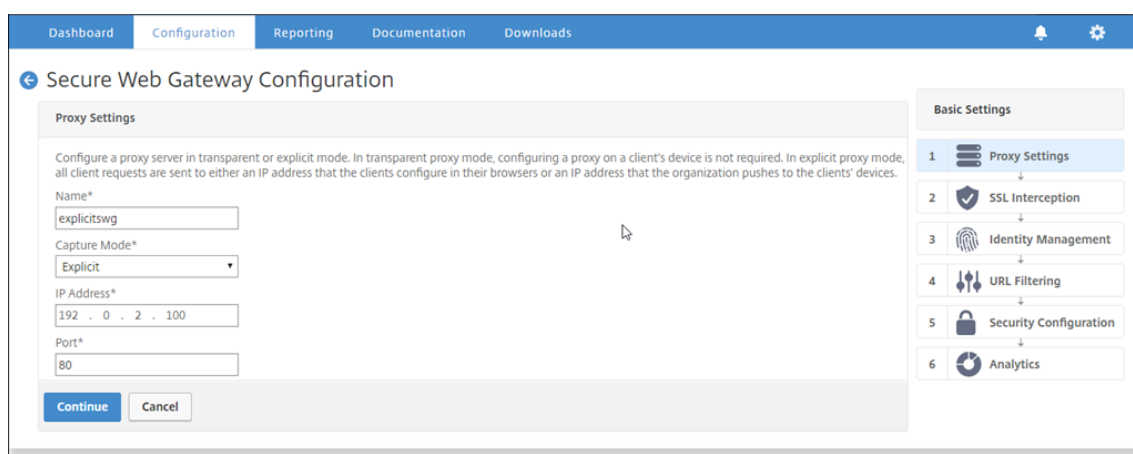
5. Cliquez dans la section **Nom d'hôte, Adresse IP DNS et Fuseau horaire**, puis entrez des valeurs pour ces champs.



6. Cliquez sur **Terminé**, puis sur **Continuer**.

Configurer les paramètres du proxy

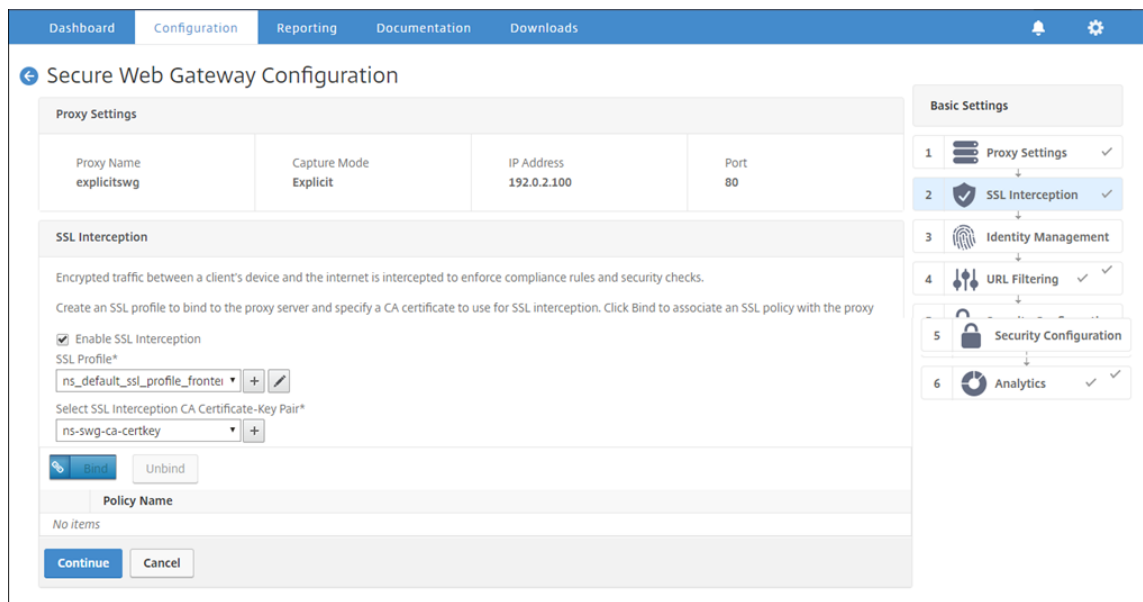
1. Accédez à **Secure Web Gateway > Assistant Passerelle Web sécurisée**.
2. Cliquez sur **Démarrer**, puis sur **Continuer**.
3. Dans la boîte de dialogue **Paramètres proxy**, entrez un nom pour le serveur proxy explicite.
4. Pour **Mode Capture**, sélectionnez **Explicite**.
5. Entrez une adresse IP et un numéro de port.



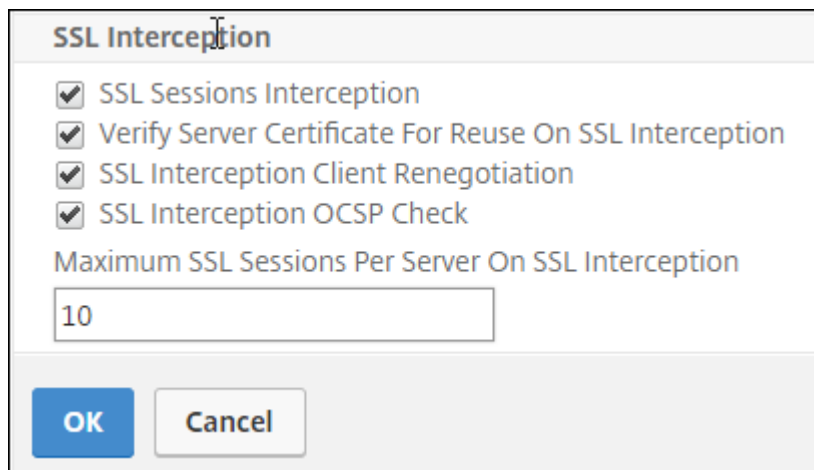
6. Cliquez sur **Continuer**.

Configurer les paramètres d'interception SSL

1. Sélectionnez **Activer l'interception SSL**.



2. Dans **Profil SSL**, cliquez sur « + » pour ajouter un nouveau profil SSL frontal et activer l'**interception des sessions SSL** dans ce profil.



3. Cliquez sur **OK**, puis sur **Terminé**.
4. Dans **Select SSL Interception CA Certificate-Key Pair**, cliquez sur « + » pour installer une paire de clés de certificat d'autorité de certification pour l'interception SSL.

Install SSL Interception CA Certificate

Certificate-Key Pair Name*

Certificate File Name*
 ?

Key File Name*
 ?

Notify When Expires

No SNMP Trap destination found. Notification will not be sent until a trap destination is configured.

Notification Period

Install **Close**

5. Cliquez sur **Installer**, puis sur **Fermer**.
6. Ajoutez une stratégie pour intercepter tout le trafic. Cliquez sur **Lier**, puis sur **Ajouter**.

SSL Interception Policies ×

Add **Edit** **Delete**

Policy Name	Pattern Set Name	Action
<i>No items</i>		

Insert **Close**

7. Entrez un nom pour la stratégie et sélectionnez **Avancé**. Dans l'éditeur d'expressions, entrez true.
8. Pour **Action**, sélectionnez **INTERCEPT**.

SSL Interception Policies / SSL Interception Policy

SSL Interception Policy

Create a policy to intercept or bypass traffic on the basis of the defined URL category, pattern set, or URL reputation score.

Name*

ssl-pol

URL Categories Create Patset Security Configuration Advanced

Expression*

Expression Editor

Operators Saved Policy Expressions Frequently Used Expressions

true

Evaluate

Action*

INTERCEPT

Create Close

9. Cliquez sur **Créer**, puis sur **Ajouter** pour ajouter une autre stratégie pour contourner les informations sensibles.
10. Entrez un nom pour la stratégie et, dans **Catégories d'URL**, cliquez sur **Ajouter**.
11. Sélectionnez les catégories **Finance** et **Email** et déplacez-les vers la liste **Configuré**.
12. Pour **Action**, sélectionnez **BYPASS**.

SSL Interception Policies / SSL Interception Policy

SSL Interception Policy

Create a policy to intercept or bypass traffic on the basis of the defined URL category, pattern set, or URL reputation score.

Name*

URL Categories
 Create Patset
 Security Configuration
 Advanced

URL Categories*

Available (17) Select All

- Illegal/Harmful
- Adult
- Malware and SPAM
- Remote Proxies
- Search
- Business and Industry
- News/Entertainment/Society
- Gambling
- Messaging/Chat/Telephony

Configured (6) Remove All

- Market Rates
- Online Trading
- Insurance
- Financial Products
- Web based Mail
- E-Mail Subscriptions

Action*

13. Cliquez sur **Créer**.

14. Sélectionnez les deux stratégies créées précédemment, puis cliquez sur **Insérer**.

SSL Interception Policies

SSL Interception Policies

<input checked="" type="checkbox"/>	Policy Name	Pattern Set Name	Action
<input checked="" type="checkbox"/>	ssli-pol_ssli		INTERCEPT
<input checked="" type="checkbox"/>	cat_pol1_ssli	cat_pol1_ssli_cat	BYPASS

15. Cliquez sur **Continuer**.

SSL Interception

Encrypted traffic between a client's device and the internet is intercepted to enforce compliance rules and security checks.

Create an SSL profile to bind to the proxy server and specify a CA certificate to use for SSL interception. Click Bind to associate an SSL policy with the proxy server.

Enable SSL Interception

SSL Profile*
 +

Select SSL Interception CA Certificate-Key Pair*
 +

<input type="checkbox"/>	Policy Name
<input type="checkbox"/>	ssli-pol_ssli
<input type="checkbox"/>	cat_pol1_ssli

Configurer les paramètres d'authentification utilisateur

1. Sélectionnez **Activer l'authentification utilisateur**. Dans le champ **Type d'authentification**, sélectionnez **LDAP**.

Dashboard Configuration Reporting Documentation Downloads

Secure Web Gateway Configuration

Proxy Settings			
Proxy Name explicitSWG	Capture Mode Explicit	IP Address 192.0.2.100	Port 80

SSL Interception	
SSL Profile ns_default_ssl_profile_frontend	SSL Intercept CA CertKey YES

Identity Management

Enable authentication to view user details in the logs and on the MAS dashboard.

Enable user authentication

Authentication Type*

LDAP Server*
 +

Basic Settings

- 1 Proxy Settings ✓
- 2 SSL Interception ✓
- 3 Identity Management
- 4 URL Filtering ✓
- 5 Security Configuration
- 6 Analytics ✓

2. Ajoutez les détails du serveur LDAP.

Create Authentication LDAP Server

Name*
explicit-auth-vs

Server Name Server IP

IP Address*
192 . 0 . 2 . 116

Security Type
PLAINTEXT

Port
389

Server Type
AD

Time-out (seconds)
3

Authentication

Connection Settings

Base DN (location of users)*
CN=Users,DC=CTXNSSFB,DC=COI

Administrator Bind DN*
CN=Administrator,CN=Users,DC=C

Administrator Password*
.....

Confirm Administrator Password*
.....

[Retrieve Attributes](#)

Test Connection

Other Settings

Server Logon Name Attribute
sAMAccountName

Search Filter

Group Attribute

Sub Attribute Name

SSO Name Attribute

Default Authentication Group

User Required
 Referrals

Maximum Referral Level
1

Referral DNS Lookup
A-REC

Validate LDAP Server Certificate

LDAP Host Name

OTP Secret

► More

Create **Close**

3. Cliquez sur **Créer**.
4. Cliquez sur **Continuer**.

Configurer les paramètres de filtrage d'URL

1. Sélectionnez **Activer la catégorisation d'URL**, puis cliquez sur **Lier**.

URL Filtering

URL Filtering restricts user access to specific websites or web pages. There are two types of filtering services - URL List and URL Categorization. Select a service to create a filter and control access to websites.

Control access to websites on the basis of the incoming URL or on the basis of metadata associated with the incoming URL.
Click Bind to associate a URL categorization policy with the proxy server.

Enable URL Categorization

Policy Name

No items

2. Cliquez sur **Ajouter**.

URL Categorization Policies ×

Policy Name	Pattern Set Name	Action
<i>No items</i>		

3. Entrez un nom pour la stratégie. Pour **Action**, sélectionnez **Refuser**. Pour **Catégories d'URL**, sélectionnez **Illegal/nuisible, Adulte, Malware et SPAM**, puis déplacez-les vers la liste **Configuré**.

URL Categorization Policies / URL Categorization Policy

URL Categorization Policy

Select Basic to choose from a predefined list of categories.
 Select Advanced to use the expression editor to create policy rules to suit your deployment.

Name*

Basic Advanced

Action*

URL Categories*

Available (16) Select All

- Remote Proxies
- Search
- Business and Industry
- News/Entertainment/Society
- Finance
- Gambling
- Messaging/Chat/Telephony
- Email
- Social Networking

Configured (29) Remove All

- Illegal Activities
- Illegal Drugs
- Medication
- Terrorism/Extremists
- Weapons
- Hate/Slander
- Violence/Suicide
- Advocacy in general
- Adult/Porn
- Nudity
- Sexual Services
- Adult Search/Links
- Dating
- Grotesque

4. Cliquez sur **Créer**.
5. Sélectionnez la stratégie, puis cliquez sur **Insérer**.

URL Categorization Policies

URL Categorization Policies

✕

Add Edit Delete

<input checked="" type="checkbox"/>	Policy Name	Pattern Set Name	Action
<input checked="" type="checkbox"/>	cat_pol2_url_cat	cat_pol2_patset	DROP

6. Cliquez sur **Continuer**.

URL Filtering

URL Filtering restricts user access to specific websites or web pages. There are two types of filtering services - URL List and URL Categorization. Select a service to create a filter and control access to websites.

Control access to websites on the basis of the incoming URL or on the basis of metadata associated with the incoming URL.
Click Bind to associate a URL categorization policy with the proxy server.

Enable URL Categorization

Enable URL List

Policy Name
cat_pol2_url_cat

Continue **Cancel**

7. Cliquez sur **Continuer**.
8. Cliquez sur **Activer Analytics**.
9. Entrez l'adresse IP de Citrix ADM et pour **Port**, spécifiez 5557.

Analytics

Enable Analytics to monitor the outbound traffic and user transactions by using NetScaler Management and Analytics System (MAS). To view the metrics, make sure that you add the NetScaler SWG appliance as an instance to NetScaler MAS.

Enable Analytics

NetScaler MAS IP Address*

192 . 0 . 2 . 41

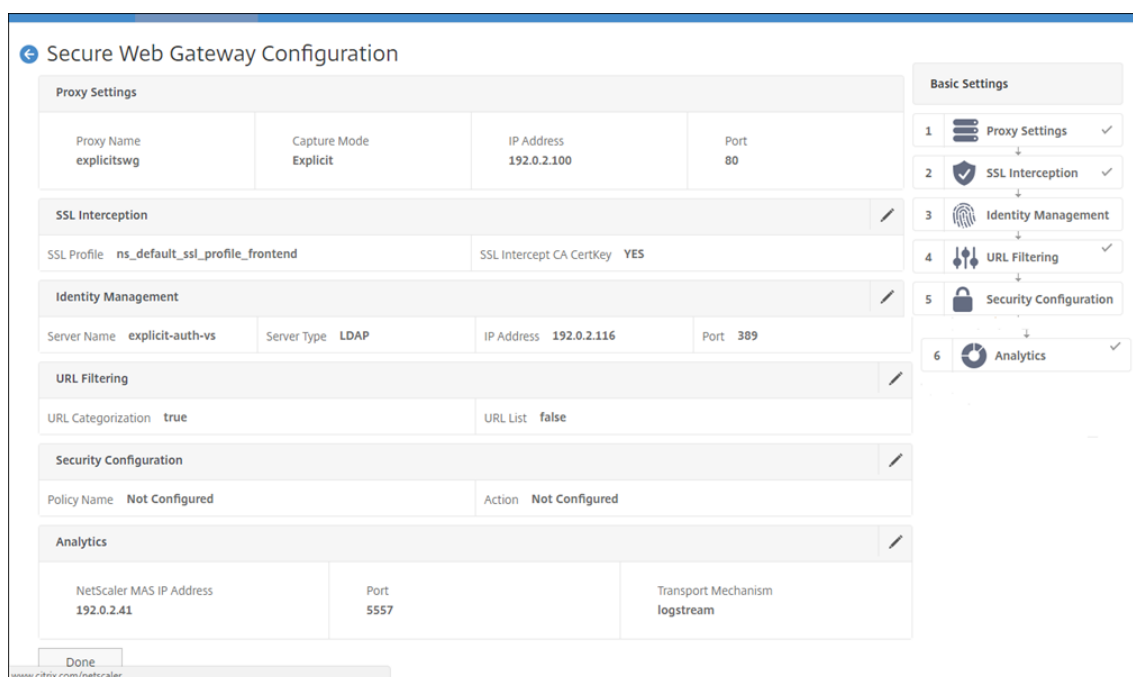
Port*

5557

Transport Mechanism: LogStream

Continue **Cancel**

10. Cliquez sur **Continuer**.
11. Cliquez sur **Terminé**.



Utilisez Citrix ADM pour afficher les mesures clés pour les utilisateurs et déterminer les éléments suivants :

- Comportement de navigation des utilisateurs de votre entreprise.
- Catégories d'URL auxquelles les utilisateurs de votre entreprise accèdent.
- Navigateurs utilisés pour accéder aux URL ou aux domaines.

Utilisez ces informations pour déterminer si le système de l'utilisateur est infecté par des logiciels malveillants ou comprendre le modèle de consommation de bande passante de l'utilisateur. Vous pouvez affiner les stratégies de votre appliance Citrix SWG pour restreindre ces utilisateurs ou bloquer d'autres sites Web. Pour plus d'informations sur l'affichage des mesures sur MAS, consultez le cas d'utilisation « Inspecter les points de terminaison » dans [Cas d'utilisation MAS](#).

Remarque

Définissez les paramètres suivants à l'aide de l'interface de ligne de commande.

```
1 set syslogparams -sslInterception ENABLED
2
3 set cacheparameter -memLimit 100
4
5 set appflow param -AAAUserName ENABLED
```

Exemple CLI

L'exemple suivant inclut toutes les commandes utilisées pour configurer l'interception et l'examen du trafic à destination et en provenance du réseau d'entreprise.

Configuration générale :

```
1 add ns ip 192.0.2.5 255.255.255.0
2
3 add ns ip 198.51.100.5 255.255.255.0 -type SNIP
4
5 add dns nameServer 203.0.113.2
6
7 add ssl certKey ns-swg-ca-certkey -cert ns_swg_ca.crt -key
  ns_swg_ca.key
8
9 set syslogparams -sslInterception ENABLED
10
11 set cacheparameter -memLimit 100
12
13 set appflow param -AAAUserName ENABLED
```

Configuration de l'authentification :

```
1 add authentication vsServer explicit-auth-vs SSL
2
3 bind ssl vsServer explicit-auth-vs -certKeyName ns-swg-ca-certkey
4
5 add authentication ldapAction swg-auth-action-explicit -serverIP
  192.0.2.116 -ldapBase "CN=Users,DC=CTXNSSFB,DC=COM" -ldapBindDn "CN=
  Administrator,CN=Users,DC=CTXNSSFB,DC=COM" -ldapBindDnPassword
  zzzzzz -ldapLoginName sAMAccountName
6
7 add authenticationpolicy swg-auth-policy -rule true -action swg-auth-
  action-explicit
8
9 bind authentication vsServer explicit-auth-vs -policy swg-auth-policy -
  priority 1
```

Configuration du serveur proxy et de l'interception SSL :

```
1 add cs vsServer explicitswg PROXY 192.0.2.100 80 - Authn401 ENABLED -
  authnVsName explicit-auth-vs
2
3 set ssl parameter -defaultProfile ENABLED
4
5 add ssl profile swg_profile -sslInterception ENABLED
6
7 bind ssl profile swg_profile -ssliCACertkey ns-swg-ca-certkey
8
9 set ssl vsServer explicitswg -sslProfile swg_profile
10
11 add ssl policy ssli-pol_ssli -rule true -action INTERCEPT
12
13 bind ssl vsServer explicitswg -policyName ssli-pol_ssli -priority 100 -
  type INTERCEPT_REQ
```

Configuration des catégories d'URL :

```
1 add ssl policy cat_pol1_ssli -rule "client.ssl.client_hello.SNI.  
    URL_CATEGORIZE(0,0).GROUP.EQ("Finance") || client.ssl.client_hello.  
    SNI.URL_CATEGORIZE(0,0).GROUP.EQ("Email")" -action BYPASS  
2  
3 bind ssl vserver explicitSWG -policyName cat_pol1_ssli -priority 10 -  
    type INTERCEPT_REQ  
4  
5 add ssl policy cat_pol2_ssli -rule "client.ssl.client_hello.sni.  
    url_categorize(0,0).GROUP.EQ("Adult") || client.ssl.client_hello.sni.  
    url_categorize(0,0).GROUP.EQ("Malware and SPAM") || client.ssl.  
    client_hello.SNI.URL_CATEGORIZE(0,0).GROUP.EQ("Illegal/Harmful")" -  
    action RESET  
6  
7 bind ssl vserver explicitSWG -policyName cat_pol2_ssli -priority 20 -  
    type INTERCEPT_REQ
```

Configuration AppFlow pour extraire des données dans Citrix ADM :

```
1 add appflow collector _swg_testSWG_apfw_cl -IPAddress 192.0.2.41 -port  
    5557 -Transport logstream  
2  
3 set appflow param -templateRefresh 60 -httpUrl ENABLED -AAAUserName  
    ENABLED -httpCookie ENABLED -httpReferer ENABLED -httpMethod ENABLED  
    -httpHost ENABLED -httpUserAgent ENABLED -httpContentType ENABLED -  
    httpVia ENABLED -httpLocation ENABLED -httpDomain ENABLED -  
    cacheInsight ENABLED -urlCategory ENABLED  
4  
5 add appflow action _swg_testSWG_apfw_act -collectors  
    _swg_testSWG_apfw_cl -distributionAlgorithm ENABLED  
6  
7 add appflow policy _swg_testSWG_apfw_pol true _swg_testSWG_apfw_act  
8  
9 bind cs vserver explicitSWG -policyName _swg_testSWG_apfw_pol -priority  
    1
```

Cas d'utilisation : sécuriser le réseau d'entreprise à l'aide d'ICAP pour l'inspection à distance des logiciels malveillants

April 27, 2021

L'apppliance Citrix Secure Web Gateway (SWG) agit comme un proxy et intercepte tout le trafic client. L'apppliance utilise des stratégies pour évaluer le trafic et transmet les demandes client au serveur d'origine sur lequel réside la ressource. L'apppliance décrypte la réponse du serveur d'origine et transmet le contenu en texte brut au serveur ICAP pour une vérification anti-programme malveillant. Le serveur ICAP répond par un message indiquant « Aucune adaptation requise », une erreur ou une demande modifiée. En fonction de la réponse du serveur ICAP, le contenu demandé est soit transféré

au client, soit un message approprié est envoyé.

Pour ce cas d'utilisation, vous devez effectuer une configuration générale, une configuration liée à l'interception par proxy et SSL et une configuration ICAP sur l'appliance Citrix SWG.

Configuration générale

Configurez les entités suivantes :

- Adresse du NSIP
- Adresse IP du sous-réseau (SNIP)
- Serveur de noms DNS
- Paire de clé de certificat CA pour signer le certificat du serveur pour l'interception SSL

Configuration du serveur proxy et de l'interception SSL

Configurez les entités suivantes :

- Serveur proxy en mode explicite pour intercepter tout le trafic HTTP et HTTPS sortant.
- Profil SSL pour définir les paramètres SSL, tels que les chiffrements et les paramètres, pour les connexions.
- Stratégie SSL pour définir des règles d'interception du trafic. Définissez sur true pour intercepter toutes les demandes client.

Pour plus de détails, consultez les rubriques suivantes :

- [Modes proxy](#)
- [Interception SSL](#)

Dans l'exemple de configuration suivant, le service de détection de logiciels malveillants réside à www.example.com.

Exemple de configuration générale :

```
1 add ns ip 192.0.2.5 255.255.255.0
2
3 add ns ip 198.51.100.5 255.255.255.0 -type SNIP
4
5 add dns nameServer 203.0.113.2
6
7 add ssl certKey ns-swg-ca-certkey -cert ns_swg_ca.crt -key ns_swg_ca.
   key
```

Exemple de configuration de serveur proxy et d'interception SSL :

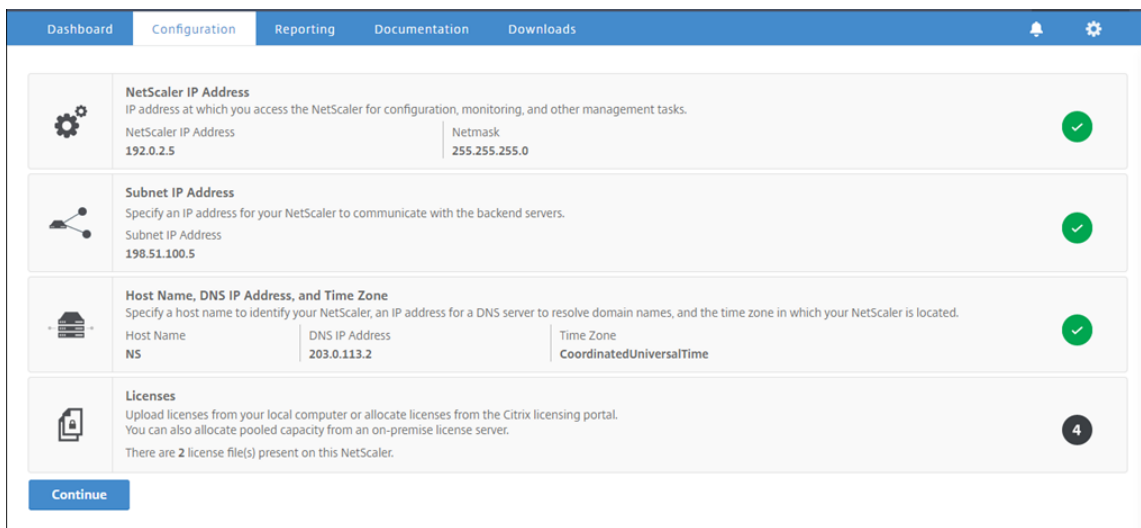
```
1 add cs vserver explicitSWG PROXY 192.0.2.100 80 - Authn401 ENABLED -  
  authnVsName explicit-auth-vs  
2  
3 set ssl parameter -defaultProfile ENABLED  
4  
5 add ssl profile swg_profile -sslInterception ENABLED  
6  
7 bind ssl profile swg_profile -ssliCACertkey ns-swg-ca-certkey  
8  
9 set ssl vserver explicitSWG -sslProfile swg_profile  
10  
11 add ssl policy ssli-pol_ssli -rule true -action INTERCEPT  
12  
13 bind ssl vserver explicitSWG -policyName ssli-pol_ssli -priority 100 -  
  type INTERCEPT_REQ
```

Exemple de configuration ICAP :

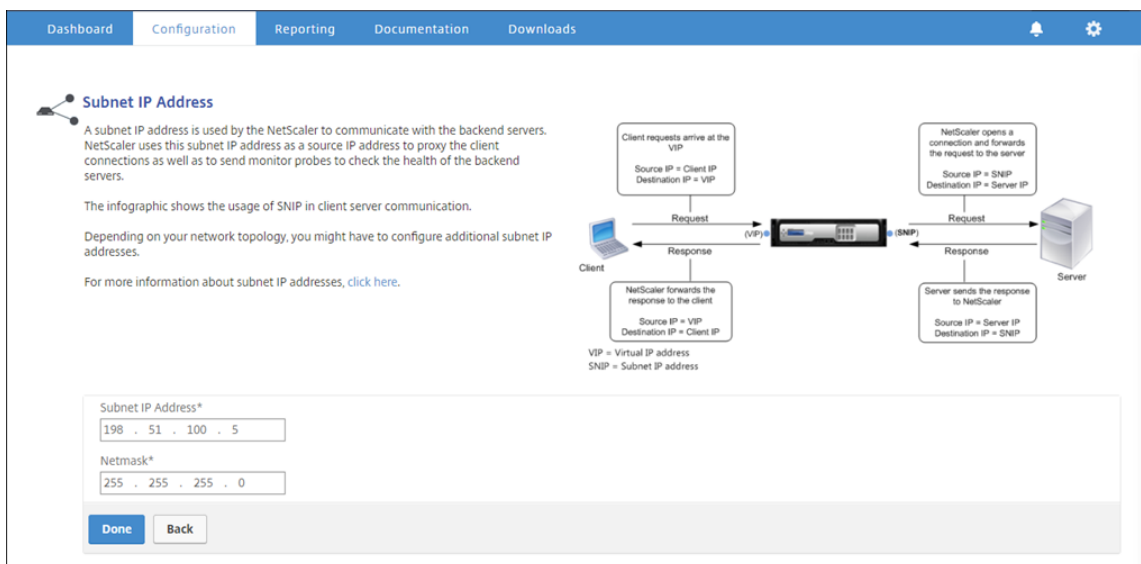
```
1 add service icap_svc 203.0.113.225 TCP 1344  
2  
3 enable ns feature contentinspection  
4  
5 add icaprofile icaprofile1 -uri /example.com -Mode RESMOD  
6  
7 add contentInspection action CiRemoteAction -type ICAP -serverName  
  icap_svc -icapProfileName icaprofile1  
8  
9 add contentInspection policy CiPolicy -rule "HTTP.REQ.METHOD.NE(""  
  CONNECT")" -action CiRemoteAction  
10  
11 bind cs vserver explicitSWG -policyName CiPolicy -priority 200 -type  
  response
```

Configurer l'adresse SNIP et le serveur de noms DNS

1. Dans un navigateur Web, tapez l'adresse NSIP. Par exemple, <http://192.0.2.5>.
2. Dans **Nom d'utilisateur** et **Mot de passe**, tapez les informations d'identification de l'administrateur. L'écran suivant s'affiche. Si l'écran suivant n'apparaît pas, passez à la section Paramètres du proxy.



3. Cliquez dans la section **Adresse IP du sous-réseau**, puis entrez une adresse IP.



4. Cliquez sur **Terminé**.

5. Cliquez dans la section **Nom d'hôte, Adresse IP DNS et Fuseau horaire**, puis entrez des valeurs pour ces champs.

The screenshot shows the 'Host Name, DNS IP Address, and Time Zone' configuration page. The page has a blue header with navigation tabs: Dashboard, Configuration, Reporting, Documentation, and Downloads. Below the header, there is a title 'Host Name, DNS IP Address, and Time Zone' and a brief instruction: 'Specify a host name to identify your NetScaler. When you generate the Universal license for NetScaler Gateway, the host name is used in the license. Specify the IP address of a DNS server if you want to allocate your licenses from the Citrix licensing portal. Specify the time zone in which your NetScaler is located.' The form contains three input fields: 'Host Name' with the value 'NS', 'DNS IP Address' with the value '203 . 0 . 113 . 2', and 'Time Zone*' with a dropdown menu set to 'CoordinatedUniversalTime'. At the bottom of the form are two buttons: 'Done' and 'Back'.

6. Cliquez sur **Terminé**, puis sur **Continuer**.

Configurer les paramètres du proxy

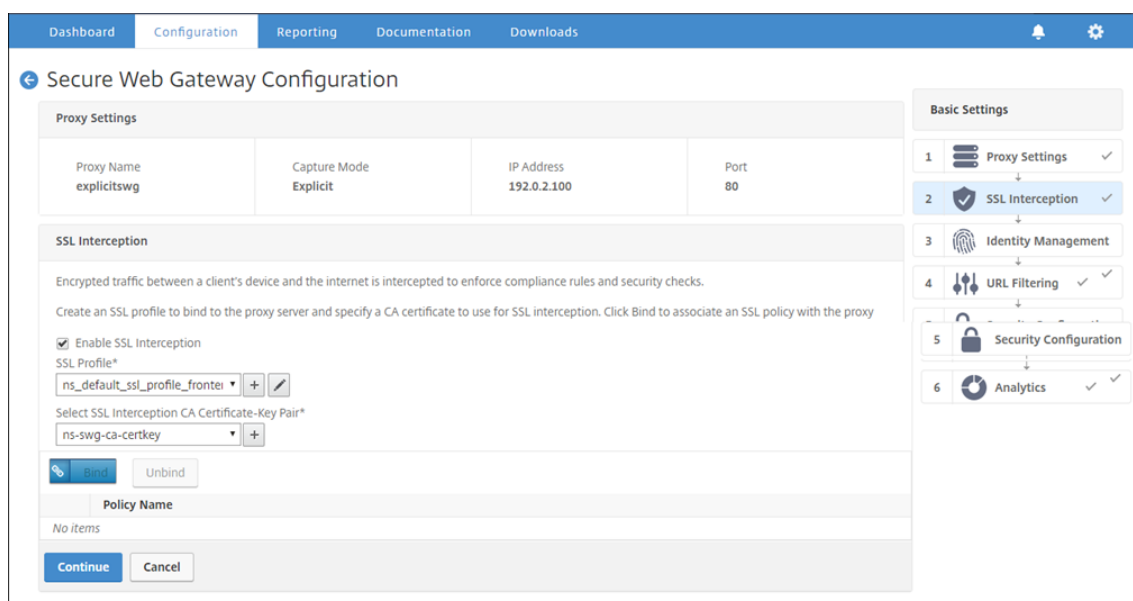
1. Accédez à **Secure Web Gateway > Assistant Passerelle Web sécurisée**.
2. Cliquez sur **Démarrer**, puis sur **Continuer**.
3. Dans la boîte de dialogue **Paramètres proxy**, entrez un nom pour le serveur proxy explicite.
4. Pour **Mode Capture**, sélectionnez **Explicite**.
5. Entrez une adresse IP et un numéro de port.

The screenshot shows the 'Secure Web Gateway Configuration' page. The page has a blue header with navigation tabs: Dashboard, Configuration, Reporting, Documentation, and Downloads. Below the header, there is a title 'Secure Web Gateway Configuration' and a sub-section 'Proxy Settings'. The 'Proxy Settings' section contains a brief instruction: 'Configure a proxy server in transparent or explicit mode. In transparent proxy mode, configuring a proxy on a client's device is not required. In explicit proxy mode, all client requests are sent to either an IP address that the clients configure in their browsers or an IP address that the organization pushes to the clients' devices.' The form contains four input fields: 'Name*' with the value 'explicitSWG', 'Capture Mode*' with a dropdown menu set to 'Explicit', 'IP Address*' with the value '192 . 0 . 2 . 100', and 'Port*' with the value '80'. At the bottom of the form are two buttons: 'Continue' and 'Cancel'. On the right side of the page, there is a 'Basic Settings' sidebar with a list of settings: 1 Proxy Settings, 2 SSL Interception, 3 Identity Management, 4 URL Filtering, 5 Security Configuration, and 6 Analytics.

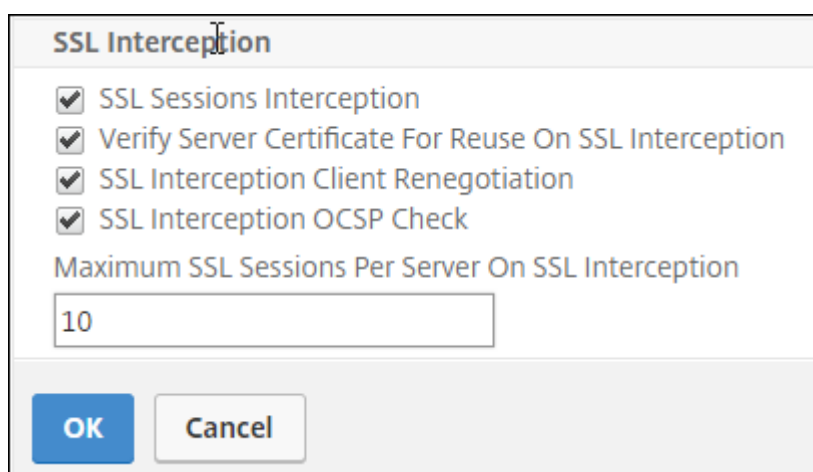
6. Cliquez sur **Continuer**.

Configurer les paramètres d'interception SSL

1. Sélectionnez **Activer l'interception SSL**.



2. Dans **Profil SSL**, sélectionnez un profil existant ou cliquez sur « + » pour ajouter un nouveau profil SSL frontal. Activez l'**interception de sessions SSL** dans ce profil. Si vous sélectionnez un profil existant, ignorez l'étape suivante.

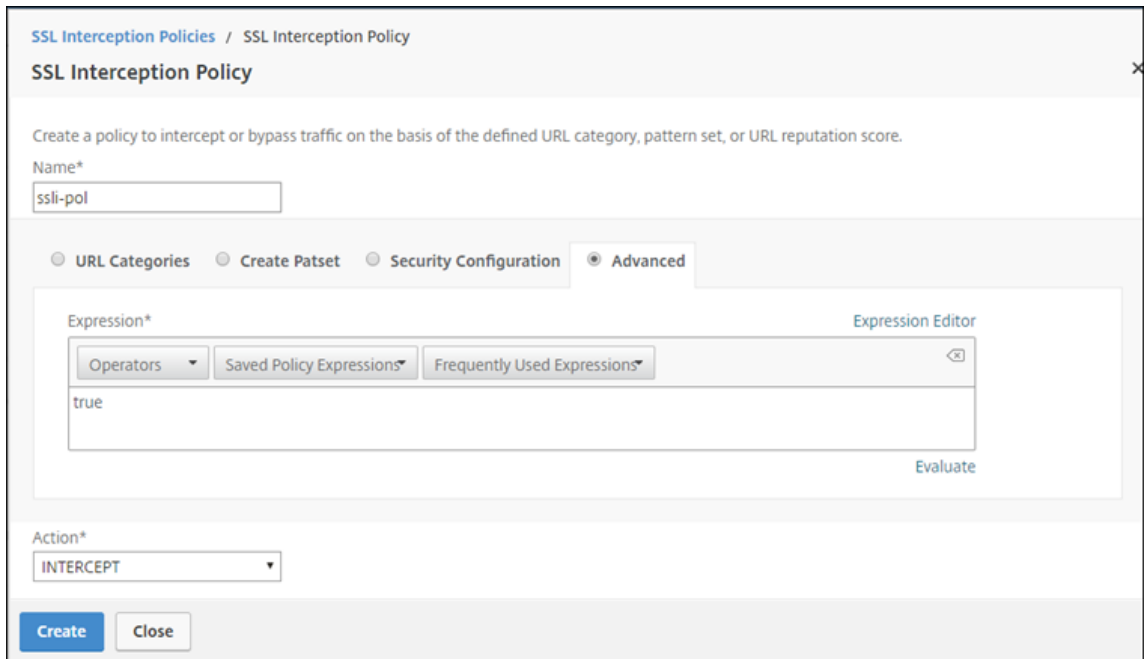


3. Cliquez sur **OK**, puis sur **Terminé**.
4. Dans **Sélectionner une paire de clés de certificat d'autorité de certification d'interception SSL**, sélectionnez un certificat existant ou cliquez sur « + » pour installer une paire de clés de certificat d'autorité de certification pour l'interception SSL. Si vous sélectionnez un certificat existant, ignorez l'étape suivante.

5. Cliquez sur **Installer**, puis sur **Fermer**.
6. Ajoutez une stratégie pour intercepter tout le trafic. Cliquez sur **Bind**. Cliquez sur **Ajouter** pour ajouter une nouvelle stratégie ou sélectionnez une stratégie existante. Si vous sélectionnez une stratégie existante, cliquez sur **Insérer**, puis ignorez les trois étapes suivantes.

Policy Name	Pattern Set Name	Action
No items		

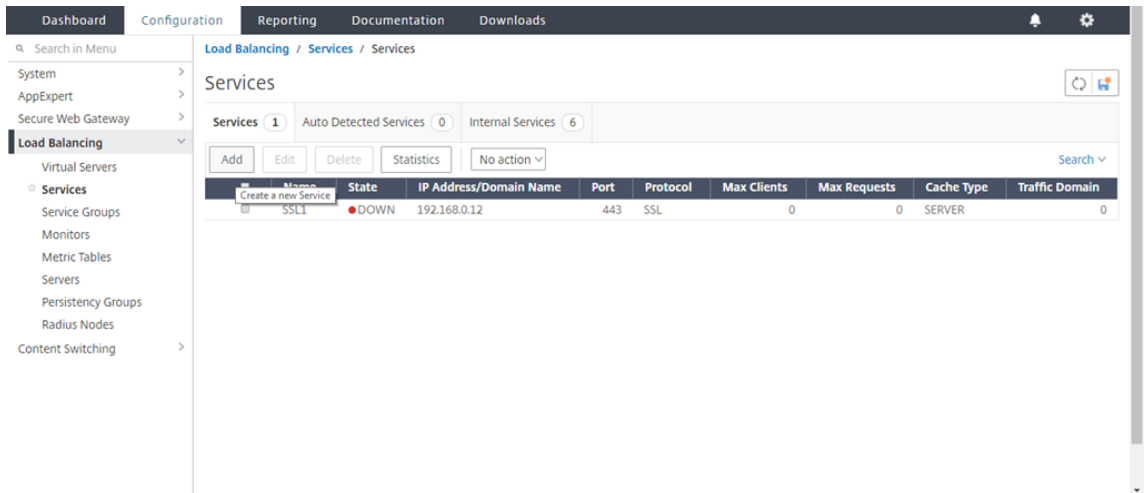
7. Entrez un nom pour la stratégie et sélectionnez **Avancé**. Dans l'éditeur d'expressions, entrez true.
8. Pour **Action**, sélectionnez **INTERCEPT**.



9. Cliquez sur **Créer**.
10. Cliquez sur **Continuer** quatre fois, puis cliquez sur **Terminé**.

Configurer les paramètres ICAP

1. Accédez à **Équilibrage de charge > Services**, puis cliquez sur **Ajouter**.



2. Tapez un nom et une adresse IP. Dans **Protocole**, sélectionnez **TCP**. Dans **Port**, tapez **1344**. Cliquez sur **OK**.

Dashboard Configuration Reporting Documentation Downloads

Load Balancing Service

Basic Settings Help >

Service Name*
icap_svc

New Server Existing Server

IP Address*
203 . 0 . 113 . 100

Protocol*
TCP

Port*
1344

More

OK Cancel

3. Accédez à **Secure Web Gateway > Serveurs virtuels proxy**. Ajoutez un serveur virtuel proxy ou sélectionnez un serveur virtuel et cliquez sur **Modifier**. Après avoir entré les détails, cliquez sur **OK**.

Dashboard Configuration Reporting Documentation Downloads

Proxy Virtual Server

Basic Settings Help >

Name*
explicitswg

IP Address Type*
IP Address

IP Address*
192 . 0 . 2 . 100

Port*
80

More

OK Cancel

Cliquez à nouveau sur **OK**.

Dashboard Configuration Reporting Documentation Downloads

Proxy Virtual Server

Basic Settings Help >

Name	explicitswg	Listen Priority	-
Target Type	NONE	Listen Policy Expression	NONE
State	UP	Range	1
IP Address	192.0.2.100	Traffic Domain	0
Port	80	RHI State	PASSIVE
		AppFlow Logging	ENABLED
		Comments	-

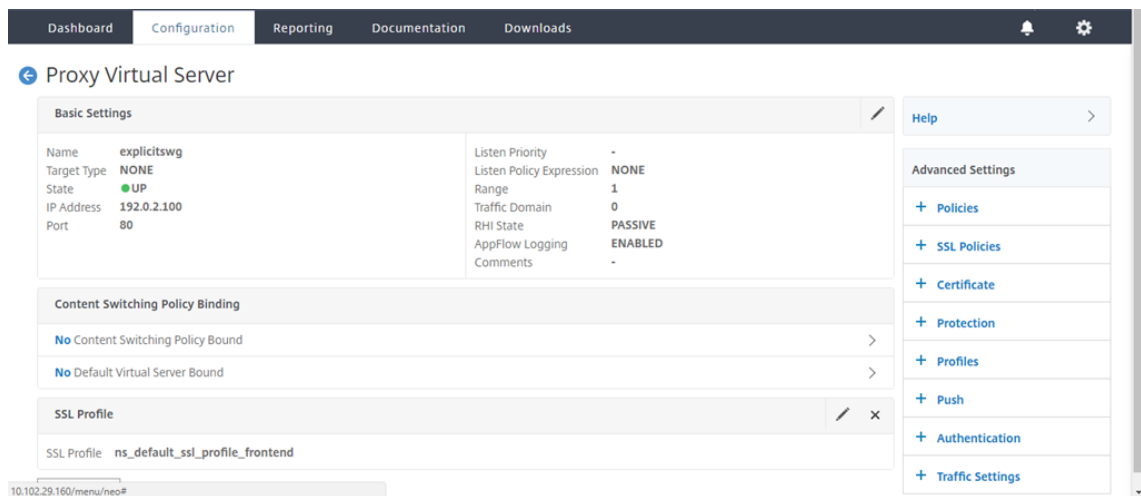
Content Switching Policy Binding

No Content Switching Policy Bound >

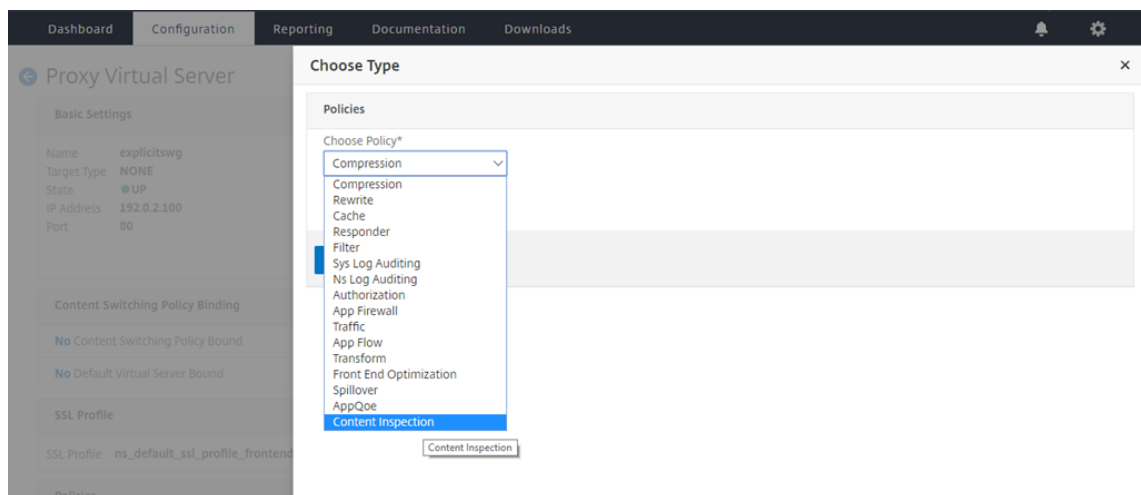
No Default Virtual Server Bound >

OK

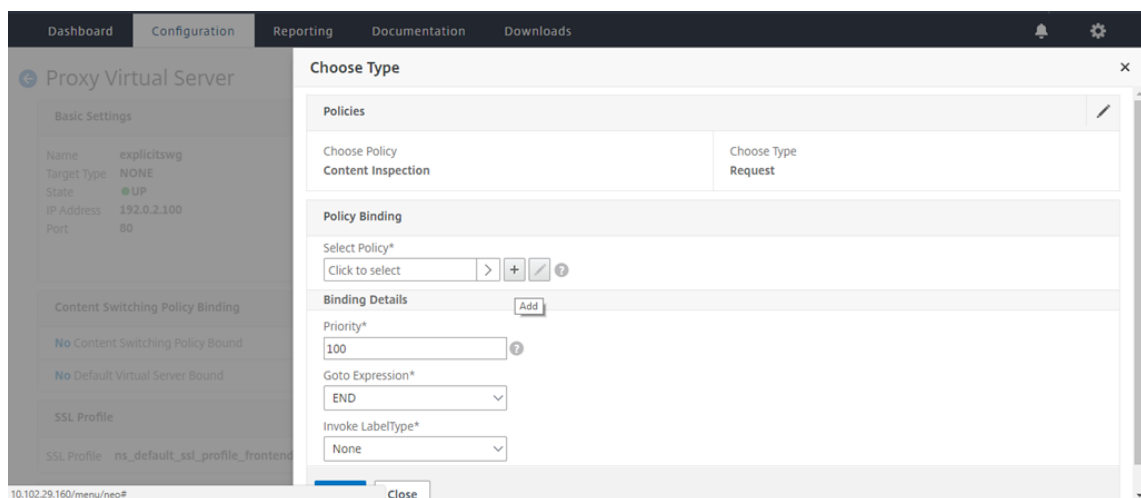
4. Dans **Paramètres avancés**, cliquez sur **Stratégies**.



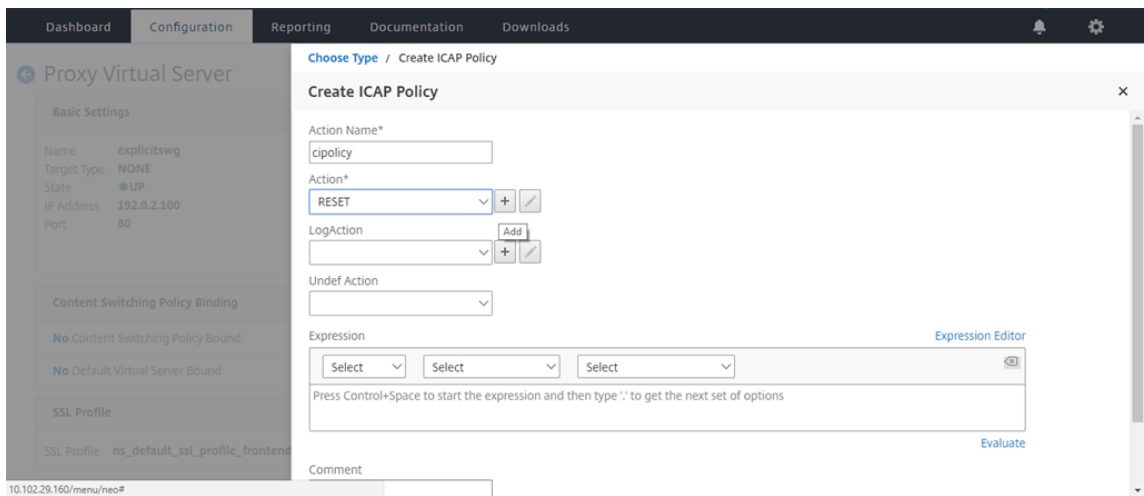
5. Dans **Choisir une stratégie**, sélectionnez **Contrôle du contenu**. Cliquez sur **Continuer**.



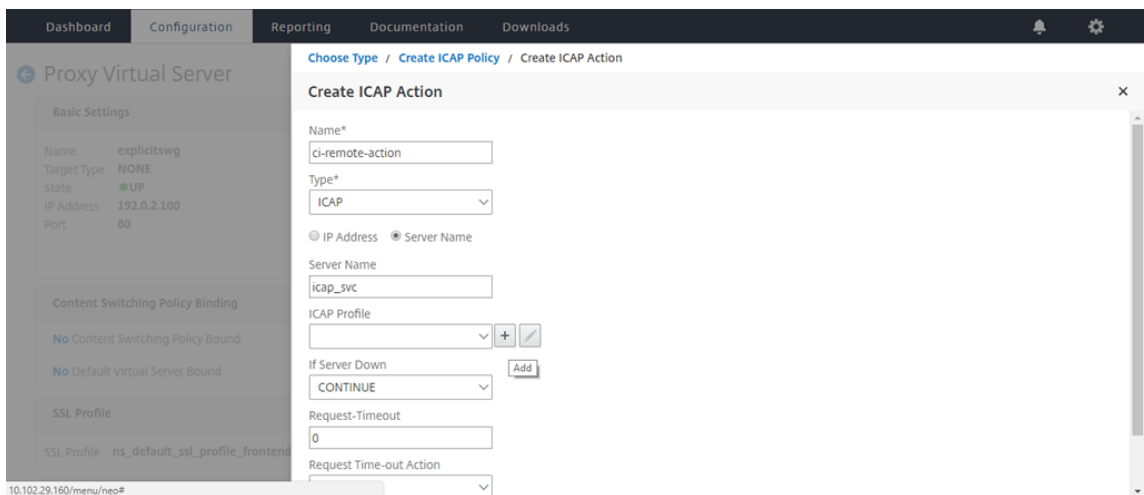
6. Dans **Sélectionner une stratégie**, cliquez sur le signe « + » pour ajouter une stratégie.



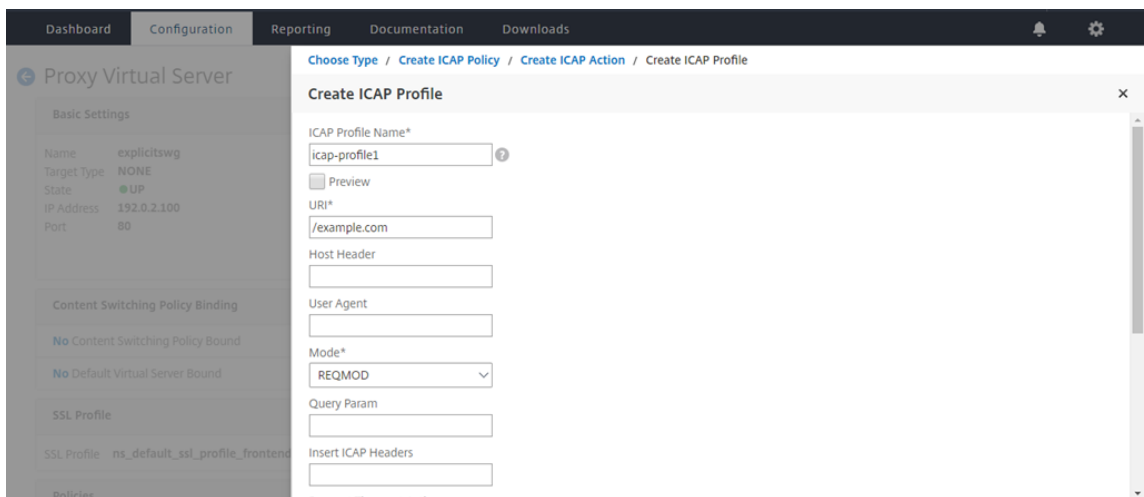
- Entrez un nom pour la stratégie. Dans **Action**, cliquez sur le signe « + » pour ajouter une action.



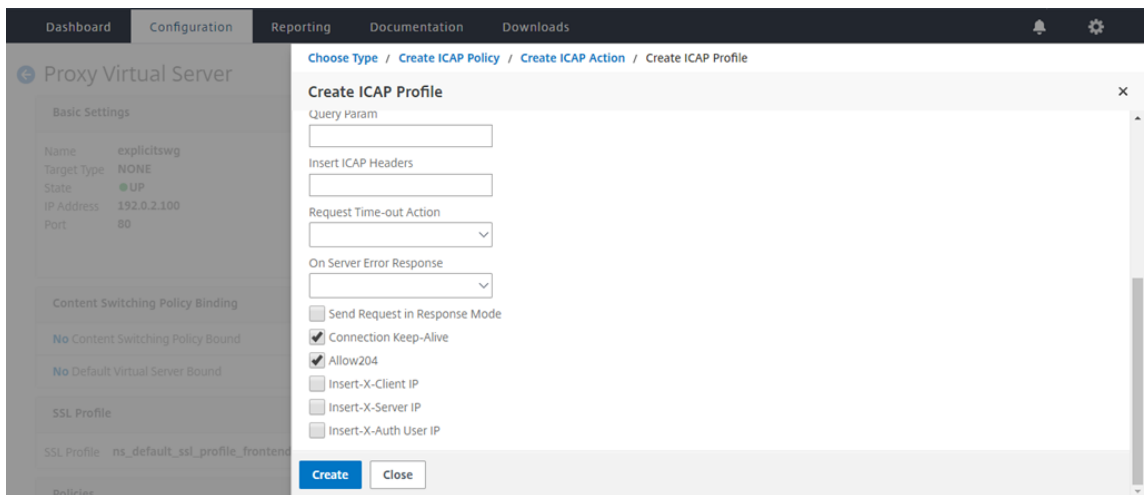
- Tapez un nom pour l'action. Dans **Nom du serveur**, tapez le nom du service TCP créé précédemment. Dans **Profil ICAP**, cliquez sur le signe « + » pour ajouter un profil ICAP.



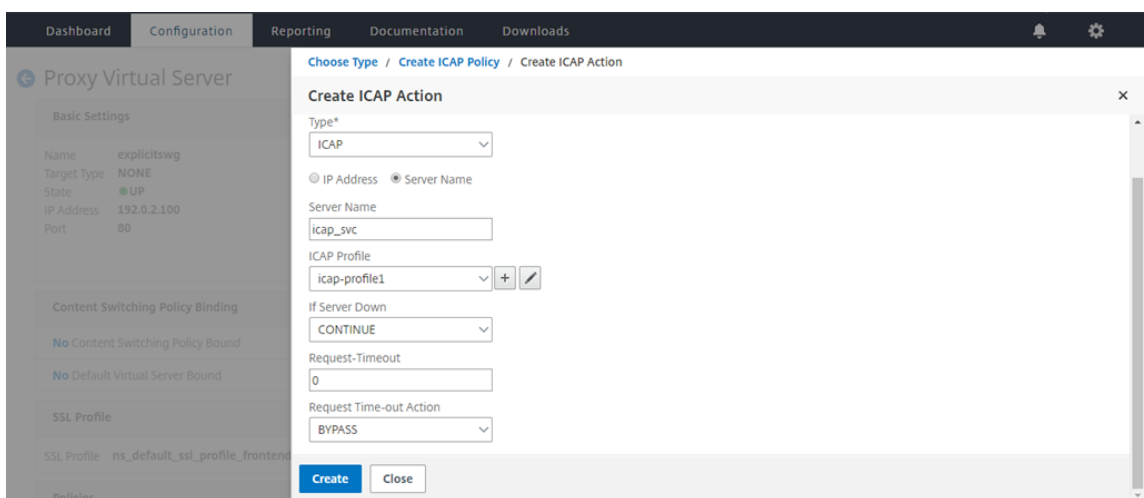
- Tapez un nom de profil, URI. Dans **Mode**, sélectionnez **REQMOD**.



10. Cliquez sur **Créer**.

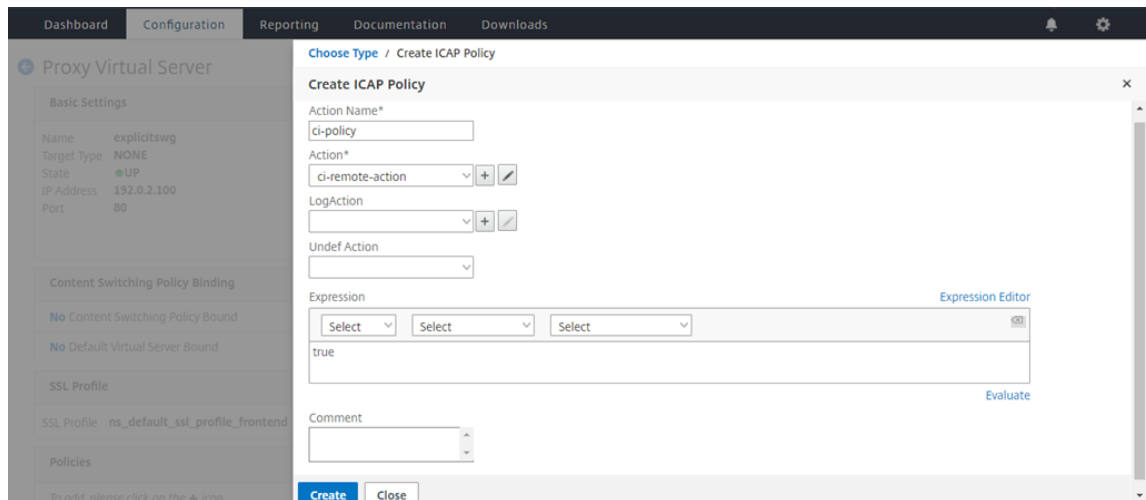


11. Dans la page **Créer une action ICAP**, cliquez sur **Créer**.

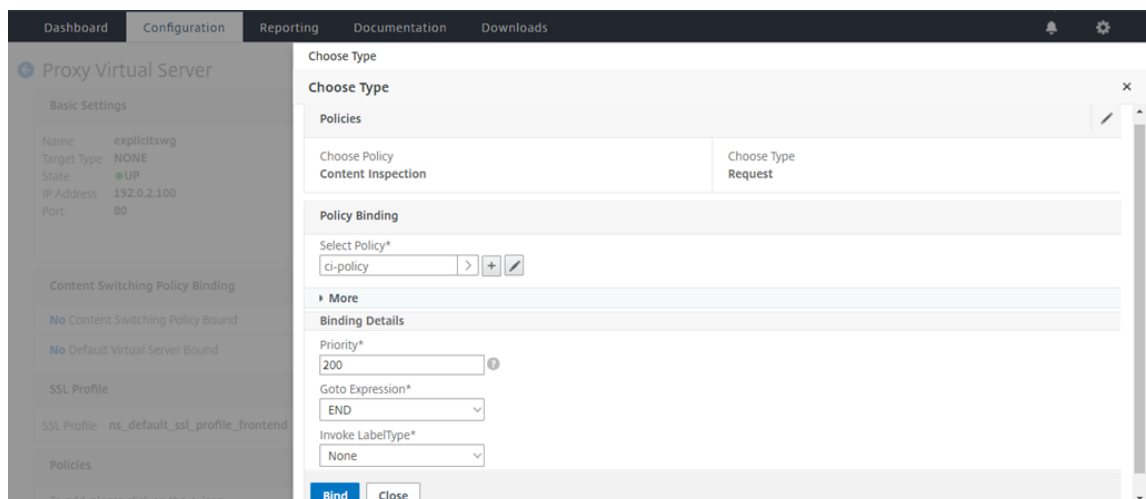


12. Dans la page **Créer une stratégie ICAP**, entrez true dans l'**éditeur d'expressions**. Cliquez en-

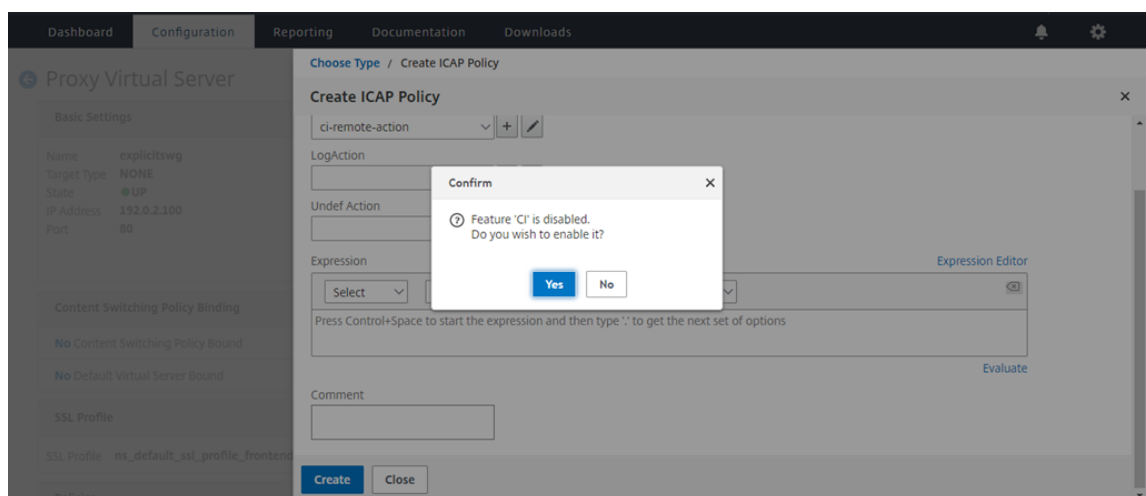
suite sur **Créer**.



13. Cliquez sur **Bind**.



14. Si vous êtes invité à activer la fonction d'inspection du contenu, sélectionnez **Oui**.



15. Cliquez sur **Terminé**.

Proxy Virtual Server

Basic Settings			
Name	explicitSWG	Listen Priority	-
Target Type	NONE	Listen Policy Expression	NONE
State	UP	Range	1
IP Address	192.0.2.100	Traffic Domain	0
Port	80	RHI State	PASSIVE
		AppFlow Logging	ENABLED
		Comments	-

Content Switching Policy Binding

- No Content Switching Policy Bound
- No Default Virtual Server Bound

SSL Profile

SSL Profile ns_default_ssl_profile_frontend

Policies

Request Policies

- 1 Content Switching Virtual Server to Content Inspection Policy Binding

Done

Help

Advanced Settings

- + SSL Policies
- + Certificate
- + Protection
- + Profiles
- + Push
- + Authentication
- + Traffic Settings

Exemples de transactions ICAP entre l'appareil Citrix SWG et le serveur ICAP dans RESPMOD

Demande de l'appareil Citrix SWG vers le serveur ICAP :

```

1  RESPMOD icap://10.106.137.15:1344/resp ICAP/1.0
2
3  Host: 10.106.137.15
4
5  Connection: Keep-Alive
6
7  Encapsulated: res-hdr=0, res-body=282
8
9  HTTP/1.1 200 OK
10
11 Date: Fri, 01 Dec 2017 11:55:18 GMT
12
13 Server: Apache/2.2.21 (Fedora)
14
15 Last-Modified: Fri, 01 Dec 2017 11:16:16 GMT
16
17 ETag: "20169-45-55f457f42aee4"
18
19 Accept-Ranges: bytes
20
21 Content-Length: 69
22
23 Keep-Alive: timeout=15, max=100
24
25 Content-Type: text/plain; charset=UTF-8
26
27 X50!P%@AP[4\PZX54(P^)7CC)7 }
```

```
28 $EICAR-STANDARD-ANTIVIRUS-TEST-FILE!$H+H*
```

Réponse du serveur ICAP à l'apppliance Citrix SWG :

```
1 ICAP/1.0 200 OK
2
3 Connection: keep-alive
4
5 Date: Fri, 01 Dec, 2017 11:40:42 GMT
6
7 Encapsulated: res-hdr=0, res-body=224
8
9 Server: IWSVA 6.5-SP1_Build_Linux_1080 $Date: 04/09/2015 01:19:26 AM$
10
11 IStag: "9.8-13.815.00-3.100.1027-1.0"
12
13 X-Virus-ID: Eicar_test_file
14
15 X-Infection-Found: Type=0; Resolution=2; Threat=Eicar_test_file;
16
17 HTTP/1.1 403 Forbidden
18
19 Date: Fri, 01 Dec, 2017 11:40:42 GMT
20
21 Cache-Control: no-cache
22
23 Content-Type: text/html; charset=UTF-8
24
25 Server: IWSVA 6.5-SP1_Build_Linux_1080 $Date: 04/09/2015 01:19:26 AM$
26
27 Content-Length: 5688
28
29 <html><head><META HTTP-EQUIV="Content-Type" CONTENT="text/html; charset
    =UTF-8"/>
30
31 ...
32
33 ...
34
35 </body></html>
```

Articles pratiques

April 27, 2021

Voici quelques instructions de configuration ou des cas d'utilisation fonctionnels disponibles sous forme d'articles « How to » pour vous aider à gérer votre déploiement SWG.

Filtrage d'URL

[Comment créer une stratégie de catégorisation d'URL](#)

[Comment créer une stratégie de liste d'URL](#)

[Comment placer sur liste verte une URL d'exception](#)

[Comment bloquer les sites Web de catégorie adultes](#)

Comment créer une stratégie de catégorisation d'URL

April 27, 2021

En tant qu'administrateur réseau, vous pouvez bloquer des catégories spécifiques de sites Web pour l'accès des utilisateurs. Pour ce faire, vous pouvez créer une stratégie de catégorisation d'URL et la lier à une liste prédéfinie de catégories que vous souhaitez restreindre l'accès.

Par exemple, vous pouvez restreindre l'accès à tous les sites Web de réseaux sociaux conformément aux stratégies d'organisation. Dans un tel scénario, vous devez créer une stratégie de catégorisation et la lier à la liste prédéfinie des sites Web de catégorie de réseaux sociaux.

Pour créer une stratégie de catégorisation d'URL à l'aide de la méthode de base :

1. Connectez-vous à l'appliance **Citrix SWG** et accédez à **Secured Web Gateway > Filtrage des URL > Catégorisation des URL**.
2. Dans le volet d'informations, cliquez sur **Ajouter** pour accéder à la page **Stratégie de catégorisation d'URL** et spécifiez les paramètres suivants.
 - a) **Stratégie de catégorisation d'URL**. Nom de la stratégie de répondeur.
 - b) **Basique**. Sélectionnez Configurer à l'aide d'une liste prédéfinie de catégories.
 - c) **Action**. Une action pour contrôler l'accès à l'URL.
 - d) **Catégories d'URL**. Liste prédéfinie de catégories à sélectionner et à ajouter à une liste configurée.
3. Cliquez sur **Créer** et **Fermer**.

URL Categorization Policies / URL Categorization Policy

URL Categorization Policy

Select Basic to choose from a predefined list of categories.
Select Advanced to use the expression editor to create policy rules to suit your deployment.

Name*

Basic Advanced

Action*

URL Categories*

Available (16) Select All

Search Categories

- + Remote Proxies
- + Search
- + Business and Industry
- + News/Entertainment/Society
- + Finance
- + Gambling
- + Messaging/Chat/Telephony
- + Email
- + Social Networking

Configured (29) Remove All

- Illegal Activities
- Illegal Drugs
- Medication
- Terrorism/Extremists
- Weapons
- Hate/Slander
- Violence/Suicide
- Advocacy in general
- Adult/Porn
- Nudity
- Sexual Services
- Adult Search/Links
- Dating
- Grotesque

Pour créer une stratégie de catégorisation d'URL à l'aide de la méthode avancée :

1. Pour configurer une nouvelle stratégie de catégorisation d'URL à l'aide de la catégorisation avancée.
2. Cliquez sur **Ajouter**.
3. Dans la page **Stratégie de catégorisation d'URL**, spécifiez les paramètres suivants.
 - a) **Stratégie de catégorisation d'URL**. Nom de la stratégie de répondeur.
 - b) **Avancé**. Configurez la stratégie à l'aide d'expressions personnalisées.
4. Cliquez sur **Créer** et **Fermer**.

← URL Categorization Policy

Select Basic to choose from a predefined list of categories.
Select Advanced to use the expression editor to create policy rules to suit your deployment.

Name*

Basic Advanced

Expression*

Operators Saved Policy Expressions Frequently Used Expressions

HTTPREQ.URL.SUFFIX.EQ("")HTTPREQ.HEADER("").CONTAINS("")

Comment créer une stratégie de liste d'URL

April 27, 2021

En tant qu'administrateur réseau, vous pouvez bloquer des catégories spécifiques de sites Web pour l'accès des utilisateurs. Pour ce faire, vous pouvez créer une stratégie de liste d'URL et la lier à un jeu d'URL importé dans l'appliance en tant que fichier texte. L'ensemble d'URL est une collection de sites Web que vous préférez filtrer.

Par exemple, vous pouvez restreindre l'accès à tous les sites Web malveillants conformément aux stratégies d'organisation. Dans un tel scénario, vous devez créer une stratégie de liste d'URL et la lier à un jeu d'URL importé dans l'appliance.

Pour configurer une stratégie de liste d'URL :

1. Connectez-vous à l'appliance **Citrix SWG** et accédez à **Secured Web Gateway > Filtrage des URL > Listes d'URL**.
2. Dans le volet d'informations, cliquez sur **Ajouter**.
3. Dans la page **Stratégie de liste d'URL**, spécifiez le nom de la stratégie.
4. Sélectionnez une option pour importer un jeu d'URL ou créer un jeu de motifs, puis effectuez l'une des procédures qui suivent la dernière étape de cette procédure.
5. Sélectionnez une action du répondeur dans la liste déroulante.
6. Cliquez sur **Créer** et **Fermer**.

Pour importer un jeu d'URL personnalisé ou un jeu d'URL tiers :

1. Dans la page de l'onglet **Stratégie de liste d'URL**, activez la case à cocher **Importer le jeu d'URL** et spécifiez les paramètres de jeu d'URL suivants.
 - a) **Nom du jeu d'URL** : nom du jeu d'URL.
 - b) **URL**—Adresse Web de l'emplacement où accéder à l'ensemble d'URL.
 - c) **Remplacer**—Remplace le jeu d'URL précédemment importé.
 - d) **Delimitier**—Séquence de caractères qui délimite un enregistrement de fichier CSV.
 - e) **Séparateur de lignes** —Séparateur de lignes utilisé dans le fichier CSV.
 - f) **Intervalle**—Intervalle en secondes, arrondi à 15 minutes près, au cours duquel le jeu d'URL est mis à jour.
 - g) **Private Set**—Option pour empêcher l'exportation du jeu d'URL.
 - h) **URL Canary** —URL interne permettant de tester si le contenu de l'ensemble d'URL doit rester confidentiel. La longueur maximale de l'URL est de 2047 caractères. Pour plus d'informations sur l'URL Canary, consultez la section Configuration d'un jeu d'URL privé.

← URL List Policy

Configure a URL List policy to filter or blacklist URLs by importing a URL set or by creating a pattern set.

Name*

Import URL Set Create Patset

URL Set Name*

URL*

Overwrite

Delimiter

Row Separator

Interval

Private Set

Canary URL

Action*

Responder Action*
 + ?

Pour créer un jeu de motifs :

1. Dans l'onglet **Créer un motif**, entrez un nom pour le jeu de motifs.
2. Cliquez sur **Insérer** pour créer un motif.
3. Sur la page **Configurer le jeu de patches de stratégie en liaison de répétition**, définissez les paramètres suivants.
 - a) **Pattern**—Chaîne de caractères constituant un motif
 - b) **Charset**—Type de jeu de caractères : format ASCII ou UTF_8
 - c) **Index** : valeur d'index attribuée par l'utilisateur, de 1 à 4294967290
4. Cliquez sur **Insérer** pour ajouter le jeu de motifs, puis cliquez sur **Fermer**.

Comment placer sur liste verte une URL d'exception

April 27, 2021

Lorsque vous utilisez un filtre d'URL pour mettre sur liste rouge une catégorie de sites Web, vous devez peut-être mettre sur liste verte ou autoriser un site Web spécifique à titre d'exception. Par exemple, si vous préférez mettre sur liste rouge les sites Web de jeux mais que vous préférez mettre sur liste verte uniquement www.supersports.com, vous devez créer un ensemble de patches avec une stratégie de liste d'URL, puis lier la stratégie au serveur proxy avec une plus grande priorité que les autres stratégies liées.

Pour créer un jeu de motifs à l'aide de l'Assistant Citrix SWG

1. Ouvrez une session sur l'appliance **Citrix SWG** et accédez à **Secured Web Gateway > Filtrage d'URL > Listes d'URL**.
2. Dans le volet d'informations, cliquez sur **Ajouter**.
3. Dans la page **Stratégie de liste d'URL**, spécifiez le nom de la stratégie.
4. Sélectionnez une option pour importer un jeu d'URL ou créer un jeu de motifs.
5. Dans l'onglet **Créer un motif**, entrez un nom pour le jeu de motifs.
6. Cliquez sur **Insérer** pour créer un motif.

7. Dans la page **Configurer le jeu de patches de stratégie en liaison de répétition**, définissez les paramètres suivants.
 - a) **Pattern**—Chaîne de caractères qui constitue un motif.
 - b) **Charset**—Le type de jeu de caractères définit au format ASCII ou UTF_8.
 - c) **Index** : valeur d'index affectée par l'utilisateur, de 1 à 4294967290
8. Cliquez sur **Insérer** pour ajouter le jeu de motifs, puis sur **Fermer** .

← URL List Policy

Configure a URL List policy to filter or blacklist URLs by importing a URL set or by creating a pattern set.

Name*
URL List

Import URL Set
 Create Patset

Patset Name*
Patset

Patset	Pattern
<input checked="" type="checkbox"/>	Pattern
<input checked="" type="checkbox"/>	Pattern

Configure Policy Patset to Pattern Binding

Pattern*
Patset

Charset
ASCII

Index
5

Action*
Respond with html page

Responder Action*

Pour définir la priorité de l'expression de stratégie à l'aide de l'interface graphique Citrix SWG :

1. Ouvrez une session sur l'appliance **Citrix SWG** et accédez à **Secure Web Gateway > Proxy Virtual Servers**.
2. Dans la page de détails, sélectionnez un serveur et cliquez sur **Modifier**.
3. Dans la page **Serveurs virtuels proxy**, accédez à la section **Stratégies** et cliquez sur l'icône crayon pour modifier les détails.
4. Sélectionnez la stratégie de jeu de patset que vous avez créée et, dans **la page Liaison de stratégie**, spécifiez la valeur de priorité inférieure à celle des autres stratégies liées.
5. Cliquez sur **Lier** et **Terminé**.

Comment bloquer les sites Web de catégorie adulte

April 27, 2021

En tant que client d'entreprise, vous pouvez bloquer les sites Web appartenant au groupe de catégorie Adulte. Ceci est fait en configurant une stratégie de répondeur qui sélectionne les demandes appartenant à une catégorie adulte et bloque l'accès à ces URL de liste rouge.

Configurer la catégorisation d'URL pour bloquer les sites Web appartenant à la catégorie adulte

Pour configurer une stratégie et bloquer les sites Web pour adultes à l'aide de l'interface de ligne de commande :

À l'invite de commandes, tapez la commande suivante :

```
1 \*\*add responder policy\*\* <name> <rule> <respondwithhtml> [<
  undefAction>] [-comment <string>] [-logAction <string>] [-
  appflowAction <string>]
```

Exemple :

```
1 add responder policy p1 ' HTTP.REQ.HOSTNAME.APPEND(HTTP.REQ.URL).
  URL_CATEGORIZE(0,0). GROUP.EQ("Adult") '
```

Configurer la catégorisation des URL pour le blocage des sites Web adultes à l'aide de l'assistant Citrix SWG

Pour bloquer les catégories adultes à l'aide de l'assistant Citrix SWG

1. Connectez-vous à l'appliance **Citrix SWG** et accédez à **Secure Web Gateway**.
2. Dans le volet d'informations, cliquez sur **Assistant Secured Web Gateway**.
3. Dans la page **Configuration de Secure Web Gateway**, spécifiez les paramètres du serveur proxy SWG.
4. Cliquez sur **Continuer** pour spécifier d'autres paramètres tels que l'interception SSL et l'identification de la gestion.
5. Cliquez sur **Continuer** pour accéder à la section **Filtrage d'URL**.
6. Cochez la **case Activer la catégorisation d'URL** pour activer la fonction.
7. Cliquez sur **Lier** pour accéder au curseur **Stratégies de catégorisation d'URL**.
8. Sélectionnez une stratégie et cliquez sur **Insérer** pour la lier.
9. Sélectionnez la stratégie de répondeur pour bloquer les sites Web pour adultes.
10. Pour ajouter une nouvelle stratégie, cliquez sur **Ajouter** pour accéder à la page **Stratégie de catégorisation d'URL** et effectuez l'une des opérations suivantes.
 - a) Pour configurer une stratégie à l'aide de la catégorisation de base, cliquez sur **Ajouter**.
 - i. Dans la page **Stratégie de catégorisation d'URL**, spécifiez les paramètres suivants.
 - A. Stratégie de catégorisation d'URL. Nom de la stratégie de répondeur.

- B. Basique. Configurez la stratégie à l'aide de la méthode de configuration de base.
- C. Action. Une action pour contrôler l'accès à l'URL.
- D. Catégories d'URL. Sélectionnez Catégorie Adulte dans la liste prédéfinie.

11. Cliquez sur **Créer** et **Fermer**.

- a) Pour configurer une nouvelle stratégie de catégorisation d'URL à l'aide de la catégorisation avancée, cliquez sur **Ajouter**.
 - i. Dans la page **Stratégie de catégorisation d'URL**, spécifiez les paramètres suivants.
 - A. **Stratégie de catégorisation d'URL**. Nom de la stratégie de répondeur.
 - B. **Avancé**. Configurez la stratégie pour bloquer les demandes du groupe de catégories Adulte.

12. Cliquez sur **Créer** et **Fermer**.

URL Categorization Policy

Select Basic to choose from a predefined list of categories.
Select Advanced to use the expression editor to create policy rules to suit your deployment.

Name*

Basic Advanced

Action*

URL Categories*

Available (18) Select All

Search Categories

- Illegal/Harmful
- Malware and SPAM
- Remote Proxies
- Search
- Business and Industry
- News/Entertainment/Society
- Finance
- Gambling
- Messaging/Chat/Telephony
- Email

Configured (11) Remove All

- Adult/Porn
- Nudity
- Sexual Services
- Adult Search/Links
- Dating
- Grotesque
- Adult Magazine/News
- Fetish
- Sexual Expression(text)
- Sex Education
- Swimsuits & Lingerie

Systeme

April 27, 2021

Les fonctionnalités système fournissent des informations conceptuelles et des instructions de configuration que vous pouvez souhaiter consulter lors de la configuration d'une appliance Citrix SWG.

Le tableau suivant décrit les fonctionnalités d'une appliance Citrix SWG.

[Opérations de base](#) - Détails du fonctionnement et de la configuration au niveau du système d'une appliance Citrix ADC.

[Authentification et autorisation](#) - Détails de configuration lors de la création d'utilisateurs, de groupes d'utilisateurs et de stratégies de commande et de l'affectation de stratégies aux comptes d'utilisateurs

[Configuration TCP](#) - Détails de configuration du profil TCP et des fonctionnalités TCP sur une appliance Citrix ADC.

[Configuration HTTP](#) - Détails de configuration du profil HTTP et des fonctionnalités HTTP sur une appliance Citrix ADC.

[SNMP](#) - Protocole de gestion réseau qui surveille l'appliance Citrix ADC et répond rapidement aux problèmes de l'appliance.

[Journalisation de l'audit](#) - Protocole standard pour consigner les états de l'appliance Citrix ADC et les informations d'état collectées par divers modules dans le noyau et dans les démons au niveau de l'utilisateur. Pour la journalisation d'audit, vous pouvez utiliser le protocole SYSLOG ou NSLOG, ou les deux.

[Call Home](#) - Système de notification permettant de surveiller et de résoudre les conditions d'erreur critiques sur une appliance Citrix SWG.

[Outil de création de rapports](#) - Interface Web accessible à partir d'une appliance Citrix SWG pour afficher les rapports de performances système sous forme de graphiques.

Mise en réseau

April 27, 2021

Les rubriques suivantes fournissent des informations de référence conceptuelles et des instructions de configuration pour les fonctionnalités de mise en réseau que vous pouvez configurer sur une appliance Citrix SWG.

- [adressage IP](#) Les adresses IP appartenant à Citrix ADC et leurs détails de configuration.
- [Interfaces](#) Accès et configuration de l'appliance Citrix SWG.
- [Listes de contrôle d'accès \(ACL\)](#) Différents types de listes de contrôle d'accès utilisées sur les appliances Citrix ADC, avec détails de configuration.
- [Routage IP](#) Les différents protocoles de routage IP utilisés sur une appliance Citrix ADC.

- [Protocole Internet version 6 \(IPv6\)](#) Prise en charge du protocole Internet sur une appliance Citrix ADC et fonctionnement de l'apppliance en tant que nœud IPv6.
- [VXLAN](#) Prise en charge de Virtual Extensible Local Area Network (VXLAN) dans l'infrastructure réseau Citrix ADC et comment VXLAN superpose les réseaux de couche 2 sur une infrastructure de couche 3 en encapsulant les trames de couche 2 dans UDP paquets.

AppExpert

April 27, 2021

Les rubriques suivantes fournissent des informations conceptuelles et des instructions de configuration pour les fonctionnalités AppExpert que vous pouvez configurer sur une appliance Citrix SWG.

[Jeux de modèles et jeux de données](#) - Expressions de stratégie pour effectuer des opérations de correspondance de chaîne sur un grand ensemble de modèles de chaîne.

Selon le type de répétition que vous souhaitez faire correspondre, vous pouvez utiliser l'une des fonctionnalités suivantes pour implémenter la correspondance de répétition :

- Un jeu de motifs est un tableau de motifs indexés utilisés pour la correspondance de chaînes lors de l'évaluation de la stratégie de syntaxe par défaut. Exemple de jeu de motifs : `imagetypes {svg, bmp, png, gif, tiff, jpg}`.
- Un ensemble de données est une forme spécialisée de jeu de motifs. Il s'agit d'un tableau de modèles de types nombre (entier), adresse IPv4 ou adresse IPv6.

[Variables](#) - Objets qui stockent des informations sous la forme de jetons et sont utilisés par les actions de stratégie du répondeur.

Les variables sont de deux types, comme indiqué ci-dessous :

- Variables singleton. Peut avoir une valeur unique de l'un des types suivants : `ulong` et `text` (taille `max-size`). Le type `ulong` est un entier 64 bits non signé, le type de texte est une séquence d'octets et la taille `max-size` est le nombre maximal d'octets dans la séquence.
- Mapper les variables. Les cartes contiennent des valeurs associées aux clés : chaque paire clé-valeur est appelée entrée de carte. La clé de chaque entrée est unique dans la carte.

[Stratégies et expressions](#) - Les stratégies contrôlent le trafic Web entrant dans une appliance Citrix SWG. Une stratégie utilise une expression logique, également appelée règle, pour évaluer les demandes, les réponses ou d'autres données, et applique une ou plusieurs actions déterminées par le résultat de l'évaluation. Une stratégie peut également appliquer un profil, qui définit une action complexe.

Répondeur - Stratégie qui envoie les réponses en fonction de qui envoie la demande, d'où elle est envoyée, et d'autres critères ayant des implications en matière de sécurité et de gestion du système. La fonctionnalité est simple et rapide à utiliser. En évitant l'invocation de fonctionnalités plus complexes, il réduit les cycles CPU et le temps passé à traiter les demandes qui ne nécessitent pas de traitement complexe. Pour le traitement de données sensibles telles que les informations financières, si vous souhaitez vous assurer que le client utilise une connexion sécurisée pour naviguer sur un site Web, vous pouvez rediriger la demande vers une connexion sécurisée à l'aide du protocole HTTPS.

Réécrire - Stratégie qui réécrit les informations dans les demandes et réponses traitées par l'appliance Citrix SWG. La réécriture peut aider à fournir l'accès au contenu demandé sans exposer des détails inutiles sur la configuration réelle du site Web.

Jeux d'URL - Expressions de stratégie avancées pour mettre sur liste rouge un million d'entrées d'URL. Pour empêcher l'accès aux sites Web restreints, une appliance Citrix SWG utilise un algorithme de correspondance d'URL spécialisé. L'algorithme utilise un jeu d'URL qui peut contenir une liste d'URL allant jusqu'à un million (1 000 000) d'entrées sur la liste rouge. Chaque entrée peut inclure des métadonnées qui définissent les catégories d'URL et les groupes de catégories en tant que modèles indexés. L'appliance peut également télécharger périodiquement des ensembles d'URL hautement sensibles gérés par des organismes d'application Internet (avec des sites Web gouvernementaux) ou des organisations Internet indépendantes.

SSL

April 27, 2021

Les rubriques suivantes fournissent des informations de référence conceptuelles et des instructions de configuration pour les fonctionnalités SSL que vous pouvez configurer sur une appliance Citrix SWG.

- [Certificats](#)
- [Listes de révocation de certificats \(CRL\)](#)
- [Stratégies SSL](#)
- [Répondeur OCSP](#)

Questions fréquentes

April 27, 2021

Q : Quelles plates-formes matérielles sont prises en charge pour Citrix Secure Web Gateway (SWG) ?

A. Citrix SWG est disponible sur les plates-formes matérielles suivantes :

- Citrix SWG MPX 14020/14030/14040
- Citrix SWG MPX 14020-40G/14040-40G
- Citrix SWG MPX 14060-40S/14080-40S/14100-40S
- Citrix SWG MPX 5901/5905/5910
- Citrix SWG MPX/SDX 8905/8910/8920/8930
- Toutes les plates-formes SDX basées sur Cavium N2 et N3

Q : Quels sont les deux modes de capture que je peux définir lors de la création d'un proxy sur l'appliance SWG ?

A. La solution SWG prend en charge les modes proxy explicites et transparents. En mode proxy explicite, les clients doivent spécifier une adresse IP et un port dans leurs navigateurs, sauf si l'organisation envoie le paramètre sur le périphérique du client. Cette adresse est l'adresse IP d'un serveur proxy configuré sur l'appliance SWG. Le proxy transparent, comme son nom l'indique, est transparent pour le client. L'appliance SWG est configurée dans un déploiement en ligne et elle accepte de manière transparente tout le trafic HTTP et HTTPS.

Q : Citrix SWG a-t-il un assistant de configuration ?

A. Oui. L'Assistant se trouve sur le nœud SWG dans l'utilitaire de configuration.

Q : Quelles fonctionnalités Citrix ADC sont utilisées lors de la configuration de Citrix SWG ?

A. Répondeur, AAA-TM, commutation de contenu, SSL, proxy de transfert, interception SSL et filtrage d'URL.

Q : Quelles méthodes d'authentification sont prises en charge sur Citrix SWG ?

A. En mode proxy explicite, les méthodes d'authentification LDAP, RADIUS, TACACS+ et NEGOTIATE sont prises en charge. En mode transparent, seule l'authentification LDAP est prise en charge.

Q : Est-il nécessaire d'installer le certificat d'autorité de certification sur la machine client ?

A. Oui. L'appliance Citrix SWG émule le certificat du serveur d'origine. Ce certificat de serveur doit être signé par un certificat d'autorité de certification approuvé, qui doit être installé sur les périphériques des clients afin que le client puisse approuver le certificat de serveur régénéré.

Q : Puis-je utiliser une licence Citrix ADC Platform sur la plate-forme Citrix SWG ?

A. Non. La plate-forme Citrix SWG requiert sa propre licence de plate-forme.

Q : La haute disponibilité est-elle prise en charge pour un déploiement Citrix Secure Web Gateway ?

A. Oui.

Q : Quel fichier contient les journaux pour Citrix SWG ?

A. Le fichier ns.log enregistre les informations Citrix SWG. Vous devez activer la journalisation à l'aide de l'interface de ligne de commande ou de l'interface graphique. À l'invite de commandes, tapez : **set syslogparams -ssli Enabled.**

Dans l'interface graphique, accédez à **Système > Audit**. Dans **Paramètres**, cliquez sur **Modifier les paramètres Syslog Audit**. Sélectionnez **Interception SSL**.

Q : Quelles commandes nsconmsg puis-je utiliser pour résoudre les problèmes ?

A. Vous pouvez utiliser l'une des commandes suivantes ou les deux :

```
1 nsconmsg -d current -g ssli
```

```
1 nsconmsg -d current -g err
```

Q : Si le paquet de certificats est intégré, comment puis-je obtenir des mises à jour ?

A. Le dernier bundle est inclus dans la build. Pour les mises à jour, contactez le support Citrix.

Q : Les données peuvent-elles être capturées sur Citrix ADM à partir de Citrix SWG ?

A. Oui. Vous devez activer **Analytics** dans l'Assistant Secure Web Gateway.

Important : Assurez-vous d'utiliser la même version 12.0 pour MAS et SWG.

Q : Qu'est-ce que le service de filtrage d'URL ?

A. Le filtrage d'URL est un filtre de contenu Web qui contrôle l'accès à une liste de sites Web et de pages Web restreints. Le filtre limite l'accès des utilisateurs au contenu inapproprié sur Internet en fonction de la catégorie d'URL, des groupes de catégories et du score de réputation. Un administrateur réseau peut surveiller le trafic Web et bloquer l'accès des utilisateurs aux sites Web à haut risque. Vous pouvez implémenter la fonctionnalité à l'aide de la fonction de catégorisation d'URL ou de liste d'URL basée sur l'application des stratégies. Pour plus d'informations, reportez-vous à la rubrique [filtrage d'URL](#).

Q : Comment le filtrage d'URL s'intègre-t-il dans Citrix SWG ?

R. Le filtrage des URL s'appuie sur l'appliance Citrix SWG pour contrôler l'accès à des sites Web spécifiques. L'appliance SWG en périphérie du réseau agit comme un proxy pour intercepter le trafic Web et effectuer des actions telles que l'authentification, l'inspection, la mise en cache et la redirection. Le filtre contrôle ensuite l'accès aux sites Web à l'aide de la fonction de catégorisation d'URL ou de liste d'URL avec application de stratégie.

Q : À quelle fréquence la base de données de catégorisation des URL est-elle mise à jour ?

A. Si vous utilisez la fonctionnalité de catégorisation d'URL pour contrôler l'accès aux sites Web restreints, vous devez périodiquement actualiser la base de données de catégorisation avec les dernières données provenant du service fournisseur basé sur le cloud. Pour mettre à jour la base de données, l'interface graphique Citrix SWG vous permet de configurer les paramètres de filtrage

d'URL tels que Heures entre les mises à jour DB ou « Heure du jour pour mettre à jour la base de données ».

Q : Quels sont les cas d'utilisation qui conviennent le mieux au service de filtrage d'URL aujourd'hui ?

R. Voici quelques-uns des cas d'utilisation ciblés pour les entreprises clientes :

- [Filtrage d'URL par score de réputation d'URL](#)
- [Contrôle de l'utilisation d'Internet dans le cadre de la conformité des entreprises](#)
- [Filtrage d'URL à l'aide d'une liste d'URL personnalisée](#)

Q : Existe-t-il une limite de mémoire pour la mise en cache dans le service de catégorisation d'URL ?

A. Oui. La limite de mémoire pour la mise en cache est définie sur 10 Go et vous pouvez la configurer via l'interface CLI uniquement.

Q : Que renvoie la base de données de catégorisation d'URL si aucune catégorie ne correspond à la demande entrante ?

A. Si la demande entrante ne correspond pas à une catégorie ou si l'URL est mal formée, l'appliance marque l'URL comme « Non classé » et envoie la demande au service basé sur le cloud géré par le fournisseur de catégorisation. L'appliance continue de surveiller les retours de requête dans le cloud et met à jour le cache afin que les demandes futures puissent bénéficier de la recherche dans le cloud.

Q : Qu'est-ce qu'un score de réputation d'URL et comment contrôler l'accès aux sites Web malveillants en fonction du score de réputation ?

A. Un score de réputation d'URL est une note que Citrix SWG attribue à un site Web. La valeur peut aller de 1 à 4, où 4 est un site Web malveillant et 1 est un site Web propre. Si un administrateur réseau surveille un utilisateur accédant à des sites Web à haut risque, l'accès à ces sites est contrôlé en fonction du score de réputation d'URL et du niveau de sécurité que vous avez configurés sur l'appliance Citrix SWG. Pour de plus amples informations, consultez la section [Score de réputation d'URL](#).

Q : Si vous filtrez des sites Web à l'aide d'un ensemble d'URL mais que vous filtrez incorrectement un site Web spécifique, quel est le processus pour activer des sites Web exceptionnels ?

R. Le filtrage d'URL utilise une stratégie de répondeur pour contrôler l'accès aux sites Web. Pour mettre sur liste verte une URL spécifique en tant qu'exception, dans l'assistant SWG, créez une stratégie de jeu de patches et ajoutez l'URL exceptionnelle avec l'action « Autoriser ». Une fois la stratégie créée, quittez l'Assistant et procédez comme suit :

Pour modifier la priorité d'une expression de stratégie à l'aide de l'interface graphique Citrix SWG :

1. Ouvrez une session sur l'appliance **Citrix SWG** et accédez à **Secure Web Gateway > Proxy Virtual Servers**.
2. Dans la page de détails, sélectionnez un serveur et cliquez sur **Modifier**.

3. Dans la page **Serveurs virtuels proxy**, accédez à la section **Stratégies** et cliquez sur l'icône crayon pour modifier les détails.
4. Sélectionnez la stratégie de jeu de patset et, dans **la page Liaison de stratégie**, spécifiez la valeur de priorité inférieure à celle des autres stratégies liées.
5. Cliquez sur **Lier** et **Terminé**.

Q : Quels sont les principaux avantages de l'utilisation de la fonctionnalité de filtrage d'URL Citrix SWG ?

A. La fonction de filtrage d'URL est facile à déployer, configurer et utiliser. Il offre les avantages suivants et permet aux entreprises clientes de :

- Surveiller le trafic Web et les transactions utilisateur
- Filtrer les logiciels malveillants et les menaces de sécurité transmises par Internet.
- Contrôler l'accès non autorisé aux sites Web malveillants.
- Appliquer les stratégies de sécurité de l'entreprise pour contrôler l'accès aux données restreintes.

Q : Si vous utilisez une fonction Liste d'URL pour filtrer des sites Web, comment modifier une stratégie de liste d'URL ?

A. Vous pouvez modifier une stratégie Liste d'URL via l'Assistant Citrix SWG en écrasant ou en supprimant la liste importée liée à la stratégie de répondeur.

Q : Que contiennent les métadonnées associées à une URL ?

A. Chaque URL de la base de données de catégorisation est associée à des métadonnées. Les métadonnées contiennent une catégorie d'URL, un groupe de catégories et des informations de score de réputation. Par exemple, si l'URL est un portail d'achat, les métadonnées seront Shopping/Retail, Shopping/Retail et 1 respectivement.

Utilisez les expressions suivantes pour obtenir ces valeurs pour l'URL entrante. Les expressions sont données ci-dessous :

```
1 URL_CATEGORIZE (0,0) .CATEGORY
```

```
1 URL_CATEGORIZE (0,0) .GROUP
```

```
1 URL_CATEGORIZE (0,0) .REPUTATION
```

Q : Quel type de licence et d'abonnement vous avez besoin pour la fonctionnalité de catégorisation des URL ?

A. La fonctionnalité de catégorisation d'URL nécessite un service d'abonnement URL Threat Intelligence (disponible pour un an ou trois ans) avec l'édition Citrix SWG.

Q : Quelles sont les façons dont je peux configurer le filtrage des URL ?

A. Il existe deux façons de configurer le filtrage d'URL. Vous pouvez le faire via l'interface de commande Citrix SWG ou via l'Assistant Citrix SWG. Citrix vous recommande d'utiliser l'Assistant pour configurer des stratégies de filtrage.

Q : Quels sont les types de catégories d'URL que vous pouvez bloquer ?

A. La base de données de catégorisation des URL contient des millions d'URL avec des métadonnées. L'administrateur peut configurer une stratégie de répondeur pour décider quelles catégories d'URL peuvent être bloquées et quelles catégories d'URL peuvent être autorisées pour l'accès utilisateur. Pour plus d'informations sur le mappage des catégories d'URL, reportez-vous à la page [Catégories de correspondance](#).

Q : Que doit-on faire si nous ne parvenons pas à accéder aux serveurs Origin qui utilisent WebSocket, tels que [Whatsapp](#)

Vous devez activer WebSocket dans le profil HTTP par défaut.

À l'interface de ligne de commande, tapez :

```
1 > set httpprofile nshttp_default_profile -websocket ENABLED
```

Qu'est-ce que l'ICAP ?

ICAP signifie Internet Content Adaption Protocol.

Quelle version de Citrix SWG prend en charge ICAP ?

ICAP est pris en charge dans Citrix SWG version 12.0 build 57.x et versions ultérieures.

Quels sont les deux modes ICAP pris en charge sur Citrix SWG ?

Le mode de modification de requête (**REQMOD**) et le mode de modification de réponse (**RESPMOD**) sont pris en charge.

Quel est le port par défaut pour ICAP ?

1344.



© 2025 Cloud Software Group, Inc. All rights reserved. This document is subject to U.S. and international copyright laws and treaties. No part of this document may be reproduced in any form without the written authorization of Cloud Software Group, Inc. This and other products of Cloud Software Group may be covered by registered patents. For details, please refer to the Virtual Patent Marking document located at <https://www.cloud.com/legal>. Citrix, the Citrix logo, NetScaler, and the NetScaler logo and other marks appearing herein are either registered trademarks or trademarks of Cloud Software Group, Inc. and/or its subsidiaries in the United States and/or other countries. Other marks are the property of their respective owner(s) and are mentioned for identification purposes only. Please refer to Cloud SG's Trademark Guidelines and Third Party Trademark Notices (<https://www.cloud.com/legal>) for more information.