# Configuration des ports proxy pour le trafic de port non standard sur WSA 1000V

## Table des matières

## Problème

Un proxy WSA 1000V hébergé sur VMware traitait correctement le trafic client sur les ports 80 et 443, mais ne traitait pas le trafic sur les ports non standard tels que le port 890. Lorsque l'accès à une destination utilisant un port non standard a été initialement bloqué par la stratégie, l'appareil de sécurité Web a correctement consigné la requête bloquée. Cependant, après l'ajout de l'adresse IP et de l'URL à une stratégie d'autorisation, le trafic a tout de même échoué et aucun journal correspondant n'a été généré sur le proxy. Ce comportement suggérait que le trafic n'atteignait pas ou n'était pas traité par le WSA après la création de la stratégie d'autorisation, ce qui impactait l'accès client aux applications utilisant des ports non standard.

## Environnement

- Proxy Cisco WSA 1000V hébergé sur VMware
- Version logicielle 15.0.0
- Le trafic sur les ports 80 et 443 fonctionne normalement.
- Le trafic de port non standard (par exemple, le port 8890) n'est pas traité par le proxy.
- Autoriser les stratégies configurées pour les destinations affectées.

## Résolution

Le problème a été résolu en configurant le WSA pour prendre en charge les ports non standard dans les paramètres du profil d'identification. La configuration des ports proxy devait être mise à jour pour inclure les numéros de port non standard requis.

### Configuration Steps

Étape 1: Accédez à l'interface du Gestionnaire de sécurité Web.

Étape 2: Accédez à la configuration Profils d'identification.

Accédez à Gestionnaire de sécurité Web > Profils d'identification.

Étape 3: Sélectionnez le profil d'identification souhaité qui nécessite la prise en charge de ports non standard.

Étape 4: Développez les options de configuration avancée.

Dans la page Profil d'identification, développez l'onglet Avancé.

Étape 5: Configurez le paramètre Ports proxy.

Sélectionnez le lien en regard de Proxy Ports pour accéder à la configuration du port.

Étape 6: Ajoutez les numéros de port non standard requis.

Ajoutez les numéros de port que les clients utilisent pour les connexions de port non standard (par exemple, 8890).

Étape 7: Enregistrez et validez les modifications de configuration.

Après avoir implémenté ces modifications de configuration, l'appareil de sécurité Web peut traiter et inspecter le trafic sur les ports non standard spécifiés, permettant au proxy de gérer correctement les connexions client et d'appliquer des politiques au trafic à l'aide de ces ports.

## Motif

Le WSA 1000V a été configuré avec des paramètres de port proxy par défaut qui incluaient uniquement les ports HTTP (port 80) et HTTPS (port 443) standard. La configuration des ports proxy du profil d'identification n'incluait pas les ports non standard requis par les applications

clientes. Sans que ces ports soient explicitement configurés dans les paramètres avancés du profil d'identification, l'appareil de sécurité Web n'a pas pu intercepter, traiter ou appliquer des stratégies au trafic à l'aide de ports non standard, même lorsque des stratégies d'autorisation ont été configurées pour les destinations.

## Autres informations utiles

- Assistance technique de Cisco et téléchargements

À propos de cette traduction
Cisco a traduit ce document en traduction automatisée vérifiée par une personne dans le cadre d'un service mondial permettant à nos utilisateurs d'obtenir le contenu d'assistance dans leur propre langue.

Il convient cependant de noter que même la meilleure traduction automatisée ne sera pas aussi précise que celle fournie par un traducteur professionnel.