Détection du trafic non autorisé sur les ports non standard

Cette rubrique contient les sections suivantes :

Survol de la détection du trafic non autorisé

Secure Web Appliance intègre une supervision du trafic de la couche 4 qui détecte le trafic non autorisé sur tous les ports du réseau et arrête les tentatives de contournement du port 80 par les programmes malveillants. Lorsque des clients internes sont infectés par des programmes malveillants et tentent de téléphoner par le biais de ports et de protocoles non standard, la supervision du trafic de la couche 4 empêche l'activité de téléphone domestique de sortir du réseau de l'entreprise. Par défaut, la supervision du trafic de la couche 4 est activée et configurée pour surveiller le trafic sur tous les ports. Cela inclut le DNS et d'autres services.

La supervision du trafic de la couche 4 utilise et gère sa propre base de données interne. Cette base de données est continuellement mise à jour avec les résultats correspondants pour les adresses IP et les noms de domaine.

Configuration de la supervision du trafic de la couche 4

Étape 1 Configurez la supervision du trafic de la couche 4 à l'intérieur du pare-feu.

Étape 2 Assurez-vous que la supervision du trafic de la couche 4 est connectée « logiquement » après les ports proxy et avant tout périphérique qui effectue la traduction d'adresses réseau (NAT) sur les adresses IP des clients.

Étape 3 Configurer les paramètres globaux

Consultez Configuration des paramètres globaux de la supervision du trafic de la couche 4, on page 2.

Étape 4 Politiques de supervision du trafic de la couche 4

Consultez Création d'une politique pour détecter le trafic non autorisé, on page 3.

Liste des sites connus

Address (Adresse)	Description
Autorisé connu	Toute adresse IP ou tout nom d'hôte répertorié dans la propriété Allow List (Liste des adresses autorisées). Ces adresses apparaissent dans les fichiers journaux en tant qu'adresses de la « liste des adresses autorisées ».
Non publiée	Toute adresse IP qui n'est pas connue pour être un site malveillant ou qui n'est pas une adresse autorisée. Elle n'est pas répertoriée dans les propriétés de la liste des autorisations, des adresses supplémentaires de programmes malveillants suspects ou dans la base de données de la supervision du trafic de la couche 4. Ces adresses ne figurent pas dans les fichiers journaux.
Douteuse	Celles-ci apparaissent dans les fichiers journaux en tant qu'adresses de la « liste grise » et comprennent : • Toute *adresse IP* qui est associée à un *nom d'hôte* non publié et à un *nom d'hôte* connu d'un programme malveillant. • Toute *adresse IP* associée à un *nom d'hôte* non publié et à un *nom d'hôte* dans la propriété Additional Suspected Malware Addresses (Adresses supplémentaires suspectées de programme malveillant)
Programme malveillant connu	Celles-ci apparaissent dans les fichiers journaux en tant qu'adresses de « liste bloquée » et comprennent : • Toute adresse IP ou nom d'hôte que la base de données de la supervision du trafic de la couche 4 détermine comme étant un site malveillant connu et *non* répertorié dans la liste des adresses autorisées. • Toute *adresse IP* qui est répertoriée dans la propriété Additional Suspected Malware Addresses (Adresses supplémentaires pour les programmes malveillants suspects), qui *ne figure pas* dans la liste des autorisations et qui *n'est pas* douteuse.

Configuration des paramètres globaux de la supervision du trafic de la couche 4

Étape 1 Choisissez **Security Services > L4 Traffic Monitor** (Services de sécurité > Supervision du trafic de la couche 4).

Étape 2 Cliquez sur **Edit Global Settings** (Modifier les paramètres globaux).

Étape 3 Choisissez d'activer ou non la supervision du trafic de la couche 4.

Étape 4 Lorsque vous activez la supervision du trafic de la couche 4, choisissez les ports à surveiller :

- **All ports** (Tous les ports). Surveille tous les ports TCP 65535 pour détecter les activités non autorisées.

- **All ports except proxy ports** (Tous les ports, à l'exception des ports du proxy). Surveille tous les ports TCP, à l'exception des ports suivants, pour détecter les activités non autorisées.
  - Ports configurés dans la propriété « HTTP Ports to Proxy » (Ports HTTP vers proxy) sur la page Security Services > Web Proxy (Services de sécurité > Proxy Web) (généralement le port 80).
  - Ports configurés dans la propriété « Transparent HTTPS Ports to Proxy » (Ports HTTPS transparents vers proxy) dans la page Security Services > HTTPS Proxy (Services de sécurité > Proxy HTTPS) (généralement le port 443).

Étape 5 Envoyez et validez les modifications.

Mise à jour des règles de protection contre les programmes malveillants de la supervision du trafic de la couche 4

Étape 1 Choisissez **Security Services > L4 Traffic Monitor** (Services de sécurité > Supervision du trafic de la couche 4).

Étape 2 Cliquez sur **Update Now** (Mettre à jour maintenant).

Création d'une politique pour détecter le trafic non autorisé

Les actions effectuées par la supervision du trafic de la couche 4 dépendent des politiques de supervision du trafic de la couche 4 que vous configurez :

Étape 1 Choisissez **Web Security Manager > L4 Traffic Monitor** (Web Security Manager > Supervision du trafic de la couche 4).

Étape 2 Cliquez sur **Edit Settings** (Modifier les paramètres).

Étape 3 Dans la page **Edit L4 Traffic Monitor Policies** (Modifier les politiques de supervision du trafic de la couche 4), configurez les politiques de supervision du trafic de la couche 4 :

a) **Définir** la **liste des autorisations**

b) Ajouter des sites efficaces connus à la **liste des autorisations**

Note N'incluez pas le nom d'hôte ou l'adresse IP Secure Web Appliance dans la liste des autorisations, sinon la supervision du trafic de la couche 4 ne bloque aucun trafic.

c) Déterminez l'action à effectuer pour les **adresses de programmes malveillants suspects** :

Action	Description
Allow (Autoriser)	Autorise toujours le trafic vers et à partir d'adresses autorisées et non répertoriées connues

Action	Description
Monitor (Superviser)	Surpervise le trafic dans les circonstances suivantes : • Lorsque l'option Action for Suspected Malware Addresses (Action pour les adresses de programmes malveillants) est réglée sur Monitor (Superviser), elle surveille toujours tout le trafic qui ne va pas vers ou en provenance d'une adresse autorisée connue. • Lorsque l'option Action for Suspected Malware Addresses (Action en cas d'adresses malveillantes présumées) est définie sur Block (Bloquer), surveille le trafic à destination et en provenance des adresses douteuses.
Block (Bloquer)	Lorsque l'option Action for Suspected Malware Addresses (Action en cas d'adresses malveillantes présumées) est réglée sur Block (Bloquer), bloque le trafic à destination et en provenance d'adresses malveillantes connues.

Note – Lorsque vous choisissez de bloquer le trafic de programmes malveillants présumés, vous pouvez également choisir de toujours bloquer ou non les adresses douteuses. Par défaut, les adresses douteuses sont surveillées.

– Si la supervision du trafic de la couche 4 est configurée pour bloquer, la supervision du trafic de la couche 4 et le proxy Web doivent être configurés sur le même réseau. Utilisez la page **Network > Routes** (Réseau > Voies de routage) pour confirmer que tous les clients sont accessibles sur les voies de routage configurées pour le trafic de données.

- Dans une configuration VM, les demandes en mode transparent sont dupliquées en transitant par les interfaces P1 et T1 avec un décalage horaire intermittent. Par conséquent, certaines adresses IP, même après avoir été bloquées, peuvent transiter par l'appliance.

d) Définir les propriétés **Additional Suspected Malware Addresses** (Autres adresses malveillantes présumées)

Note L'ajout d'adresses IP internes à la liste d'adresses supplémentaires pour les programmes malveillants suspects fait que les URL de destination légitimes s'affichent comme des programmes malveillants dans les rapports de supervision du trafic de la couche 4. Pour éviter cela, n'entrez pas d'adresses IP internes dans le champ « **Additional Suspected Malware Addresses** » (Autres adresses malveillantes présumées) de la page **Web Security Manager > L4 Traffic Monitor Policies** (Web Security Manager > Politiques de supervision du trafic de la couche 4).

Étape 4 Envoyez et validez les modifications.

What to do next

Thèmes connexes

- Survol de la détection du trafic non autorisé, on page 1
- Formats valides, on page 5.

Formats valides

Lorsque vous ajoutez des adresses à la liste d'autorisation ou aux propriétés d'adresses supplémentaires pour les programmes malveillants suspects, séparez les entrées par des espaces ou des virgules. Vous pouvez saisir des adresses dans l'un des formats suivants :

- **Adresse IP IPv4.** Exemple : Format IPv4 : 10.1.1.0. Format IPv6 : 2002:4559:1FE2::4559:1FE2
- **Adresse CIDR** Exemple : 10.1.1.0/24.
- **Nom de domaine.** Exemple : exemple.com.
- **Nom d'hôte.** Exemple : crm.exemple.com.

Affichage de l'activité de la supervision du trafic de la couche 4

L'appliance S Series prend en charge plusieurs options pour générer des rapports spécifiques aux fonctionnalités et des affichages interactifs de statistiques sommaires.

Activité de supervision et affichage des statistiques sommaires

La page **Reporting > L4 Traffic Monitor** (Rapports > Supervision du trafic de la couche 4) fournit des résumés statistiques de l'activité de supervision. Vous pouvez utiliser les affichages et outils de création de rapports suivants pour afficher les résultats de l'activité de la supervision du trafic de la couche 4 :

Pour afficher...	Voir...
Statistiques relatives aux clients	Reporting > Client Activity (Rapports > Activité des clients)
Statistiques sur les programmes malveillants Statistiques relatives aux ports	Reporting > L4 Traffic Monitor (Rapports > Supervision du trafic de la couche 4)
Fichiers journaux de supervision du trafic de la couche 4	System Administration > Log Subscriptions (Administration système > Abonnements au journal) • trafmon_errlogs • trafmonlogs

Note Si le proxy Web est configuré comme proxy de transfert et que la supervision du trafic de la couche 4 est configurée pour surveiller tous les ports, l'adresse IP du port de données du proxy est enregistrée et affichée en tant qu'adresse IP client dans le rapport d'activité du client dans la page **Reporting > Client Activity** (Rapports > Activité du client). Si le proxy Web est configuré comme un proxy transparent, activez l'usurpation d'adresses IP pour enregistrer et afficher correctement les adresses IP des clients.

Entrées du fichier journal de supervision du trafic de la couche 4

Le fichier journal de supervision du trafic de la couche 4 fournit un enregistrement détaillé de l'activité de supervision.

À propos de la traduction

Cisco peut fournir des traductions du présent contenu dans la langue locale pour certains endroits. Veuillez noter que des traductions sont fournies à titre informatif seulement et, en cas d’incohérence, la version anglaise du présent contenu prévaudra.