Rapports sur les appliances Secure

Cette rubrique contient les sections suivantes :

Page Overview (Survol)

La page **Reporting > Overview** (Rapports > Survol) fournit un synopsis de l'activité sur Secure Web Appliance. Elle contient des graphiques et des tableaux sommaires pour le trafic Web traité par Secure Web Appliance.

Table 1: Survol du système

Section	Description
Caractéristiques du trafic du proxy Web	Liste de la moyenne des transactions par seconde au cours de la dernière minute, de la bande passante moyenne (bit/s) au cours de la dernière minute, du temps de réponse moyen (ms) au cours de la dernière minute et du total des connexions actuelles.

Section	Description
Utilisation des ressources système	Liste de la `charge globale du processeur`, de `la RAM` et de l'utilisation `des disques pour les rapports et les` journaux. Cliquez sur **System Status Details** (Détails sur l'état du système) pour passer à la page System Status (État du système) (voir Page System Status (État du système) sur la nouvelle interface Web pour en savoir plus). **Note** La valeur d'utilisation du processeur affichée sur cette page et la valeur du processeur affichée sur la page System Status (État du système) peuvent différer légèrement, car elles sont lues séparément, à des moments différents.

Table 2: Catégories et résumés basés sur des plages de temps

Section	Description
Plage de temps : choisissez une plage de temps pour les données affichées dans les sections suivantes. Les options sont Hour (Heure), Day (Jour), Week (Semaine), 30 Days (30 jours), Yesterday (Hier) ou Custom Range (Plage personnalisée).	
Total Web Proxy Activity (Activité totale du proxy Web)	Affiche le nombre réel de transactions (échelle verticale) ainsi que la date approximative à laquelle l'activité (proxy Web) s'est produite (chronologie horizontale).
Web Proxy Summary (Résumé du proxy Web)	Vous permet d'afficher le pourcentage d'activités de proxy Web suspectes ou saines.
L4 Traffic Monitor Summary (Résumé de la supervision du trafic de la couche 4)	Rapports sur le trafic surveillé et bloqué par la supervision du trafic de la couche 4.
Suspect Transactions (Transactions suspectes)	Vous permet d'afficher les transactions Web qui ont été marquées comme suspectes par les divers composants de sécurité. Affiche le nombre réel de transactions ainsi que la date approximative à laquelle l'activité a eu lieu.
Suspect Transactions Summary (Résumé des transactions suspectes)	Vous permet d'afficher le pourcentage de transactions bloquées ou avec avertissement qui sont suspectes.
Top URL Categories: Total Transactions (Principales catégories d'URL : Total des transactions)	Affiche les 10 principales catégories d'URL qui ont été bloquées.
Top Application Types: Total Transactions (Principaux types d'application : Total des transactions)	
Top Malware Categories: Monitored or Blocked (Principales catégories de programmes malveillants : surveillés ou bloqués)	Affiche toutes les catégories de programmes malveillants qui ont été détectées.

Section	Description
Top Users: Blocked or Warned Transactions (Principaux utilisateurs : Transactions bloqués ou avec avertissement)	Affiche les utilisateurs qui génèrent les transactions bloquées ou avec avertissement. Les utilisateurs authentifiés sont affichés par nom d'utilisateur et les utilisateurs non authentifiés par adresse IP.
Web Traffic Tap Status (État de dérivation du trafic Web)	Affiche les transactions de trafic dérivé et non dérivé du trafic dans un format de graphique.
Web Traffic Tap Summary (Résumé des dérivations du trafic Web)	Affiche le résumé des transactions de trafic dérivé et non dérivé ainsi que le total des transactions de trafic.
Tapped HTTP/HTTPS Traffic (Trafic HTTP/HTTPS dérivé)	Affiche les transactions de trafic HTTP et HTTPS dérivé au format graphique.
Tapped Traffic Summary (Résumé du trafic dérivé)	Affiche le résumé des transactions de trafic HTTP et HTTPS ainsi que le total des transactions de trafic HTTP/HTTPS.
EUP Transactions (Transactions EUP)	Affiche les transactions URL encapsulées. Il s'agit de transactions effectuées par l'intermédiaire de sites Web comme *translate.google.com*.
EUP Transaction Summary (Résumé des transactions EUP)	Affiche le résumé des transactions d'URL encapsulées.
EUP Suspect Transactions (Transactions suspectes de EUP)	Affiche les transactions URL encapsulées qui se sont avérées suspectes.
EUP Suspect Transaction Summary (Résumé des transactions suspectes pour les EUP)	Affiche le résumé des transactions d'URL encapsulées jugées suspectes.

Page Users (Utilisateurs)

La page **Reporting > Users** (Rapports > Utilisateurs) fournit plusieurs liens qui vous permettent d'afficher les renseignements sur le trafic Web pour les utilisateurs individuels. Vous pouvez afficher le temps que les utilisateurs du réseau ont passé sur Internet, sur un site Web ou une URL en particulier, et la quantité de bande passante utilisée.

Section	Description
Time Range (Plage de temps) (liste déroulante)	Menu qui permet de choisir la plage de temps des données contenues dans le rapport.
Top Users by Transactions Blocked (Principaux utilisateurs par transactions bloquées)	Répertorie les utilisateurs (échelle verticale) qui ont le plus grand nombre de transactions bloquées (échelle horizontale).

Top Users by Bandwidth Used (Principaux utilisateurs par bande passante utilisée)	Affiche les utilisateurs (échelle verticale) qui utilisent le plus de bande passante sur le système (échelle horizontale exprimée en gigaoctets).
Users Table (Tableau des utilisateurs)	Répertorie les utilisateurs individuels et affiche plusieurs statistiques pour chaque utilisateur.

Page User Details (Détails des utilisateurs)

La page **User Details** (Détails relatifs à l'utilisateur) affiche des informations sur un utilisateur spécifique sélectionné dans le tableau Users (Utilisateurs) de la page **Reporting > Users** (Rapports > Utilisateurs).

Section	Description
Time Range (Plage de temps) (liste déroulante)	Menu qui permet de choisir la plage de temps des données contenues dans le rapport.
URL Categories by Total Transactions (Catégories d'URL par transactions totales)	Répertorie les catégories d'URL spécifiques utilisées par un utilisateur donné.
Trend by Total Transaction (Tendance par transaction totale)	Affiche l'heure à laquelle l'utilisateur a accédé au Web.
URL Categories Matched (Catégories d'URL correspondantes)	Affiche toutes les catégories d'URL correspondantes pendant une plage de temps spécifiée pour les transactions terminées et bloquées.
Domains Matched (Domaines correspondants)	Affiche des informations sur un domaine ou une adresse IP spécifique auquel cet utilisateur a accédé. **Note** Si vous exportez les données de ce domaine vers un fichier CSV, sachez que seules les 300 000 premières entrées seront exportées dans le fichier.
Applications Matched (Applications correspondantes)	
Malware Threats Detected (Programmes malveillants détectés)	Affiche les principaux programmes malveillants déclenchés par un utilisateur spécifique.
Policies Matched (Politiques correspondantes)	Affiche une politique spécifique appliquée à cet utilisateur en particulier.

Page User Count (Nombre d'utilisateurs)

La page **Reporting** > **User Count** (Rapports > Nombre d'utilisateurs) affiche des informations sur le nombre total d'utilisateurs authentifiés et non authentifiés sur l'appliance. La page répertorie le nombre d'utilisateurs uniques pour les 30, 90 et 180 derniers jours.

Remarque Le système calcule le nombre total d'utilisateurs authentifiés et non authentifiés une fois par jour.

Par exemple, si vous affichez le rapport sur le nombre d'utilisateurs au plus tard le 22 mai 23:59, le système affichera le nombre total d'utilisateurs jusqu'au 22 mai minuit.

Page Web Sites (Sites Web)

La page **Reporting > Web Sites** (Rapports > Sites Web) est une agrégation globale de l'activité qui se produit sur Secure Web Appliance.

Section	Description
Time Range (Plage de temps) (liste déroulante)	Le menu vous permet de choisir la plage de temps des données contenues dans le rapport.
Top Domains by Total Transactions (Principaux domaines par total des transactions)	Répertorie les principaux domaines visités sur le site au format graphique.
Top Domains by Transactions Blocked (Principaux domaines par transactions bloquées)	Répertorie les principaux domaines qui ont déclenché une action de blocage par transaction au format graphique.
Domains Matched (Domaines correspondants)	Répertorie les domaines qui sont visités sur le site dans un tableau interactif. **Note** Si vous exportez les données de ce domaine vers un fichier CSV, sachez que seules les 300 000 premières entrées seront exportées dans le fichier.

Page URL Categories (Catégories d'URL)

La page **Reporting > URL Categories** (Rapports > Catégories d'URL) peut être utilisée pour afficher les catégories d'URL consultées par les utilisateurs sur le réseau. La page URL Categories (Catégories d'URL) peut être utilisée conjointement avec la page Application Visibility (Visibilité des applications) et la page Users (Utilisateurs) pour enquêter sur un utilisateur particulier ainsi que sur les types d'applications ou de sites Web auxquels un utilisateur particulier tente d'accéder.

Note L'ensemble de catégories d'URL prédéfinies est mis à jour occasionnellement.

Section	Description
Time Range (Plage de temps) (liste déroulante)	Choisissez la plage de temps de votre rapport.
Top URL Categories by Total Transactions (Principales catégories d'URL par nombre total de transactions)	Cette section répertorie les principales catégories d'URL visitées sur le site au format graphique.
Top URL Categories by Blocked and Warned Transactions (Principales catégories d'URL par transactions bloquées et avec avertissement)	Répertorie les principales URL qui ont déclenché un blocage ou un avertissement par transaction au format graphique.
URL Categories Matched (Catégories d'URL correspondantes)	Affiche la disposition des transactions par catégorie d'URL pendant la plage de temps spécifiée, ainsi que la bande passante utilisée et le temps passé dans chaque catégorie. Si le pourcentage d'URL non classées est supérieur à 15 à 20 %, envisagez les options suivantes : • Pour des URL localisées précises, vous pouvez créer des catégories d'URL personnalisées et les appliquer à des utilisateurs ou à des groupes de politiques spécifiques. • Vous pouvez signaler les URL non classées et mal classées et à Cisco pour une évaluation et une mise à jour de la base de données. • Vérifiez que le filtrage de réputation Web et le filtrage contre les programmes malveillants sont activés.

Mises à jour et rapports des ensembles de catégories d'URL

L'ensemble de catégories d'URL prédéfinies peut être mis à jour régulièrement et automatiquement sur votre Secure Web Appliance.

Lorsque ces mises à jour se produisent, les noms des anciennes catégories continueront d'apparaître dans les rapports jusqu'à ce que les données associées aux anciennes catégories soient trop anciennes pour être incluses dans les rapports. Les données de rapport générées après la mise à jour d'un ensemble de catégories d'URL utiliseront les nouvelles catégories. Vous pouvez donc voir les anciennes catégories et les nouvelles dans le même rapport.

Page Application Visibility (Visibilité des applications)

Section	Description
Time Range (Plage de temps) (liste déroulante)	Menu qui permet de choisir la plage de temps des données contenues dans le rapport.
Top Application Types by Total Transactions (Principaux types d'application par nombre total de transactions)	Cette section répertorie, au format graphique, les principaux types d'applications visitées sur le site.
Top Applications by Blocked Transactions (Principales applications par transactions bloquées)	Répertorie les principaux types d'applications qui ont déclenché un blocage par transaction au format graphique.
Application Types Matched (Types d'application correspondants)	Vous permet d'afficher des détails granulaires sur les types d'applications répertoriés dans le graphique Top Applications Type by Total Transactions (Types d'applications principales par total des transactions).
Applications Matched (Applications correspondantes)	Affiche toutes les applications pendant une plage de temps spécifiée.

Page Anti-Malware (Protection contre les programmes malveillants)

La page **Reporting > Anti-Malware** (Rapports > Protection contre les programmes malveillants) vous permet de surveiller et d'identifier les programmes malveillants détectés par le moteur Cisco DVS.

Section	Description
Time Range (Plage de temps) (liste déroulante)	Menu qui permet de choisir la plage de temps des données contenues dans le rapport.
Top Malware Categories Detected (Principales catégories de programmes malveillants détectés)	Affiche les principales catégories de programmes malveillants détectées par le moteur DVS.
Top Malware Threats Detected (Principaux programmes malveillants détectés)	Affiche les principaux programmes malveillants détectés par le moteur DVS.
Malware Categories (Catégorie de programmes malveillants)	Affiche des informations sur des catégories particulières de programmes malveillants qui sont indiquées dans la section Top Malware Categories Detected (Principales catégories de programmes malveillants détectées).

Section	Description
Malware Threats (Programmes malveillants)	Affiche des informations sur des programmes malveillants particuliers qui sont indiqués dans la section Top Malware Threats (Principaux programmes malveillants).

Page Malware Category Report (Rapports sur les catégories de programmes malveillants)

Étape 1 Choisissez **Reporting > Anti-Malware** (Rapports > Protection contre les programmes malveillants).

Étape 2 Dans le tableau interactif Malware Categories (Catégories de programmes malveillants), cliquez sur une catégorie dans la colonne Malware Category (Catégorie de programmes malveillants).

Page Malware Threat Report (Rapport sur les menaces des programmes malveillants)

Étape 1 Choisissez **Reporting > Anti-Malware** (Rapports > Protection contre les programmes malveillants).

Étape 2 Dans le tableau Malware Threat (Programmes malveillants), cliquez sur une catégorie dans la colonne Malware Catégorie (Catégorie de programmes malveillants).

Page Cisco Secure Endpoint

Consultez Filtrage de réputation de fichiers et analyse de fichiers.

Page File Analysis (Analyse des fichiers)

Consultez Création de rapports et suivi de la réputation et de l'analyse des fichiers.

Page Cisco Secure Endpoint Verdict Updates (Mises à jour des verdicts Cisco Secure Endpoint

Consultez Filtrage de réputation de fichiers et analyse de fichiers.

Consultez .

Page Client Malware Risk (Risques de programmes malveillants des clients)

La page **Reporting > Client Malware Risk** (Rapports > Risques liés aux programmes malveillants pour les clients) est une page de rapport sur la sécurité qui peut être utilisée pour surveiller les activités à risque des programmes malveillants pour les clients. La page Client Malware Risk (Risques liés aux programmes malveillants pour les clients) répertorie également les adresses IP des clients impliqués dans les connexions fréquentes de programmes malveillants, comme identifiées par la supervision du trafic de la couche 4 (L4TM).

Section	Description
Time Range (Plage de temps) (liste déroulante)	Menu qui vous permet de choisir la plage de temps des données contenues dans le rapport.
Web Proxy: Top Clients by Malware Risk (Proxy Web : Principaux clients par risque lié aux programmes malveillants)	Ce tableau affiche les dix principaux utilisateurs qui ont rencontré un risque lié à des programmes malveillants.
L4 Traffic Monitor: Malware Connections Detected (Supervision du trafic de la couche 4 : connexions à des programmes malveillants détectées)	Ce tableau affiche les adresses IP des ordinateurs de votre entreprise qui se connectent le plus souvent aux sites de programmes malveillants.
Web Proxy: Top Clients by Malware Risk (Proxy Web : Principaux clients par risque lié aux programmes malveillants)	Le tableau Web Proxy: Clients by Malware Risk (Proxy Web : clients par risque lié aux programmes malveillants) présente des informations détaillées sur des clients particuliers qui sont affichés dans la section Web Proxy: Top Clients by Malware Risk (Proxy Web : Principaux clients par risque lié aux programmes malveillants).
L4 Traffic Monitor: Clients by Malware Risk (Supervision du trafic de la couche 4 : clients par risque lié aux programmes malveillants)	Ce tableau affiche les adresses IP des ordinateurs de votre organisation qui se connectent fréquemment à des sites malveillants.

Page Client Detail (Détails des clients) pour le proxy Web – Clients par risque de programme malveillant

La page **Client Details** (Détails sur le client) affiche toutes les données sur l'activité Web et les risques liés aux programmes malveillants pour un client particulier au cours de la plage de temps spécifiée.

Étape 1 Choisissez **Reporting > Client Malware Risk** (Rapports > Risques liés aux programmes malveillants pour le client).

Étape 2 Dans la section **Web Proxy - Client Malware Risk** (Proxy Web > Risques liés aux programmes malveillants pour le client), cliquez sur un nom d'utilisateur dans la colonne « User ID/Client IP Address » (ID utilisateur/Adresse IP du client).

What to do next

Page User Details (Détails des utilisateurs), on page 4

Page Web Reputation Filters (Filtres de réputation Web)

La page **Reporting > Web Reputation Filters** (Rapports > Filtres de réputation Web) est une page de rapports liés à la sécurité qui vous permet d'afficher les résultats des filtres de réputation Web définis pour les transactions effectuées pendant une plage de temps spécifiée.

Section	Description
Time Range (Plage de temps) (liste déroulante)	Menu qui permet de choisir la plage de temps des données contenues dans le rapport.
Web Reputation Actions (Trend) [Actions de réputation Web (tendance)]	Affiche le nombre total d'actions de réputation de sites Web (verticales) dans le temps spécifié (chronologie horizontale).
Web Reputation Actions (Volume) [Actions de réputation Web (volume)]	Affiche le volume d'actions de réputation Web en pourcentages par transaction.
Web Reputation Threat Types by Blocked Transactions (Types de menaces pour la réputation Web par transactions bloquées)	Affiche les types de menaces qui ont été bloquées en raison d'un faible score de réputation.
Web Reputation Threat Types by Scanned Further Transactions (Types de menaces pour la réputation Web par transactions supplémentaires analysées)	Affiche les types de menaces qui ont entraîné un score de réputation nécessitant l'analyse de la transaction.
Web Reputation Actions (Breakdown by Score) [Actions de réputation Web (répartition par score de réputation)]	Affiche les scores de réputation Web décomposés pour chaque action.

Page L4 Traffic Monitor (Supervision du trafic de la couche 4)

La page **Reporting> L4 Traffic Monitor** (Rapports > Supervision du trafic de la couche 4) est une page de rapports de sécurité qui affiche des informations sur les ports et les sites malveillants que le processus de supervision du trafic de la couche 4 a détectés au cours de la plage de temps spécifiée. Cette page affiche également les adresses IP des clients qui rencontrent fréquemment des sites malveillants.

La supervision du trafic de la couche 4 écoute le trafic réseau qui arrive par tous les ports de l'appliance et fait correspondre les noms de domaine et les adresses IP avec les entrées de ses propres tables de base de données pour déterminer s'il faut autoriser le trafic entrant et sortant.

Section	Description
Time Range (Plage de temps) (liste déroulante)	Menu qui vous permet de choisir la plage de temps sur laquelle doit porter le rapport.
Top Client IPs (Principales adresses IP client)	Affiche, au format graphique, les adresses IP des ordinateurs de votre organisation qui se connectent le plus souvent aux sites malveillants.
Top Malware Sites (Principaux sites malveillants)	Affiche, au format graphique, les principaux domaines de programmes malveillants détectés par la supervision du trafic de la couche 4.
Client Source IPs (Adresses IP source client)	Affiche les adresses IP des ordinateurs de votre entreprise qui se connectent fréquemment à des sites malveillants.
Malware Ports (Ports de programmes malveillants)	Affiche les ports sur lesquels la supervision du trafic de la couche 4 a le plus souvent détecté des programmes malveillants.
Malware Sites Detected (Sites malveillants détectés)	Affiche les domaines dans lesquels la supervision du trafic de la couche 4 détecte le plus souvent des programmes malveillants.

Page SOCKS Proxy (Serveur mandataire SOCKS)

La page **Reporting > SOCKS Proxy** (Rapports > Serveur mandataire SOCKS) vous permet d'afficher les données et les tendances pour les transactions traitées par l'intermédiaire du mandataire SOCKS, notamment des informations sur les principales destinations et les principaux utilisateurs.

Page Reports by User Location (Rapports par emplacement des utilisateurs)

La page **Reporting > Reports by User Location** (Rapports > Rapports par emplacement d'utilisateur) vous permet de découvrir les activités de vos utilisateurs locaux et distants.

Les activités sont les suivantes :

- Catégories d'URL auxquelles accèdent les utilisateurs locaux et distants.
- Activité de la solution de protection contre les programmes malveillants déclenchée par les sites auxquels accèdent les utilisateurs locaux et distants.
- Réputation Web des sites consultés par les utilisateurs locaux et distants.
- Applications auxquelles les utilisateurs locaux et distants accèdent.
- Utilisateurs (locaux et distants).
- Domaines accessibles par les utilisateurs locaux et distants.

Section	Description
Time Range (Plage de temps) (liste déroulante)	Menu qui permet de choisir la plage de temps des données contenues dans le rapport.

Section	Description
Total Web Proxy Activity: Remote Users (Activité totale du proxy Web : utilisateurs à distance)	Affiche l'activité de vos utilisateurs à distance (vertical) au cours de la période spécifiée (horizontal).
Web Proxy Summary (Résumé du proxy Web)	Affiche un résumé des activités des utilisateurs locaux et distants sur le réseau.
Total Web Proxy Activity: Local Users (Activité totale du proxy Web : utilisateurs locaux)	Affiche l'activité de vos utilisateurs à distance (vertical) au cours de la période spécifiée (horizontal).
Suspect Transactions Detected: Remote Users (Transactions suspectes détectées : utilisateurs à distance)	Affiche les transactions suspectes qui ont été détectées en raison des politiques d'accès définies pour les utilisateurs à distance (vertical) sur la période précisée (horizontal).
Suspect Transactions Summary (Résumé des transactions suspectes)	Affiche un résumé des transactions suspectes des utilisateurs à distance sur le réseau.
Suspect Transactions Detected: Local Users (Transactions suspectes détectées : utilisateurs locaux)	Affiche les transactions suspectes qui ont été détectées en raison des politiques d'accès définies pour vos utilisateurs à distance (vertical) au cours de la période spécifiée (horizontal).
Suspect Transactions Summary (Résumé des transactions suspectes)	Affiche un résumé des transactions suspectes des utilisateurs locaux sur le réseau.

Page Web Tracking (Suivi Web)

Utilisez la page de suivi Web pour rechercher et obtenir des détails sur des transactions individuelles ou des tendances de transactions qui peuvent être problématiques. Selon vos besoins, effectuez une recherche dans l'un des onglets suivants :

Page Web Tracking (Suivi Web)	Lien vers la tâche
Transactions processed by the Web Proxy (Transactions traitées par le proxy Web)	Recherche de transactions traitées par le proxy Web , on page 13
Transactions processed by the L4 Traffic Monitor (Transactions traitées par la supervision du trafic de la couche 4)	Recherche de transactions traitées par la supervision du trafic de la couche 4 , on page 15
Transactions processed by the SOCKS Proxy (Transactions traitées par le proxy SOCKS)	Recherche de transactions traitées par le serveur proxy SOCKS , on page 16

Vous pouvez également utiliser le nom de domaine complet pour rechercher des données de site Web dans la page **Web Tracking** (Suivi Web) pour certains cas, comme l'interconnexion transparente.

Note Une demande transparente affiche le nom du domaine ou du serveur sur la page de suivi. Cependant, lorsque des demandes transparentes, y compris l'intercommunication transparente, sont envoyées sans SNI, l'adresse IP est affichée.

Recherche de transactions traitées par le proxy Web

Vous pouvez utiliser l'onglet **Proxy Services** (Services proxy) sur la page **Reporting > Web Tracking** (Rapports > Suivi Web) pour suivre et produire un rapport sur l'utilisation du Web pour un utilisateur en particulier ou pour tous les utilisateurs.

Vous pouvez afficher les résultats de la recherche pour le type de transactions enregistrées (bloquées, surveillées, ayant fait l'objet d'un avertissement et terminées) pendant une période particulière. Vous pouvez également filtrer les résultats de données en utilisant plusieurs critères, tels que la catégorie d'URL, le programme malveillant et l'application.

Note Le proxy Web fournit uniquement des rapports sur les transactions qui comprennent une balise de décision ACL autre que OTHER-NONE.

Étape 1 Choisissez **Reporting > Web Tracking** (Rapports > Suivi Web).

Étape 2 Cliquez sur l'onglet **Proxy Services** (Services proxy).

Étape 3 Configurez les paramètres.

Paramètres	Description
Time Range (Plage de temps)	Choisissez la plage de temps sur laquelle porte le rapport.
IP de l'utilisateur ou du client	(Facultatif) Saisissez le nom d'utilisateur d'authentification tel qu'il apparaît dans les rapports ou une adresse IP du client que vous souhaitez suivre. Vous pouvez également saisir une plage d'adresses IP au format CIDR. Si vous laissez ce champ vide, la recherche renvoie des résultats pour tous les utilisateurs.
Website (Site Web)	(Facultatif) Saisissez un site Web que vous souhaitez suivre. Lorsque vous laissez ce champ vide, la recherche renvoie des résultats pour tous les sites Web. **Note** Vous pouvez rechercher les termes SNI (Server Name Indication). SNI, une extension du protocole TLS, permet aux clients de spécifier en toute sécurité des noms d'hôte lors de transactions Web. Vous devez spécifier des mots entiers. Pour que le SNI fonctionne, Cisco Secure Endpoint et les services de réputation doivent être activés.
Transaction Type (Type de transaction)	Choisissez le type de transactions que vous souhaitez suivre, soit All Transactions (Toutes les transactions), Completed (Terminé), Blocked (Bloqué), Monitored (Surpervisé) ou Warned (Ayant fait l'objet d'un avertissement).

Étape 4 (Facultatif) Développez la section Advanced (Avancé) et configurez les champs pour filtrer les résultats du suivi Web avec des critères plus avancés.

Paramètres	Description
URL Category (Catégorie URL)	Pour filtrer les données par catégorie d'URL, sélectionnez **Filter by URL Category** (Filtrer par catégorie d'URL) et saisissez la première lettre de la catégorie d'URL en fonction de laquelle effectuer le filtrage. Choisissez la catégorie dans la liste qui apparaît.
Application	Pour filtrer les données par application, sélectionnez **Filter by Application** (Filtrer par application) et choisissez une application en fonction de laquelle effectuer le filtrage. Pour filtrer les données par type d'application, sélectionnez **Filter by Application Type** (Filtrer par type d'application) et choisissez un type d'application selon lequel effectuer le filtrage.
Policy (Politique)	Pour filtrer les données par nom de la politique responsable de la décision finale pour cette transaction, sélectionnez **Filter by Action Policy** (Filtrer par politique d'action) et saisissez un nom de groupe de politiques [Access Policy (Politique d'accès), Decryption Policy (Politique de déchiffrement) ou Data Security Policy (Politique de sécurité des données)] selon lequel effectuer le filtrage. Consultez la description de PolicyGroupName dans la section Informations sur le proxy Web dans les fichiers journaux d'accès pour de plus amples renseignements.
Cisco Secure Endpoint	Consultez À propos du suivi des messages et des fonctionnalités de Cisco Secure Endpoint.
Malware Threat (Programmes malveillants)	Pour filtrer les données par programme malveillant spécifique, sélectionnez **Filter by Malware Threat** (Filtrer par programme malveillant) et entrez le nom du programme malveillant selon lequel effectuer le filtrage. Pour filtrer les données par catégorie de programmes malveillants, sélectionnez **Filter by Malware Category** (Filtrer par catégorie de programmes malveillants) et choisissez une catégorie de programmes malveillants en fonction de laquelle effectuer le filtrage.
WBRS	Dans la section WBRS, vous pouvez filtrer les données par score de réputation de sites Web et par menace particulière pour la réputation de sites Web. • Pour filtrer les données par score de réputation Web, sélectionnez **Score range** (Plage de score de réputation), puis les valeurs supérieure et inférieure selon lesquelles effectuer le filtrage. Vous pouvez également filtrer les sites Web qui n'ont aucun score de réputation en sélectionnant **No Score** (Aucun score de réputation). • Pour filtrer les données par menace pour la réputation Web, sélectionnez **Filter by Reputation Threat** (Filtrer par menace pour la réputation) et saisissez une menace pour la réputation Web en fonction de laquelle effectuer le filtrage.
AnyConnect Secure Mobility	Pour filtrer les données selon l'emplacement des utilisateurs (distants ou locaux), sélectionnez **Filter by User Location** (Filtrer par emplacement des utilisateurs) et choisissez le type d'utilisateur selon lequel effectuer le filtrage.
User Request (Demande utilisateur)	Pour filtrer les données selon les transactions initiées par le client, sélectionnez **Filter by User-Demanded Transactions** (Filtrer selon les transactions demandées par l'utilisateur). **Note** Lorsque vous activez ce filtre, les résultats de la recherche incluent des transactions de type « meilleure estimation ».

Paramètres	Description
Encapsulated URL Protection (Protection encapsulée pour les URL)	Activez ce filtre pour les transactions URL encapsulées. **Note** • Vous devez activer le proxy HTTPS. Voir la section Activation du proxy HTTPS. • Assurez-vous que la plage du score de réputation Web pour https://translate.google.com est définie sur decrypt (déchiffrer). Voir la section Configuration des paramètres de filtre de réputation Web pour les groupes de politiques de déchiffrement.

Étape 5 Cliquez sur **Search** (Recherche).

Les résultats sont triés par horodatage, le plus récent en premier.

Le nombre entre parenthèses sous le lien « Display Details » (Afficher les détails) désigne le nombre de transactions connexes générées par la transaction initiée par l'utilisateur, telles que les images chargées, les scripts javascript exécutés et les sites secondaires consultés.

Étape 6 (Facultatif) Cliquez sur **Display Details** (Afficher les détails) dans la colonne Transactions pour afficher des renseignements plus détaillés sur chaque transaction.

Note Si vous devez afficher plus de 1000 résultats, cliquez sur le lien de **Printable Download** (Téléchargement imprimable) pour obtenir un fichier CSV qui comprend l'ensemble complet des données brutes, à l'exclusion des détails des transactions connexes.

Tip Si une URL dans les résultats est tronquée, vous pouvez trouver l'URL complète dans le journal des accès.

Pour afficher les détails de jusqu'à 500 transactions connexes, cliquez sur le lien **Related Transactions** (Transactions connexes).

What to do next

- Mises à jour et rapports des ensembles de catégories d'URL , on page 6
- Descriptions des catégories de programmes malveillants
- À propos du suivi des messages et des fonctionnalités de Cisco Secure Endpoint

Recherche de transactions traitées par la supervision du trafic de la couche 4

L'onglet L4 Traffic Monitor (Supervision du trafic de la couche 4) de la page **Reporting > Web Tracking** (Rapports > Suivi Web) fournit des détails sur les connexions aux ports et aux sites de programmes malveillants. Vous pouvez rechercher des connexions vers des sites de programmes malveillants à l'aide des types d'informations suivants :

- Plage de temps
- Site, utilisant l'adresse IP ou le domaine
- Port

- Adresse IP associée à un ordinateur au sein de votre organisation
- Type de connexion

Les 1000 premiers résultats de recherche correspondants s'affichent.

Recherche de transactions traitées par le serveur proxy SOCKS

Vous pouvez rechercher des transactions qui répondent à divers critères, notamment des transactions bloquées ou terminées; les utilisateurs; et le domaine de destination, l'adresse IP ou le port de destination.

Étape 1 Choisissez **Web > Reporting > Web Tracking** (Web > Rapports > Suivi Web).

Étape 2 Cliquez sur l'onglet **SOCKS Proxy** (Proxy SOCKS).

Étape 3 Pour filtrer les résultats, cliquez sur **Advanced** (Avancé).

Étape 4 Saisissez les critères de recherche.

Étape 5 Cliquez sur **Search** (Recherche).

What to do next

Page SOCKS Proxy (Serveur mandataire SOCKS) , on page 11

Page System Capacity (Capacité du système)

La page **Reporting > System Capacity** (Rapports > Capacité du système) affiche des informations actuelles et historiques sur l'utilisation des ressources dans la Secure Web Appliance.

Lors du choix des plages de temps pour l'affichage des données sur la page System Capacity (Capacité du système), il est important de vous rappeler les éléments suivants :

- **Hour Report** (Rapport horaire). Le rapport sur les heures interroge la table des minutes et affiche le nombre exact d'éléments, tels que les octets et la connexion, qui ont été enregistrés par l'appliance minute par minute sur une période de 60 minutes.
- **Day Report** (Rapport journalier). Le rapport journalier interroge la table des heures et affiche le nombre exact d'éléments, tels que les octets et la connexion, qui ont été enregistrés par l'appliance sur une base horaire pendant une période de 24 heures. Ces informations sont recueillies à partir de la table des heures.

Le rapport hebdomadaire et le rapport sur 30 jours fonctionnent de manière similaire aux rapports horaire et journalier.

Page System Status (État du système)

Utilisez la page **Reporting> System Status** (Rapports > État du système) pour surveiller l'état du système. Cette page affiche l'état et la configuration actuels de Secure Web Appliance.

Cette section...	Écrans
État Secure Web Appliance	• Disponibilité du système • Utilisation des ressources système : utilisation du processeur, de la RAM et pourcentage d'espace disque utilisé pour les rapports et la journalisation. La valeur d'utilisation du processeur affichée sur cette page et la valeur du processeur affichée sur la page de présentation du système (Page Overview (Survol), on page 1) peuvent différer légèrement, car elles sont lues séparément, à des moments différents. L'utilisation de la RAM pour un système qui fonctionne efficacement peut être supérieure à 90 %, car la RAM qui n'est pas autrement utilisée par le système est utilisée par le cache d'objets Web. Si votre système ne connaît pas de problèmes de performances graves et que cette valeur n'est pas bloquée à 100 %, le système fonctionne normalement. **Note** La mémoire tampon du proxy est un composant qui utilise cette RAM.
Proxy Traffic Characteristics (Caractéristiques du trafic du proxy)	• Transactions par seconde • Bande passante • Temps de réponse • Ratio de résultats du cache • Connexions
Dérivation du trafic Web	Utilisation du processeur de dérivation du trafic Web.
High Availability (Haute disponibilité)	État du service à haute disponibilité.
Services externes	• Identity Service Engine (ISE)

Cette section...	Écrans
Configuration actuelle	Paramètres du proxy Web : • Web Proxy Status (État du proxy Web) : activé ou désactivé. • Deployment Topology (Topologie du déploiement). • Web Proxy Mode (Mode du proxy Web) : direct ou transparent. • IP Spoofing (Usurpation d'adresses IP) : activée ou désactivée. Paramètres de supervision du trafic de la couche 4 : • L4 Traffic Monitor Status (État de la supervision du trafic de la couche 4) : activé ou désactivé. • L4 Traffic Monitor Wiring (Câblage pour la supervision du trafic de la couche 4). • L4 Traffic Monitor Action (Action de supervision du trafic de la couche 4) : superviser ou bloquer. Paramètres de dérivation du trafic Web : • Web Traffic Tap Status (État de la dérivation du trafic Web) : activé ou désactivé • Web Traffic Tap Interface (Interface de dérivation du trafic Web) : P1, P2, TI ou T2 Information de version de Secure Web Appliance Informations sur le matériel

Thèmes connexes

Page System Capacity (Capacité du système), on page 16

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.