Didacticiel de démarrage rapide pour les nouveaux utilisateurs

Solutions Websense® Web Security

v7.7

10240 Sorrento Valley Rd., San Diego, CA 92121, États-Unis

Publié en 2012
Imprimé aux États-Unis et en Irlande

Marques déposées

Table des matières

1 Bienvenue

Bienvenue dans les solutions Websense® Web Security.

Ce didacticiel de démarrage rapide va vous permettre de découvrir les bases de la gestion des stratégies et de la génération de rapports. Ce didacticiel se compose d'une suite de brèves leçons, divisées en 4 sections :

Configuration initiale	Gestion des stratégies
Conseils de navigation	Génération de rapports

Chaque leçon dure entre 5 et 10 minutes.

Pour commencer, cliquez sur votre rôle ci-dessous.

- Si votre organisation n'utilise pas ou n'a pas encore configuré de rôles d'administration déléguée, cliquez sur **Super administrateur**.
- Si vous gérez des stratégies pour un groupe spécifique de clients, cliquez sur **Administrateur délégué**.
- Si vous êtes autorisé à générer des rapports pour vos clients gérés, mais que leurs stratégies sont gérées par un autre rôle, cliquez sur **Administrateur de génération de rapports**.

Super administrateur (y compris admin)

Administrateur délégué

Administrateur de génération de rapports

Super administrateur

Si vous êtes un Super administrateur (ou si vous vous êtes connecté(e) avec le compte **admin**), toutes les leçons de ce didacticiel vous concernent :

- Utilisez la section *Conseils de navigation* pour vous familiariser avec l'interface de TRITON - Web Security. Cette section décrit la configuration du filtrage Internet et de la génération de rapports Websense et vous explique comment obtenir de l'aide, le cas échéant.

- *Leçon 1 : Utilisation de TRITON - Web Security*, page 9
- *Leçon 2 : Accès à l'aide*, page 14

- Utilisez la section *Configuration initiale* pour vérifier que la base de données principale a bien été téléchargée.

  Si un autre Super administrateur a déjà configuré votre logiciel Websense, passez à la section suivante.
- Utilisez la section *Gestion des stratégies* pour apprendre à créer et à modifier des filtres et des stratégies et à appliquer des stratégies aux clients.
  - *Leçon 4 : Stratégie Par défaut*, page 19
  - *Leçon 5 : Fonctionnement des clients*, page 21
  - *Leçon 6 : Utilisation d'exemples de stratégie*, page 23
  - *Leçon 7 : Filtrage de sites Web par catégorie*, page 26
  - *Leçon 8 : Création de stratégies personnalisées*, page 27
- Utilisez la section *Génération de rapports* pour découvrir le fonctionnement des options de génération de rapports disponibles et pour activer une option de génération de rapports destinée à améliorer continuellement la base de données principale Websense.
  - *Leçon 9 : Rapports du Tableau de bord*, page 32
  - *Leçon 10 : Rapports de présentation*, page 37
  - *Leçon 11 : Rapports d'investigation*, page 40
  - *Leçon 12 : Real-Time Monitor*, page 45
  - *Leçon 13 : Amélioration de Websense*, page 48

À la fin du didacticiel, la section *Prochaines étapes*, page 51 propose des liens vers d'autres rubriques et ressources, y compris vers la base de connaissances de Websense et vers des didacticiels vidéo en ligne.

Pour revenir ultérieurement à ce didacticiel, cliquez sur le bouton **Aide** dans n'importe quelle page de TRITON - Web Security et développez l'option **Mise en route**.

Administrateur délégué

Si vous êtes un administrateur délégué et que vous pouvez créer des stratégies pour vos clients et exécuter des rapports sur leurs activités, toutes les leçons suivantes vous concernent.

Si vous êtes administrateur délégué et que vous ne disposez que d'autorisations de stratégie, les leçons 1 à 2 et 4 à 8 vous concernent.

Si vous êtes administrateur délégué et que vous êtes autorisé à générer des rapports pour certains ou la totalité des clients de votre entreprise, les leçons 1 à 2 et 9 à 12 vous concernent.

- Utilisez la section *Conseils de navigation* pour vous familiariser avec l'interface de TRITON - Web Security. Cette section décrit la configuration du filtrage et de la génération de rapports de Websense et vous explique comment obtenir de l'aide, le cas échéant.
  - *Leçon 1 : Utilisation de TRITON - Web Security*, page 9
  - *Leçon 2 : Accès à l'aide*, page 14
- Utilisez la section *Gestion des stratégies* pour apprendre à créer et à modifier des filtres et des stratégies et à appliquer des stratégies de filtrage aux clients.
  - *Leçon 4 : Stratégie Par défaut*, page 19
  - *Leçon 5 : Fonctionnement des clients*, page 21
  - *Leçon 6 : Utilisation d'exemples de stratégie*, page 23
  - *Leçon 7 : Filtrage de sites Web par catégorie*, page 26
  - *Leçon 8 : Création de stratégies personnalisées*, page 27
- Utilisez la section *Génération de rapports* pour découvrir le fonctionnement des options disponibles pour les rapports dans Websense. (La dernière leçon de cette section, la Leçon 13, ne concerne que les Super administrateurs.)
  - *Leçon 9 : Rapports du Tableau de bord*, page 32
  - *Leçon 10 : Rapports de présentation*, page 37
  - *Leçon 11 : Rapports d'investigation*, page 40
  - *Leçon 12 : Real-Time Monitor*, page 45

À la fin du didacticiel, la section *Prochaines étapes*, page 51 propose des liens vers d'autres rubriques et ressources, y compris vers la base de connaissances de Websense et vers des didacticiels vidéo en ligne.

Pour revenir ultérieurement à ce didacticiel, cliquez sur le bouton **Aide** dans n'importe quelle page de TRITON - Web Security et développez l'option **Mise en route**.

Administrateur de génération de rapports

Si vous êtes administrateur avec un ou plusieurs rôles de rapports d'investigation, et que vous êtes autorisé à générer des rapports pour des clients dont les stratégies sont gérées par d'autres rôles, les leçons suivantes vous concernent :

- *Leçon 1 : Utilisation de TRITON - Web Security*, page 9
- *Leçon 2 : Accès à l'aide*, page 14
- *Leçon 11 : Rapports d'investigation*, page 40

Pour revenir ultérieurement à ce didacticiel, cliquez sur le bouton **Aide** dans n'importe quelle page de TRITON - Web Security et développez l'option **Mise en route**.

2 Conseils de navigation

TRITON™ Unified Security Center est l'interface administrative du logiciel Websense. Il permet d'accéder aux paramètres de configuration, aux outils de filtrage et aux fonctions de génération de rapports.

Cette section comprend 2 leçons qui vous aideront à naviguer rapidement dans Websense :

- La *Leçon 1 : Utilisation de TRITON - Web Security* introduit le module Web Security de TRITON Unified Security Center, en insistant sur les outils et les raccourcis utiles.
- La *Leçon 2 : Accès à l'aide* présente les ressources d'aide disponibles dans TRITON - Web Security.

Leçon 1 : Utilisation de TRITON - Web Security

Découvrez comment accéder aux fonctions de sécurité Web de votre logiciel Websense via TRITON Unified Security Center.

TRITON Unified Security Center (la console TRITON) est l'interface qui permet d'accéder aux fonctions de configuration, d'administration et de génération de rapports de votre logiciel Websense. Un administrateur peut être autorisé à accéder à un ou plusieurs modules de la console TRITON (Web Security, Data Security et Email Security), et avoir des autorisations spécifiques pour chaque module.

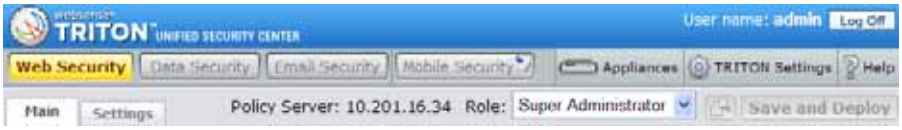
Le compte administratif par défaut de la console TRITON est le compte **admin**. Le mot de passe initial de ce compte est défini pendant l'installation. Ce compte admin dispose d'un accès complet à tous les modules TRITON. Dans le module Web Security, l'accès complet équivaut à des autorisations de Super administrateur inconditionnel.

Si vous êtes connecté en tant qu'administrateur délégué avec des autorisations plus limitées, certaines fonctions (indiquées ci-dessous) risquent d'être invisibles.

Le module Web Security de la console TRITON (TRITON - Web Security) est divisé en 4 sections principales :

	Dans la partie supérieure de l'écran : • La **bannière TRITON** donne des informations sur votre session de connexion. • La **barre d'outils TRITON** permet de passer aisément d'un module à l'autre, d'accéder aux paramètres de TRITON, de lancer Appliance Manager pour tous les dispositifs V-Series enregistrés et d'obtenir de l'aide. • La **barre d'outils Web Security** vous permet de passer d'un serveur Policy Server à l'autre, de changer de rôle administratif et de vérifier et enregistrer les modifications.
	Le **panneau de navigation** (à gauche) permet d'accéder aux fonctions d'état, de génération de rapports et de gestion des stratégies (onglet **Principal**), ainsi qu'aux tâches d'administration du système (onglet **Paramètres**).
	Le **panneau de raccourcis** (à droite) sert à accéder rapidement aux tâches d'administration courantes et aux outils de recherche.
	Le **panneau de contenu** apparaît au centre de la console TRITON. Vos sélections dans le panneau de navigation ou dans le panneau de raccourcis déterminent les éléments qui s'affichent dans le panneau de contenu.

Section 1 : bannière, barre d'outils TRITON et barre d'outils Web Security :



Les fonctions de TRITON - Web Security que vous pouvez voir lorsque vous vous connectez dépendent de votre **rôle** d'administration. La bannière affiche le nom d'utilisateur du compte connecté. Si votre organisation n'utilise pas l'administration déléguée, le compte utilisé est toujours admin, et il a un accès complet à toutes les fonctions de TRITON - Web Security.

La bannière comprend également un bouton **Déconnecter** qui vous permet de mettre fin à votre session.

Juste sous la bannière, la barre d'outils TRITON présente un onglet pour chaque module de la console TRITON. Le module actuel est surligné en jaune, et les autres modules disponibles s'affichent en bleu. Les modules non disponibles apparaissent en gris. La barre d'outils TRITON comprend également les boutons suivants :

- **Appliances**, utilisé pour lancer Appliance Manager pour tous les dispositifs V-Series associés à l'actuel serveur Policy Server.
- **Paramètres TRITON**, utilisé pour exécuter les tâches de configuration qui affectent tous les modules TRITON installés, telles que la création de comptes d'administrateur.

- **Aide**, utilisé pour accéder aux instructions contextuelles et aux matériaux de dépannage, aux didacticiels et aux outils de support en ligne. Vous trouverez davantage d'informations dans la *Leçon 2 : Accès à l'aide*, page 14.

Sous le module, la barre d'outils de Web Security fournit des informations et l'accès aux fonctions qui s'appliquent à toutes les pages de TRITON - Web Security :

- L'adresse IP du serveur **Policy Server** actif

  Lorsque vous ouvrez une session dans TRITON - Web Security, vous vous connectez à un composant logiciel de Websense appelé **Policy Server**. En vous connectant à un serveur Policy Server spécifique, vous choisissez le segment de l'installation Websense à administrer.
- Votre **Rôle** actuel d'administration déléguée.

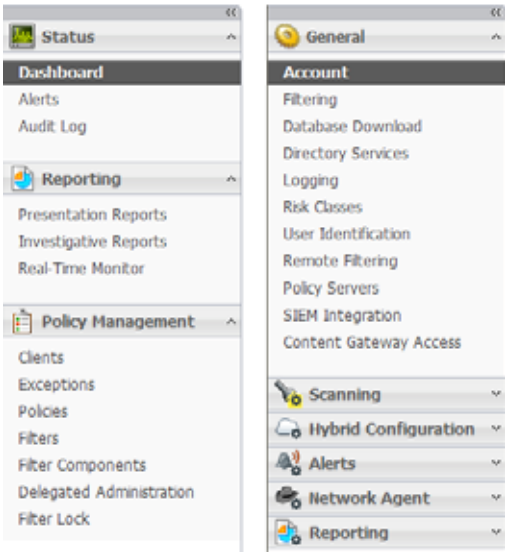
  Lorsque des rôles d'administration déléguée sont définis, les administrateurs qui gèrent plusieurs rôles peuvent utiliser cette liste pour passer d'un rôle à l'autre. Les Super administrateurs peuvent utiliser cette liste pour passer à l'un des rôles qui ont été définis.
- Un bouton **Afficher les modifications en attente** qui s'active lorsque des modifications ont été mises en cache, mais pas encore appliquées.

  Utilisez ce bouton pour vérifier le résumé des modifications mises en cache avant de les enregistrer, ou pour abandonner toutes les modifications en attente.
- Un bouton **Save and Deploy (Enregistrer et déployer)**, dont la couleur indique si des modifications mises en cache sont en attente d'enregistrement.

  Chaque fois que vous exécutez une tâche dans TRITON - Web Security et que vous cliquez sur **OK**, vos modifications sont mises en cache. Vous devez ensuite cliquer sur **Save and Deploy (Enregistrer et déployer)** pour enregistrer et implémenter ces modifications.

Section 2 : Panneau de navigation (à gauche) :

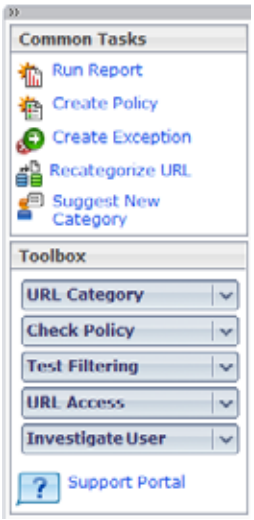
Ce panneau de navigation comprend 2 onglets : Principal (à gauche de l'image ci-dessous) et Paramètres (à droite).



- L'onglet **Principal** permet d'accéder aux informations sur l'état du système, aux fonctions de génération de rapports et aux outils de gestion et de configuration des stratégies. Il est disponible pour tous les administrateurs, mais certains liens de navigation sont masqués pour les Super administrateurs conditionnels et les administrateurs délégués.
- L'onglet **Paramètres** permet d'accéder aux fonctions de gestion des comptes Websense et d'exécuter les tâches globales et locales d'administration du système. Il est masqué pour certains administrateurs et présente des options différentes selon les autorisations.

Pour réduire le panneau de navigation sur la gauche, agrandissez l'espace du panneau de contenu en cliquant sur l'icône en forme de flèche double (<<) au-dessus du groupe État. Lorsque le panneau de navigation gauche est réduit, il affiche une petite icône pour chaque section de l'onglet ouvert. Pour afficher le menu des fonctions de ce groupe, survolez une icône avec votre souris.

Section 3 : Panneau de raccourcis (à droite) :



Pour le compte admin par défaut et les Super administrateurs inconditionnels, le panneau de raccourcis présente toutes les options des sections décrites ci-dessous. Certaines options sont masquées pour les autres administrateurs.

- La section **Tâches communes** fournit des raccourcis vers les tâches administratives les plus utilisées.
  - Cliquez sur **Exécuter le rapport** pour ouvrir directement la page Rapports de présentation et parcourir le catalogue de rapports pour générer un rapport.
  - Cliquez sur **Créer une stratégie** pour ouvrir directement la page Stratégies, puis sur **Ajouter** pour créer une stratégie.
  - Cliquez sur **Create Exception (Créer une exception)** pour accéder directement à la page **Exceptions > Ajouter une exception** afin d'autoriser ou de bloquer une ou plusieurs URL pour tous les clients (exception globale), pour tous les clients d'un rôle d'administration déléguée ou pour un ou plusieurs clients individuels.

- Cliquez sur **Recatégoriser une URL** pour ouvrir la page Composants de filtre > Modifier les catégories, puis sélectionnez la nouvelle catégorie de l'URL que vous souhaitez recatégoriser.
- Cliquez sur **Suggérer une nouvelle catégorie** pour ouvrir le portail MyWebsense. Une fois connecté à MyWebsense, vous êtes dirigé vers l'outil de recherche sur le site. Commencez par identifier la catégorie actuelle du site, puis suggérez une nouvelle catégorie.

◆ La section **Boîte à outils** contient des outils de recherche rapide qui vous permettent de vérifier votre configuration du filtrage.

- Cliquez sur **Catégorie d'URL** pour identifier rapidement la catégorie d'une URL.
- Cliquez sur **Vérifier la stratégie** pour identifier la stratégie actuellement appliquée à un utilisateur.
- Cliquez sur **Tester le filtrage** pour découvrir comment une URL spécifique est actuellement filtrée (autorisée, bloquée, etc.) pour un utilisateur.
- Cliquez sur **Accès à l'URL** pour créer un rapport d'investigation indiquant si un site a été consulté depuis votre réseau au cours des 14 derniers jours.
- Cliquez sur **Analyser l'utilisateur** pour créer un rapport d'investigation indiquant les sites consultés par un utilisateur au cours des 14 derniers jours.

Section 4 : Panneau de contenu :

Le panneau de contenu apparaît au centre de la console TRITON Unified Security Center. Lorsque vous ouvrez TRITON - Web Security pour la première fois, le tableau de bord Web Security apparaît dans le panneau de contenu, présentant des informations sur les activités de contenu malveillant avancé détectées dans votre réseau.

Lorsque vous cliquez sur un lien du panneau de navigation ou du panneau de raccourcis, le panneau de contenu change en fonction de vos sélections. La plupart des pages qui vous permettent d'effectuer des modifications comprennent des boutons **OK** et **Annuler**. Cliquez sur OK pour mettre en cache les modifications apportées à la page, ou sur Annuler pour abandonner ces modifications. Pour enregistrer les modifications mises en cache, cliquez sur **Save and Deploy (Enregistrer et déployer)** dans la barre d'outils de Web Security.

Important

Évitez de double-cliquer ou de triple-cliquer sur les boutons OK et Save and Deploy (Enregistrer et déployer). Plusieurs clics rapides sur le même bouton peuvent provoquer des problèmes d'affichage dans votre navigateur, problèmes qui ne peuvent être résolus qu'en fermant et en rouvrant le navigateur.

La plupart des autres leçons de ce didacticiel de démarrage rapide décrivent l'utilisation des options du panneau de contenu.

Passez à la *Leçon 2 : Accès à l'aide*, page 14.

Leçon 2 : Accès à l'aide

Découvrez comment obtenir des informations et de l'aide lorsque vous avez des questions sur Websense.

Pour vous permettre d'exploiter au mieux votre logiciel Websense, TRITON - Web Security comprend 5 types d'assistance pour les utilisateurs :

1	Une icône  accompagne toutes les fonctions importantes du produit. Placez votre souris sur cette icône pour obtenir une brève description de la fonction.
2	Pour de nombreuses tâches, un texte d'aide s'affiche directement sur la page et fournit des directives ou d'autres conseils sur l'utilisation d'un outil ou d'un champ.
3	Le bouton  fournit un accès à des informations détaillées sur chaque page de TRITON - Web Security, incluant souvent des instructions pour les procédures. Cliquez sur **Aide**, puis sélectionnez **Expliquer cette page**.
4	Pour parcourir le système d'aide de TRITON - Web Security, cliquez sur **Aide**, puis sélectionnez **Sommaire**. Le système d'aide s'affiche dans une nouvelle fenêtre de navigateur ou dans un nouvel onglet. Pour obtenir une version imprimable du système d'aide au format PDF, cliquez sur l'icône  dans la barre d'outils de l'Aide.
5	Si vous ne trouvez pas les informations dont vous avez besoin dans TRITON - Web Security, le menu Aide fournit un lien vers le Portail de support de Websense. Ce portail offre un accès à toutes les ressources techniques des produits et du support client, y compris la documentation, les articles de la base de connaissances et les forums.

Vous avez terminé la section Conseils de navigation de ce didacticiel Démarrage rapide. Passez à la section *Configuration initiale*.

3 Configuration initiale

Cette section comprend 1 leçon :

- *Leçon 3 : Téléchargement de la base de données principale Websense* décrit le rôle de la base de données principale dans le filtrage de Websense et donne des instructions sur la configuration et le déclenchement des téléchargements de la base de données.

  Si vous avez déjà téléchargé la base de données principale et configuré un planning de téléchargement, vous pouvez ignorer cette leçon.

Lorsque vous avez terminé cette section, passez à la leçon *Gestion des stratégies*.

Leçon 3 : Téléchargement de la base de données principale Websense

Cette leçon présente les abonnements et la base de données principale Websense. Elle comprend des instructions sur la saisie d'une clé d'abonnement et sur la création d'un planning de téléchargement de la base de données.

Pour pouvoir terminer ce didacticiel, un administrateur doit saisir la clé d'abonnement utilisée pour activer votre solution de sécurité Web. La saisie de cette clé d'abonnement :

1. Active une version partielle de la base de données principale installée avec toutes les solutions Websense Web Security.
2. Active votre logiciel Websense.
3. Déclenche le téléchargement de la base de données principale Websense, qui contient les dernières définitions de catégories et de protocoles utilisées pour classifier les sites Web et les applications Internet.

Exercice 1 : Saisie de votre clé d'abonnement et configuration des paramètres de téléchargement de la base de données:

1. Connectez-vous à la console TRITON Unified Security Center.
2. Si la clé de votre abonnement n'a pas encore été saisie, une boîte dialogue vous y invite. Entrez cette clé, puis cliquez sur **OK**. La page État > Tableau de bord s'affiche.

   Autrement, passez à l'étape 3.

3. Ouvrez l'onglet **Paramètres** en haut du panneau de navigation à gauche, puis accédez à la page **Compte** (sélectionnée par défaut lorsque vous ouvrez l'onglet Paramètres). Des informations sur votre abonnement Websense apparaissent près de la partie supérieure de la page.

   Les informations complètes sur votre abonnement ne s'affichent pas avant la fin du premier téléchargement de la base de données.

4. Cliquez sur **Téléchargement de la base de données** dans le panneau de navigation. Les informations relatives à la configuration de la base de données apparaissent dans le panneau de contenu.

5. Servez-vous des cases à cocher **Jours de téléchargement** et des listes déroulantes **Délai de téléchargement** pour établir le planning de téléchargement de la base de données principale.

   Par défaut, Websense est configuré pour tenter de télécharger la base de données tous les jours entre 21:00 et 6:00. Ces téléchargements quotidiens vous garantissent que le filtrage s'effectue avec les informations les plus récentes. La base de données doit être téléchargée au moins une fois par semaine.

   > **Remarque**
   >
   > Si vous ne téléchargez pas la base de données principale pendant 14 jours, le filtrage cesse.
   >
   > Lorsqu'aucun jour de téléchargement n'est sélectionné dans la page Téléchargement de la base de données, Websense tente de la télécharger tous les 7 jours.

6. Si votre réseau exige une authentification auprès d'un serveur proxy ou d'un pare-feu, procédez comme suit. Autrement, passez à l'étape 7.
   a. Dans la zone Authentification, située au bas de l'écran, cochez la case **Utiliser l'authentification**.
   b. Entrez le **Nom d'utilisateur** et le **Mot de passe** requis par le serveur proxy ou le pare-feu.

      Il vous faudra peut-être également configurer votree serveur proxy ou votre pare-feu pour qu'il accepte du texte en clair ou une authentification de base.

7. Si votre réseau exige que les navigateurs utilisent un serveur proxy en amont pour accéder à Internet, procédez comme suit. Autrement, passez à l'étape 8.
   a. Dans la section Serveur proxy, cochez la case **Utiliser un serveur proxy ou un pare-feu**.
   b. Entrez le nom ou l'adresse IP du serveur proxy ou de l'ordinateur qui sert de pare-feu dans le champ **IP ou nom du serveur**.
   c. Dans le champ **Port**, entrez le numéro du port utilisé par le serveur proxy ou le pare-feu (le port par défaut est le 8080).

8. Cliquez sur **OK** pour mettre vos paramètres en cache, puis sur **Save and Deploy (Enregistrer et déployer)** dans la barre d'outils pour les implémenter.

Dès que vous avez saisi votre clé d'abonnement, le téléchargement de la base de données principale commence en arrière-plan.

Exercice 2 : Vérification de l'état du téléchargement de la base de données principale

Pour afficher l'état du téléchargement de la base de données ou démarrer un téléchargement manuel à tout moment :

1. Ouvrez l'onglet Principal dans le panneau de navigation à gauche, puis accédez à **État > Tableau de bord** et ouvrez l'onglet **Système**.

   Le Résumé sur les alertes d'état (affiché par défaut en haut du tableau de bord Système) fournit des informations d'ordre général sur l'état du téléchargement.
2. Pour obtenir des informations détaillées sur le téléchargement, cliquez sur **Téléchargement de la base de données** (dans la barre d'outils située en haut de la page).
   - Par défaut, la page Téléchargement de la base de données présente un résumé de tous les ordinateurs Filtering Service, la version de la base de données principale actuellement utilisée dans chacun d'eux et l'état du dernier téléchargement.
   - Pour démarrer manuellement un téléchargement de la base de données à partir de cette page, cliquez sur le bouton **Mettre à jour** d'une instance de Filtering Service. Si une tentative de téléchargement est déjà en cours, ce bouton est désactivé.
3. Cliquez sur une adresse IP de Filtering Service dans la liste située à gauche pour obtenir des informations détaillées sur le téléchargement et sur la progression des téléchargements en cours.
4. Cliquez sur **Fermer** pour revenir à la page Tableau de bord. La fermeture de la page Téléchargement de la base de données n'a aucun effet sur les mises à jour éventuellement en cours.

Important

Si vous possédez Websense Web Security Gateway Anywhere, à la fin du premier téléchargement réussi de la base de données principale, déconnectez-vous de TRITON - Web Security et reconnectez-vous. Ceci permet d'afficher plusieurs pages de paramètres qui sont uniquement disponibles avec Websense Web Security Gateway Anywhere.

Chaque fois qu'une mise à jour de base de données ajoute ou supprime des catégories et des protocoles définis par Websense, vous devez vous déconnecter de TRITON - Web Security et vous reconnecter à nouveau pour voir la liste des catégories et des protocoles mise à jour. Cette mesure de précaution permet de s'assurer que les mises à jour de la base de données n'affectent pas les mises à jour des stratégies éventuellement effectuées par les administrateurs à ce moment.

Une mise à jour de base de données ajoutant ou supprimant des catégories et des protocoles est susceptible de se produire :

- Lorsque vous entrez votre clé d'abonnement pour la première fois et téléchargez la base de données principale.
- Après l'achat d'autres catégories ou protocoles, ou lorsque vous passez de Websense Web Filter à Websense Web Security ou à Web Security Gateway (Anywhere).

De façon générale, les ajouts et les suppressions de catégories ou de protocoles sont rares, et vous serez prévenus plusieurs semaines avant leur mise à jour. Si vous avez configuré Websense pour qu'il signale les alertes système aux administrateurs, une notification vous signale l'ajout ou la suppression de catégories et de protocoles.

Vous avez terminé la section Configuration initiale de ce didacticiel Démarrage rapide. Passez à la section *Gestion des stratégies*.

4 Gestion des stratégies

Cette section comprend 5 leçons :

- La *Leçon 4 : Stratégie Par défaut* présente la stratégie qui joue le rôle de filet de sécurité en gérant l'accès à Internet des clients qui ne sont pas explicitement attribués à une autre stratégie.
- La *Leçon 5 : Fonctionnement des clients* décrit l'ajout d'utilisateurs, de groupes et d'ordinateurs en tant que clients du filtrage dans TRITON - Web Security.
- La *Leçon 6 : Utilisation d'exemples de stratégie* présente les stratégies prédéfinies livrées avec le logiciel Websense et la procédure de modification des stratégies.
- La *Leçon 7 : Filtrage de sites Web par catégorie* présente le concept de filtres de catégories et vous guide tout au long de la procédure de création de vos propres filtres personnalisés.
- La *Leçon 8 : Création de stratégies personnalisées* vous montre comment développer vos propres stratégies et les imposer aux clients.

Leçon 4 : Stratégie Par défaut

Découvrez la stratégie qui joue le rôle de filet de sécurité en gérant l'accès à Internet des clients auxquels aucune autre stratégie n'est attribuée.

Pour déterminer comment et à quel moment les requêtes Internet sont filtrées pour les utilisateurs, les groupes, les ordinateurs et les réseaux, les solutions de sécurité Web de Websense utilisent des **stratégies**. Chaque stratégie comprend des informations sur les sites Web et les protocoles de communication Internet bloqués ou autorisés, et les jours et les heures auxquels ces règles doivent être imposées.

Votre logiciel Websense inclut une stratégie **Par défaut**, appliquée 24 heures sur 24, 7 jours sur 7. Au départ, cette stratégie surveille le trafic Internet sans appliquer de

blocage. Lorsque vous installez Websense pour la première fois, la stratégie Par défaut s'applique à tout le monde sur le réseau.

> **Remarque**
> Si votre organisation utilise l'administration déléguée, chaque rôle possède sa propre stratégie Par défaut. La stratégie Par défaut d'un rôle est imposée à tous les clients de ce rôle auxquels aucune autre stratégie n'a été attribuée.

Exercice : Découverte de la stratégie Par défaut

1. Dans TRITON - Web Security, ouvrez l'onglet Principal dans le panneau de navigation, puis sélectionnez **Stratégies**, sous Gestion des stratégies.

   La liste des stratégies existantes apparaît.
2. Cliquez sur **Par défaut** pour afficher les détails de cette stratégie dans la page Modifier la stratégie.
3. Examinez la section supérieure du panneau de contenu.
   - Le nom de la stratégie s'affiche, suivie d'une brève description de son objectif.
   - Un résumé des clients régis de façon spécifique par cette stratégie apparaît également. Notez que, même lorsqu'aucun client n'apparaît dans la liste, la stratégie **Par défaut** s'applique à tout client non géré par une autre stratégie.
4. Examinez la section **Planification**.
   - Après une nouvelle installation, les colonnes Heure de début, Heure de fin et Jours montrent que la stratégie **Par défaut** est appliquée 24 heures sur 24 et 7 jours sur 7.
   - La colonne Filtre de catégories/d'accès limité montre que le filtrage de catégories **Surveiller uniquement** est en vigueur.

     Un **filtre de catégories** est une liste des catégories et des actions (par exemple Autoriser ou Bloquer) qui leurs sont attribuées. Le filtre de catégories imposé par une stratégie détermine le traitement des requêtes de sites Web des utilisateurs.

     Il existe une alternative au filtre de catégories. Il s'agit d'un **filtre d'accès limité**, ou liste des URL spécifiques auxquelles les utilisateurs ont accès. Lorsqu'un filtre d'accès limité est imposé par une stratégie, les utilisateurs régis par cette stratégie ne peuvent consulter que les sites de cette liste.
   - La colonne Filtre de protocoles montre que le filtrage de protocole **Surveiller uniquement** est en vigueur.

     Un **filtre de protocoles** est une liste de protocoles (généralement non HTTP) et des actions (par exemple Autoriser ou Bloquer) qui leur sont attribuées. Lorsque Network Agent est installé, le filtre de protocoles imposé par une stratégie détermine le traitement des tentatives d'accès à des protocoles spécifiques par les utilisateurs (par exemple aux protocoles utilisés pour la messagerie instantanée ou pour le partage de fichiers en peer-to-peer).

5. Deux colonnes apparaissent au-dessous du planning de la stratégie. Examinez la colonne Filtre de catégories.
   - Le nom du filtre de catégories actuel s'affiche à côté de la description de la colonne.
   - Vous pouvez parcourir la liste pour voir quelles catégories sont autorisées et bloquées. En bas de la page, une légende décrit les icônes qui s'affichent à côté de chaque catégorie.

   Vous apprendrez à créer et à modifier les filtres de catégories dans une prochaine leçon.

Dans les leçons suivantes, vous allez apprendre à exploiter les stratégies et leurs éléments essentiels. Vous pouvez maintenant mettre en pratique ce que vous avez appris pour modifier la stratégie Par défaut en fonction des besoins de votre organisation.

Passez à la *Leçon 5 : Fonctionnement des clients*, page 21.

Leçon 5 : Fonctionnement des clients

Découvrez les clients utilisateur, ordinateur et réseau, puis entraînez-vous à ajouter des clients dans TRITON - Web Security.

Les stratégies de filtrage sont appliquées à des clients : utilisateurs, groupes et domaines de votre service d'annuaire ou plages d'ordinateurs et de sous-réseaux de votre réseau.

- Un **ordinateur** constitue le type de client le plus simple. Il s'agit d'une machine située sur le réseau, identifiée par une adresse IP.
- Un **réseau** est un groupe d'ordinateurs identifié par une plage d'adresses IP contiguës.
- Un client **d'annuaire** peut être un utilisateur, un groupe, un domaine ou une unité d'organisation (UO) défini(e) dans votre service d'annuaire. Des informations supplémentaires sur les services d'annuaire sont disponibles dans la section Clients du système d'aide de TRITON - Web Security.

Exercice 1 : Ajout d'un client ordinateur

1. Dans TRITON - Web Security, sélectionnez **Clients** (sous Gestion des stratégies) dans le panneau de navigation.
2. Sous l'arborescence des Clients, cliquez sur **Ajouter**. La page Ajouter des clients apparaît.
3. Entrez l'**adresse IP** de l'ordinateur que vous souhaitez ajouter en tant que client, puis cliquez sur la flèche droite (>) pour ajouter ce client dans la liste Clients sélectionnés.

Si vous êtes un administrateur délégué, vous ne pouvez ajouter que des adresses IP attribuées à votre rôle en tant que clients gérés. Ouvrez la liste **Gestion des stratégies > Administration déléguée** et cliquez sur le nom de votre rôle pour voir la liste des clients gérés associés à votre rôle.

4. Cliquez sur **OK** pour mettre en cache vos modifications et revenir à la page Clients.
5. Développez le nœud **Ordinateurs** dans l'arborescence Clients. L'adresse IP que vous venez d'ajouter apparaît dans la liste.

   Des informations sur les paramètres appliqués au nouveau client s'affichent à droite de son adresse IP. La colonne **Stratégie** indique que ce client est actuellement régi par la stratégie **Par défaut**.
6. Cliquez sur **Save and Deploy (Enregistrer et déployer)** pour implémenter vos modifications.

Exercice 2 : Ajout d'un client d'annuaire

Si votre logiciel Websense a été configuré pour récupérer des informations dans un service d'annuaire pris en charge, vous pouvez appliquer des stratégies de filtrage à des utilisateurs, groupes et unités d'organisation (UO).

Des informations sur la configuration de Websense pour qu'il communique avec un service d'annuaire sont disponibles dans la section Clients du système d'aide de TRITON - Web Security Help.

Une fois la configuration terminée, vous pouvez ajouter des clients d'annuaire en utilisant la même page que pour l'ajout de clients ordinateur et réseau :

1. Dans TRITON - Web Security, sélectionnez **Clients** (sous Gestion des stratégies) dans le panneau de navigation.
2. Sous l'arborescence des Clients, cliquez sur **Ajouter**. La page Ajouter des clients apparaît.
3. Pour localiser une entrée dans votre service d'annuaire, procédez de l'une des manières suivantes :
   - Parcourez l'arborescence **Annuaire**.
   - Entrez tout ou partie d'un nom d'utilisateur, de groupe ou de domaine dans le champ de recherche, si disponible, puis cliquez sur **Ok**.
4. Sélectionnez un utilisateur, un groupe ou un domaine à ajouter en tant que client, puis cliquez sur la flèche droite (>) pour ajouter ce client dans la liste Clients sélectionnés.

   Si vous êtes un administrateur délégué, vous ne pouvez ajouter que des utilisateurs attribués à votre rôle en tant que clients gérés. Ouvrez la liste **Gestion des stratégies > Administration déléguée** et cliquez sur le nom de votre rôle pour voir la liste des clients gérés associés à votre rôle.
5. Lorsque l'ajout des utilisateurs est terminé, cliquez sur **OK** pour mettre vos modifications en cache et revenir à la page Clients.
6. Cliquez sur **Save and Deploy (Enregistrer et déployer)** pour implémenter vos modifications.

Développez le nœud **Annuaire** de l'arborescence des clients pour voir la liste des clients utilisateur, groupe, domaine et unité d'organisation actuels.

Dans la leçon suivante, vous allez utiliser un exemple de stratégie pour modifier le filtrage de l'activité Internet des clients.

Passez à la *Leçon 6 : Utilisation d'exemples de stratégie*, page 23.

Leçon 6 : Utilisation d'exemples de stratégie

Servez-vous d'un exemple de stratégie pour apprendre à appliquer des filtres différents aux utilisateurs selon les heures et les jours de la semaine.

Outre la stratégie **Par défaut**, Websense comprend deux exemples de stratégie que vous pouvez utiliser pour découvrir le filtrage de l'activité Internet plus en profondeur.

- La stratégie **Illimité** applique les filtres de catégories et de protocoles **Autoriser tout**, 24 heures sur 24 et 7 jours sur 7. Appliquez cette stratégie aux membres de votre organisation pour lesquels l'activité Internet ne doit jamais être limitée.
- La stratégie **Exemple - Utilisateur standard** montre comment une stratégie peut appliquer des filtres différents selon les moments.

Remarque

Si vous êtes un administrateur délégué et que vous ne voyez pas la stratégie Exemple - Utilisateur standard, demandez à un Super administrateur de copier cet exemple de stratégie dans votre rôle.

Exercice 1 : Application de l'exemple de stratégie à des clients

1. Dans TRITON - Web Security, sélectionnez **Stratégies** (sous Gestion des stratégies) dans le panneau de navigation.

   La liste des stratégies et leur description s'affichent dans le panneau de contenu.
2. Cliquez sur **Exemple - Utilisateur standard** pour afficher cet exemple de stratégie.
3. Sous le nom de la stratégie et la description en haut de la page, regardez si la stratégie est déjà appliquée à des **Clients**.

   Lorsque vous modifiez une stratégie, tous les clients qu'elle gère sont affectés.
4. Examinez la section **Planification** de la stratégie.

   Cette stratégie comprend plusieurs lignes. Chaque ligne correspond à une période de temps. Pour imposer des filtres différents à des heures différentes, ajoutez plusieurs périodes à une stratégie. Dans cet exemple de stratégie :

   - Les filtres de catégories et de protocoles Par défaut sont appliqués de 8:00 à 17:00, du lundi au vendredi.

- Les filtres de catégories et de protocoles De base sont appliqués de 17:00 à 8:00, du lundi au vendredi. Notez que, lorsqu'une période de filtrage va au-delà de minuit, vous devez créer deux périodes : l'une se terminant à 24:00 (minuit) et l'autre commençant à 00:00 (minuit).
- Les filtres de catégories et de protocoles Surveiller uniquement sont appliqués le samedi et le dimanche, et autorisent l'accès à tous les sites.

5. Sélectionnez chaque période l'une après l'autre. Le filtre de catégories et de protocoles imposé pendant cette période apparaît dans la partie inférieure de l'écran.

   Lorsqu'une période est sélectionnée, vous pouvez modifier les filtres imposés pendant cette période dans la page Modifier la stratégie.
6. Pour attribuer cet exemple de stratégie à un client, cliquez sur **Appliquer aux clients** dans la barre d'outils située en haut de l'écran.
7. Parcourez l'arborescence des **Clients** pour identifier celui qui doit être régi par l'exemple de stratégie. Choisissez un client ajouté au cours de la leçon 6 afin de tester les effets de cette modification.
8. Cochez la case accolée à chaque nom de client ou adresse IP, puis cliquez sur **OK** pour mettre en cache vos modifications et revenir à la page Modifier la stratégie.
9. Cliquez sur **Save and Deploy (Enregistrer et déployer)** pour implémenter vos modifications.

Le client sélectionné est à présent filtré par la stratégie Exemple - Utilisateur standard.

Exercice 2 : Vérification manuelle du comportement du filtrage :

Pour évaluer les effets de l'application d'une stratégie à un client, une méthode consiste à accéder à cet ordinateur client ou à se connecter à l'aide de ses identifiants de connexion réseau et d'utiliser un navigateur pour identifier les sites autorisés et bloqués.

Important

Avant de commencer cette leçon, assurez-vous que le téléchargement de la base de données principale Websense soit terminé. Dans TRITON - Web Security, accédez à **État > Tableau de bord**, puis cliquez sur **Téléchargement de base de données** dans la barre d'outils située en haut du panneau de contenu. Vérifiez que l'état du téléchargement est **Successfully updated (Mise à jour réussie)**.

Il vous faudra éventuellement vous déconnecter de TRITON - Web Security, puis vous reconnecter, pour que la nouvelle base de données puisse terminer son chargement.

1. Si vous appliquez l'exemple de stratégie à un client ordinateur de l'exercice précédent, connectez-vous à l'ordinateur filtré par cet exemple de stratégie.

   Si vous appliquez l'exemple de stratégie à un client utilisateur ou groupe, connectez vous à l'aide du compte de l'utilisateur affecté.

2. Ouvrez une fenêtre de navigateur et accédez au site **www.ucsd.edu**.

   Ce site fait partie de la catégorie **Institutions scolaires**, qui est autorisée par les filtres de catégories Par défaut, De base et Surveiller uniquement.

3. Accédez au site **www.calottery.com**.

   Ce site appartient à la catégorie **Jeux de hasard**. Les filtres de catégories De base et Par défaut bloquent tous deux cette catégorie. Si vous effectuez cet exercice du lundi au vendredi, une page de blocage Websense apparaît.

4. Accédez au site **www.amazon.com**.

   Ce site appartient à la catégorie **Shopping**. Si le filtre de catégories Par défaut est appliqué, vous êtes invité à utiliser du temps contingenté pour accéder à ce site. (Des informations sur le temps contingenté sont disponibles à la leçon suivante.) Si le filtre de catégories De base est appliqué, ce site est autorisé.

Lorsque votre exploration des sites autorisés et bloqués par l'exemple de stratégie est terminée, revenez dans TRITON - Web Security.

Exercice 3 : Vérification du comportement du filtrage avec l'outil **Tester le filtrage** :

TRITON - Web Security comprend des outils qui vous permettent de voir comment un client est filtré sans vous connecter avec son compte ni accéder à Internet à partir d'un ordinateur spécifique.

- Vérifiez que la stratégie appropriée est bien appliquée.
- Vérifiez que la stratégie active bloque et autorise les sites comme prévu.

Pour voir si un client demandant un site spécifique peut y accéder :

1. Cliquez sur **Tester le filtrage** dans le panneau de navigation.
2. Pour identifier le client auquel vous avez appliqué la stratégie Exemple - Utilisateur standard, procédez de l'une des manières suivantes :
   - Entrez l'**Adresse IP** d'un client ordinateur.
   - Entrez le nom complet d'un client d'annuaire dans le champ **Utilisateur** ou cliquez sur **Rechercher un utilisateur** pour parcourir l'annuaire ou utiliser sa fonction de recherche. La fonction de recherche n'est disponible que si vous utilisez un service d'annuaire de type LDAP.
3. Entrez l'**URL** d'un site à vérifier.
4. Cliquez sur **Ok**.

Une fenêtre contextuelle présente alors le nom et la description de la catégorie du site, l'action appliquée à ce dernier et la raison de cette action.

Dans les sections suivantes, vous allez apprendre à créer des filtres de catégories personnalisés, puis des stratégies personnalisées pour filtrer les clients.

Passez à la *Leçon 7 : Filtrage de sites Web par catégorie*, page 26.

Leçon 7 : Filtrage de sites Web par catégorie

Découvrez comment les filtres de catégories sont utilisés dans le filtrage Internet, puis créez et modifiez un filtre de catégories personnalisé.

Les filtres de catégories déterminent le traitement des requêtes de sites HTTP, HTTPS, FTP et Gopher.

Chaque site Web est identifié par une adresse IP ou une URL unique. La base de données principale Websense classe ces adresses dans des catégories, telles que Section pour adultes, Enseignement ou Shopping.

Dans un filtre de catégories, une action, telle que **Autoriser** ou **Bloquer**, est attribuée à chaque catégorie. Chaque site de la catégorie est filtré en fonction de l'action que vous attribuez.

Pour vous aider à commencer, Websense fournit plusieurs modèles de filtrage et de filtres de catégories. Vous pouvez modifier les filtres en fonction des besoins de votre organisation, mais pas les modèles. Lorsque vous créez un nouveau filtre, vous pouvez partir d'un modèle ou d'un filtre de catégories existant.

Pour comprendre le fonctionnement des filtres de catégories, imaginez que certains utilisateurs de votre organisation ne soient autorisés à consulter que les sites Web affiliés aux institutions d'enseignement. Effectuez les exercices suivants pour créer un filtre pour ces utilisateurs.

Exercice 1 : Création d'un filtre de catégories Enseignement uniquement

1. Dans TRITON - Web Security, accédez à **Gestion des stratégies > Filtres** dans le panneau de navigation.
2. Dans la section **Filtres de catégories**, cliquez sur **Ajouter**. La page Ajouter un filtre de catégories apparaît.
3. Nommez le nouveau filtre de catégories **Enseignement uniquement**.
4. Entrez la description du filtre (par exemple, « Pour les assistants de recherche, autorise uniquement l'accès aux sites de la catégorie Enseignement »).
5. Sélectionnez le modèle **Bloquer tout** à utiliser comme base du nouveau filtre.
6. Cliquez sur **OK** pour mettre en cache vos modifications et revenir à la page Filtres. Le nouveau filtre apparaît dans la liste Filtres de catégories.

Vous personnaliserez bientôt ce filtre à l'Exercice 2.

Exercice 2 : Modification du filtre de catégories Enseignement uniquement

1. Cliquez sur **Enseignement uniquement** dans la section Filtres de catégories. La page Modifier un filtre de catégories apparaît.
2. Sélectionnez **Enseignement** dans l'arborescence des catégories, puis cliquez sur **Autoriser**. Le bouton Autoriser apparaît sous l'arborescence Catégories.
3. Développez le nœud **Enseignement**. Notez que les sous-catégories Enseignement sont systématiquement bloquées.

4. La catégorie parente **Enseignement** étant toujours sélectionnée, cliquez sur **Appliquer aux sous-catégories**. Toutes les sous-catégories Enseignement (Institutions culturelles, Institutions scolaires, etc.) sont autorisées.
5. Cliquez sur **OK** pour mettre en cache vos modifications et revenir à la page Filtres.
6. Cliquez sur **Save and Deploy (Enregistrer et déployer)** pour implémenter vos modifications.

Après avoir créé des filtres de catégories personnalisés, vous pouvez les ajouter à des stratégies et les appliquer à des clients.

Passez à la *Leçon 8 : Création de stratégies personnalisées*, page 27.

Leçon 8 : Création de stratégies personnalisées

Apprenez à créer des stratégies différentes pour personnaliser le filtrage en fonction de différents groupes de clients.

Créez de nouvelles stratégies pour assouplir la gestion des accès à Internet de vos employés. Au lieu de tenter d'appliquer la stratégie **Par défaut** à tout le monde, créez des stratégies personnalisées pour les différents groupes de clients.

Exercice 1 : Pour créer une nouvelle stratégie, partez d'une stratégie existante.

1. Dans TRITON - Web Security, accédez à **Gestion des stratégies > Stratégies**.
2. Sous la liste des stratégies existantes, cliquez sur **Ajouter**. La page Ajouter une stratégie apparaît.
3. Nommez la nouvelle stratégie **Assistants de recherche**.
4. Décrivez brièvement la nouvelle stratégie (par exemple, « Pour les assistants de recherche, applique le filtre de catégories Enseignement uniquement »).
5. Cochez la case **Baser sur une stratégie existante**, puis sélectionnez la stratégie **Par défaut** dans la liste déroulante.
6. Cliquez sur **OK** pour mettre en cache vos modifications et revenir à la page Modifier la stratégie.

Vous personnaliserez bientôt cette stratégie à l'Exercice 2.

Exercice 2 : Modification de la stratégie Assistants de recherche :

1. Dans la page Modifier la stratégie, sous Planification, développez la liste déroulante **Jours**, puis désélectionnez **Sam** et **Dim**.

   Cette stratégie ne sera appliquée que du lundi au vendredi. Vous pouvez ajouter plusieurs lignes au planning pour qu'une stratégie applique des filtres différents selon les jours ou les heures.
2. Développez la liste déroulante **Filtre de catégories/d'accès limité** et sélectionnez le filtre de catégories **Enseignement uniquement**.

3. Développez la liste déroulante **Filtre de protocoles** et sélectionnez le filtre de protocoles **Par défaut**.

   Les filtres de protocoles sont utilisés pour filtrer les protocoles Internet non HTTP, tels que ceux qu'utilise la messagerie instantanée ou le streaming multimédia. Des informations supplémentaires sur le filtrage des protocoles sont disponibles dans le système d'aide de TRITON - Web Security.

4. Au bas de la section Planification, cliquez sur **Ajouter** pour ajouter une autre ligne au planning.

   Une période par défaut s'affiche dans les colonnes **Début** et **Fin**.

5. Développez la liste déroulante **Jours** et sélectionnez uniquement **Sam** et **Dim**.
6. Dans les colonnes **Filtre de catégories/d'accès limité** et **Filtre de protocoles**, appliquez le filtre **Surveiller uniquement**.

   Le filtre **Surveiller uniquement** autorise et journalise toutes les requêtes Internet.

7. Cliquez sur **OK** pour mettre en cache vos modifications et revenir à la page Stratégies.
8. Cliquez sur **Save and Deploy (Enregistrer et déployer)** pour implémenter vos modifications.

Exercice 3 : Application de la nouvelle stratégie à un client :

Dans la leçon 7, vous avez appris à appliquer des stratégies aux clients à partir de la page Modifier la stratégie. Vous pouvez également appliquer des stratégies aux clients à partir de la page Clients.

1. Dans TRITON - Web Security, cliquez sur **Clients** (sous Gestion des stratégies) dans le panneau de navigation.
2. Développez le nœud approprié dans l'arborescence des clients, puis effectuez l'une des opérations suivantes :
   - Cochez la case accolée au nom du client ou à son adresse IP, puis cliquez sur **Editer**.
   - Cliquez sur le nom ou l'adresse IP du client.

   La page Modifier le client apparaît.

3. Sous Stratégie, ouvrez la liste déroulante **Nom** et sélectionnez **Assistants de recherche**.
4. Cliquez sur **OK** pour mettre vos modifications en cache et revenir à la page Clients.
5. Cliquez sur **Save and Deploy (Enregistrer et déployer)** pour implémenter vos modifications.

Exercice 4 : Vérification de l'application de la nouvelle stratégie au client :

1. Accédez à l'ordinateur auquel vous avez appliqué la stratégie Assistants de recherche.
2. Ouvrez un navigateur et accédez au site **www.ucsd.edu**.

   Le site est autorisé car il est classé dans la catégorie Enseignement > Institutions Scolaires.

3. Accédez ensuite au site **en.wikipedia.org**.

   Le site est également autorisé car il appartient à la catégorie Enseignement > Matériaux de référence.

4. Accédez ensuite à un site de moteur de recherche tel que **www.google.com** ou **www.yahoo.com**.

   Le site est bloqué car il appartient à la catégorie Informatique > Moteurs de recherche et portails.

Vous pouvez également utiliser l'outil Tester le filtrage (selon les descriptions de la Leçon 7, Exercice 3) pour vérifier que la stratégie est bien appliquée correctement.

Si vous disposez d'autorisations de génération de rapports, continuez à la section *Génération de rapports*.

Si vous ne disposez pas de ces autorisations, ce didacticiel est terminé. Consultez la section *Prochaines étapes* pour découvrir d'autres ressources.

5 Génération de rapports

Avant de pouvoir afficher des graphiques dans le tableau de bord de Web Security, ou de générer des rapports d'investigation ou de présentation, vous devez installer un composant essentiel propre à Windows pour les rapports : Log Server. Si Log Server n'est pas installé, passez à la *Leçon 12 : Real-Time Monitor*, page 45.

Real-Time Monitor collecte ses informations auprès d'un autre composant, Usage Monitor, qui est généralement installé avec Policy Server. Si vous avez un accès administratif à Real-Time Monitor, la Leçon 12 vous concerne, même si les autres composants de génération de rapports ne sont pas installés.

Cette section comprend 5 leçons :

- La *Leçon 9 : Rapports du Tableau de bord* présente le Tableau de bord de Web Security, utilisé pour surveiller les activités à risque, les risques de sécurité, l'usage général et l'état du système pour votre déploiement.
- La *Leçon 10 : Rapports de présentation* montre comment générer des rapports prédéfinis et comment les copier pour appliquer des filtres de sélection de données personnalisés, et comment configurer un travail de rapport planifié.
- La *Leçon 11 : Rapports d'investigation* décrit l'affichage interactif des données des journaux, l'identification d'une rubrique spécifique et l'exploration permettant d'obtenir davantage de détails. Vous y apprendrez également à générer et à planifier des rapports.
- La *Leçon 12 : Real-Time Monitor* explique comment surveiller le filtrage Internet actuel dans votre réseau. Elle comprend des informations sur la personnalisation de l'affichage du trafic actuel afin de ne présenter que certains clients, sites, etc.
- La *Leçon 13 : Amélioration de Websense* décrit l'implémentation des fonctions qui vous permettent d'améliorer le filtrage en autorisant le logiciel Websense à envoyer les informations appropriées à Websense, Inc.

Dans les réseaux qui utilisent l'administration déléguée, les Super administrateurs choisissent les personnes autorisées à accéder à ces fonctions.

Leçon 9 : Rapports du Tableau de bord

Obtenez une vue graphique et instantanée de l'état actuel et récent de votre système. Apprenez à personnaliser les informations affichées.

Les graphiques et les informations affichés dans les onglets de la page État > Tableau de bord offrent une vue graphique et instantanée de l'état actuel et récent du système et de l'activité Internet.

Chaque onglet du tableau de bord affiche un ensemble de graphiques et de compteurs par défaut, ainsi que des informations de synthèse.

- Des éléments peuvent être ajoutés et retirés des tableaux de bord Risques, Usage et Système.
  - Chacun de ces tableaux de bord peut afficher jusqu'à 12 éléments.
  - Lorsque vous cliquez sur la plupart des graphiques et des compteurs de ces tableaux de bord, un rapport d'investigation plus détaillé s'affiche.
- Dans tous les tableaux de bord, de nombreux graphiques peuvent être configurés pour inclure différentes périodes, pour afficher différents jeux d'informations (les 5 principaux, les 5 suivants, etc.), pour s'afficher dans différents formats (graphique à barres empilées, graphique à barres, graphique à courbes multi-séries, etc.).

  D'autres options de configuration peuvent être disponibles, selon le tableau de bord ou l'élément sélectionné.
- Les informations des tableaux de bord sont mises à jour toutes les 2 minutes.

Dans les organisations qui utilisent l'administration déléguée, le Super administrateur désigne les utilisateurs autorisés à afficher les graphiques dans le Tableau de bord de Web Security. L'accès au tableau de bord Menaces est configuré indépendamment de l'accès aux tableaux de bord Risques, Usage et Système.

Par défaut, TRITON - Web Security expire après 30 minutes d'inactivité. Pour afficher les mises à jour des tableaux de bord ou travailler dans les autres pages, vous devez vous reconnecter.

Section 1 : Tableau de bord Menaces

Utilisez le tableau de bord Menaces pour vérifier les informations sur les activités suspectes qui ont lieu dans votre réseau. Ce type d'activités est souvent associé à des programmes malveillants avancés.

Le type d'informations et le nombre de détails affichés dépendent de votre niveau d'abonnement. Web Security Gateway ou Web Security Gateway Anywhere est exigé pour afficher des informations sur les menaces sortantes et pour fournir des données d'analyse détaillées à propos des menaces.

- Dans l'onglet Menaces, vous ne pouvez ni ajouter ni retirer des éléments.
- Un clic sur un graphique du tableau de bord Menaces modifie les informations affichées dans le tableau de synthèse, situé en bas de la page. Aucun rapport d'investigation ne s'affiche.

Le tableau de bord Menaces comprend les éléments suivants :

Élément du tableau de bord	Description
Top Security Destinations (Principales destinations de sécurité)	Présente les pays associés aux activités suspectes détectées dans votre réseau. Il peut s'agir de pays hébergeant des sites des catégories associées à des menaces, ou de pays auxquels des programmes malveillants de votre réseau tentent d'envoyer des données. Par défaut, les 5 principaux pays s'affichent. Cliquez sur un pays en surbrillance pour n'afficher que le trafic de cette destination dans le Suspicious Event Summary (Résumé des événements suspects).
Severity Events by Type (Événements de gravité par type)	Présente le nombre de requêtes d'URL bloquées dans des catégories associées à des menaces sous forme graphique. Par défaut, les 5 principales catégories associées à des menaces s'affichent. Cliquez sur une catégorie dans le graphique pour afficher uniquement les requêtes de cette catégorie dans le Suspicious Event Summary (Résumé des événements suspects).
Suspicious Event Summary (Résumé des événements suspects)	Donne des informations sur la gravité, l'utilisateur, l'ordinateur, la catégorie, l'heure et la direction de l'activité Internet éventuellement liée à du contenu malveillant avancé Cliquez sur une gravité, un nom d'utilisateur, une adresse IP ou un nom de périphérique (si disponible ; requiert Web Security Gateway ou Gateway Anywhere) pour ouvrir une page de détails sur l'événement présentant davantage d'informations sur l'activité du type sélectionné.

Les filtres présents en haut du tableau de bord Menaces permettent de limiter les données affichées dans la page à une certaine période ou action (autorisée ou bloquée) ou à un certain niveau de gravité.

Le champ Rechercher de la section Suspicious Event Summary (Résumé des événements suspects) vous permet d'affiner encore davantage les données du tableau.

Section 2 : Tableau de bord Risques

Le tableau de bord Risques vous permet de surveiller les requêtes d'URL autorisées et bloquées de la classe Risques de sécurité. Les éléments suivants s'affichent par défaut :

Élément du tableau de bord	Description
30-Day Risk Trends (Tendances des risques sur 30 jours)	Présente les tendances de blocage des requêtes pour certaines catégories de sécurité et de responsabilité légale. Cliquez sur une courbe de tendances pour ouvrir le tableau de bord Menaces ou un rapport d'investigation (selon la catégorie) présentant davantage d'informations.
Clients with Security Risks (Clients présentant des risques de sécurité)	Présente les ordinateurs qui ont été utilisés pour accéder aux sites de la classe Risques de sécurité. Vous pouvez éventuellement vous assurer ensuite que ces ordinateurs ne sont pas infectés par des virus ou des logiciels espion.
Top Security Risk Categories (Principales catégories de Risques de sécurité)	Présente les catégories de Risques de sécurité qui ont reçu le plus de requêtes Risques de sécurité est une **classe de risques** : un regroupement de catégories dont les caractéristiques sont similaires. Les catégories Risques de sécurité comprennent les catégories Phishing, Logiciels espion et Piratage, entre autres.
Classes de risque	Présente le nombre de requêtes qui ont été autorisées et bloquées pour chaque classe de risques (Risques de sécurité, Responsabilité légale, Productivité, Utilisation professionnelle)
Top Uncategorized (Principaux sites non catégorisés)	Présente les URL non classées par la Base de données principale Websense que les utilisateurs consultent le plus souvent. Ouvrez la page **Tâches communes > Recatégoriser l'URL** pour attribuer une URL à une catégorie de filtrage.
Analyses : Risques de sécurité	Websense Web Security Gateway ou Gateway Anywhere uniquement Présente le nombre de requêtes que l'analyse Content Gateway a affecté à de nouvelles catégories parce que le contenu a été modifié ou que le site a été compromis

Section 3 : Tableau de bord Usage

Le tableau de bord Usage présente les tendances générales de l'activité Internet pour votre organisation. Les éléments suivants s'affichent par défaut :

Élément du tableau de bord	Description
Principaux utilisateurs bloqués	Présente les utilisateurs qui ont demandé le plus d'URL bloquées
Top Requested Categories (Catégories les plus demandées)	Présente les catégories les plus demandées par les utilisateurs en donnant des précisions sur les problèmes potentiels de sécurité, de bande passante ou de productivité
Enforcement Summary (Résumé de l'application)	Présente les demandes récemment autorisées, les demandes bloquées pour les sites appartenant à la classe Risques de sécurité et les autres demandes bloquées
Catégories Web 2.0	Websense Web Security Gateway ou Gateway Anywhere uniquement Présente les principales catégories affectées aux URL Web 2.0 demandées, mesurées par requête
Web 2.0 URL Bandwidth (Bande passante : URL Web 2.0)	Websense Web Security Gateway ou Gateway Anywhere uniquement Présente les URL Web 2.0 qui utilisent le plus de bande passante
Analyses : Catégories principales	Websense Web Security Gateway ou Gateway Anywhere uniquement Présente les principales catégories auxquelles des URL ont été affectées après que l'analyse de Content Gateway ait déterminé qu'elles ne convenaient plus à leur catégorie d'origine

Section 4 : Tableau de bord Système

Le tableau de bord Système donne des informations sur le fonctionnement et l'état général de votre logiciel Web Security. Les éléments suivants s'affichent par défaut :

Élément du tableau de bord	Description
Résumé sur les alertes d'état	Présente de brefs messages d'état ou d'erreur liés aux composants du système. Cliquez sur un message pour obtenir plus de détails et trouver des solutions.
Activité utilisateur : Zoom Trend (Tendance - Zoom)	Présente le nombre de demandes Internet filtrées et traitées dans la Base de données d'activité. L'unité de mesure dépend de la période affichée dans le graphique. Par défaut, l'activité est donnée par intervalle de 3 heures et 30 minutes.
Protocol Bandwidth Use (Bande passante par protocole)	Présente les protocoles (par exemple HTTP, SMTP, BitTorrent ou Spotify) qui utilisent le plus de bande passante
Filtering Service Status (État du service de filtrage)	Répertorie l'état de chaque instance de Filtering Service associée au serveur Policy Server actif
Hybrid Bandwidth Summary (Résumé de la bande passante hybride)	Websense Web Security Gateway Anywhere uniquement Présente la bande passante consommée par les requêtes Internet des utilisateurs filtrés par le service hybride
Hybrid Requests Processed (Requêtes hybrides traitées)	Websense Web Security Gateway Anywhere uniquement Présente le nombre de requêtes Internet, effectuées par les utilisateurs de votre organisation, que le service hybride a autorisées et bloquées

Exercice : Personnalisation des onglets Risques, Usage et Système

Les administrateurs autorisés à consulter les graphiques du tableau de bord Web Security peuvent personnaliser ceux qui sont affichés dans les onglets Risques, Usage et Système.

1. Ouvrez l'onglet Risques, Usage ou Système du tableau de bord Web Security, puis cliquez sur **Add Chart (Ajouter un graphique)** dans la barre d'outils située en haut de la page.

   La page Personnaliser répertorie les éléments disponibles pour le tableau de bord. Un cercle bleu désigne les graphiques et autres éléments (compteurs, résumés) actuellement présents dans l'onglet sélectionné.

   Deux des graphiques répertoriés ne s'affichent pas par défaut dans aucun onglet :

   - **30-Day Value Estimates (Estimations des valeurs sur 30 jours)** évalue les économies de temps et de bande passante réalisées par Websense sur une période de 30 jours (date du jour comprise).

- **Activity Today (Activité du jour)** donne quelques exemples de la protection réalisée par le filtrage Websense dans votre réseau, le nombre total de requêtes traitées jusque-là, le nombre de requêtes bloquées et le nombre de mises à jour de bases de données traitées en temps réel.

2. Sélectionnez un onglet dans la liste déroulante **Add elements to tab (Ajouter des éléments à un onglet)**.
3. Sélectionnez un élément (graphique, compteur, résumé) dans la liste **Éléments du tableau de bord**.
   - Chaque onglet peut afficher jusqu'à 12 éléments.
   - Les éléments déjà présents dans l'onglet sélectionné sont désignés par une icône en forme de cercle bleu.
   - Vous pouvez ajouter plusieurs copies d'un même élément dans un onglet (par exemple, avec une période différente).
4. L'élément sélectionné s'affiche dans le volet **Aperçu**. Actualisez éventuellement le graphique **Nom**, puis les éléments suivants s'ils sont disponibles :
   - **Chart type (Type de graphique)** : la plupart des graphiques peuvent être affichés sous forme de courbes, colonnes et barres multi-séries ou d'histogramme empilés ou non. Certains peuvent être affichés sous forme de graphique à barres, de courbe ou de graphique en secteurs. Les différents types disponibles dépendent des données affichées.
   - **Période** : la plupart des graphiques peuvent porter sur une période variable allant de la date du jour (période de 24 heures commençant à minuit le jour même) à 30 jours ou plus (selon la configuration choisie par le Super administrateur dans la page Paramètres > Génération de rapports > Tableau de bord).
   - **Top (Principaux)** : les graphiques qui présentent des informations sur les principaux utilisateurs, les principales catégories, URL, etc., peuvent généralement afficher jusqu'à 5 valeurs. Vous pouvez choisir d'afficher les 5 valeurs principales ou les valeurs 6 à 10, 11 à 15 ou 16 à 20.

   Pour certains éléments, seul le nom est personnalisable.
5. Cliquez sur **OK** pour implémenter vos modifications et revenir dans la page Tableau de bord.

Passez à la *Leçon 10 : Rapports de présentation*, page 37.

Leçon 10 : Rapports de présentation

Découvrez les rapports de présentation et apprenez à générer des rapports à partir de modèles et à créer des rapports personnalisés.

Les rapports de présentation donnent une vue des informations de filtrage Internet stockées dans la base de données d'activité Websense. Les graphiques prédéfinis et les rapports tabulaires, appelés modèles, simplifient la présentation cohérente des données sur un sujet particulier, par exemple les catégories les plus bloquées au cours d'une période spécifique.

Dans les réseaux qui utilisent l'administration déléguée, les Super administrateurs choisissent les personnes autorisées à accéder à ces fonctions.

Exercice 1 : Création d'un rapport à partir d'un modèle

1. Dans TRITON - Web Security, accédez à **Génération de rapports > Rapports de présentation**.
2. Dans l'arborescence Catalogue de rapports, développez le titre **Activité Internet**, puis sélectionnez le rapport **Principaux sites visités**.

   Immédiatement après l'installation, seuls les modèles de rapport s'affichent dans l'arborescence. Si le logiciel a déjà été utilisé pendant un certain temps, l'arborescence peut également inclure :

   - Les rapports favoris (signalés par une étoile)
   - Les rapports personnalisés
3. Cliquez sur **Exécuter** en haut ou en bas de la liste.
4. Renseignez la page Exécuter le rapport comme suit :

Champ	Description
Date de début Date de fin	Conservez les dates par défaut qui définissent un rapport couvrant les activités du jour.
Format de sortie	Sélectionnez HTML pour afficher le rapport final dans la fenêtre du navigateur.
N premiers	Conservez le paramètre 10 par défaut (le rapport porte sur les 10 premiers sites).

5. Désactivez l'option **Schedule the report to run in the background (Planifier l'exécution du rapport en arrière-plan)**. Le rapport s'affichera au premier plan dans une fenêtre contextuelle.

Conseil

L'exécution des rapports en arrière-plan est généralement plus efficace. Vous pouvez choisir de recevoir une notification par e-mail lorsque le rapport est terminé, puis utiliser la page **Rapports de présentation > Review Reports (Examiner les rapports)** pour accéder au rapport.

6. Cliquez sur **Exécuter**.

   Une fenêtre de progression s'affiche pendant que Websense collecte les enregistrements appropriés dans la base de données d'activité. Websense vous invite ensuite à afficher le rapport dans une nouvelle fenêtre.

Exercice 2 : Création d'un rapport personnalisé et modification du filtre

1. Sélectionnez **Rapports de présentation** dans le panneau de navigation, puis le rapport **Principaux sites visités** sous Activité Internet.
2. Cliquez sur le bouton **Enregistrer sous**.
3. Dans la page Save As New Report (Enregistrer sous forme de nouveau rapport), remplacez le **nom du catalogue Rapport** par **5 nouveaux premiers sites visités**. Ce nom s'affiche dans la page Rapports de présentation.
4. Cliquez sur **Enregistrer et modifier** pour afficher la page Edit Report (Modifier le rapport), qui vous permet de personnaliser les éléments de ce rapport.
5. Acceptez les paramètres par défaut (le rapport porte sur tous les éléments), puis cliquez sur **Suivant** pour parcourir les onglets Clients, Catégories, Protocoles et Actions.

   Lorsque vous générerez vos futurs rapports, ces onglets vous permettront d'affiner leur contenu.
6. Dans l'onglet **Options**, définissez le paramètre **Show only top (Afficher les premiers seulement)** sur **5** pour que le rapport ne présente que les 5 premiers sites consultés. Cliquez ensuite sur **Suivant**.
7. Dans l'onglet **Confirmer**, sélectionnez **Enregistrer et exécuter**, puis cliquez sur **Terminer**.
8. Dans la page Run Report (Exécuter le rapport), définissez le format de sortie sur **HTML**, désactivez l'option **Run the report in the background (Exécuter le rapport en arrière-plan)**, puis cliquez sur **Exécuter**.

   Websense collecte les enregistrements appropriés dans la base de données d'activité, puis affiche le rapport dans une nouvelle fenêtre.

   Les modifications apportées au filtre du rapport sont enregistrées avec le nouveau rapport. Le nouveau nom s'affiche dans la page Rapports de présentation. Chaque fois que vous exécutez ce rapport, il utilise le filtre que vous avez défini.

Exercice 3 : Configuration de la distribution des rapports planifiés

Quelques paramètres de base doivent être configurés avant que vous ne puissiez planifier la distribution des rapports de présentation. Si ces paramètres ont déjà été configurés, passez directement à l'Exercice 4.

S'ils n'ont pas encore été configurés et que vous êtes un Super administrateur, vous pouvez effectuer la configuration. Sinon, demandez à un Super administrateur d'effectuer la configuration avant de passer à l'Exercice 4.

1. Dans TRITON - Web Security, sélectionnez **Paramètres**, puis cliquez sur **Génération de rapports** dans le panneau de navigation de gauche.
2. Cliquez sur **Préférences**.
3. Entrez l'**Adresse de messagerie** à laquelle les rapports doivent être envoyés.
4. Entrez l'adresse IP ou le nom du serveur de messagerie devant distribuer les rapports planifiés aux destinataires du courrier électronique dans le champ **IP ou nom du serveur SMTP**.
5. Cliquez sur **Enregistrer** pour implémenter vos modifications.

Exercice 4 : Planification de l'exécution périodique des rapports

1. Ouvrez l'onglet **Principal**, puis sélectionnez **Génération de rapports > Rapports de présentation**.
2. Cliquez sur **Scheduler (Planificateur)** dans la barre d'outils située en haut de la page.
3. Servez-vous de l'onglet **Planifier le rapport** pour définir les options suivantes. Cliquez ensuite sur **Suivant**.
   - **Nom de tâche :** Test
   - **Modèle de récurrence :** Quotidien
   - **Planifier l'heure :** 10 minutes après l'heure actuelle du système
   - **Planifier la période :** fin après 2 occurrences
4. Dans l'onglet **Sélectionner un rapport**, choisissez le rapport **5 nouveaux premiers sites visités** et cliquez sur la flèche droite (**>**) pour l'envoyer dans la liste **Sélectionné**. Cliquez sur **Suivant**.
5. Dans l'onglet **Intervalle de dates**, sélectionnez **Dates relatives** dans la liste déroulante, puis **Deux dernier(ère)s** et **Jour(s)**. Cliquez sur **Suivant**.
6. Dans l'onglet **Sortie**, définissez les éléments suivants :
   - **Format de fichier :** PDF
   - **Adresses de messagerie des destinataires (Cc) :** entrez votre propre adresse de messagerie.
7. Cliquez sur **Enregistrer une tâche** pour enregistrer et implémenter ce planning.

   10 minutes après, Websense collecte les enregistrements appropriés dans la base de données d'activité, puis crée le report sous forme de fichier PDF qu'il vous envoie ensuite par courrier électronique. Ce rapport sera généré à deux reprises : aujourd'hui et demain.

Passez à la *Leçon 11 : Rapports d'investigation*, page 40.

Leçon 11 : Rapports d'investigation

Découvrez les rapports d'investigation et comment obtenir des informations spécifiques. Générez et modifiez un rapport détaillé et créez des rapports Favoris pouvant être planifiés de façon périodique.

Les rapports d'investigation permettent d'interagir directement avec les informations du filtrage Internet stockées dans la base de données d'activité Websense. Au départ, un graphique à barres présente l'activité du jour par classe de risques. Examinez les zones qui vous intéressent en cliquant sur les éléments appropriés du graphique pour obtenir davantage de détails.

- Faites quelques sélections pour afficher plusieurs niveaux d'informations, par exemple les 5 premiers utilisateurs des 5 premières catégories.

- Une vue détaillée distincte présente les informations associées dans un rapport tabulaire. Vous pouvez personnaliser les colonnes affichées et créer une vue résumée de ce tableau.
- Pour plus d'informations sur les éléments pouvant être affichés dans les rapports d'investigation, consultez la section *Rapports d'investigation de référence*, page 43.

Dans les réseaux qui utilisent l'administration déléguée, les Super administrateurs choisissent les personnes autorisées à accéder à ces fonctions.

Exercice 1 : Localisation de données spécifiques

Vous pouvez explorer les données initialement affichées dans la page Rapports d'investigation (activité du jour par classe de risques) pour découvrir les détails les plus pertinents pour votre organisation.

1. Dans la page **Génération de rapports > Rapports d'investigation**, cliquez sur **Perte de productivité** pour afficher la liste des options d'approfondissement.

   S'il n'y a pas d'entrée Perte de productivité, cela signifie que les clients de votre réseau n'ont pas demandé de sites appartenant à cette classe de risques. Dans ce cas, sélectionnez une autre classe de risques.
2. Cliquez sur **par Catégorie** dans la liste des options.

   Le graphique change pour afficher l'activité du jour dans les catégories attribuées à la classe de risques sélectionnée.
3. Cliquez sur le nom de la première catégorie du graphique (par exemple, **Actualités et médias**) pour afficher une nouvelle liste d'options d'approfondissement.
4. Cliquez sur **Utilisateur** pour que le graphique présente la liste des utilisateurs ayant demandé des sites de la catégorie sélectionnée.

Vous pouvez continuer à sélectionner des options d'approfondissement pour obtenir davantage de détails sur les éléments qui vous intéressent.

Vous pouvez par ailleurs afficher un intervalle de temps différent en choisissant la période désirée ou en saisissant une plage de dates spécifique dans l'option Afficher située au-dessus du graphique, ou modifier la mesure utilisée pour quantifier l'activité en sélectionnant une nouvelle option dans la liste déroulante Mesure située dans la barre d'outils, en haut du panneau de contenu.

Exercice 2 : Création d'un rapport multi-niveaux

À partir d'un rapport de la page principale Rapports d'investigation, vous pouvez définir un second niveau d'informations à afficher. Cela vous permet, par exemple, de comparer les utilisateurs les plus actifs d'une catégorie à ceux d'une autre catégorie.

1. Dans les chemins de navigation accolés à la liste **Utilisation d'Internet par**, cliquez sur **Catégorie**.

   Le graphique présente les catégories de la classe de risques sélectionnée à l'exercice précédent.

2. Dans la barre située au-dessus du graphique, définissez les éléments suivants :
   - Sélectionnez **5 premiers**
   - par **Utilisateur**
   - et afficher **10** résultats
3. Cliquez sur le bouton **Afficher les résultats**.

   Le graphique s'actualise pour n'afficher que les barres des 5 premières catégories. Au-dessous de chaque barre est présentée la liste des 10 utilisateurs ayant demandé le plus de sites de cette catégorie pendant cette période.

Vous pouvez créer un rapport multi-niveaux avec différentes combinaisons de données. Modifiez simplement le graphique à barres pour afficher les données de premier niveau qui vous intéressent, puis définissez le second niveau selon la procédure décrite ci-dessus.

Exercice 3 : Utilisation de rapports détaillés flexibles

Les rapports détaillés flexibles donnent une vue tabulaire des données liées à un élément spécifique du graphique à barres. Vous pouvez modifier l'affichage pour obtenir une vue résumée des mêmes données et modifier les colonnes d'informations affichées.

1. Dans la page principale Rapports d'investigation, sélectionnez **Catégorie** dans la liste **Utilisation d'Internet par**.
2. Cliquez sur la barre ou sur le numéro d'une catégorie indiquant un nombre significatif d'accès.

   Une vue détaillée apparaît, présentant sous forme de tableau le trafic du jour pour la catégorie sélectionnée. Le rapport par défaut comprend les colonnes Utilisateur, Jour, Heure, Nom hôte URL et Accès.
3. Cliquez sur **Modifier le rapport** dans la barre d'outils située en haut du panneau de contenu. Une boîte de dialogue apparaît.
4. Servez-vous des commandes de cette boîte de dialogue pour supprimer la colonne **Heure**, puis ajoutez la colonne **Action**, entre les colonnes Jour et Nom hôte URL.

   Cette boîte de dialogue vous permet de choisir jusqu'à 7 colonnes. Veillez à choisir des colonnes appropriées aux données utilisées dans le rapport, sinon la colonne sera vide.

   Notez que, bien que le rapport présente les accès, Accès n'apparaît pas comme une entrée de la liste. Les rapports sur les accès doivent inclure la colonne Accès placée le plus à droite.
5. Cliquez sur **Appliquer** pour fermer la boîte de dialogue et actualiser le rapport.

   Notez que les nouvelles colonnes s'affichent à présent dans l'ordre spécifié.
6. Cliquez sur **Résumé** dans le coin supérieur droit du panneau de contenu.

   Notez que le rapport actualisé combine tous les accès présentant le même nom d'hôte URL et la même date dans une seule entrée présentant le nombre total des accès.

L'option de rapport Résumé n'est disponible que si la colonne Heure n'est pas affichée. Cette option combine les lignes qui partagent un élément commun.

L'élément combiné dépend des informations utilisées dans le rapport. Dans cet exemple, elle combine les lignes présentant le même nom d'hôte d'URL.

Exercice 4 : Enregistrement et planification de favoris

Les favoris sont des définitions de rapport que vous souhaitez pouvoir reproduire aisément et éventuellement planifier de façon périodique. Vous pouvez enregistrer les rapports affichés dans la page Rapports d'investigation principale ou dans la vue détaillée flexible.

1. Générez un rapport présentant les informations que vous souhaitez pouvoir reproduire aisément.
2. Cliquez sur **Rapports favoris** en haut du panneau de contenu.
3. La page Rapports favoris suggère un nom pour ce rapport. Acceptez le nom proposé ou entrez-en éventuellement un autre.

   Le nom de fichier ne peut contenir que des lettres, des chiffres et des caractères de soulignement (_).
4. Cliquez sur **Ajouter** pour enregistrer le rapport en tant que Favori.
5. Sélectionnez le rapport ajouté dans la liste, puis cliquez sur **Planifier** pour l'exécuter de façon périodique.
6. Renseignez les informations demandées.

   Pour créer une liste de destinataires, entrez une adresse dans le champ **Adresses de courrier électronique supplémentaires**, puis cliquez sur **Ajouter**. N'oubliez pas de surligner une ou plusieurs adresses électroniques de destination.
7. Cliquez sur **Suivant** lorsque toutes les entrées sont terminées pour afficher un écran de confirmation présentant vos sélections.
8. Cliquez sur **Enregistrer** pour afficher le travail du rapport planifié et la liste de tous les rapports planifiés.

Le travail s'exécutera en fonction du planning défini et enverra le rapport aux destinataires sélectionnés par courrier électronique. À tout moment, vous pouvez vérifier la liste des travaux planifiés, modifier une définition de travail ou supprimer un travail obsolète en cliquant sur **File d'attente de tâches** dans la page Rapports d'investigation principale.

Si vous êtes administrateur de rapports avec un rôle de génération de rapports d'investigation, ce didacticiel est terminé. Consultez la section *Prochaines étapes*, page 51, pour découvrir d'autres ressources.

Si vous disposez d'autorisations Real-Time Monitor, passez à la *Leçon 12 : Real-Time Monitor*.

Rapports d'investigation de référence

Les informations affichables dans un rapport d'investigation dépendent des éléments déjà sélectionnés. Par exemple, si vous examinez les requêtes par utilisateur, vous ne pouvez pas ajouter d'informations sur les groupes. De la même façon, si vous examinez un rapport par catégorie, vous ne pouvez pas afficher simultanément les données des classes de risques.

Le tableau ci-dessous répertorie les différents types de données affichables dans un rapport d'investigation. Si vous avez exploré ces données pour créer un rapport détaillé, il s'agit des colonnes que vous pouvez ajouter au rapport pour en personnaliser l'affichage.

Nom de la colonne	Description
Utilisateur	Nom de l'utilisateur à l'origine de la requête. Les informations relatives à l'utilisateur doivent être disponibles dans la Base de données d'activité pour être incluses dans les rapports. Les informations relatives aux groupes ne sont pas disponibles dans les rapports basés sur les utilisateurs.
Jour	Date de la requête Internet
Nom hôte URL	Nom de domaine (hôte) du site demandé
Domaine	Domaine du service d'annuaire du client (utilisateur ou groupe, domaine ou unité d'organisation) à l'origine de la requête
Groupe	Nom du groupe auquel le demandeur appartient. Les noms des utilisateurs individuels ne sont pas fournis dans les rapports basés sur les groupes. Si l'utilisateur qui a demandé le site appartient à plusieurs groupes dans le service d'annuaire, le rapport affiche plusieurs groupes dans cette colonne.
Classe de risques	Classe de risques associée à la catégorie à laquelle le site demandé appartient. Si la catégorie appartient à plusieurs classes de risques, toutes les classes de risques concernées apparaissent dans la liste.
Objet d'annuaire	Chemin d'accès au répertoire de l'utilisateur à l'origine de la requête, sans le nom d'utilisateur. Cela donne généralement plusieurs lignes pour le même trafic, car chaque utilisateur appartient à plusieurs chemins d'accès. Si vous utilisez un service d'annuaire non LDAP, cette colonne n'est pas disponible.
Disposition	Action exécutée par Websense en résultat de la requête (par exemple, catégorie autorisée ou catégorie bloquée)
Serveur source	Adresse IP de l'ordinateur qui envoie les requêtes à Filtering Service. Dans les déploiements autonomes, il s'agit de l'adresse IP de Network Agent. Dans les déploiements intégrés, il s'agit de l'adresse IP de la passerelle, du pare-feu ou du cache. Avec Websense Web Security Gateway Anywhere, cette option vous permet d'identifier les requêtes des utilisateurs sur site (emplacement filtré) et hors site, filtrées par le service hybride.
Protocole	Protocole de la demande (par exemple, HTTP ou FTP)
Groupe de protocoles	Groupe de la Base de données principale dans lequel se situe le protocole demandé (par exemple, Accès à distance ou Médias en temps-réel)
IP source	Adresse IP de l'ordinateur à partir duquel la demande a été effectuée Avec Websense Web Security Gateway Anywhere, cette option vous permet d'examiner les requêtes provenant d'un emplacement hybride et filtré spécifique.
IP de destination	Adresse IP du site demandé

Nom de la colonne	Description
URL complète	Nom de domaine et chemin d'accès du site demandé (exemple : http://www.mondomaine.com/products/ref=abc123?string/). Si vous ne journalisez pas les URL complètes, cette colonne sera vide.
Mois	Mois du calendrier au cours duquel la demande a été effectuée
Port	Port TCP/IP par lequel l'utilisateur a communiqué avec le site
Bande passante	Quantité de données, en kilo-octets, contenues dans la requête initiale de l'utilisateur et dans la réponse du site Web. Il s'agit du total combiné des valeurs Envoyé et Reçu. N'oubliez pas que certains produits d'intégration n'envoient pas ces informations à Websense. Les pare-feu Check Point FireWall-1 et Cisco PIX Firewall en sont deux exemples. Si votre intégration n'envoie pas ces informations et que Websense Network Agent est installé, activez l'option **Journaliser les demandes HTTP** de la carte d'interface réseau appropriée pour activer la génération de rapports sur les informations de bande passante.
Octets envoyés	Nombre d'octets envoyés dans la requête Internet. Cela représente la quantité de données transmises, pouvant correspondre à une simple demande d'URL, ou d'une soumission plus importante, par exemple si l'utilisateur s'enregistre auprès d'un site Web.
Octets reçus	Nombre d'octets reçus d'Internet en réponse à la requête. Cela comprend l'ensemble du texte, des graphiques et des scripts qui composent le site. Dans le cas des sites bloqués, le nombre d'octets dépend du logiciel qui crée l'enregistrement du journal. Lorsque Websense Network Agent journalise les enregistrements, le nombre d'octets reçus pour un site bloqué correspond à la taille de la page de blocage. Si l'enregistrement de journal est créé par Websense Security Gateway en résultat d'une analyse, les octets reçus représentent la taille de la page analysée. Lorsqu'un autre produit d'intégration crée les enregistrements du journal, les octets reçus pour un site bloqué peuvent correspondre à zéro (0), à la taille de la page bloquée ou à la valeur obtenue du site demandé.
Heure	Heure à laquelle le site a été demandé, au format HH:MM:SS, sur 24 heures
Catégorie	Catégorie à laquelle la requête a été affectée. Il peut s'agir d'une catégorie de la Base de données principale ou d'une catégorie personnalisée.

Leçon 12 : Real-Time Monitor

Apprenez à utiliser Real-Time Monitor pour surveiller le filtrage de l'activité Internet en cours dans votre réseau. Appliquez des filtres pour cibler un trafic présentant des caractéristiques spécifiques.

Real-Time Monitor présente une vue simplifiée du filtrage de l'activité Internet actuelle dans votre réseau. Vous pouvez contrôler la fréquence d'actualisation des données et la quantité de données disponibles, et appliquer des filtres pour examiner des clients, sites ou types de requêtes spécifiques (bloquées ou autorisées).

Contrairement aux autres outils de génération de rapports, Real-Time Monitor ne présente que les données actuelles.

- Ces données proviennent directement d'Usage Monitor, qui surveille l'accès des clients aux sites et aux protocoles à utiliser dans les alertes.
- Chaque enregistrement est récupéré par la base de données de Real-Time Monitor en vue de son affichage. Cette base de données contient un nombre d'enregistrements limité (configurable).
- Lorsque la base de données de Real-Time Monitor est saturée, chaque nouvel enregistrement en remplace un ancien. Les anciennes informations ne sont donc plus disponibles. (Ces informations étant également collectées par Log Server et stockées dans la base de données d'activité, d'autres outils de génération de rapports permettent d'y accéder, par exemple les rapports d'investigation.)

Real-Time Monitor présente l'activité d'une instance de Policy Server à la fois. Policy Server est le composant chargé de coordonner les divers autres composants de Websense Web Security. Si votre organisation est vaste ou distribuée, il est possible que plusieurs instances de Policy Server soient déployées pour équilibrer la charge du filtrage.

TRITON - Web Security se connecte également à une instance de Policy Server à la fois, Real-Time Monitor se connectant à cette même instance de Policy Server au démarrage. Tant qu'il est affiché dans le panneau de contenu de TRITON, Real-Time Monitor change sa connexion à Policy Server chaque fois que TRITON - Web Security change la sienne.

Lorsqu'il est ouvert en mode plein écran, Real-Time Monitor reste connecté à la même instance de Policy Server, que TRITON - Web Security se connecte ou non à une autre instance.

Par conséquent, plusieurs instances de Real-Time Monitor peuvent s'exécuter en mode plein écran dans le même ordinateur, chacune connectée à une instance de Policy Server distincte. L'adresse IP du serveur Policy Server est affichée dans la barre de titre de Real-Time Monitor. Si vous êtes administrateur de la sécurité du réseau, vous pouvez donc surveiller votre installation Websense Web Security dans son intégralité en ouvrant une instance de Real-Time Monitor pour chaque instance de Policy Server déployée dans votre réseau.

Exercice 1 : Principes de base de Real-Time Monitor

1. Pour démarrer Real-Time Monitor, ouvrez la page Génération de rapports > Real-Time Monitor dans TRITON - Web Security.
2. Cliquez sur **Démarrer** pour renseigner la page. La page présente alors les requêtes Internet récentes, dont :

- L'adresse IP ou le nom de l'**utilisateur** à l'origine de la demande. Si vous utilisez le filtrage par utilisateur dans votre réseau et que l'adresse IP s'affiche, survolez une entrée avec votre souris pour voir le nom de l'utilisateur.
- L'**URL** demandée. Si l'URL est tronquée, survolez une entrée avec votre souris pour voir l'URL complète.
- Si le site demandé a été ou non classé dans une catégorie après une analyse de Content Gateway.

  La présence d'une icône signale que l'analyse a entraîné un reclassement dynamique du site. Son absence indique que la Base de donnée principale ou une catégorie personnalisée définie par l'administrateur a été utilisée. Survolez l'icône avec votre souris pour identifier la catégorie d'origine.
- La **Catégorie** affectée au site. La véritable catégorie utilisée pour filtrer la requête est indiquée, qu'il s'agisse de la catégorie Base de données principale, de la catégorie des URL personnalisées ou d'une catégorie affectée dynamiquement suite à une analyse.
- L'**Action** (autorisée ou bloquée) appliquée à la requête.
- L'**Heure** à laquelle la requête a été envoyée à Real-Time Monitor. Real-Time Monitor récupérant les informations sur les requêtes auprès d'Usage Monitor en temps réel (sans lire dans la Base de données d'activité), l'heure de la requête indiquée ici peut ne pas correspondre à celle indiquée dans les rapports d'investigation ou de présentation.

3. Pour examiner les données actuelles, cliquez sur **Pause** pour interrompre l'actualisation continuelle de la page. Lorsque vous êtes prêt à surveiller de nouvelles informations, cliquez de nouveau sur **Démarrer**.

Selon vos paramètres actuels, Real-Time Monitor stocke un nombre défini d'enregistrements (250, 500 ou 1 000) et affiche systématiquement le jeu d'enregistrements le plus récent à sa disposition. Lorsque vous interrompez l'affichage des nouveaux enregistrements pour examiner les données en cours, les centaines, voire les milliers de requêtes pouvant survenir entre-temps ne sont jamais affichées. (Ces requêtes sont toutefois stockées dans la Base de données d'activité et s'afficheront dans les rapports d'investigation et de présentation.)

Si vous êtes un administrateur délégué ou un administrateur de génération de rapports, ce didacticiel est terminé. Consultez la section *Prochaines étapes* pour découvrir des liens vers les étapes suivantes éventuelles.

Si vous êtes un Super administrateur, passez à la *Leçon 13 : Amélioration de Websense*.

Leçon 13 : Amélioration de Websense

Activez WebCatcher pour envoyer les URL non catégorisées et les URL liées à la sécurité à Websense, Inc., à des fins d'analyse. Vous pouvez également choisir d'envoyer les données d'utilisation des protocoles et des catégories pour aider Websense à améliorer sans cesse les capacités de filtrage.

Deux options du logiciel vous permettent d'aider Websense, Inc. à améliorer le filtrage :

- Activez **WebCatcher** pour envoyer les URL non reconnues et liées à la sécurité pour qu'elles puissent être catégorisées et analysées quant aux risques qu'elles représentent pour la sécurité ou la responsabilité légale.

  Une fois catégorisés, ces sites seront ajoutés à la Base de données principale en vue de leur utilisation pour le filtrage et la génération de rapports.
- Pour aider Websense, Inc. à améliorer constamment les capacités de filtrage, autorisez-nous à collecter les données d'utilisation des catégories et des protocoles.

WebCatcher

Lorsque WebCatcher envoie des URL liées à la sécurité et non reconnues à Websense, Inc., les prochains téléchargements de la Base de données principale Websense comprendront les améliorations et les corrections de catégories résultant des données de WebCatcher. Seuls les Super administrateurs peuvent modifier ces paramètres.

Important

Les informations envoyées à Websense, Inc. ne contiennent que les URL, pas les informations relatives aux utilisateurs individuels.

Lorsque vous activez WebCatcher, les types d'informations suivants sont envoyés à Websense. L'adresse IP correspond à celle de l'ordinateur qui héberge l'URL, pas à celle du demandeur.

```
<URL HREF="http://www.ack.com/uncategorized/" CATEGORY="153"
IP_ADDR="200.102.53.105" NUM_HITS="1" />
```

Pour activer WebCatcher :

1. Ouvrez la page **Paramètres > Général > Compte** dans TRITON - Web Security.
2. Sous WebCatcher, cochez l'option **Send URL information to Websense (Envoyer les informations sur les URL à Websense)**.

- Pour envoyer les URL non catégorisées afin qu'elles soient évaluées, puis classées, cochez l'option **Send uncategorized URLs to improve URL categorization (Envoyer les URL non catégorisées pour améliorer la catégorisation des URL)**.
- Pour envoyer les URL liées à la sécurité et participer au suivi de l'activité des sites Web malveillants, cochez l'option **Send security URLs to improve security effectiveness (Envoyer les URL de sécurité pour améliorer l'efficacité de la sécurité)**.
- Pour conserver une copie locale des informations envoyées à Websense, Inc. et pouvoir ensuite les examiner, cochez l'option **Enregistrer une copie des données envoyées à Websense**.

  Lorsque cette option est activée, WebCatcher enregistre les données sous forme de fichiers XML non cryptés dans le répertoire **Websense\Web Security\bin** de l'ordinateur Log Server. Ces fichiers comportent une date et une heure.
- Sélectionnez le **Pays d'origine** de votre organisation. Il doit s'agir du pays où la majeure partie de l'activité Internet est enregistrée.
- Spécifiez une **Taille maximale du fichier de téléchargement**. Lorsque la taille maximale est atteinte, les données collectées par WebCatcher sont envoyées automatiquement et un nouveau fichier est créé.
- Le champ **Heure de début chaque jour** vous permet d'indiquer l'heure à laquelle WebCatcher doit envoyer chaque jour les données collectées lorsque la taille maximale définie pour ce fichier n'a pas été atteinte.

3. Cliquez sur **OK** pour mettre vos modifications en cache, puis sur **Save and Deploy (Enregistrer et déployer)** pour les implémenter.

Données d'utilisation des protocoles et des catégories

Lorsque vous décidez d'envoyer vos données d'utilisation des catégories et des protocoles à Websense, Inc., ces données ne sont collectées que pour les catégories et les protocoles définis par Websense. Les catégories ou les protocoles personnalisé(e)s que vous avez défini(e)s ne sont pas inclus(es).

Websense, Inc. ne collecte pas de données relatives à l'utilisation de votre réseau sans votre autorisation. Vous avez la possibilité de désactiver la collecte des données d'utilisation pendant l'installation (cette option est activée par défaut).

Les données d'utilisation de catégories et de protocoles aident Websense, Inc. à améliorer les capacités de filtrage du logiciel Websense.

Pour configurer la collecte des données d'utilisation des catégories et des protocoles :

1. Dans TRITON - Web Security, ouvrez la page **Paramètres > Général > Compte**.
2. Activez ou désactivez la case à cocher **Envoyer les données de catégorie ou de protocole à Websense, Inc**.
3. Cliquez sur **OK** pour mettre votre modification en cache, puis sur **Save and Deploy (Enregistrer et déployer)** pour l'implémenter.

Ce didacticiel est à présent terminé. Consultez la section *Prochaines étapes* pour découvrir des liens vers les étapes suivantes éventuelles.

6 Prochaines étapes

Ce didacticiel de démarrage rapide pour les nouveaux utilisateurs est à présent terminé. Vous disposez des outils de base nécessaires pour commencer à exploiter Websense.

Un certain nombre de solutions supplémentaires de Websense Web Security peuvent vous permettre d'accroître la précision et la souplesse de la configuration de votre filtrage. Ces fonctions sont décrites en détail dans le système d'aide de TRITON - Web Security (accessible via le bouton Aide de la barre d'outils de TRITON).

Pour les administrateurs autorisés à gérer les stratégies :

- Créez des catégories personnalisées ou recatégorisez des sites individuels (URL recatégorisées).

  Sélectionnez **Gestion des stratégies > Composants de filtre** et cliquez sur **Modifier les catégories**.
- Définissez des exceptions pour autoriser ou bloquer une ou plusieurs URL pour un ou plusieurs clients sans recatégoriser les sites.

  Sélectionnez **Gestion des stratégies > Exceptions**, puis cliquez sur **Ajouter**.
- Configurez des filtres de protocoles pour accroître votre contrôle sur les protocoles Internet, par exemple sur ceux qu'utilisent la messagerie instantanée et le partage de fichiers en P2P.

  Sélectionnez **Gestion des stratégies > Filtres**, puis cliquez sur un nom de filtre ou sur **Ajouter**.
- Créez des filtres d'accès limité pour cantonner certains utilisateurs à une liste restreinte de sites Web.

  Sélectionnez **Gestion des stratégies > Filtres**, puis cliquez sur **Ajouter**.
- Définissez des mots-clés pour mieux contrôler les sites auxquels les clients filtrés peuvent accéder.

  Sélectionnez **Gestion des stratégies > Composants de filtre**, puis cliquez sur **Modifier les catégories** et sélectionnez une catégorie.

Pour les administrateurs de rapports, le Guide Démarrage rapide des rapports d'investigation fournit les procédures nécessaires pour localiser les informations les plus pertinentes pour votre organisation.

Les super administrateurs peuvent désirer configurer des alertes pour que les problèmes potentiels, liés à Websense ou à l'activité Internet des utilisateurs, soient signalés aux administrateurs. Sélectionnez **Paramètres > Alertes > Activer les alertes** pour configurer les méthodes d'alerte.

Tout au long de votre exploitation de TRITON - Web Security, pour toute question sur une fonction ou son utilisation, sélectionnez **Aide > Expliquer cette page**.

Pour découvrir des conseils, des didacticiels vidéo, une vaste Base de connaissances et la documentation du produit, vous pouvez également visiter le site Portail de support de Websense à tout moment.