Comment configurer l'appareil de sécurité Web Cisco et le réseau RSA DLP pour interagir ?

Contenu

Question :

Comment configurer l'appareil de sécurité Web Cisco et le réseau RSA DLP pour interagir ?

Aperçu:

Ce document fournit des informations supplémentaires au-delà du Guide de l'utilisateur Cisco WSA AsyncOS et du Guide de déploiement de RSA DLP Network 7.0.2 pour aider les clients à interagir avec les deux produits.

Description du produit:

Cisco Web Security Appliance (WSA) est un périphérique robuste, sécurisé et efficace qui protège les réseaux d'entreprise contre les programmes malveillants et les logiciels espions basés sur le Web qui peuvent compromettre la sécurité de l'entreprise et exposer la propriété intellectuelle. L'appliance de sécurité Web offre une inspection approfondie du contenu des applications en proposant un service proxy Web pour les protocoles de communication standard tels que HTTP, HTTPS et FTP.

La suite RSA DLP comprend une solution complète de prévention des pertes de données qui permet aux clients de détecter et de protéger les données sensibles dans l'entreprise en exploitant des politiques communes sur l'ensemble de l'infrastructure pour détecter et protéger les données sensibles dans le data center, sur le réseau et sur les terminaux. La suite DLP comprend les composants suivants :

- **Data center RSA DLP**. Le data center DLP vous aide à localiser les données sensibles, où qu'elles se trouvent dans le data center, sur les systèmes de fichiers, les bases de données, les systèmes de messagerie et les grands environnements SAN/NAS.
- **Réseau RSA DLP**. Le réseau DLP surveille et applique la transmission d'informations sensibles sur le réseau, telles que le trafic de messagerie électronique et Web.
- **Point de terminaison RSA DLP**. Le terminal DLP vous aide à détecter, surveiller et contrôler les informations sensibles sur les terminaux tels que les ordinateurs portables et de bureau.

Cisco WSA peut interagir avec RSA DLP Network.

Le réseau RSA DLP comprend les composants suivants :

- **Contrôleur réseau**. Dispositif principal qui gère les informations relatives aux politiques de transmission de données et de contenu confidentielles. Le contrôleur de réseau gère et met à jour les périphériques gérés avec une définition de stratégie et de contenu sensible, ainsi que toute modification apportée à leur configuration après la configuration initiale.
- **Périphériques gérés**. Ces périphériques aident le réseau DLP à surveiller la transmission réseau et à signaler ou intercepter la transmission :
  Capteurs. Installés aux limites du réseau, les capteurs surveillent passivement le trafic sortant du réseau ou traversant les limites du réseau, en l'analysant pour détecter la présence de contenu sensible. Un capteur est une solution hors bande ; il peut uniquement surveiller et signaler les violations de politiques.**Intercepteurs**. Également installés aux frontières du réseau, les intercepteurs vous permettent de mettre en oeuvre la mise en quarantaine et/ou le rejet du trafic de messagerie (SMTP) contenant du contenu sensible. Un intercepteur est un proxy réseau en ligne et peut donc empêcher les données sensibles de quitter l'entreprise.**Serveurs ICAP**. Périphériques serveur spéciaux qui vous permettent d'implémenter la surveillance ou le blocage du trafic HTTP, HTTPS ou FTP contenant du contenu sensible. Un serveur ICAP fonctionne avec un serveur proxy (configuré en tant que client ICAP) pour surveiller ou bloquer les données sensibles de quitter l'entreprise

Cisco WSA interagit avec RSA DLP Network ICAP Server.

Limitations connues

L'intégration DLP externe de Cisco WSA avec RSA DLP Network prend en charge les actions suivantes : Autoriser et Bloquer. Il ne prend pas encore en charge l'action Modifier / Supprimer le contenu (également appelée Redaction).

Conditions requises pour l'interopérabilité

L'interopérabilité du réseau Cisco WSA et RSA DLP a été testée et validée avec les modèles de produits et les versions logicielles dans le tableau suivant. Bien que cette intégration puisse fonctionner avec des variantes du modèle et du logiciel, le tableau suivant représente les seules combinaisons testées, validées et prises en charge. Il est fortement recommandé d'utiliser la dernière version prise en charge des deux produits.

Product (produit)	Version du logiciel
Appareil de sécurité Web Cisco (WSA)	AsyncOS versions 6.3 et ultérieures
Réseau RSA DLP	7.0.2

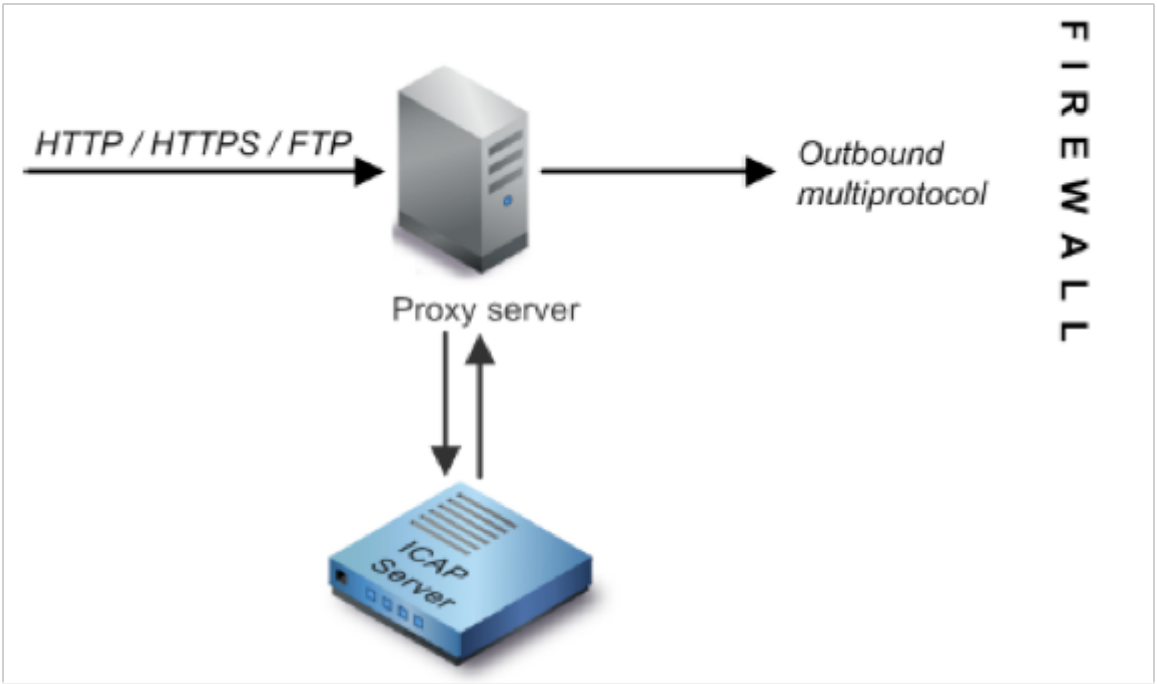
Fonction DLP externe

Àl'aide de la fonction DLP externe de Cisco WSA, vous pouvez transférer tout ou partie du trafic sortant HTTP, HTTPS et FTP du WSA vers le réseau DLP. Tout le trafic est transféré à l'aide du protocole ICAP (Internet Control Adaptation Protocol).

Architecture

Le Guide de déploiement du réseau RSA DLP présente l'architecture générique suivante pour le réseau DLP RSA interopérant avec un serveur proxy. Cette architecture n'est pas spécifique au WSA, mais s'applique à tout proxy qui interagit avec le réseau RSA DLP.

Figure 1 : Architecture de déploiement pour RSA DLP Network et Cisco Web Security Appliance



Configuration de l'appareil de sécurité Web Cisco

1. Définissez un système DLP externe sur le WSA qui fonctionne avec le serveur DLP Network ICAP. Pour obtenir des instructions, reportez-vous à l'extrait ci-joint du Guide de l'utilisateur WSA intitulé User Guide Instructions Defining External DLP Systems.

2. Créez une ou plusieurs stratégies DLP externes qui définissent le trafic que le WSA envoie au réseau DLP pour l'analyse de contenu à l'aide des étapes suivantes :

- Sous **GUI > Gestionnaire de sécurité Web > Stratégies DLP externes > Ajouter une stratégie**
- Cliquez sur le lien sous la colonne ***Destinations*** pour le groupe de stratégies que vous voulez configurer.
- Dans la section « Modifier les paramètres de destination », sélectionnez ?Définir les destinations Analyser les paramètres personnalisés ? dans le menu déroulant
- Nous pouvons ensuite configurer la stratégie pour 'analyser tous les téléchargements' ou pour analyser les téléchargements vers certains domaines/sites spécifiés dans des catégories d'URL personnalisées

Configuration du réseau RSA DLP

Ce document suppose que RSA DLP Network Controller, ICAP Server et Enterprise Manager ont

été installés et configurés.

1. Utilisez RSA DLP Enterprise Manager pour configurer un serveur ICAP réseau. Pour obtenir des instructions détaillées sur la configuration de votre serveur ICAP réseau DLP, reportez-vous au Guide de déploiement réseau RSA DLP. Les principaux paramètres que vous devez spécifier sur la page de configuration du serveur ICAP sont les suivants : Nom d'hôte ou adresse IP du serveur ICAP.Dans la section **Paramètres généraux** de la page de configuration, saisissez les informations suivantes : Durée, en secondes, après laquelle le serveur est réputé avoir expiré dans le champ **Délai d'attente du serveur en secondes**.Sélectionnez l'une des réponses suivantes en tant que réponse **Au délai d'attente du serveur** :**Échec de l'ouverture**. Sélectionnez cette option si vous souhaitez autoriser la transmission après un délai d'attente du serveur.**Échec Fermé**. Sélectionnez cette option si vous souhaitez bloquer la transmission après un délai d'attente du serveur.
2. Utilisez RSA DLP Enterprise Manager pour créer une ou plusieurs stratégies spécifiques au réseau afin d'auditer et de bloquer le trafic réseau qui contient du contenu sensible. Pour obtenir des instructions détaillées sur la création de stratégies DLP, reportez-vous au RSA DLP Network User Guide ou à l'aide en ligne d'Enterprise Manager. Les principales étapes à effectuer sont les suivantes : Àpartir de la bibliothèque de modèles de stratégie, activez au moins une stratégie qui convient à votre environnement et au contenu que vous allez surveiller.Dans cette stratégie, configurez des règles de violation de stratégie spécifiques au réseau DLP qui spécifient les actions que le produit réseau effectuera automatiquement lorsque des événements (violations de stratégie) se produisent. Définissez la règle de détection de stratégie pour détecter tous les protocoles. Définissez l'action de stratégie sur « audit et blocage ».

Éventuellement, nous pouvons utiliser RSA Enterprise Manager pour personnaliser la notification réseau envoyée à l'utilisateur en cas de violation de stratégie. Cette notification est envoyée par DLP Network en remplacement du trafic d'origine.

Tester la configuration

1. Configurez votre navigateur pour diriger le trafic sortant de votre navigateur vers le proxy WSA.

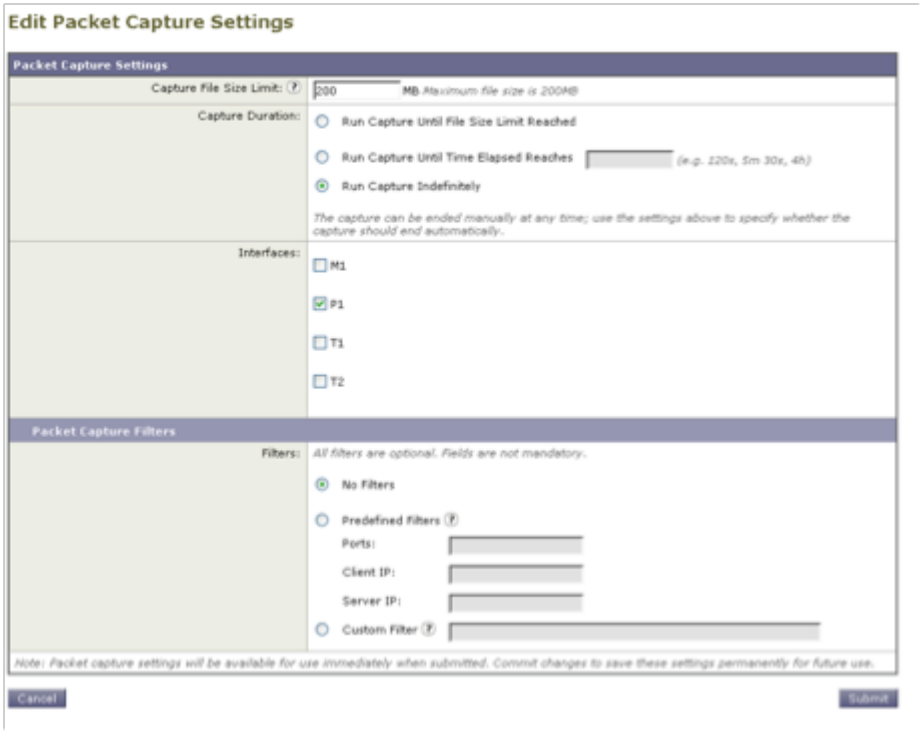
   Par exemple, si vous utilisez le navigateur Mozilla FireFox, procédez comme suit : Dans le navigateur FireFox, sélectionnez **Outils > Options**. La boîte de dialogue Options s'affiche.Cliquez sur l'onglet **Réseau**, puis sur **Paramètres**. La boîte de dialogue Paramètres de connexion s'affiche.Cochez la case **Configuration manuelle du proxy**, puis saisissez l'adresse IP ou le nom d'hôte du serveur proxy WSA dans le champ **Proxy HTTP** et le numéro de port 3128 (par défaut).Cliquez sur **OK**, puis **OK** à nouveau pour enregistrer les nouveaux paramètres.
2. Tentative de téléchargement d'un contenu dont vous savez qu'il contrevient à la stratégie de réseau DLP que vous avez précédemment activée.
3. Un message de suppression ICAP réseau doit s'afficher dans le navigateur.
4. Utilisez 'Enterprise Manager' pour afficher l'événement et l'incident résultant qui ont été créés à la suite de cette violation de la stratégie.

Dépannage

1. Lors de la configuration d'un serveur DLP externe sur l'appliance de sécurité Web pour le réseau RSA DLP, utilisez les valeurs suivantes :

   Adresse du serveur : Adresse IP ou nom d'hôte du serveur ICAP du réseau RSA DLPPort : Port TCP utilisé pour accéder au serveur de réseau RSA DLP, généralement **1344**Format d'URL de service : **icap://*<hostname_or_ipaddress>*/srv_conalarme**Exemple : icap://dlp.example.com/srv_conalarm
2. Activez la fonctionnalité de capture du trafic de WSA pour capturer le trafic entre le proxy WSA et le serveur ICAP du réseau. Ceci est utile lors du diagnostic des problèmes de connectivité. Pour ce faire, procédez comme suit :

   Sur l'interface utilisateur graphique WSA, accédez au menu **Support and Help** en haut à droite de l'interface utilisateur. Sélectionnez **Capture de paquets** dans le menu, puis cliquez sur le bouton **Modifier les paramètres**. La fenêtre Edit Capture Settings s'affiche.



   Dans la section **Packet Capture** Filters de l'écran, saisissez l'adresse IP du serveur ICAP réseau dans le champ **Server IP**.Cliquez sur **Submit pour enregistrer les modifications.**
3. Utilisez le champ personnalisé suivant dans les journaux d'accès WSA (sous ***GUI > Administration système > Inscriptions au journal >journaux d'accès***) pour obtenir plus d'informations :
   %Xp : Verdict d'analyse du serveur DLP externe (0 = aucune correspondance sur le serveur ICAP ; 1 = correspondance de stratégie avec le serveur ICAP et '- (tiret)' = Aucune analyse n'a été initiée par le serveur DLP externe)

[Instructions du Guide de l'utilisateur Définition des systèmes DLP externes.]

_