Comment configurer l'appliance de sécurité Web de Cisco et le réseau DLP RSA pour interopérer ?

Contenu

Question :

Comment configurer l'appliance de sécurité Web de Cisco et le réseau DLP RSA pour interopérer ?

Aperçu :

Ce document fournit les informations supplémentaires au delà du guide utilisateur de Cisco WSA AsyncOS et du guide de déploiement du réseau 7.0.2 DLP RSA pour aider des clients à interopérer les deux Produits.

Description de produit :

L'appliance de sécurité Web de Cisco (WSA) est un périphérique robuste, sécurisé, efficace qui protège des réseaux d'entreprise contre les programmes basés sur le WEB de malware et de logiciel espion qui peuvent compromettre la propriété intellectuelle entreprise de Sécurité et d'exposition. L'appliance de sécurité Web fournit l'inspection profonde de contenu d'application en offrant un service proxy de Web pour des protocoles de communication standard tels que le HTTP, le HTTPS, et le FTP.

La suite DLP RSA comporte une solution complète de prévention de perte de données qui permet à des clients de découvrir et protéger des données sensibles à l'entreprise en accroissant des stratégies communes à travers l'infrastructure pour découvrir et protéger des données sensibles dans le centre d'hébergement, sur le réseau, et sur des points finaux. La suite DLP inclut les composants suivants :

- **Centre d'hébergement DLP RSA**. Le centre d'hébergement DLP vous aide à localiser des données sensibles n'importe où il réside dans le centre d'hébergement, sur des systèmes de fichiers, des bases de données, des systèmes de courrier électronique et de grands environnements SAN/NAS.
- **Réseau DLP RSA**. Les surveillances réseau DLP et impose la transmission des informations confidentielles sur le réseau, tel que l'email et le trafic web.
- **Point final DLP RSA**. Le point final DLP vous aide à découvrir, surveiller et contrôler les informations confidentielles sur des points finaux tels que des ordinateurs de bureau et ordinateur portable.

Cisco WSA a la capacité d'interopérer avec le réseau DLP RSA.

Le réseau DLP RSA inclut les composants suivants :

- **Contrôleur réseau**. L'appliance principale qui met à jour des informations sur des stratégies de transmission des informations confidentielles et de contenu. Le contrôleur réseau gère et met à jour des périphériques gérés avec la stratégie et la définition satisfaite sensible avec en change en leur configuration après configuration initiale.
- **Périphériques gérés**. Ces périphériques aident la transmission réseau et l'état de surveillance réseau DLP ou interceptent la transmission :
  Capteurs. Installé aux limites du réseau, les capteurs surveillent passivement le trafic partant du réseau ou croisant des limites du réseau, l'analysant la présence du contenu sensible. Un capteur est une solution hors bande ; il peut seulement surveillent et signalent des violations de stratégie.**Intercepteurs**. Également installé aux limites du réseau, les intercepteurs te permettent pour implémenter mettre en quarantaine et/ou rejet du trafic d'email (SMTP) qui contient le contenu sensible. Un intercepteur est un proxy intégré de réseau et peut donc bloquer des données sensibles de laisser l'entreprise.**Serveurs ICAP**. Périphériques de serveur de but spécifique qui te permettent pour implémenter la surveillance ou le blocage du HTTP, du HTTPS, ou du trafic FTP contenant le contenu sensible. Un serveur ICAP travaille avec un serveur proxy (configuré en tant que client ICAP) pour surveiller ou bloquer des données sensibles de laisser l'entreprise

Cisco WSA interopère avec le serveur ICAP de réseau DLP RSA.

Limitations connues

Intégration externe DLP de Cisco WSA avec des supports réseau DLP RSA les actions suivantes : Laissez et bloquez. Il ne prend en charge pas encore « modifient/enlèvent l'action de contenu » (également appelé Redaction).

Conditions requises de produit pour l'Interopérabilité

L'interopérabilité de Cisco WSA et du réseau DLP RSA a été testée et validée avec les modèles et les versions de logiciel dans le tableau suivant. Tandis que parler fonctionellement cette intégration peut fonctionner avec des variations au modèle et au logiciel, le tableau suivant représente les seules combinaisons testées, validées, et prises en charge. Il est fortement recommandé pour utiliser la dernière version prise en charge des deux Produits.

Produit	Version de logiciel
Appliance de sécurité Web de Cisco (WSA)	Versions 6.3 d'AsyncOS et en haut
Réseau DLP RSA	7.0.2

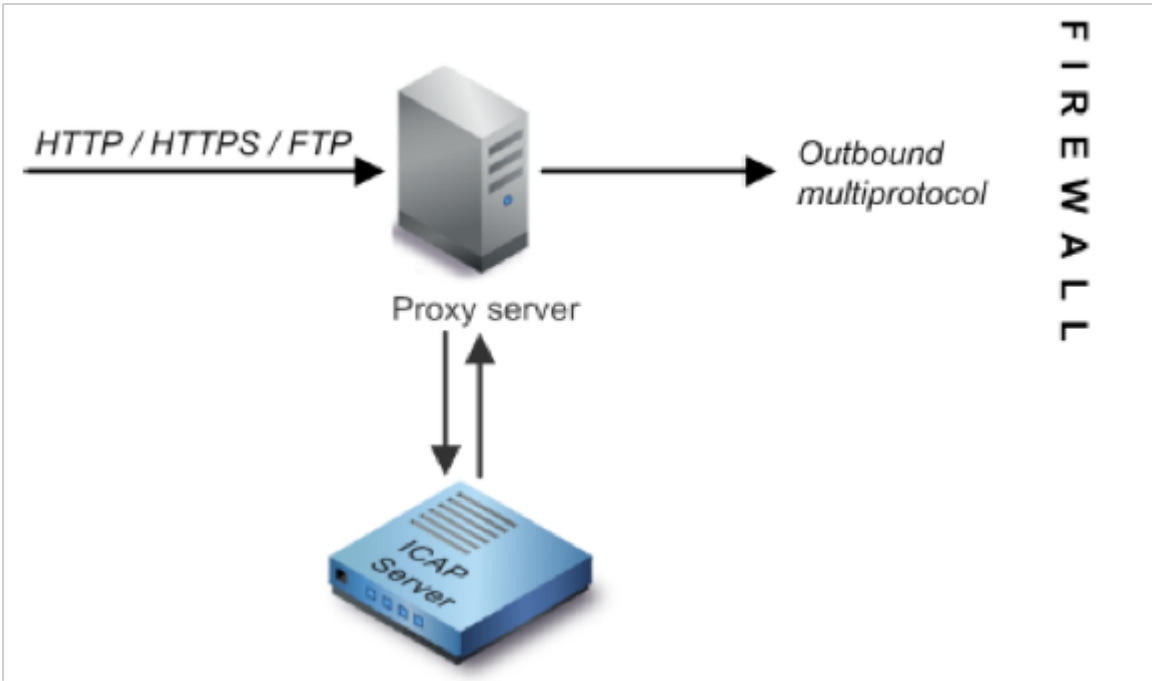
Caractéristique externe DLP

Utilisant la caractéristique externe DLP de Cisco WSA, vous pouvez expédier tous ou HTTP, HTTPS, et trafic FTP sortants spécifiques du WSA au réseau DLP. Tout le trafic est transféré utilisant l'adaptation de contrôle d'Internet Protocol (ICAP).

Architecture

Le guide de déploiement de réseau DLP RSA affiche l'architecture générique suivante pour interopérer le réseau DLP RSA avec un serveur proxy. Cette architecture n'est pas spécifique au WSA, mais s'applique à tout proxy qui interopère avec le réseau DLP RSA.

Figure 1 : Architecture de déploiement pour le réseau DLP RSA et l'appliance de sécurité Web de Cisco



Configurer l'appliance de sécurité Web de Cisco

1. Définissez un système externe DLP sur le WSA qui fonctionne avec le serveur ICAP de réseau DLP. Pour des instructions, voyez s'il vous plaît l'extrait relié du guide utilisateur « instructions WSA de guide utilisateur définir les systèmes externes DLP ».

2. Créez un ou plusieurs stratégies externes DLP qui définissent qui trafiquent le WSA envoient au réseau DLP pour la lecture satisfaite utilisant les étapes ci-dessous :

- Sous le **GUI >** le **gestionnaire de sécurité Web >** des **stratégies externes DLP > ajoutent la stratégie**
- Cliquez sur le lien sous la colonne de ***destinations*** pour le policy group que vous voulez configurer
- Sous la section « éditez de destination configurations », choisissent ? Définissez les destinations balayant des paramètres personnalisés ? de baisse du menu vers le bas
- Nous pouvons alors configurer la stratégie « pour balayer tous les téléchargements » ou pour

balayer des téléchargements à de certains domaines/sites spécifiés dans des catégories faites sur commande URL

Configurer le réseau DLP RSA

Ce document suppose que le contrôleur réseau DLP RSA, le serveur ICAP et le gestionnaire d'entreprise ont été installés et configurés.

1. Utilisez le gestionnaire d'entreprise DLP RSA pour configurer un serveur ICAP de réseau. Pour le mode d'emploi détaillé sur installer votre serveur ICAP de réseau DLP, référez-vous au guide de déploiement de réseau DLP RSA. Les paramètres principaux que vous devriez spécifier à la page de configuration du serveur ICAP sont : L'adresse Internet ou l'adresse IP du serveur ICAP.Dans la section de **paramètres généraux de la** page de configuration, écrivez les informations suivantes : La durée dans les secondes après quoi le serveur est considérée pour avoir chronométré dans le **délai de temporisation du serveur dans le** domaine de **secondes**.Sélectionnez un du suivant comme réponse **sur le délai de temporisation du serveur** :**Échouer ouvert**. Sélectionnez cette option si vous voulez permettre la transmission après un délai de temporisation du serveur.**Échouer clôturé**. Sélectionnez cette option si vous voulez au transmission par blocs après un délai de temporisation du serveur.
2. Utilisez le gestionnaire d'entreprise DLP RSA pour créer un ou plusieurs stratégies de Réseau-particularité pour apurer et bloquer le trafic réseau qui contient le contenu sensible. Pour le mode d'emploi détaillé pour créer des stratégies DLP, référez-vous au guide d'utilisateur du réseau DLP RSA ou à l'aide de Manageronline d'entreprise. Les étapes principales à exécuter sont les suivantes : De l'enable de bibliothèque de modèle de stratégie au moins une stratégie qui semble raisonnable pour votre environnement et le contenu vous surveillera.Dans cette stratégie, les règles installées de violation de stratégie de Réseau-particularité DLP qui spécifient des actions le produit de réseau exécuteront automatiquement quand les événements (violations de stratégie) se produisent. Placez la règle de détection de stratégie de détecter tous les protocoles. Placez l'action de stratégie « d'apurer et bloquer ».

Sur option nous pouvons utiliser le gestionnaire d'entreprise RSA pour personnaliser la notification de réseau qui est envoyée à l'utilisateur quand les violations de stratégie se produisent. Cette notification est envoyée par le réseau DLP comme remplacement pour le trafic d'origine.

Testez l'installation

1. Configurez votre navigateur pour diriger le trafic sortant de votre navigateur aller directement au proxy WSA.

   Par exemple, si vous utilisez le navigateur de Mozilla Firefox, faites ce qui suit : Dans le navigateur Firefox, **outils** choisis **> options**. Le dialogue d'options apparaît.Cliquez sur l'onglet de **réseau**, puis cliquez sur les **configurations**. Le dialogue de paramètres de connexion apparaît.Sélectionnez la case à cocher **manuelle de configuration de proxy**, puis entrez dans

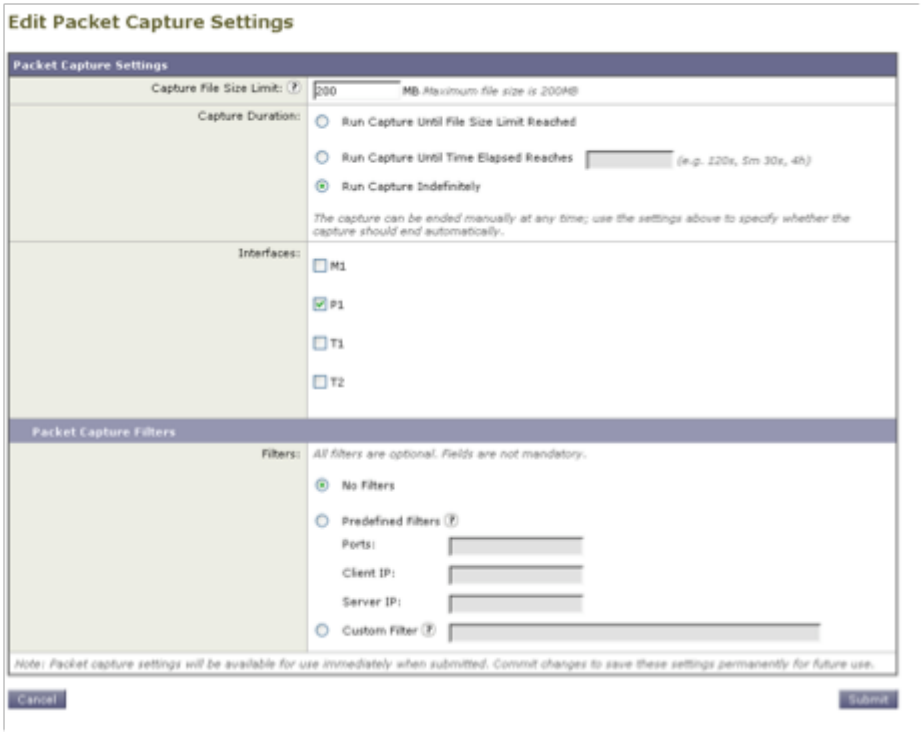
l'adresse IP ou l'adresse Internet du serveur proxy WSA dans le champ et le numéro de port 3128 (le par défaut) de **proxy HTTP**.Cliquez sur OK, puis **CORRECT** de nouveau pour sauvegarder les nouveaux paramètres.
2. La tentative de télécharger un certain contenu que vous connaissez est en violation de la politique réseau DLP que vous avez précédemment activée.
3. Vous devriez voir un message d'écart ICAP de réseau dans le navigateur.
4. Utilisez le « gestionnaire d'entreprise » pour visualiser l'événement et l'incident en résultant qui ont été créés en raison de cette violation de stratégie.

Dépannage

1. En configurant un serveur externe DLP sur l'appliance de sécurité Web pour le réseau DLP RSA, utilisez les valeurs suivantes :

   Adresse du serveur : L'adresse IP ou le nom d'hôte du serveur ICAP de réseau DLP RSAPort : Le port TCP utilisé pour accéder au serveur de réseau DLP RSA, en général **1344**Entretenez le format URL : **icap:// *<hostname_or_ipaddress>/srv_conalarm***Exemple : icap://dlp.example.com/srv_conalarm
2. Activez le trafic capturant la caractéristique de WSA pour capturer le trafic entre le proxy WSA et le serveur ICAP de réseau. C'est utile en diagnostiquant des problèmes de connectivité. Pour faire ceci, faites ce qui suit :

   Sur le GUI WSA, allez au **support et au menu Help** dans l'en haut à droite de l'interface utilisateur. **La capture** choisie de **paquet du** menu, cliquent sur alors le **bouton Settings d'éditer**. La fenêtre de configurations de capture d'éditer apparaît.



   Dans la section de filtres de **capture de paquet de l'**écran, écrivez l'adresse IP du serveur ICAP de réseau dans le domaine **IP de serveur**.Cliquez sur **Submit** pour enregistrer les modifications.
3. Employez le champ fait sur commande suivant dans les logs d'accès WSA (sous ***GUI > administration système > abonnements > accesslogs de log***) pour obtenir plus d'informations

:

%Xp : Verdict externe de lecture de serveur DLP (0 = aucune correspondance sur le serveur ICAP ; 1 = match de stratégie contre le serveur ICAP et « - (trait d'union) » = aucune lecture n'a été initiée par le serveur externe DLP)

Instructions de guide utilisateur définissant les systèmes externes DLP.

_