Come configurare Cisco Web Security Appliance e la rete RSA DLP per l'interoperabilità?

Sommario

Domanda:

Come configurare Cisco Web Security Appliance e la rete RSA DLP per l'interoperabilità?

Panoramica:

Questo documento offre informazioni aggiuntive rispetto alla Guida per l'utente di Cisco WSA AsyncOS e alla Guida all'installazione di RSA DLP Network 7.0.2 per consentire ai clienti di interagire con i due prodotti.

Descrizione del prodotto:

Cisco Web Security Appliance (WSA) è un dispositivo solido, sicuro ed efficiente che protegge le reti aziendali da malware e programmi spyware basati sul Web che possono compromettere la sicurezza aziendale ed esporre la proprietà intellettuale. Web Security Appliance offre un'analisi approfondita del contenuto delle applicazioni offrendo un servizio proxy Web per protocolli di comunicazione standard quali HTTP, HTTPS e FTP.

La suite RSA DLP comprende una soluzione completa per la prevenzione della perdita dei dati che consente ai clienti di individuare e proteggere i dati sensibili all'interno dell'azienda utilizzando regole comuni a tutta l'infrastruttura per individuare e proteggere i dati sensibili nel centro dati, sulla rete e sugli endpoint. La suite DLP include i seguenti componenti:

- **RSA DLP Datacenter**. Il centro dati DLP consente di individuare i dati sensibili, indipendentemente dalla loro posizione all'interno del centro dati, su file system, database, sistemi di posta elettronica e ambienti SAN/NAS di grandi dimensioni.
- **RSA DLP Network**. DLP Network esegue il monitoraggio e l'imposizione della trasmissione di informazioni riservate sulla rete, ad esempio e-mail e traffico Web.
- **Endpoint RSA DLP**. DLP Endpoint consente di individuare, monitorare e controllare le informazioni riservate su endpoint quali notebook e desktop.

Cisco WSA è in grado di interagire con RSA DLP Network.

RSA DLP Network include i seguenti componenti:

- **Controller di rete**. Principale dispositivo che gestisce le informazioni relative ai criteri di trasmissione dei dati riservati e dei contenuti. Controller di rete gestisce e aggiorna i dispositivi

gestiti con la definizione di criteri e contenuti sensibili insieme a eventuali modifiche alla configurazione dopo la configurazione iniziale.

- **Dispositivi gestiti**. Questi dispositivi aiutano DLP Network a monitorare la trasmissione di rete e a segnalare o intercettare la trasmissione:
  Sensori. Installati ai confini della rete, i sensori monitorano passivamente il traffico che esce dalla rete o che attraversa i confini della rete, analizzandoli per rilevare la presenza di contenuti sensibili. Un sensore è una soluzione fuori banda; può solo monitorare e segnalare violazioni dei criteri.**Intercettori**. Installati anche ai limiti della rete, gli intercettori consentono di implementare la quarantena e/o il rifiuto del traffico di posta elettronica (SMTP) che contiene contenuti riservati. Un intercettore è un proxy di rete in linea e può quindi bloccare l'uscita dei dati sensibili dall'azienda.**server ICAP**. Dispositivi server per scopi speciali che consentono di implementare il monitoraggio o il blocco del traffico HTTP, HTTPS o FTP con contenuti riservati. Un server ICAP opera con un server proxy (configurato come client ICAP) per monitorare o bloccare l'uscita dall'azienda dei dati riservati

Cisco WSA interagisce con RSA DLP Network ICAP Server.

Limitazioni note

L'integrazione DLP esterna Cisco WSA con RSA DLP Network supporta le seguenti azioni: Consenti e blocca. Non supporta ancora l'azione "Modifica/Rimuovi contenuto" (chiamata anche Redazione).

Requisiti del prodotto per l'interoperabilità

L'interoperabilità di Cisco WSA e RSA DLP Network è stata testata e convalidata con i modelli e le versioni software del prodotto riportati nella tabella seguente. Dal punto di vista funzionale questa integrazione può funzionare con variazioni del modello e del software, ma la tabella seguente rappresenta le uniche combinazioni testate, convalidate e supportate. Si consiglia di utilizzare la versione più recente supportata di entrambi i prodotti.

Prodotto	Versione del software
Cisco Web Security Appliance (WSA)	AsyncOS versione 6.3 e successive
RSA DLP Network	7.0.2

Funzione DLP esterna

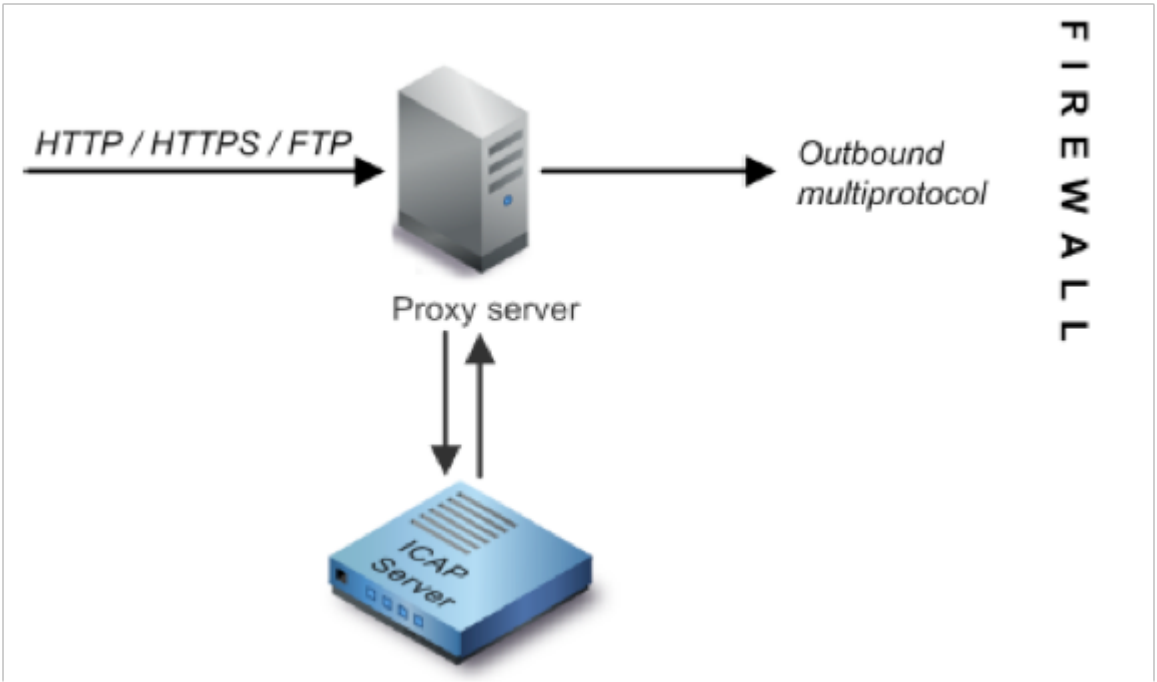
Utilizzando la funzionalità DLP esterno di Cisco WSA, è possibile inoltrare tutto o parte del traffico HTTP, HTTPS e FTP in uscita o specifico da WSA alla rete DLP. Tutto il traffico viene trasferito utilizzando il protocollo ICAP (Internet Control Adaptation Protocol).

Architettura

La Guida all'implementazione della rete RSA DLP mostra la seguente architettura generica per la

rete RSA DLP interoperativa con un server proxy. Questa architettura non è specifica per il server WSA, ma si applica a qualsiasi proxy che interagisce con RSA DLP Network.

Figura 1: Architettura di implementazione per la rete DLP RSA e Cisco Web Security Appliance



Configurazione di Cisco Web Security Appliance

1. Definire un sistema DLP esterno sul server WSA che funzioni con il server ICAP della rete DLP. Per istruzioni, fare riferimento al brano allegato del manuale dell'utente WSA "User Guide Instructions Defining External DLP Systems".

2. Creare uno o più criteri di prevenzione della perdita dei dati esterni che definiscono il traffico inviato dal server di prevenzione della perdita dei dati alla rete di prevenzione della perdita dei dati per la scansione dei contenuti utilizzando i passaggi seguenti:

- In **GUI > Web Security Manager > Criteri di prevenzione della perdita dei dati esterni > Aggiungi criterio**
- Fare clic sul collegamento nella colonna ***Destinazioni*** per il gruppo di criteri che si desidera configurare
- Nella sezione 'Modifica impostazioni di destinazione', scegliere ?Definisci le destinazioni Scansione impostazioni personalizzate? dal menu a discesa
- Èquindi possibile configurare il criterio per l'analisi di tutti i caricamenti o per l'analisi dei caricamenti in determinati domini/siti specificati nelle categorie URL personalizzate

Configurazione della rete RSA DLP

in questo documento si presume che RSA DLP Network Controller, ICAP Server ed Enterprise Manager siano stati installati e configurati.

1. Utilizzare RSA DLP Enterprise Manager per configurare un server ICAP di rete. Per istruzioni dettagliate sulla configurazione del server ICAP della rete DLP, consultare la Guida all'installazione della rete DLP RSA. I parametri principali da specificare nella pagina Configurazione server ICAP sono: Il nome host o l'indirizzo IP del server ICAP.Nella sezione **Impostazioni generali** della pagina di configurazione, immettere le informazioni riportate di seguito. Quantità di tempo in secondi dopo la quale si ritiene che il server sia scaduto nel campo **Timeout server in secondi**.Selezionare una delle opzioni seguenti come risposta al **timeout del server**:**Impossibile aprire**. Selezionare questa opzione se si desidera consentire la trasmissione dopo un timeout del server.**Errore Chiuso**. Selezionare questa opzione se si desidera bloccare la trasmissione dopo un timeout del server.
2. Utilizzare RSA DLP Enterprise Manager per creare uno o più criteri specifici della rete per controllare e bloccare il traffico di rete che contiene contenuti riservati. Per istruzioni dettagliate sulla creazione dei criteri di prevenzione della perdita dei dati, consultare la Guida dell'utente di RSA DLP Network o la Guida in linea di Enterprise Manager. I passaggi principali da eseguire sono i seguenti: Dalla libreria dei modelli di criteri abilitare almeno un criterio appropriato per l'ambiente e il contenuto che verrà monitorato.All'interno di tale criterio, impostare le regole di violazione dei criteri di prevenzione della perdita dei dati specifiche della rete che specificano le azioni che il prodotto di rete eseguirà automaticamente quando si verificano eventi (violazioni dei criteri). Impostare la regola di rilevamento dei criteri per rilevare tutti i protocolli. Impostare l'azione del criterio su "audit e blocco".

Facoltativamente, è possibile utilizzare RSA Enterprise Manager per personalizzare la notifica di rete inviata all'utente quando si verificano violazioni delle regole. Questa notifica viene inviata da DLP Network in sostituzione del traffico originale.

Verifica dell'installazione

1. Configurare il browser in modo che indirizzi il traffico in uscita dal browser per passare direttamente al proxy WSA.

   Se ad esempio si utilizza il browser Mozilla FireFox, eseguire le operazioni seguenti: Nel browser FireFox, selezionare **Strumenti > Opzioni**. Viene visualizzata la finestra di dialogo Opzioni.Fare clic sulla scheda **Rete**, quindi su **Impostazioni**. Viene visualizzata la finestra di dialogo Impostazioni di connessione.Selezionare la casella di controllo **Manual Proxy Configuration** (Configurazione proxy manuale), quindi immettere l'indirizzo IP o il nome host del server proxy WSA nel campo **HTTP Proxy** (Proxy HTTP) e il numero di porta 3128 (predefinito).Fare clic su **OK**, quindi di nuovo su **OK** per salvare le nuove impostazioni.
2. Tenta di caricare del contenuto che non rispetta i criteri di prevenzione della perdita dei dati precedentemente abilitati.
3. Nel browser dovrebbe essere visualizzato il messaggio Network ICAP discard.
4. Utilizzare 'Enterprise Manager' per visualizzare l'evento e l'evento imprevisto risultante dalla violazione dei criteri.

Risoluzione dei problemi

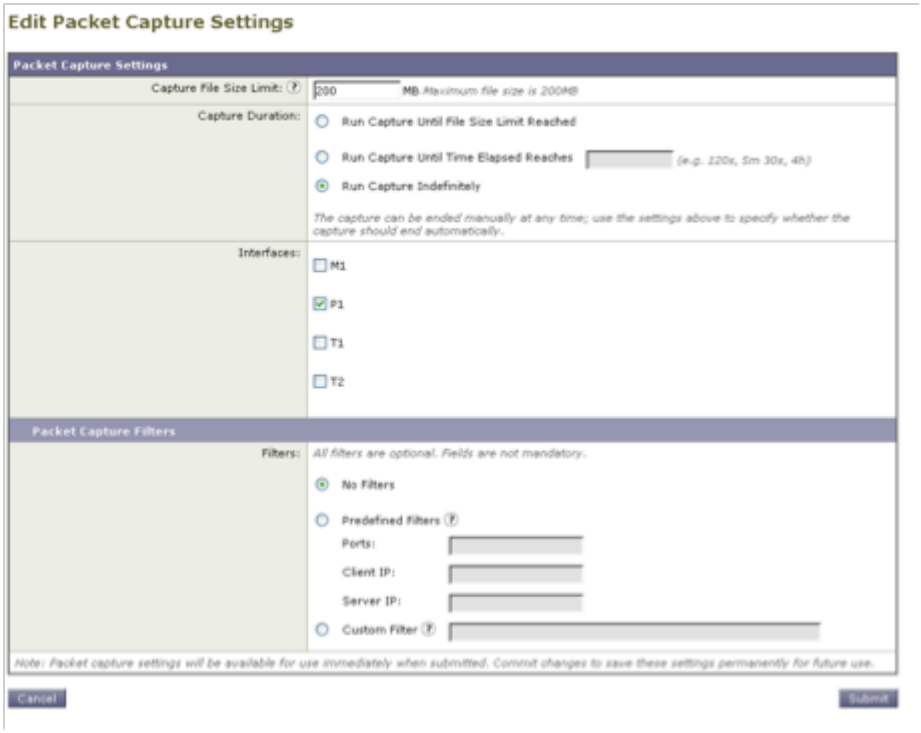
1. Quando si configura un server DLP esterno su Web Security Appliance per RSA DLP

Network, utilizzare i seguenti valori:

Indirizzo server: Indirizzo IP o nome host del server RSA DLP Network ICAPPort: La porta TCP utilizzata per accedere al server RSA DLP Network, in genere **1344**Formato URL servizio: **icap://*<hostname_or_ipaddress>*/srv_conalarm**Esempio: icap://dlp.example.com/srv_conalarm

2. Abilitare la funzionalità di acquisizione del traffico di WSA per acquisire il traffico tra il proxy WSA e il server ICAP di rete. Ciò è utile quando si diagnosticano problemi di connettività. A tale scopo, eseguire le operazioni seguenti:

   Dalla GUI di WSA, accedere al menu **Support and Help** in alto a destra dell'interfaccia utente. Selezionare **Packet Capture** dal menu, quindi fare clic sul pulsante **Edit Settings** (Modifica impostazioni). Viene visualizzata la finestra Modifica impostazioni di cattura.



   Nella sezione **Packet Capture** Filters della schermata, immettere l'indirizzo IP del server ICAP di rete nel campo **Server IP**.Fare clic su **Invia** per salvare le modifiche.

3. Utilizzare il seguente campo personalizzato nei log degli accessi WSA (in ***GUI > Amministrazione sistema > Registra sottoscrizioni >log degli accessi***) per ottenere ulteriori informazioni:
   %Xp: Verdetto di scansione del server DLP esterno (0 = nessuna corrispondenza sul server ICAP; 1 = corrispondenza dei criteri con il server ICAP e '- (trattino)' = Nessuna analisi avviata dal server DLP esterno)

[Istruzioni della Guida per l'utente Definizione dei sistemi DLP esterni.]