Wie werden die Cisco Web Security Appliance und das RSA DLP-Netzwerk für die Interoperabilität konfiguriert?

Inhalt

Frage:

Wie werden die Cisco Web Security Appliance und das RSA DLP-Netzwerk für die Interoperabilität konfiguriert?

Überblick:

Dieses Dokument enthält zusätzliche Informationen, die über das Cisco WSA AsyncOS-Benutzerhandbuch und den RSA DLP Network 7.0.2 Deployment Guide hinausgehen, um Kunden bei der Interoperabilität der beiden Produkte zu unterstützen.

Produktbeschreibung:

Die Cisco Web Security Appliance (WSA) ist ein robustes, sicheres und effizientes Gerät, das Unternehmensnetzwerke vor webbasierter Malware und Spyware-Programmen schützt, die die Unternehmenssicherheit gefährden und geistiges Eigentum offenlegen. Die Websicherheits-Appliance bietet eine tief greifende Überprüfung von Anwendungsinhalten, indem sie einen Webproxy-Dienst für Standardkommunikationsprotokolle wie HTTP, HTTPS und FTP bereitstellt.

Die RSA DLP Suite ist eine umfassende Lösung zur Verhinderung von Datenverlusten, die es Kunden ermöglicht, vertrauliche Daten im Unternehmen zu erkennen und zu schützen, indem sie allgemeine Richtlinien in der gesamten Infrastruktur nutzt, um sensible Daten im Rechenzentrum, im Netzwerk und an Endpunkten zu erkennen und zu schützen. Die SvD-Suite umfasst die folgenden Komponenten:

- RSA-SvD-Rechenzentrum. Das DLP-Rechenzentrum unterstützt Sie bei der Lokalisierung vertraulicher Daten, unabhängig vom Standort im Rechenzentrum, auf Dateisystemen, Datenbanken, E-Mail-Systemen und großen SAN-/NAS-Umgebungen.
- RSA-SvD-Netzwerk. Das DLP-Netzwerk überwacht und erzwingt die Übertragung vertraulicher Informationen im Netzwerk, z. B. E-Mail- und Web-Datenverkehr.
- RSA-SvD-Endpunkt. DLP Endpoint unterstützt Sie bei der Erkennung, Überwachung und Kontrolle vertraulicher Informationen auf Endgeräten wie Laptops und Desktops.

Die Cisco WSA kann mit dem RSA-DLP-Netzwerk zusammenarbeiten.

Das RSA-DLP-Netzwerk umfasst die folgenden Komponenten:

- **Netzwerk-Controller**. Die wichtigste Appliance, die Informationen über vertrauliche Daten und Content-Übertragungsrichtlinien verwaltet. Der Netzwerk-Controller verwaltet und aktualisiert verwaltete Geräte mit Richtlinien und der Definition vertraulicher Inhalte sowie allen Änderungen an deren Konfiguration nach der Erstkonfiguration.
- **Verwaltete Geräte**. Mithilfe dieser Geräte kann das DLP-Netzwerk die Netzwerkübertragung überwachen und die Übertragung melden oder abfangen:
  Sensoren. An den Netzwerkgrenzen installiert, überwachen Sensoren passiv den Datenverkehr, der das Netzwerk verlässt oder die Netzwerkgrenzen überschreitet, und analysieren ihn auf sensible Inhalte. Ein Sensor ist eine Out-of-Band-Lösung. können Richtlinienverletzungen nur überwacht und gemeldet werden.**Interceptoren**. Die an den Netzwerkgrenzen installierten Interceptors ermöglichen Ihnen die Implementierung von Quarantäne- und/oder Ablehnungsfunktionen für E-Mail-Verkehr (SMTP), der sensible Inhalte enthält. Ein Interceptor ist ein Inline-Netzwerk-Proxy und kann daher vertrauliche Daten davon abhalten, das Unternehmen zu verlassen.**ICAP-Server**. Servergeräte für spezielle Zwecke, mit denen Sie HTTP-, HTTPS- oder FTP-Datenverkehr, der sensible Inhalte enthält, überwachen oder blockieren können. Ein ICAP-Server arbeitet mit einem Proxyserver (der als ICAP-Client konfiguriert ist) zusammen, um vertrauliche Daten zu überwachen oder zu blockieren, damit diese das Unternehmen verlassen.

Die Cisco WSA ist mit dem RSA DLP Network ICAP Server kompatibel.

Bekannte Einschränkungen

Die Integration von Cisco WSA mit dem RSA-DLP-Netzwerk für externen SvD unterstützt die folgenden Aktionen: Zulassen und Blockieren. Die Aktion "Ändern/Entfernen von Inhalten" (auch als "Redaktion" bezeichnet) wird noch nicht unterstützt.

Produktanforderungen für die Interoperabilität

Die Interoperabilität des Cisco WSA- und RSA DLP-Netzwerks wurde mit den in der folgenden Tabelle aufgeführten Produktmodellen und Softwareversionen getestet und validiert. Funktionell kann diese Integration mit Variationen des Modells und der Software funktionieren, die folgende Tabelle stellt jedoch die einzige getestete, validierte und unterstützte Kombination dar. Es wird dringend empfohlen, die neueste unterstützte Version beider Produkte zu verwenden.

Produkt	Softwareversion
Cisco Web Security Appliance (WSA)	AsyncOS-Versionen 6.3 und höher
RSA-DLP-Netzwerk	7,0/2

Funktion für externen SvD

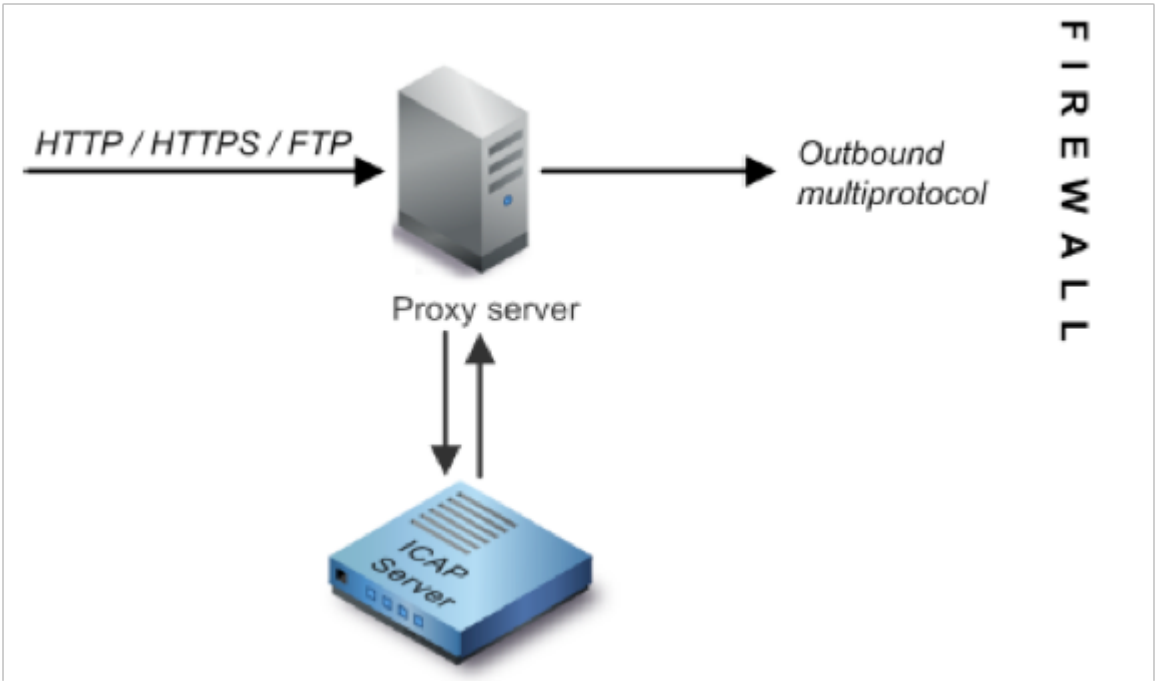
Mit der Funktion für externen SvD der Cisco WSA können Sie den gesamten oder einen bestimmten ausgehenden HTTP-, HTTPS- und FTP-Datenverkehr von der WSA an das DLP-

Netzwerk weiterleiten. Der gesamte Datenverkehr wird über das Internet Control Adaptation Protocol (ICAP) übertragen.

Architektur

Der RSA SvD-Netzwerkbereitstellungsleitfaden zeigt die folgende generische Architektur für RSA-SvD-Netzwerk mit einem Proxyserver für den Betrieb. Diese Architektur ist nicht spezifisch für die WSA, sondern gilt für jeden Proxy, der mit dem RSA DLP-Netzwerk zusammenarbeitet.

Abbildung 1: Bereitstellungsarchitektur für das RSA DLP-Netzwerk und die Cisco Web Security Appliance



Konfigurieren der Cisco Web Security Appliance

1. Definieren Sie ein externes SvD-System auf der WSA, das mit dem SvD-Netzwerk-ICAP-Server zusammenarbeitet. Anweisungen hierzu finden Sie im angehängten Auszug aus dem WSA-Benutzerhandbuch "Anleitungen zur Definition von Systemen für externe DLP".

2. Erstellen Sie eine oder mehrere Richtlinien für externen SvD, die definieren, welchen Datenverkehr die WSA zum SvD-Netzwerk sendet, um Inhalte zu prüfen. Gehen Sie dazu wie folgt vor:

- Unter **GUI > Web Security Manager > Richtlinien für externen SvD > Richtlinie hinzufügen**
- Klicken Sie auf den Link in der Spalte ***Ziele*** für die Richtliniengruppe, die Sie konfigurieren möchten.
- Wählen Sie im Abschnitt "Edit Destination Settings" (Zieleinstellungen bearbeiten) die Option ?Destinationen definieren, die benutzerdefinierte Einstellungen scannen?. aus dem Dropdown-Menü
- Anschließend können wir die Richtlinie so konfigurieren, dass alle Uploads geprüft oder

Uploads auf bestimmte Domänen/Sites geprüft werden, die in benutzerdefinierten URL-Kategorien angegeben sind.

Konfigurieren des RSA SvD-Netzwerks

In diesem Dokument wird davon ausgegangen, dass RSA DLP Network Controller, ICAP Server und Enterprise Manager installiert und konfiguriert wurden.

1. Verwenden Sie RSA DLP Enterprise Manager, um einen Netzwerk-ICAP-Server zu konfigurieren. Detaillierte Anweisungen zum Einrichten des DLP-Netzwerk-ICAP-Servers finden Sie im RSA SvD-Netzwerkbereitstellungsleitfaden. Die wichtigsten Parameter, die Sie auf der Konfigurationsseite des ICAP-Servers angeben sollten, sind: Der Hostname oder die IP-Adresse des ICAP-Servers.Geben Sie im Abschnitt **Allgemeine Einstellungen** der Konfigurationsseite die folgenden Informationen ein: Die Zeitdauer in Sekunden, nach der der Server im Feld **Server Timeout in Sekunden** als Zeitüberschreitung gilt.Wählen Sie eine der folgenden Optionen als Antwort **Beim Server-Timeout aus**:**Fail Open**. Wählen Sie diese Option aus, wenn die Übertragung nach einem Server-Timeout zugelassen werden soll.**Fehlgeschlagen**. Wählen Sie diese Option aus, wenn die Übertragung nach einem Server-Timeout blockiert werden soll.
2. Erstellen Sie mit dem RSA DLP Enterprise Manager eine oder mehrere netzwerkspezifische Richtlinien, um Netzwerkdatenverkehr mit vertraulichen Inhalten zu überwachen und zu blockieren. Ausführliche Anweisungen zum Erstellen von SvD-Policys finden Sie im RSA SvD-Netzwerk-Benutzerhandbuch oder in der Online-Hilfe des Enterprise Managers. Die wichtigsten Schritte sind die folgenden: Aktivieren Sie in der Richtlinienvorlagenbibliothek mindestens eine Richtlinie, die für Ihre Umgebung und die zu überwachenden Inhalte sinnvoll ist.Legen Sie in dieser Richtlinie netzwerkspezifische SvD-Policy-Verletzungsregeln fest, die festlegen, welche Aktionen das Netzwerkprodukt automatisch ausführt, wenn Ereignisse (Richtlinienverletzungen) auftreten. Legen Sie die Richtlinien-Erkennungsregel fest, um alle Protokolle zu erkennen. Legen Sie für die Richtlinienaktion "Audit and Block" (Audit und Blockierung) fest.

Optional können wir RSA Enterprise Manager verwenden, um die Netzwerkbenachrichtigung anzupassen, die an den Benutzer gesendet wird, wenn Richtlinienverletzungen auftreten. Diese Benachrichtigung wird vom DLP-Netzwerk gesendet, um den ursprünglichen Datenverkehr zu ersetzen.

Testen des Setups

1. Konfigurieren Sie Ihren Browser so, dass ausgehender Datenverkehr vom Browser direkt an den WSA-Proxy geleitet wird.

   Wenn Sie beispielsweise den Browser Mozilla FireFox verwenden, gehen Sie wie folgt vor: Wählen Sie im FireFox-Browser **Extras > Optionen**. Das Dialogfeld Optionen wird angezeigt.Klicken Sie auf die Registerkarte **Netzwerk** und anschließend auf **Einstellungen**. Das Dialogfeld Verbindungseinstellungen wird angezeigt.Aktivieren Sie das Kontrollkästchen

Manual Proxy Configuration (Manuelle Proxy-Konfiguration), und geben Sie dann die IP-Adresse oder den Hostnamen des WSA-Proxyservers im Feld **HTTP Proxy** und die Portnummer 3128 (Standard) ein.Klicken Sie auf **OK**, und **OK** erneut, um die neuen Einstellungen zu speichern.

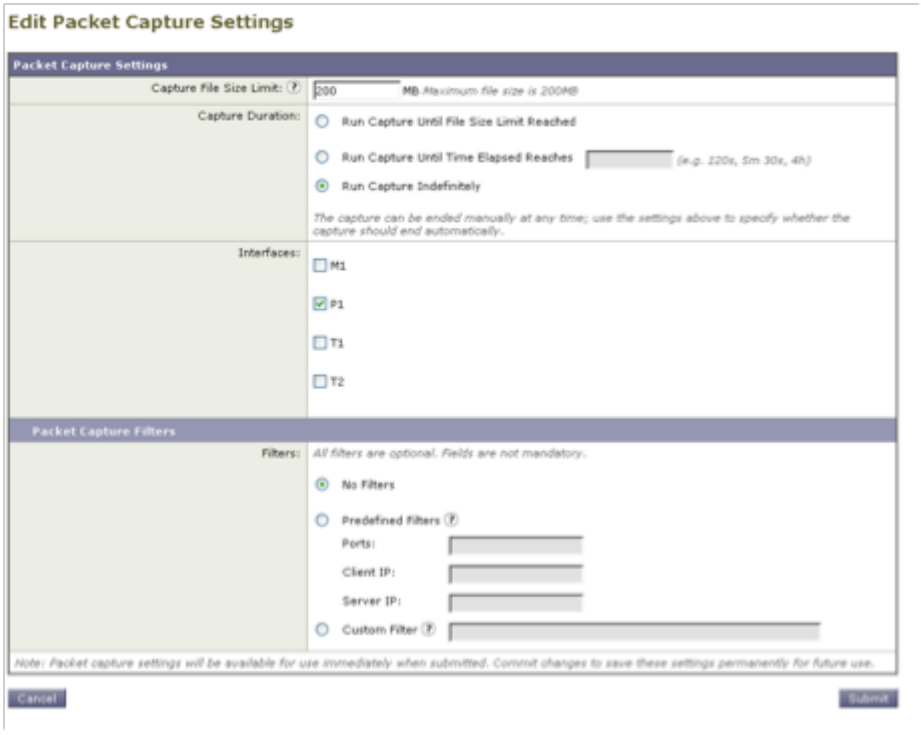
2. Versuchen Sie, Inhalte hochzuladen, von denen Sie wissen, dass sie gegen die DLP-Netzwerkrichtlinie verstoßen, die Sie zuvor aktiviert haben.
3. Im Browser sollte eine Network ICAP-Nachricht zur Rücknahme angezeigt werden.
4. Verwenden Sie "Enterprise Manager", um das aus dieser Richtlinienverletzung resultierende Ereignis und den daraus resultierenden Vorfall anzuzeigen.

Fehlerbehebung

1. Verwenden Sie beim Konfigurieren eines externen SvD-Servers in der Websicherheits-Appliance für das RSA-SvD-Netzwerk die folgenden Werte:

   Serveradresse: Die IP-Adresse oder der Hostname des RSA DLP Network ICAP-ServersPort: Der TCP-Port, der für den Zugriff auf den RSA SvD-Netzwerkserver (in der Regel **1344)** verwendet wirdService-URL-Format: **icap://*<hostname_or_ipaddress>*/srv_conalarm**Beispiel: icap://dlp.example.com/srv_conalarm
2. Aktivieren Sie die Traffic Capturing-Funktion der WSA, um den Datenverkehr zwischen dem WSA-Proxy und dem Netzwerk-ICAP-Server zu erfassen. Dies ist hilfreich bei der Diagnose von Verbindungsproblemen. Gehen Sie dazu wie folgt vor:

   Gehen Sie auf der WSA-GUI zum Menü **Support und Hilfe** oben rechts auf der Benutzeroberfläche. Wählen Sie **Paketerfassung** aus dem Menü aus, und klicken Sie dann auf die Schaltfläche **Einstellungen bearbeiten**. Das Fenster Einstellungen für die Erfassung bearbeiten wird angezeigt.



Geben Sie im Bereich **Packet Capture** Filters (**Paketerfassungsfilter**) des Bildschirms die IP-Adresse des Netzwerk-ICAP-Servers im **Server-IP-**Feld ein.Klicken Sie auf **Senden**, um die Änderungen zu

speichern.

3. Verwenden Sie das folgende benutzerdefinierte Feld in den WSA-Zugriffsprotokollen (unter *GUI > Systemverwaltung > Protokoll-Subscriptions >Zugriffsprotokolle*), um weitere Informationen abzurufen:
   %XP: Scanning-Verdict für Server mit externem SvD (0 = keine Übereinstimmung auf dem ICAP-Server); 1 = Übereinstimmung der Richtlinien mit dem ICAP-Server und '- (Bindestrich)' = Vom externen SvD-Server wurde kein Scan initiiert.)

Anleitungen zum Definieren externer SvD-Systeme.