

Hoe te om Cisco web security applicatie en RSA DLP netwerk te configureren voor samenwerking?

Inhoud

Vraag:

Hoe te om Cisco web security applicatie en RSA DLP netwerk te configureren voor samenwerking?

Overzicht:

Dit document biedt extra informatie buiten de Cisco WSA AsyncOS-gebruikersgids en de RSA DLP Network 7.0.2 implementatiegids om klanten te helpen bij de samenwerking met de twee producten.

Productbeschrijving:

Cisco Web Security Appliance (WSA) is een robuust, veilig, efficiënt apparaat dat bedrijfsnetwerken beschermt tegen op internet gebaseerde malware- en spyware-programma's die de bedrijfsbeveiliging kunnen aantasten en intellectueel eigendom kunnen blootstellen. Het apparaat voor webbeveiliging biedt een diepe inspectie van toepassingsinhoud door een web proxy-service aan te bieden voor standaard communicatieprotocollen zoals HTTP, HTTPS en FTP.

De RSA DLP Suite omvat een uitgebreide oplossing voor de preventie van gegevensverlies die klanten in staat stelt om gevoelige gegevens in de onderneming te ontdekken en te beschermen door gebruik te maken van gemeenschappelijk beleid over de infrastructuur om gevoelige gegevens in het datacenter, op het netwerk en op endpoints te ontdekken en te beschermen. DLP Suite bevat de volgende onderdelen:

- **RSA DLP Datacenter.** DLP Datacenter helpt u gevoelige gegevens te lokaliseren, ongeacht waar ze zich in het datacenter bevinden, op bestandssystemen, databases, e-mailsystemen en grote SAN/NAS-omgevingen.
- **RSA DLP-netwerk.** DLP Network bewaakt en dwingt de overdracht van gevoelige informatie op het netwerk, zoals e-mail en webverkeer, af.
- **RSA DLP-eindpunt.** DLP-endpoint helpt u gevoelige informatie op endpoints zoals laptops en desktops te detecteren, bewaken en beheersen.

De Cisco WSA heeft de mogelijkheid om met het DLPnetwerk van RSA samen te werken.

RSA DLP Network bevat de volgende onderdelen:

- **Netwerkcontroller.** Het hoofdapparaat dat informatie over vertrouwelijke gegevens en inhoud transmissiebeleid bijhoudt. De netwerkcontroller beheert en werkt beheerde apparaten bij met beleid en gevoelige contentdefinitie samen met wijzigingen in hun configuratie na eerste configuratie.
- **Beheerde apparaten.** Deze apparaten helpen DLP Network Monitoring Network Transformer en melden of onderscheppen de overdracht:
 - Sensoren.** Geïnstalleerd aan netwerkgrenzen, controleren Sensors passief verkeer voorbij het netwerk of overschrijden netwerkgrenzen, en analyseren het op de aanwezigheid van gevoelige inhoud. Een sensor is een out-of-band oplossing; zij kan alleen maar overtredingen van het beleid controleren en melden.
 - Interceptoren.** Ook geïnstalleerd op netwerkgrenzen, staan Interceptors u toe om quarantaine en/of afwijzing van e-mail (mtd) verkeer uit te voeren dat gevoelige inhoud bevat. Een Interceptor is een in-line netwerk proxy en kan daarom gevoelige gegevens blokkeren om de onderneming te verlaten.
 - ICAP-servers.** Speciale serverapparaten die u in staat stellen om controle of blokkering van HTTP, HTTPS of FTP-verkeer te implementeren die gevoelige inhoud bevatten. Een ICAP-server werkt met een proxy-server (geconfigureerd als een ICAP-client) om gevoelige gegevens te controleren of te blokkeren vanaf het verlaten van de onderneming

Cisco WSA interopereert met RSA DLP Network ICAP Server.

Bekende beperkingen

Cisco WSA Externe DLP-integratie met RSA DLP-netwerk ondersteunt de volgende acties: Laat staan. Deze ondersteunt de actie "Content wijzigen / verwijderen" (ook Redactie genoemd) nog niet.

Productvereisten voor interoperabiliteit

De interoperabiliteit van het Cisco WSA- en RSA DLP-netwerk is getest en gevalideerd met de productmodellen en softwareversies in de volgende tabel. Hoewel deze integratie functioneel kan werken met variaties in het model en de software, representeert de volgende tabel de enige geteste, gevalideerde en ondersteunde combinaties. Het is sterk aanbevolen de laatste ondersteunde versie van beide producten te gebruiken.

Product	Softwareversie
Cisco web security applicatie (WSA)	AsyncOS-versies 6.3 en hoger
RSA DLP-netwerk	7.0.2

Externe DLP-functies

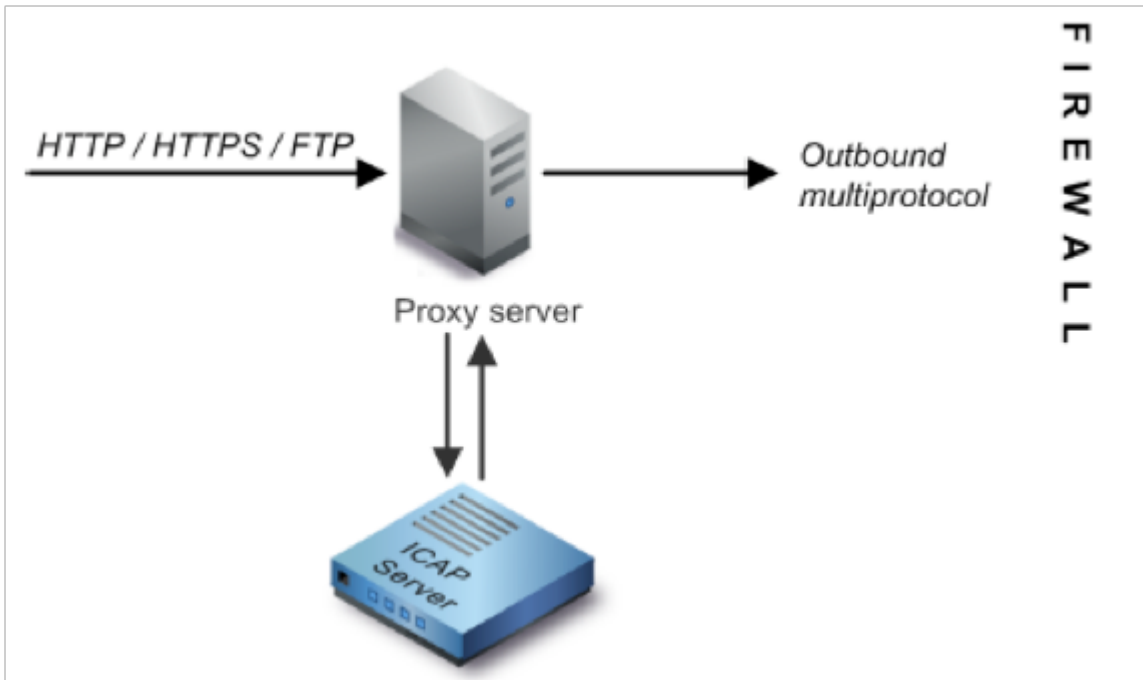
Met behulp van de externe DLP-functie van Cisco WSA kunt u alle of specifieke uitgaande HTTP-, HTTPS- en FTP-verkeer van het WSA naar DLP-netwerk doorsturen. Al het verkeer wordt

overgedragen via het Internet Control Adapter Protocol (ICAP).

Architectuur

De RSA DLP Network Deployment Guide toont de volgende algemene architectuur voor interactief RSA DLP Network met een proxy-server. Deze architectuur is niet specifiek voor de WSA, maar is van toepassing op elke proxy die interopereert met RSA DLP Network.

Afbeelding 1: Deployment Architecture for RSA DLP Network en Cisco Web Security Appliance



De Cisco web security applicatie configureren

1. Definieer een extern DLP-systeem op de WSA-server die met de DLP Network ICAP-server werkt. Raadpleeg voor meer informatie het bijgevoegde fragment uit de WSA-gebruikershandleiding "Gebruikershandleiding met instructies voor externe DLP-systemen".
2. Maak een of meer extern DLP-beleid dat definieert welk verkeer de WSA naar DLP Network stuurt voor het scannen van content met behulp van de volgende stappen:
 - Onder **GUI > Web security Manager > Extern DLP-beleid > Toevoegen-beleid**
 - Klik op de link onder de kolom **Bestanden** voor de beleidsgroep die u wilt configureren
 - Selecteer in het gedeelte "Bestemmingsinstellingen bewerken" de optie Bestanden scannen door aangepaste instellingen te definiëren? in het uitrolmenu
 - We kunnen dan het beleid configureren om 'alle uploads te scannen' of het uploaden naar bepaalde domeinen/sites, gespecificeerd in aangepaste URL-categorieën

Het RSA DLP-netwerk configureren

Dit document gaat ervan uit dat RSA DLP Network Controller, ICAP Server en Enterprise Manager zijn geïnstalleerd en geconfigureerd.

1. Gebruik RSA DLP Enterprise Manager om een Network ICAP Server te configureren. Raadpleeg de RSA DLP Network Deployment Guide voor uitgebreide instructies voor het instellen van uw DLP Network ICAP-server. De belangrijkste parameters die u op de configuratie van de ICAP-server moet specificeren, zijn: De hostnaam of IP-adres van de ICAP-server. Geef in het gedeelte **Algemene instellingen** van de configuratiescherm de volgende informatie op: De hoeveelheid tijd in seconden waarna de server geacht wordt te zijn uitgezet in het veld **Time-out server in seconden**. Selecteer een van de volgende opties als reactie op **Time-out bij servers: Niet open**. Selecteer deze optie als u transmissie na een server timeout wilt toestaan. **Gevallen gesloten**. Selecteer deze optie als u transmissie na een server onderbreking wilt blokkeren.
2. Gebruik RSA DLP Enterprise Manager om één of meer netwerkspecifiek beleid te maken om netwerkverkeer te controleren en te blokkeren dat gevoelige inhoud bevat. Raadpleeg voor gedetailleerde instructies voor het maken van DLP-beleid de RSA DLP-netwerkgebruikershandleiding of de Enterprise Manager online ondersteuning. De volgende stappen moeten worden uitgevoerd: In de bibliotheek van het beleidssjabloon kunt u ten minste één beleid maken dat zinvol is voor uw omgeving en de inhoud controleren. Binnen dat beleid, zal de opstelling van DLPnetwerk-specifieke regels van de beleidsschending die acties specificeren het Networkproduct automatisch zal uitvoeren wanneer gebeurtenissen (beleidsschendingen) zich voordoen. Stel de regel voor beleidsdetectie in om alle protocollen te detecteren. Stel de beleidsactie in op "audit and block".

Optioneel kunnen we RSA Enterprise Manager gebruiken om het netwerkbericht aan te passen dat naar de gebruiker wordt verzonden wanneer beleidsovertredingen optreden. Dit bericht wordt door DLP Network verstuurd als vervanging voor het oorspronkelijke verkeer.

De instelling testen

1. Configureer de browser om uitgaande verkeer van uw browser af te leiden om direct naar de WSA proxy te gaan.

Als u bijvoorbeeld de browser Mozilla FireFox gebruikt, gaat u als volgt te werk: Selecteer in de browser FireFox **Gereedschappen > Opties**. Het dialoogvenster Opties verschijnt. Klik op het tabblad **Netwerk** en vervolgens op **Instellingen**. Het dialoogvenster Connection-instellingen verschijnt. Selecteer het selectieteken **Handmatige proxy** en voer vervolgens het IP-adres of de hostnaam van de WSA-proxyserver in het veld **HTTP Proxy** en het poortnummer 3128 (de standaardinstelling) in. Klik op **OK**, dan **OK** opnieuw om de nieuwe instellingen op te slaan.

2. Probeer bepaalde inhoud te uploaden waarvan u weet dat deze in strijd is met het DLP-netwerkbeleid dat u eerder hebt ingeschakeld.
3. U dient een Network ICAP disard-bericht te zien in de browser.
4. Gebruik 'Enterprise Manager' om de gebeurtenis en het incident te bekijken die zijn ontstaan als gevolg van deze beleidsschending.

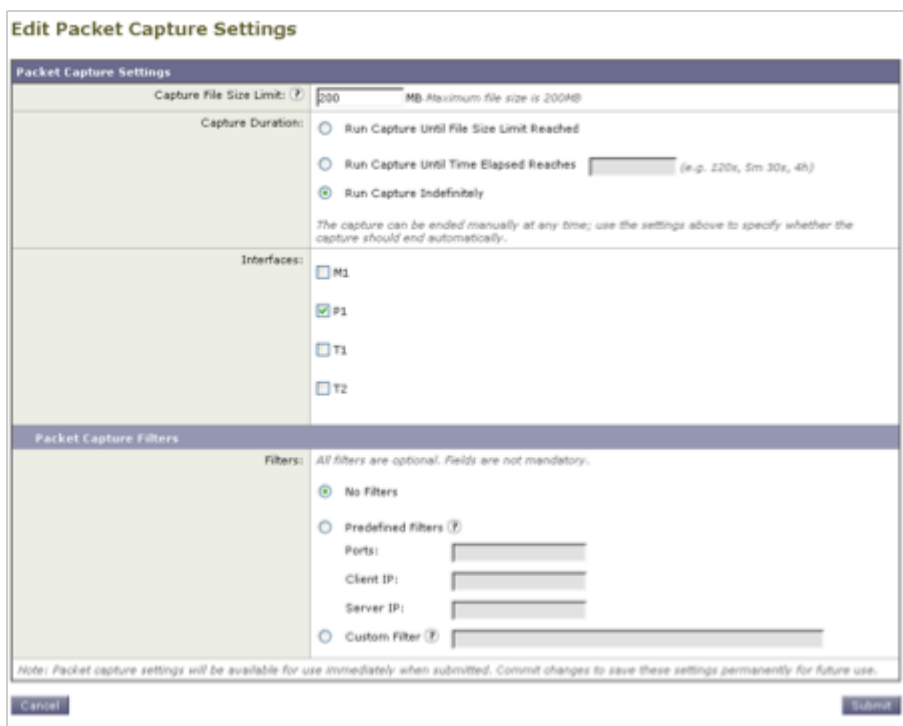
Probleemoplossing

1. Gebruik bij het configureren van een externe DLP-server op het Web security apparaat voor RSA DLP-netwerk de volgende waarden:

Serveradres: Het IP-adres of de hostnaam van de RSA DLP Network ICAP-server
Port: De TCP poort die wordt gebruikt voor toegang tot de RSA DLP-netwerkserver, doorgaans 1344
URL-indeling voor service: `icap://<hostname_or_ipaddress>/srv_conalarm`
Voorbeeld: `icap://dlp.example.com/srv_conalarm`

2. Schakel de opnamefunctie van WSA in om het verkeer tussen WSA-proxy en de Network ICAP-server op te nemen. Dit is handig bij het diagnosticeren van problemen met connectiviteit. U kunt dit als volgt doen:

Ga in WSA GUI naar het menu **Ondersteuning en Help** rechtsboven in de gebruikersinterface. Selecteer **Packet Capture** in het menu en klik vervolgens op de knop **Instellingen bewerken**. Het venster Opname-instellingen bewerken verschijnt.



Voer in het gedeelte **Packet Capture Filters** van het scherm het IP-adres in van de Network ICAP server in het **IP-veld Server**. Klik op **Inzenden** om de wijzigingen op te slaan.

3. Gebruik het volgende aangepaste veld in de WSA-toegangslogbestanden (onder **GUI > Stroombeheer > Inscripties > accessoires**) om meer informatie te krijgen:
%p: Externe DLP-serverscanuitspraak (0 = geen overeenkomst op de ICAP-server; 1 = beleidsmatch tegen de ICAP server en '-' (koppeltteken) = Er is geen scannen gestart door de externe DLP server)

[Gebruikershandleiding: instructies voor het definiëren van externe DLP-systemen.](#)