ESA DHAP-functiemogelijkheid

Inhoud

Inleiding

Dit document beschrijft hoe u de functie Directory Harvest Attack Prevention (DHAP) op de Cisco Email Security Applicatie (ESA) kunt inschakelen om Directory Harvest Attacks (DHA's) te voorkomen.

Voorwaarden

Vereisten

Cisco raadt kennis van de volgende onderwerpen aan:

- Cisco ESA
- AsyncOS

Gebruikte componenten

De informatie in dit document is gebaseerd op alle versies van AsyncOS.

De informatie in dit document is gebaseerd op de apparaten in een specifieke laboratoriumomgeving. Alle apparaten die in dit document worden beschreven, hadden een opgeschoonde (standaard)configuratie. Als uw netwerk live is, moet u de potentiële impact van elke opdracht begrijpen.

Achtergrondinformatie

Een DHA is een techniek die door spammers wordt gebruikt om geldige e-mailadressen te vinden. Er zijn twee hoofdtechnieken die worden gebruikt om de adressen te genereren die DHA beoogt:

- De spammer maakt een lijst van alle mogelijke combinaties van letters en cijfers en voegt vervolgens de domeinnaam toe.

- De spammer gebruikt een standaard woordenboek aanval met de creatie van een lijst die gemeenschappelijke voornamen, familienamen, en initialen combineert.

DHAP is een ondersteunde functie op de Cisco Content Security Appliances die kunnen worden ingeschakeld wanneer LDAP-acceptatie (Lichtgewicht Directory Access Protocol) wordt gebruikt. De DHAP-functie houdt bij hoeveel ongeldige geadresseerde adressen van een bepaalde afzender worden gegenereerd.

Zodra een afzender een door de beheerder gedefinieerde drempel overschrijdt, wordt de afzender geacht niet te worden vertrouwd en wordt de e-mail van die afzender geblokkeerd zonder Network Design Requirement (NDR) of het genereren van foutcodes. U kunt de drempel configureren op basis van de reputatie van de afzender. Onbetrouwbare of verdachte afzenders kunnen bijvoorbeeld een lage DHAP-drempel hebben, en vertrouwde of achtenswaardige afzenders kunnen een hoge DHAP-drempel hebben.

DHAP inschakelen

Om de DHAP-functie in te schakelen, navigeer naar **Mail Policies > Host Access Table (HAT)** vanuit de Content Security Appliance GUI en selecteer **Mail Flow Policies**. Kies het beleid dat u wilt bewerken in de kolom **Beleidsnaam**.

De HAT heeft vier basistoegangsregels die worden gebruikt om te reageren op verbindingen van externe hosts:

- **AANVAARDEN**: De verbinding wordt geaccepteerd en e-mailacceptatie wordt verder beperkt door de instellingen van de luisteraar. Dit omvat de Begunstigde Toegangstabel (voor openbare luisteraars).
- **AFWIJZEN**: De verbinding wordt aanvankelijk geaccepteerd, maar de client die probeert verbinding te maken, ontvangt een 4XX- of 5XX-groet. Geen email wordt geaccepteerd.
- **TCPREFUSE**: De verbinding wordt geweigerd op TCP-niveau.
- **RELAY**: De verbinding wordt geaccepteerd. Ontvangen voor elke ontvanger is toegestaan en wordt niet beperkt door de ontvangende toegangstabel. Domain Keys-ondertekening is alleen beschikbaar op beleid voor doorgifte van e-mail.

In de sectie **Mail Flow Limits** van het geselecteerde beleid, vind en stel de **Directory Harvest Attack Prevention (DHAP) configuratie in door de Max.** Ongeldige ontvangers per uur. U kunt ook kiezen om de Max. Ongeldige ontvangers per uur code en Max. Ongeldige ontvangers per uur Tekst als u dat wenst.

U moet deze sectie herhalen om DHAP voor extra beleid te configureren.

Zorg ervoor dat u alle wijzigingen in de GUI indient en vastlegt.

> **Opmerking:** Cisco raadt u aan een maximum aantal tussen vijf en tien te gebruiken voor het **maximale aantal ongeldige ontvangers per uur vanaf een externe host-**instelling.

> **Opmerking:** Raadpleeg de **AsyncOS-gebruikershandleiding** op het Cisco-ondersteuningsportal voor meer informatie.

Over deze vertaling

Cisco heeft dit document vertaald via een combinatie van machine- en menselijke technologie om onze gebruikers wereldwijd ondersteuningscontent te bieden in hun eigen taal. Houd er rekening mee dat zelfs de beste machinevertaling niet net zo nauwkeurig is als die van een professionele vertaler. Cisco Systems, Inc. is niet aansprakelijk voor de nauwkeurigheid van deze vertalingen en raadt aan altijd het oorspronkelijke Engelstalige document (link) te raadplegen.