Begrijp parameters met betrekking tot Mail Flow-beleid en doelcontroles

Inhoud

Inleiding

In dit document worden een aantal configuratieaspecten van de e-mail security applicatie (ESA) beschreven in welke richting u de Senders en de Delivery System wilt bedienen. De functies die in het artikel zullen worden beschreven zijn het beleid van de Mail Flow en de Bestemmingscontroles.

Voorwaarden

Vereisten

Cisco raadt kennis van de volgende onderwerpen aan:

- Basisbegrip van het beleid ten aanzien van de Mail Flow en de Destination Control
- Bekendheid met het gebruik van deze kenmerken in de configuratie van het ESA

Gebruikte componenten

Dit document is niet beperkt tot specifieke software- en hardware-versies.

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 levend is, zorg er dan voor dat u de mogelijke impact van om het even welke opdracht begrijpt.

Voordelen van Mail Flow-beleid en doelcontroles

Er is één zeer belangrijke functie die beide functies hebben, namelijk snelheidsbeperking/Throttling. Dit aspect helpt de beheerder de controle te hebben over het vrije verkeer en over het verkeer dat met beperkingen moet worden toegestaan.

Mail Flow-beleid

Dit is het beleid dat van toepassing is op de verzendende Groepen van het ESA, op basis waarvan het e-mailverkeer wordt gemoduleerd.

Het beleid van de Mail Flow is altijd van toepassing op het verkeer dat de ESA binnenkomt, ongeacht of de e-mail een inkomende of uitgaande e-mail is.

Het beleid van Mail Flow werkt in het achterste met betrekking tot het geselecteerde verbindingsgedrag voor dat beleid. De verschillende verbindingsgedragingen die in ESA's beschikbaar zijn, zijn:

1. aanvaarden
2. afwijzen
3. Relay
4. TCP-herkenning
5. Doorgaan

Aanvaard: De verbinding wordt geaccepteerd en de e-mailacceptatie wordt vervolgens verder beperkt door luisteraarinstellingen, inclusief de Content Access Table (voor openbare luisteraars). Dit verbindingsgedrag behandelt een e-mail als inkomende

Afwijzen: De client die probeert verbinding te maken krijgt een 4XX of 5XX status code met een MTP-status. Een e-mail is niet geaccepteerd. Dit wordt voornamelijk gebruikt voor Blacklisting-zenders

Relay: Verbinding wordt geaccepteerd. Het ontvangen voor elke ontvanger is toegestaan en wordt niet beperkt door de ontvangstentabel. Dit behandelt een e-mail als een uitgaande e

TCP-weigering: Verbinding wordt geweigerd op het TCP-niveau.

Doorgaan: Het in kaart brengen in het HAT wordt genegeerd en de verwerking van het HAT gaat door. Als de inkomende verbinding overeenkomt met een latere ingang die niet VERDER is, dan wordt die ingang gebruikt. De CONTINUE-regel wordt gebruikt om het bewerken van de HAT in de GUI te vergemakkelijken.

Componenten voor een Mail Flow Policy

Max. Berichten per verbinding: Het maximum aantal berichten dat door deze luisteraar per verbinding van een afstandsbediening kan worden verstuurd. Elk ICID toont één verbinding

Max. Ontvangers per bericht: Het maximum aantal ontvangers per bericht dat van deze host wordt geaccepteerd die wordt verwerkt met behulp van dit Mail Flow Policy

Max. Berichtgrootte: De maximum grootte van een bericht dat door deze luisteraar zal worden aanvaard die aan het beleid van de Mail Flow wordt getagd. De kleinste mogelijke maximale berichtgrootte is 1 kilobyte.

Max. Gelijktijdige verbindingen vanaf één IP: Het maximum aantal gelijktijdige verbindingen is toegestaan om aan deze luisteraar te verbinden van één enkel IP adres.

Aangepaste MTP-banner-code: De terugkerende code van het KMO wanneer een verbinding met deze luisteraar wordt gevestigd.

Aangepaste MTP-tekst: De terugkerende tekst van de mtp-banner wanneer een verbinding met deze luisteraar tot stand wordt gebracht. U kunt een aantal variabelen in dit veld gebruiken.

Toon de Hostname van het Kremmer van de Kant van het KRG met voeten: Standaard zal het apparaat de hostname omvatten verbonden met de interface van de luisteraar wanneer de MTP-banner wordt weergegeven naar externe hosts (bijvoorbeeld 220-hostname ESMTP). U kunt ervoor kiezen om deze banner te omzeilen door hier een andere hostname in te voeren. Daarnaast kunt u het veld hostname blanco laten om ervoor te kiezen *geen* hostname in de banner weer te geven.

Grenswaarden voor Mail-Flow

Max. Ontvangers per uur: Het maximum aantal ontvangers per uur deze luisteraar zal van een afstandsbediening ontvangen. Het aantal ontvangers per verzender IP-adres wordt mondiaal gevolgd. Elke luisteraar volgt zijn eigen snelheidsbeperkende drempel, echter, omdat alle luisteraars tegen één enkele teller waarderen, is het waarschijnlijker dat de snelheidsgrens zal worden overschreden als het zelfde IP adres (afzender) met meerdere luisteraars verbonden is. U kunt een aantal variabelen in dit veld gebruiken.

Max. Ontvangers per uur-code: De terug te geven code van de partij is wanneer een gastheer het maximum aantal ontvangers per uur overschrijdt dat voor deze luisteraar is bepaald.

Max. Ontvangst per uur tekst: De terug te geven tekst van de kastdroog van de partij wanneer een host het maximum aantal ontvangers per uur overschrijdt dat voor deze luisteraar is gedefinieerd.

Snelheidsbeperking voor zenders voor ondernemingen

Max. Ontvangers per tussenkomst: Het maximum aantal ontvangers gedurende een bepaalde periode dat deze luisteraar van een unieke envelopzender zal ontvangen, gebaseerd op de mail-van-adres. Het aantal ontvangers wordt wereldwijd gevolgd. Elke luisteraar volgt zijn eigen snelheidsbeperkende drempel; omdat alle luisteraars echter tegen één teller waarderen, is het waarschijnlijker dat de tarieflimiet zal worden overschreden als berichten van hetzelfde mailadres door meerdere luisteraars worden ontvangen.

Foutcode voor verzendsnelheid: De terug te geven MTP-code wanneer een envelop het maximum

aantal ontvangers voor het voor deze luisteraar vastgestelde tijdsinterval overschrijdt.

Fout bij sturen van snelheidsbeperking: De terug te geven tekst van de mtp banner wanneer een envelopzender het maximum aantal ontvangers voor het tijdinterval overschrijdt dat voor deze luisteraar is bepaald.

Uitzonderingen: Als u wilt dat bepaalde envelopzenders worden vrijgesteld van de gedefinieerde tarieflimiet, selecteert u een adreslijst die de envelopverzendaars bevat.

De adreslijst is gedefinieerd op basis van een adreslijst per e-mail (volledige e-mailadressen, domeinen, IP-adressen kunnen voor vrijstellingen worden gebruikt)

Gebruik SenderBase voor Flow Control: Schakel "lookups" in op de SenderBase Reputation Service voor deze luisteraar.

Gelijksoortige groep IP-adressen: Gebruikt om inkomende e-mail op een per-IP adresbasis te volgen en te snellen terwijl u ingangen in de Host Access Table (HAT) van een luisteraar beheert in grote CIDR-blokken. U definieert een reeks significante bits (van 0 tot 32) waarmee u soortgelijke IP-adressen kunt groeperen voor het beperken van snelheden, terwijl u nog steeds een individuele teller voor elk IP-adres binnen dat bereik houdt.

OPMERKING: Vereist dat "Gebruik SenderBase" wordt uitgeschakeld.

Directory Harvest Prevention (DHAP)

Max. Ongeldige ontvangers per uur: Het maximum aantal ongeldige ontvangers per uur deze luisteraar zal van een afstandsbediening ontvangen. Deze drempel vertegenwoordigt het totale aantal RAT-afwijzingen en de afwijzingen van de TCP-server in het midden van de MTP-verbinding, gecombineerd met het totale aantal berichten naar ongeldige LPDP-ontvangers die in de MTP-discussie zijn gevallen of in de werkwachtrij zijn aangekondigd (zoals in de LDAP-modus wordt bepaald, accepteert instellingen op de aangesloten luisteraar).

Vervalverbinding als de drempel van DHAP binnen een gesprek wordt bereikt MTP:

Het apparaat laat een verbinding met een host vallen wanneer de drempel voor ongeldige ontvangers is bereikt.

Max. Ongeldige ontvangers per uur code: Specificeer de te gebruiken code bij het laten vallen van verbindingen. De standaardcode is 550.

Max. Ongeldige ontvangers per uur tekst: Specificeer de tekst die voor verbroken verbindingen moet worden gebruikt. De standaardtekst is "Te veel ongeldige ontvangers.

Beveiligingsfuncties

APM / AMP / Virus / Sender Domain Reputation Verification / Outbreak Filters / Advanced Phishing Protection / Graymail / Content & Message Filters: Het scannen van security engines / scannen en filters kan vanaf hier worden ingeschakeld of uitgeschakeld

Encryptie en verificatie: We kunnen instellingen als Uit wijzigen, voorkeuren of transportlaag beveiliging (TLS) in TCP-gesprekken voor deze luisteraar vereisen.

Met de optie Klantencertificaat controleren wordt het apparaat voor e-mail beveiliging aangestuurd om een TLS-verbinding op te zetten met de e-mailtoepassing van de gebruiker indien het clientcertificaat geldig is.

Voor de TLS voorkeursbehandeling biedt het apparaat nog steeds een non-TLS verbinding als de gebruiker geen certificaat heeft, maar wijst het een verbinding af als de gebruiker een ongeldig certificaat heeft.

Voor de instelling van het TLS schrijft u voor deze optie dat de gebruiker over een geldig certificaat moet beschikken zodat het apparaat kan worden aangesloten.

TCP-verificatie: hiermee wordt een TCP-verificatie mogelijk, verboden of vereist van externe hosts die verbinding maken met de luisteraar

Als zowel TLS als TCP verificatie zijn ingeschakeld: Vereist dat TLS-verificatie TCP aanbiedt

Domain Key/DKIM-signalering: Domain Keys of DKIM-ondertekening op deze luisteraar inschakelen

DKIM-verificatie : Schakel DKIM-verificatie in.

S/MIME-decryptie/verificatie: S/MIME-decryptie of verificatie inschakelen.

Handtekening na verwerking: Kies of u de digitale handtekening na een S/MIME-verificatie uit de berichten wilt behouden of verwijderen.

S/MIME openbare sleutel voor het verzamelen van: S/MIME voor het weergeven van openbare toetsen inschakelen.

Oogstcertificaten bij niet-naleving van verificaties: Kies of u publieke sleutels wilt oogsten als de verificatie van de inkomende ondertekende berichten mislukt.

Bewaar bijgewerkt certificaat: Kies of u bijgewerkte openbare toetsen wilt oogsten

SFP-/SIDF-verificatie: SPF/SIDF inschakelen voor deze luisteraar.

Conformiteitsniveau : Stel het SPF/SIDF-conformiteitsniveau in. U kunt kiezen uit compatibel met SPF, SIDF of SIDF

Resultaat PRA-verificatie als 'Resent-Sender:' of 'Resent-From:' zijn gebruikt: Als u een conformiteitsniveau van SIDF-compatibel kiest, moet u dan configureren of u Pass-resultaat van de PRA Identity-verificatie wilt downloaden naar No indien er Sent-Sender is: of beantwoord: kopregels in het bericht

HELO-test: Configureer of u een test wilt uitvoeren met de HELO-identiteit (gebruik deze voor SPF- en SIDF-compatibele conformiteitsniveaus)

DMARC-verificatie: Controleer DMARC op deze luisteraar inschakelen

Verificatieprofiel gebruiken: Selecteer het DMARC-verificatieprofiel dat u op deze luisteraar wilt gebruiken. Dit zelfde wordt gemaakt van postbeleid —> DMARC —> Profiel toevoegen

DMARC-feedback meldt: Inschakelen van het verzenden van DMARC-aggregatierapporten.

Stapelverificatie

U vindt niet-gelabelde bruggen geldig: Is alleen van toepassing als controle-tagging in de vorm van een ounce is ingeschakeld. Standaard beschouwt het apparaat niet-gelabelde bounces ongeldig en wijst het de aanloop af of voegt een aangepaste header toe, afhankelijk van de instellingen voor verificatie bij de aanbellen. Als u ervoor kiest om niet-gelabelde bounces geldig te vinden, accepteert het apparaat het weerkaatste bericht.

Kwantenverificatie

DNS-verificatie van zender:

Senders kunnen om verschillende redenen niet worden geverifieerd. Niet-geverifieerde zenders worden ingedeeld in de volgende categorieën:

- Het aansluiten van PTR-host-record bestaat niet in de DNS.
- Het aansluiten van het PTR-opnameverzicht op host verloopt niet vanwege tijdelijke DNS-storing.
- Connected host reverse DNS-lookup (PTR) komt niet overeen met de voorwaartse DNS-raadpleging (A).

We kunnen de functie Sender Verification inschakelen of uitschakelen.

Uitzonderingstabel gebruiken Verzender Verificatie: We kunnen de afwijkingslijst van het verificatiedomein van de afzender gebruiken om vrijstellingen toe te staan. We kunnen slechts één uitzonderingstabel hebben, maar per post-mail-stroombeleid mogelijk maken.

De uitzonderingstabel kan worden gemaakt via het beleid per e-mail —> Afdruktabel verzenden —> Afwijking verzender-verificatie toevoegen

Bestemmingscontroles

Dit is een functie die de e-mailleveringen controleert. Alle e-mails die klaar zijn met verwerking via de ESA's en die op het punt staan de ESA's te verlaten voor verdere leveringen, kunnen worden gecontroleerd door de functie Bestemmingscontrole.

Het profiel van de **standaard** Bestandsregeling is van toepassing op alle leveringen. Voor het geval er behoefte is aan domeinspecifieke leveringscontroles, dan moeten we een aangepast profiel van de doelcontroles maken.

Onderdelen van een profiel van doelbesturingselementen

Limieten

Gelijklopende verbindingen : Aantal gelijktijdige verbindingen (DCID’s) naar externe hosts waarop het apparaat is gericht, zal proberen te openen voor de voltooiing van de levering.

Maximum aantal berichten per verbinding: Aantal berichten dat het ESA via een verbinding naar een doeldomein zal verzenden (DCID) voordat het apparaat een nieuwe verbinding start.

Ontvangers: Aantal ontvangers van het apparaat zal binnen een bepaalde periode naar een bepaalde afstandsbediening sturen.

Limieten toepassen: Deze aspecten helpen te beslissen hoe we de grenzen toepassen die we hebben opgegeven op een per-bestemming- en MGA-hostname-basis.

TLS-ondersteuning

Dit helpt te beslissen of TLS-verbindingen naar verafgelegen hosts worden ingesteld op Geen / Voorkeurig / Vereiste

DANE-ondersteuning: Als u DSAN als 'opportunistisch' instelt en de afstandsbediening DANE niet ondersteunt, heeft u opportunistische TLS de voorkeur om TCP-gesprekken te versleutelen.

Als u DANE als 'Mandatory' instelt en de afstandsbediening DANE niet ondersteunt, wordt er geen verbinding met de bestemmingstoegang ingesteld.

Als u DANE als 'Verplicht' of 'opportunistisch' instelt en de afstandsbediening DANE ondersteunt, heeft u de voorkeur voor het versleutelen van MTP-gesprekken.

OPMERKING: DANE zal niet worden afgedwongen voor domeinen die MTP Routes hebben gevormd.

Stapelverificatie

Dit helpt om te beslissen of het al dan niet uitvoeren van envelopverkant adresmarkering (prvs-xxxxxx) via Bounce Verificatie.

Stemverificatie kan worden ingesteld op basis van postbeleid —> Stekverificatie —> Nieuwe sleutel toevoegen

Profiel oproepen

Het stuitprofiel kan door het apparaat voor een bepaalde externe host worden gebruikt. Hij besluit hoe lang een e-mail zal worden bewaard in de Delivery Quissie van het ESA als er leveringsproblemen zijn, voordat Hard Bounge een e-mail ontvangt

Het stuitprofiel wordt ingesteld via het netwerk —> Bounce Profiles

Mondiale instellingen

Certificaat: Dit is het aspect waar we de certificaten definiëren die gebruikt moeten worden bij het opzetten van SSL/TLS verbindingen terwijl e-mailleveranties aan de volgende hop worden gestart. Aanbevolen wordt altijd een door de certificaatinstantie (CA) ondertekend certificaat in dit aspect te gebruiken.

Verzend een waarschuwing wanneer een vereiste TLS-verbinding mislukt: We kunnen specificeren of het apparaat een waarschuwing verstuurt als de TLS-onderhandeling mislukt bij het verzenden van berichten naar een domein dat een TLS-verbinding vereist. Het waarschuwingsbericht bevat de naam van het doeldomein voor de mislukte TLS-onderhandeling. Het apparaat stuurt het waarschuwingsbericht naar alle ontvangers die zijn ingesteld voor het ontvangen van waarschuwingen **met** betrekking tot de ernst van de **systeemmeldingen**.

We kunnen alarmontvangers beheren via systeemadministratie —> Waarschuwingen