Wat zijn de beste praktijken voor het gebruik van SenderBase?

Inhoud

Inleiding

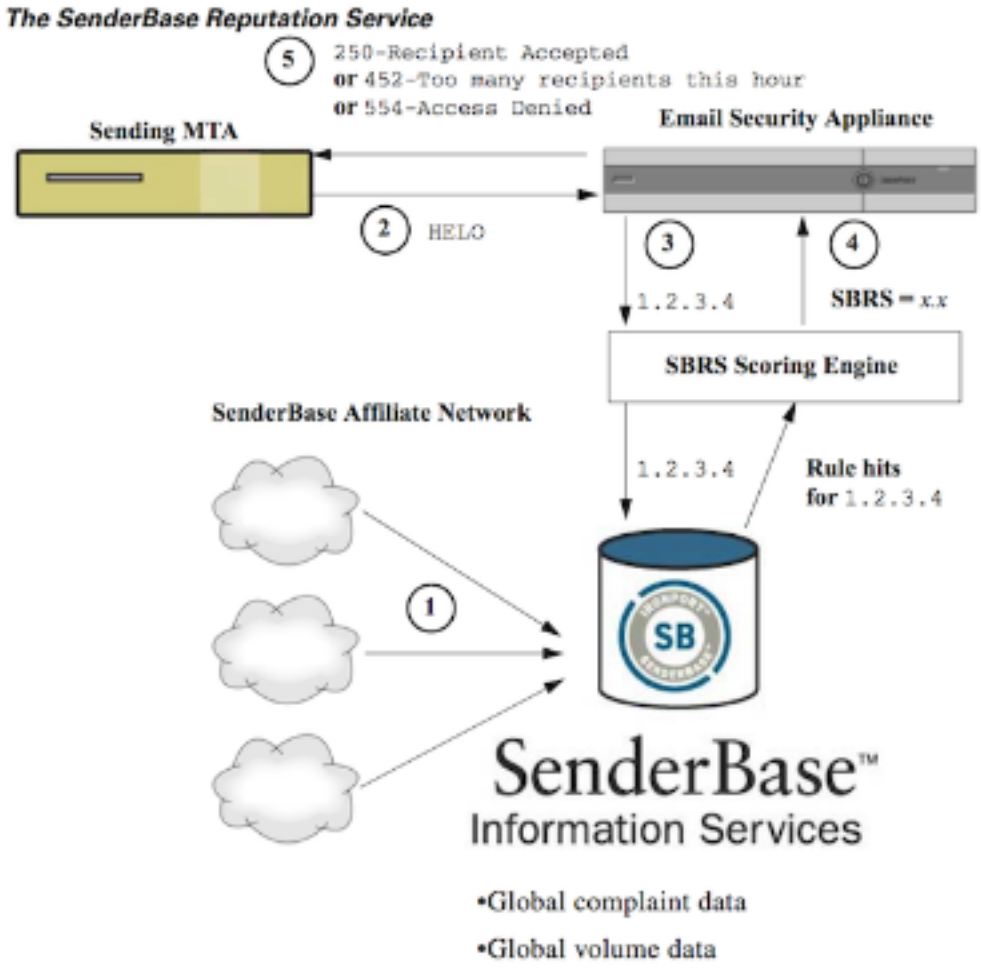
Dit document beschrijft de best practices voor het gebruik van SenderBase.

Wat zijn de beste praktijken voor het gebruik van SenderBase?

De SenderBase Reputation Service (SBRS) biedt u een nauwkeurige, flexibele manier om systemen te weigeren of te blokkeren waarvan vermoed wordt dat ze spam verzenden, gebaseerd op het aangesloten IP-adres van de afstandsbediening. De SBRS geeft een score op basis van de waarschijnlijkheid dat een bericht van een bepaalde bron spam is, variërend van -10 (zeker om spam te zijn) tot +10 (zeker niet spam te zijn). Hoewel SBRS kan worden gebruikt als een zelfstandige anti-spam oplossing, is het meest effectief in combinatie met een content-gebaseerde anti-spamscanner.

SenderBase-scores kunnen worden gebruikt in de Host Access Table (HAT) op een mpBase-luisteraar om binnenkomende TCP-verbindingen naar verschillende Sender-groepen in kaart te brengen. Elke SenderGroup heeft er een beleid mee geassocieerd dat van invloed is op hoe binnenkomende e-mail wordt verwerkt. De meest voorkomende dingen die te maken hebben met SenderBase-scores zijn om of de mail geheel af te wijzen, of de verdachte spam-zender te gooien.

Je kunt SBRS-scores in het HAT gebruiken om e-mail te verwerpen of te blokkeren. U kunt ook berichtfilters maken om "drempels" voor SBRS scores te specificeren om verder te handelen op berichten die door het systeem verwerkt zijn. In het onderstaande schema is een overzicht opgenomen van de manier waarop SBRS-scores kunnen worden gebruikt om verdachte zenders te blokkeren of te blokkeren:



1. SenderBase-filialen sturen real-time, mondiale data.
2. Het verzenden van MTA opent de verbinding met het apparaat.
3. Applicatie controleert wereldwijde gegevens voor het aangesloten IP-adres.
4. SenderBase Reputation Service berekent de waarschijnlijkheid dat dit bericht spam is en wijst een SenderBase Reputations Score toe.
5. De applicatie retourneert de respons (of het afwijzen van e-mail of het wegwentelen van de zender) op basis van de SenderBase Reputation Score.

Hoe u SBRS-scores gebruikt, hangt af van hoe agressief u wilt zijn in pre-filteren e-mail. De e-mail security applicatie (ESA) biedt drie verschillende strategieën voor het implementeren van SenderBase:

- **Conservatief**: Een conservatieve benadering is om berichten met een SenderBase Reputation Score van minder dan -7.0 te blokkeren, die tussen -7.0 en -2.0 lopen, het standaardbeleid tussen -2.0 en +6.0 toe te passen en het vertrouwde beleid toe te passen op berichten met een score groter dan +6.0. Gebruik deze benadering garandeert een bijna nul valse positieve snelheid terwijl het behalen van betere systeemprestaties.
- Middelmatig: Een gematigde benadering is om berichten met een SenderBase Reputation Score van minder dan -4.0 te blokkeren, van -4.0 tot 0 te gaan, het standaardbeleid tussen 0 en +6.0 toe te passen en het vertrouwde beleid toe te passen op berichten met een score hoger dan +6.0. Deze benadering zorgt voor een zeer klein fout-positief cijfer terwijl het systeem beter presteert (omdat meer mail wordt weggestuurd van de verwerking van Anti-Spam).
- **agressief:** Een agressieve benadering is om berichten met een SenderBase Reputation Score van minder dan -1.0 te blokkeren, die tussen -1.0 en 0 lopen, het standaardbeleid tussen 0 en

+4.0 toe te passen en het vertrouwde beleid toe te passen voor berichten met een score groter dan +4.0. Met deze benadering zou je een paar valse positieven kunnen maken; Deze benadering maximaliseert echter de systeemprestaties door de meeste post weg te sturen van de verwerking van anti-Spam.

De onderstaande tabel geeft een overzicht van deze drie beleidsmaatregelen:

benaderen	Kenmerken	toelatingslijst	Bloglijst	verdachte	Onbekende
		Sender Base Reputation Score range:			
conservatief	Bijna geen valse positieven, betere prestaties	7 tot 10	-10 tot -4	-4 t/m -2	-2 tot 7
Gematigd (standaard)	Zeer weinig valse positieven, hoge prestaties	Sender Base Reputation Scores worden niet gebruikt.	-10 tot -3	-3 t/m -1	-1 t/m +10
agressief	Sommige valse positieven, maximale prestaties Met deze optie kunt u de meeste e-mail verwijderen van Anti-Spam-verwerking.	4 tot 10	-10 tot -2	-2 t/m -1	-1 tot 4
Alle benaderingen		Mail Flow Policy: Trusted	geblokkeerd	gedraaid	aanvaard

SenderBase-routing of -blokkering implementeren

De beste manier om SenderBase-scores te gebruiken betekent het volgen van een simpele, 2-delige methodologie. Ten eerste beslis je je beleid (je kunt bijvoorbeeld beginnen met het ‘Conservative' beleid hierboven) en je kunt dat beleid in kaart brengen naar Sender-groepen. Dan breng je die verzendgroepen in kaart aan het beleid dat je wilt. Het ESA heeft al een matrix gemaakt van Sender Group and Mail Flow Policies die kan dienen als een sjabloon voor uw implementatie van SBRS.

Om SenderBase-tellen toe te passen op basis van het standaardbeleid, zult u de vier sendergroepen (Toestellijst, Blocklist, Verkenner en Onbekende lijst) bij Mail Policies > Host Access Tabel (HAT) Overzicht bewerken. Start door op "Toestellijst" te klikken. Vervolgens klikt u in het vervolgkeuzemenu in het tabblad Senders op "SenderBase" met "Toevoegen utation Score (SBRS)" geselecteerd. Dit voegt een SBRS-regel toe aan de lijst met zenders. Vul uw SBRS-score in (in dit geval 6.0 tot 10.0) en klik op de knop **Indienen**.

Het beleid voor de Allowlist sender groep is 'Trusted'. Standaard zal dit beleid de anti-spam verwerking overslaan, wat de systeemprestaties zal verhogen. Omdat zenders met zeer hoge SBRS scores zeer waarschijnlijk niet spam verzenden, zal deze stap alleen de productie verhogen. Bewerk de overige drie Sender-groepen om SBRS-scores toe te voegen, volgens de onderstaande tabel:

Sender-groep	Score-bereik	Resultaat
toelatingslijst	6 tot 10	Bekende goede zenders worden niet gescand

Onbekende	-2 t/m +6	Senders met weinig informatie worden normaal gescand
verdachte	-7 t/m -2	Senders met een slechte reputatie worden zwaar getroffen door het vermind van de hoeveelheid spam die ze kunnen sturen
Bloglijst	-10 tot -7	Post van bekende spammers zal op tijd met een 5xx-respons worden verwor

Als u een score oploopt voor het toevoegen van scores, vergeet dan niet om op "**Commit Changes** te klikken." Wanneer u SBRS-scoring-regels toevoegt aan bestaande sendergroepen, plaats ze dan onderaan in de lijst met zenders in elke groep. Bestellen is van belang bij het definiëren van sendergroepen in de HAT van een luisteraar, omdat de groepen van boven naar onder worden beoordeeld. Binnen elke groep wordt elke regel afzonderlijk beoordeeld, van boven naar onder. In een HAT wordt de eerste regel die een zender afstemt, gebruikt om een beleid te selecteren. Als een inkomende verbinding van een verzendend domein een duidelijke SBRS score heeft en de bereik in een regel in een HAT van de luisteraar aanpast, zal het beleid van de poststroom worden toegepast, zelfs als andere regels verder beneden in de lijst van afzender groepen ook zouden kunnen passen.

Als uw beleid om zenders in sendergroepen te plaatsen vereist dat alle niet-SBRS-regels worden geëvalueerd voordat SBRS-scores worden overwogen, kunt u simpelweg vier nieuwe sendergroepen toevoegen aan het eind van de lijst met bestaande sendergroepen, specifiek voor SBRS-beleid dat overeenkomt met hun relevante beleid.

Gerelateerde informatie

- SenderBase-vragen vaak gesteld
- Technische ondersteuning en documentatie – Cisco Systems