Een Whitelist-beleid maken op een Cisco ESA voor phishing Education Tests

Inhoud

Inleiding

Dit document beschrijft hoe u een Whitelist-beleid kunt maken voor de Cisco Email Security Appliance (ESA) of Cloud Email Security (CES) instantie om phishing-onderwijstesten/campagnes mogelijk te maken.

Voorwaarden

Vereisten

Cisco raadt kennis van de volgende onderwerpen aan:

- Navigeren en configureren van regels op Cisco ESA/CES op WebUI.
- Berichtfilters maken op Cisco ESA/CES op de Opdrachtlijn Interface (CLI).
- Kennis van de voor de phishing campagne/test gebruikte middelen.

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.

Achtergrondinformatie

Administrateurs die phishing education tests of campagnes uitvoeren zullen e-mails gegenereerd hebben met informatie die zal worden aangepast aan de huidige Taloregels over de Anti-Spam en/of Outbreak Filter reeksen. In dat geval zullen de phishing-campagne-e-mails niet de eindgebruikers bereiken en door de Cisco ESA/CES zelf worden bediend waardoor de test wordt stopgezet. Administrateurs zouden ervoor moeten zorgen dat de ESA/CES via deze e-mails hun campagne/test kan uitvoeren.

Configureren

Waarschuwing: Het standpunt van Cisco over wereldwijde whiteling van phishing simulation & onderwijs vendors is niet toegestaan. We adviseren beheerders om met de phishing simulator service te werken *(bijvoorbeeld: PhishMe)* om hun IP's te verkrijgen en deze vervolgens lokaal aan de Whitelist toe te voegen. Cisco moet onze ESA/CES-klanten tegen die IP's beschermen als ze ooit van hand veranderen of daadwerkelijk een bedreiging worden.

Voorzichtig: Beheerders dienen deze IP's tijdens het testen alleen in een Whitelist te houden, waarbij externe IP's gedurende een lange periode na het testen aan een Whitelist worden overgelaten, kunnen ongevraagde of kwaadaardige e-mails aan eindgebruikers opleveren indien deze IP's gecompromitteerd worden.

Op de Cisco Email Security Appliance (ESA) maakt u een nieuwe Sender Group voor uw phishing simulatie en wijst deze toe aan het beleid van de $TRUSTED Mail Flow. Hierdoor kunnen alle phishing simulatie-e-mails aan de eindgebruikers worden geleverd. Leden van deze nieuwe sendergroep zijn niet onderworpen aan snelheidsbeperking, en de inhoud van die zenders wordt niet gescand door Cisco IronPort Anti-Spam-motor, maar wordt nog steeds gescand met software tegen het virus.

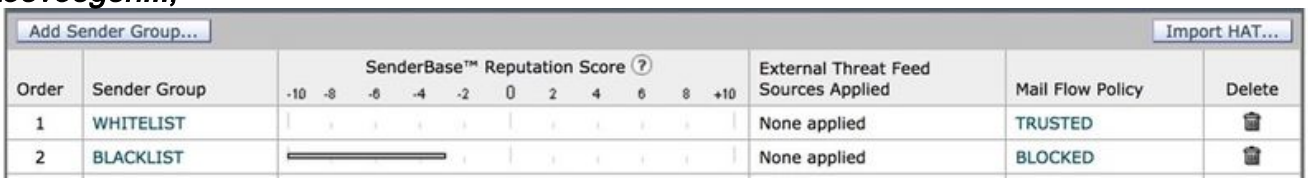
Opmerking: Standaard is het beleid van de $TRUSTED-mail flow ingeschakeld tegen het virus, maar anti-Spam is uitgeschakeld.

De verzendgroep maken

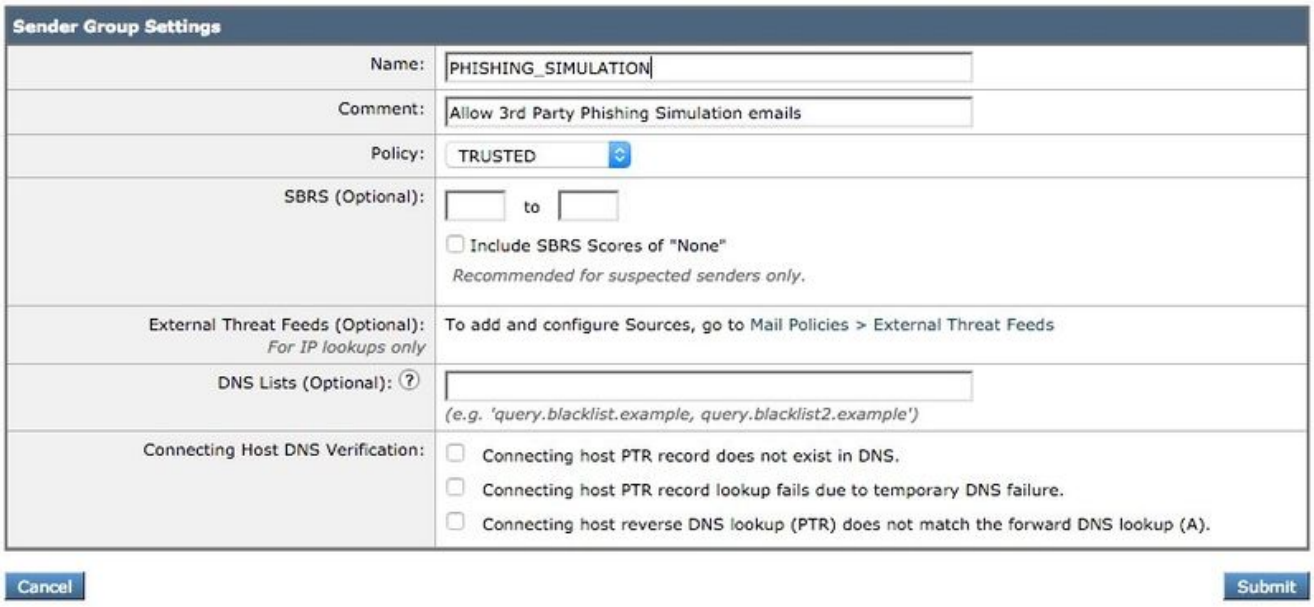
1. Klik op het tabblad ***Mail*** Policy.
2. Selecteer onder het gedeelte ***Host Access Tabel*** de optie ***HAT - Overzicht***

3. Zorg er rechts voor dat de luisteraar van de ***inkomendeMail*** momenteel is geselecteerd,

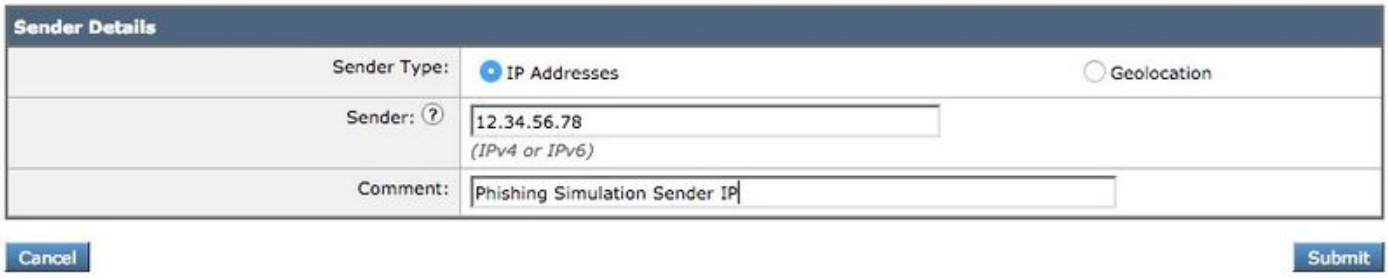
4. Klik in de kolom ***Sender Group*** hieronder op ***Sender Group toevoegen...,***



5. Vul het veld ***Naam*** en ***Opmerking in.*** Selecteer onder de **vervolgkeuzelijst '$TRUSTED'** en klik vervolgens op ***Inzenden en Toevoegen Senders >>.***



6. Voer in het eerste veld de IP- of hostnaam in die u aan Whitelist wilt toevoegen. Uw Phishing Simulation-partner zal u van de Zender IP-informatie voorzien.



Klik op de knop ***Indienen*** als u klaar bent met het toevoegen van items. Denk eraan om op de knop ***Aanpassen*** aan ***het*** opdracht ***wijzigen*** te klikken om de wijzigingen op te slaan.

Het berichtfilter maken

Nadat u de Sender Group hebt gemaakt om de bypass van Anti-Spam en Anti-Virus toe te staan, is er een Berichtfilter nodig om de andere beveiligingsmotoren over te slaan die mogelijk overeenkomen met de Phishing campagne/test.

1. Sluit aan op de CLI van de ESA.
2. Start de opdrachtfilters.
3. Start de opdracht ***nieuw*** om een nieuw berichtfilter te maken.

4. Kopieer en plak het volgende filtervoorbeeld, waarbij u indien nodig de namen van uw echte verzender-groepsnamen maakt:

```
skip_amp_graymail_vof_for_phishing_campaigns:
if(sendergroup == "PHISHING_SIMULATION")
{
skip-ampcheck();
skip-marketingcheck();
skip-socialcheck();
skip-bulkcheck();
skip-vofcheck();
}
```

5. Ga terug naar de hoofdprompt en druk op ENTER.
6. Start de configuratie op.

Verifiëren

Gebruik de middelen van de derde om een Phishing campagne/test te verzenden en controleer de resultaten op de meldingen in het volglogbestand om te verzekeren dat alle motoren werden overgeslagen en de e-mail werd afgeleverd.