Hoe behandel ik de vraag waarom een bericht niet werd ontvangen door de Cisco Secure Email Gateway?

Inhoud

Inleiding

Dit document beschrijft waarom een bericht niet wordt ontvangen door de Cisco Secure Email Gateway en opties om de probleem op te lossen.

Hoe behandel ik de vraag waarom een bericht niet werd ontvangen door de Cisco Secure Email Gateway?

Om bericht van de probleemoplossing te ontvangen, moet u de IP adressen kennen die worden gebruikt om post te verzenden door de organisatie die de mail heeft verzonden. De meest accurate manier om deze informatie te verkrijgen is gewoonlijk om contact op te nemen met de mail beheerder van de verzender organisatie. Bij gebrek aan deze resource kunt u een van deze andere opties gebruiken:

- **SenderBase** - Als u een domein in het zoekveld op http://www.senderbase.org ingeeft, ontvangt u een lijst met bekende verzendende IP-adressen voor dat domein.
- **Mail Logs** - Als u in het verleden e-mail hebt ontvangen van het domein, kunt u in e-maillogs kijken voor een van die succesvolle leveringen.
- **Domain Name System (DNS)** - U kunt de MX-records (e-mail) voor het domein bekijken. De meeste kleinere organisaties gebruiken dezelfde inkomende en uitgaande servers. Voor grotere of meer gesegmenteerde organisaties zal deze optie waarschijnlijk niet de benodigde informatie onthullen.

Zodra u de IP-adressen kent, moet u de e-maillogbestanden doorzoeken. Het grep-hulpprogramma is een goed instrument voor dit doel. Als u Microsoft Windows doorvoert, kunt u Zoeken in Word Pad of Kladblok gebruiken of een grep hulpprogramma vanuit het internet downloaden. Unix en Mac OSX hebben een ingebouwd grep en kunnen vanuit een shell benaderd worden. De grep opdrachtregel ziet er zo uit, waar '10.2.3.4' het IP-adres is om naar te zoeken:

```
host> grep '10.2.3.4' file.log
```

Als de server van de afzender met succes met uw server verbindt, zult u een lijn zien gelijkend op dit voorbeeld wanneer u hun IP adres(sen) zoekt:

```
Wed Feb  2 23:43:11 2008 Info: New SMTP ICID 6 interface Management (10.0.0.1)
address 10.2.3.4 reverse dns host test.ironport.com verified no
```

U kunt vervolgens alle lijnen zoeken die de inkomende ID (ICID) omvatten. De regels die je vindt, zullen je vertellen of ze uit informatie zijn verzonden, of ze naar informatie zijn verzonden en de Bericht ID's (MID's) gekoppeld aan de verbinding. Uit een zoekopdracht op de MID(s) zal blijken of het bericht door het systeem is geaccepteerd, of de scanresultaten en of de levering is geprobeerd.

Een ander beschikbaar gereedschap voor het oplossen van problemen is de **Debug Logs van de injectie**. U hebt eerst het IP-adres van de verzendende server(s) nodig. Als u dit heeft, gebruik dan de **logconfig** en selecteer dit logtype. Nadat het logbestand is geconfigureerd en geëngageerd, kunt u de gebruiker een testbericht laten verzenden en (ervan uitgaande dat de serververbindingen met uw Cisco Secure Email Gateway) de Cisco Secure Email Gateway het gehele TCP-gesprek zal registreren. Dit stelt je in staat om het uitsplitsingspunt in de communicatie te zien.

Als er nog steeds geen verbindingen zijn en er dus geen berichten worden ontvangen, is de volgende stap dat de beheerder van de verzendende servers hun logbestanden controleert en/of telnet gebruikt om het verzenden van een bericht van de mailserver handmatig te testen. Dit bootst de server na die probeert aan uw Cisco Secure Email Gateway te leveren en uw Cisco Secure Email Gateway zal reageren op dezelfde manier als wanneer de verzendende servertoepassing deze verzonden heeft.

Als de test doorgaat maar de servertoepassing faalt wanneer het probeert om mail te verzenden, geeft dit leveringsproblemen op de afstandsserver aan. De beheerder van de externe server moet de logbestanden bekijken om de fouten te diagnosticeren.

Eén veel voorkomende oorzaak van vertraagde of mislukte ontvangst van berichten is dat het IP-adres van de verzendende server niet correct omgekeerde DNS heeft, wat een lange vertraging (30+ seconden) veroorzaakt voor de Cisco Secure Email Gateway om een TCP-banner te leveren. Sommige servertoepassingen zullen hun geconfigureerde tijd bereiken en de sessie sluiten voordat de mail wordt verstuurd vanwege de vertraagde banner. De oplossing in dit geval is de tijdelijke versie te verlengen of omgekeerde DNS te implementeren. De aanbevolen actie is het implementeren van omgekeerde DNS voor alle mail servers die andere Internet mail servers leveren. Het wordt beschouwd als een goed internet-etiquette en stelt mailservers in staat om de identiteit van de server op een zeer basisniveau te bevestigen.