Probleemoplossing bij problemen oplossen en verbindingen tijdens ontvangst en levering van e-mail

Inhoud

Inleiding

Dit document beschrijft hoe u problemen met tussenpozen kunt oplossen en hoe u verbindingen kunt maken tijdens ontvangst en levering van e-mail.

Voorwaarden

Cisco raadt kennis van de volgende onderwerpen aan:

- Cisco Private Internet eXchange (PIX) voor adaptieve security applicatie (ASA) versie 7.x en hoger
- Cisco e-mail security applicatie (ESR)

Achtergrondinformatie

De Cisco ESA e-mailgateways zijn inherent e-mailfirewalls. Dit neemt de noodzaak van een stroomopwaartse firewall, zoals een Cisco PIX of ASA, om e-mailverkeer van en naar een ESA te controleren af. Aanbevolen wordt om de Extended Simple Mail Transfer Protocol (ESMTP) uit te schakelen-toepassingsfuncties in de firewall voor alle host-adressen van het beveiligingsapparaat. Standaard is ESMTP-protocolinspectie ingeschakeld voor alle verbindingen die door de Cisco-firewalls lopen. Dit betekent dat alle opdrachten tussen mailgateways via TCP poort 25, zowel als individuele berichtkopregels, geanalyseerd worden om strikt te volgen om Commision for Comments (RFC) specificaties die RFC's 821, 1123 en 1870 omvatten. Er zijn gedefinieerde standaardwaarden voor het maximale aantal ontvangers en berichtgrootte die problemen kunnen

veroorzaken bij levering aan en van uw ESA. Deze specifieke configuratiestandaardinstellingen worden hier beschreven (die uit het Cisco Opname Tool-menu zijn overgenomen).

De opdracht **inspect** esmtp bevat de eerder door de opdracht **fixup smtp** geboden functionaliteit en biedt extra ondersteuning voor bepaalde ESMTP-opdrachten. ESMTP-toepassingsinspectie voegt ondersteuning toe voor acht ESMTP-opdrachten, waaronder AUTH, EHLO, ETRN, HELP, SAML, SEND, **SOML** en **VRFY.** Samen met de ondersteuning voor zeven opdrachten van RFC 821 (**DATA**, **HELO**, **MAIL**, **NOOP**, **QUIT, RCPT, RSET) ondersteunt het beveiligingsapparaat in totaal 15 opdrachten van MTP.** Andere ESMTP-opdrachten, zoals **ATRN**, **STARTLS**, **ONEX**, **VERB**, **CHUNKING en privé-uitbreidingen, worden niet ondersteund.** Niet-ondersteunde opdrachten worden vertaald in XS, die worden verworpen door de interne server. Dit resulteert in een bericht zoals **500 Opdracht onbekend: XXX**. Onvolledige opdrachten worden afgedankt.

De opdracht **inspecteer** esmtp wijzigt de tekens in de server-mtp-banner in sterretjes, behalve de tekens "2", "0", "0". Carriage return (CR) en linefeed (LF) tekens worden genegeerd. Als een MTP-inspectie is ingeschakeld, wacht een sessie die gebruikt wordt voor interactieve MTP op een geldig opdracht en behoudt de MTP-statustemachine van de firewall de juiste status voor de sessie als deze regels niet worden nageleefd:

- Mtd-opdrachten moeten ten minste vier tekens lang zijn.
- MTP-opdrachten moeten worden afgesloten met postuur- en lijnVOER.
- De opdrachten in het programma moeten op een reactie wachten voordat u het volgende antwoord geeft.

Een MTP-server reageert op clientverzoeken met numerieke antwoordcodes en optionele menselijke leesbare snaren. Hiermee beperkt u de opdrachten die de gebruiker kan gebruiken, evenals de berichten die de server teruggeeft. De MTP-inspectie voert drie primaire taken uit:

- Beperkt de verzoeken van MSTM tot zeven basisopdrachten van de MSTP en acht uitgebreide opdrachten.
- Controleert de opdracht-responssequentie van de MTP.
- genereert een controlespoor. Controlegegevens 108002 worden gegenereerd wanneer een ongeldig teken in het postadres wordt vervangen. Zie RFC 821 voor meer informatie.

Een MTP-inspectie volgt de opdracht- en responsvolgorde voor de volgende abnormale handtekeningen:

- Opdrachten met truncatie.
- Onjuiste opdrachtbeëindiging (niet afgesloten met <CR><LR>).
- Als de PHY Interface voor PCI Express (PIPE) signatuur wordt gevonden als een parameter van een **MAIL** van of **RCPT** naar opdracht, wordt de sessie gesloten. Het kan niet worden ingesteld door de gebruiker.
- Onverwachte overgang door de MTP-server.
- Voor onbekende opdrachten verandert het security apparaat alle tekens in het pakket in **X**. In dit geval genereert de server een foutcode voor de client. Vanwege de wijziging in het pakket moet de TCP-checksum opnieuw worden berekend of aangepast.
- TCP stream bewerking.

De output van **show service-policy inspectie ESMTP** levert de standaardinspectiewaarden en de bijbehorende acties.

```
Global policy:
Service-policy: global_policy
```

```
Class-map: inspection_default
Inspect: esmtp _default_esmtp_map, packet 104468, drop 0, reset-drop 0
mask-banner, count 639 obfuscate the SMTP banner greeting
match cmd line length gt 512 deny all SMTP commands (and close connection)
drop-connection log, packet 0
match cmd RCPT count gt 100 drop all messages (and connection) with more
than 100 recipients
drop-connection log, packet 0
match body line length gt 998 log all messages with lines > 998 chars
log, packet 0
match header line length gt 998 drop all messages (and connection)
with headers > 998 chars
drop-connection log, packet 41
match sender-address length gt 320 drop all messages (and connection) with
envelope sender > 320 bytes
drop-connection log, packet 0
match MIME filename length gt 255 drop all messages (and connection) with
MIME attachment filenames > 255 bytes
drop-connection log, packet 0
match ehlo-reply-parameter others obfuscate extended commands not explicitly
noted in the RFCs (such as STARTTLS)
mask, packet 2555
```

Probleem

Af en toe zullen de berichten niet correct door Cisco ESA worden geleverd of ontvangen. Een of meer van deze berichten worden gezien in Cisco ESA device mail_logs:

- Bericht afgebroken MID XXX
- Ontvangst van afgebroken ICID 21916 verloren
- ICID 21916 gesloten
- verbindingsfout: DCID: XXX-domein:voorbeeld.com IP: 10.1.2.3-poort: 25 details : [Fout 60] Time-outinterface voor bewerking: 10.10.10.1 reden: netwerkfout

Oplossing

Sommige van deze standaardinstellingen kunnen gevolgen hebben zoals het leveren van gecodeerde berichten van de Vervoerslaag (TLS), het mailen van lijstcampagnes en het oplossen van problemen. Bij een beter beleid kunt u de firewall gebruiken om al het resterende e-mailverkeer te inspecteren dat niet eerst door het security apparaat gaat, terwijl u alle verkeer dat dit heeft vrijgesteld van betaling vrijstelt. Dit voorbeeld illustreert hoe de standaardconfiguratie (eerder genoteerd) moet worden aangepast om ESMTP-toepassingsinspectie voor één enkel veiligheidshost-adres vrij te stellen.

U kunt al het verkeer naar en van het interne adres van Cisco ESA's definiëren ter referentie in een modulair beleidskader (MPF) class-map:

```
access-list ironport_esa_internal extended permit ip any 192.168.1.1
access-list ironport_esa_internal extended permit ip 192.168.1.1 any
```

Dit creëert een nieuwe class-map om verkeer specifiek aan te passen of om verkeer te selecteren dat anders moet worden behandeld:

```
class-map ironport_esa
match address ironport_esa_internal
```

Deze sectie koppelt de nieuwe Cisco class-map en schakelt de ESMTP-inspectiemogelijkheden in:

```
policy-map global_policy
class ironport_esa
no inspect esmtp
```

Noteer ook de adresvertaalverklaring die kan helpen het aantal inkomende en halfopen (embryonale) verbindingen naar het adres te controleren. Dit is nuttig voor het bestrijden van 'denial of service'-aanvallen (DoS), maar kan de leveringstarieven beïnvloeden.

Opmaak om parameters van **NAT** en **STATIC** opdrachten te volgen ... [tcp (max_conns)] [max_embryonic].
Dit voorbeeld specificeert limieten van 50 totale TCP connecties en 100 halfopen of embryonale verbindingspogingen:

```
static (inside,outside) 1.1.1.1 192.168.1.1 netmask 255.255.255.255 tcp 50 100
```