Contenido

[Introducción](#)
[prerrequisitos](#)
[Antecedentes](#)
[Problema](#)
[Solución](#)

Introducción

Este documento describe cómo resolver problemas los problemas intermitentes y las conexiones abortadas durante el recibo y la salida del correo.

Prerrequisitos

Cisco recomienda que tenga conocimiento sobre estos temas:

- Private internet exchange (PIX) de Cisco o versión 7.x y posterior adaptante del dispositivo de seguridad (ASA)
- Dispositivo de seguridad del correo electrónico de Cisco (ESA)

Antecedentes

Los gateways del correo electrónico de Cisco ESA son intrínsecamente Firewall del correo electrónico. Esto niega la necesidad de un Firewall por aguas arriba, tal como un Cisco PIX o un ASA, de examinar el tráfico de correo a y desde un ESA. Se sugiere para inhabilitar protocolo de transferencia de correo simple extendido las características de la Inspección de la aplicación (ESMTP) en el Firewall para cualquier dirección de host del dispositivo de seguridad. Por abandono, el examen del protocolo ESMTP se habilita para todas las conexiones que pasen con los Firewall de Cisco. Esto significa que analizan a los comandos all publicados entre los gateways del correo vía el puerto TCP 25, así como los encabezados del mensaje individuales, para adherirse estrictamente a las especificaciones de la Solicitud de comentarios (RFC) que incluyen RFC 821, 1123, y 1870. Hay valores predeterminados definidos para el número máximo de beneficiarios y de tamaños del mensaje que pudieron causar los problemas con la salida a y desde su ESA. Estos valores por defecto específicos de la configuración se delinean aquí (tomado de la herramienta de búsqueda del comando cisco).

El comando inspect esmtp incluye las funciones proporcionadas previamente por el comando **smtp del fixup**, y proporciona el soporte adicional para algunos comandos ESMTP. La Inspección

de la aplicación ESMTP agrega el soporte para ocho comandos ESMTP, incluyendo el **AUTH**, **EHLO**, **ETRN**, **AYUDA**, **SAML**, **ENVÍA**, **SOML** y **VRFY**. Junto con el soporte para siete comandos del RFC 821 (**DATA**, **HELO**, **CORREO**, **NOOP**, **SALIDO**, **RCPT**, **RSET**), el dispositivo de seguridad soporta un total de 15 comandos S TP. El otro ESMTP ordena, por ejemplo el **ATRN**, **STARTLS**, **ONEX**, el **VERBO**, el **CHUNKING**, y las extensiones privadas y no se soporta. Los comandos sin apoyo se traducen a Xs, que son rechazados por el servidor interno. Esto da lugar a un mensaje tal como **desconocido de 500 comandos: XXX**. Desechan a los comandos incompletos.

El comando inspect esmtp cambia los caracteres en el anuncio SMTP del servidor a los asteriscos a excepción del "2", el "0", los caracteres del "0". Se ignoran los caracteres del retorno de carro (CR) y del avance de línea (LF). Con la inspección SMTP habilitada, una sesión usada para el S TP interactivo espera un comando válido y la máquina de estado del esmtp del Firewall guarda los estados correctos para la sesión si estas reglas no se observan:

- Los comandos S TP deben ser por lo menos cuatro caracteres de largo.
- Los comandos S TP se deben terminar con el retorno de carro y el Line Feedavance de línea.
- Los comandos S TP deben esperar una respuesta antes de publicar la contestación siguiente.

Un servidor SMTP responde a los pedidos de cliente con los códigos numéricos de la contestación y las cadenas legibles opcionales. La Inspección de la aplicación S TP controla y reduce los comandos que el usuario puede utilizar, así como los mensajes esos el servidor vuelven. La inspección SMTP realiza tres tareas primarias:

- Restringe las peticiones S TP a siete comandos básicos S TP y a ocho comandos ampliados.
- Monitorea la secuencia de comando response S TP.
- Genera un rastro de auditoría. Se genera el registro de auditoría 108002 cuando un carácter no válido integrado en el direccionamiento del correo se substituye. Para más información, vea el RFC 821.

Una inspección SMTP monitorea la secuencia del comando y de la respuesta para las firmas anómalas siguientes:

- Comandos truncados.
- Terminación incorrecta del comando (no terminada con <CR><LR>).
- Si la interfaz PHY para la firma de PCI Express (TUBO) se encuentra como parámetro a un **CORREO** de o a un **RCPT** para ordenar, la sesión es cerrada. No es configurable por el usuario.
- Transición inesperada del servidor SMTP.
- Para los comandos desconocidos, el dispositivo de seguridad cambia todos los caracteres en el paquete al **X.** en este caso, el servidor generará un código de error al cliente. Debido al cambio en el paquete, la suma de comprobación TCP tiene que ser recalculada o ser ajustada.
- El editar de la secuencia TCP.

La salida de la servicio-**directiva de la demostración examina el ESMTP** proporciona los valores predeterminados del examen y sus acciones correspondientes.

```
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
```

Problema

De vez en cuando, los mensajes no podrán ser entregados o ser recibidos correctamente por Cisco ESA. Uno o más de estos mensajes se ven en los mail_logs del dispositivo de Cisco ESA:

- MEDIADOS DE XXX abortado mensaje
- Recibiendo ICID abortado 21916 perdido
- Cierre ICID 21916
- Error de conexión: DCID: Dominio del XXX: IP example.com: puerto de 10.1.2.3: 25 detalles: [Error 60]
  La operación medida el tiempo hacia fuera interconecta: razón de 10.10.10.1: Error de red

Solución

Algunas de estas configuraciones predeterminadas podrían afectar las cosas como la salida de los mensajes encriptados de Transport Layer Security (TLS), de las campañas de la lista de correo, y del troubleshooting. Una mejor directiva pudo tenerle utilizar el Firewall para examinar todo el tráfico restante del correo electrónico que primero no pasa a través del dispositivo de seguridad, mientras que exime todo el tráfico que tiene. Este ejemplo ilustra cómo ajustar la configuración predeterminada (conocida previamente) para eximir la Inspección de la aplicación ESMTP para una sola dirección de host de la Seguridad.

Usted puede definir todo el tráfico a y desde la dirección interna de Cisco ESA para la referencia en un clase-mapa modular del Marco de políticas (MPF):

```
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
```

Esto crea un nuevo clase-mapa para hacer juego específicamente o el tráfico selecto que se tratará diferentemente:

```
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
```

Esta sección conecta el nuevo clase-mapa de Cisco y inhabilita las características del examen del protocolo ESMTP:

```
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
```

También observe la declaración de la traducción de la dirección que puede ayudar a controlar el número de conexiones (embrionarias) entrantes y medio abiertas al direccionamiento. Esto es útil para combatir los establecimientos de rechazo del servicio (DOS), pero puede interferir con las tarifas de la salida.

Formate para arrastrar los parámetros del NAT y del [tcp (max_conns)] de los comandos static… [max_embryonic].
Este ejemplo especifica los límites de 50 conexiones TCP totales y de 100 tentativas medio abiertas o de la conexión embrionaria:

```
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
```