Pesquise defeitos edições intermitentes e conexões abortadas durante o recibo e a entrega do correio

Índice

[Introdução](#)
[Pré-requisitos](#)
[Informações de Apoio](#)
[Problema](#)
[Solução](#)

Introdução

Este documento descreve como pesquisar defeitos edições intermitentes e conexões abortadas durante o recibo e a entrega do correio.

Pré-requisitos

A Cisco recomenda que você tenha conhecimento destes tópicos:

- Intercâmbio de Internet privada (PIX) de Cisco ou versão 7.x e mais recente adaptável da ferramenta de segurança (ASA)
- Cisco envia por correio eletrónico a ferramenta de segurança (o ESA)

Informações de Apoio

Os gateways de e-mail de Cisco ESA são inerentemente Firewall do email. Isto nega a necessidade para um Firewall ascendente, tal como Cisco PIX ou ASA, de inspecionar o tráfego de correio a e de um ESA. Sugere-se para desabilitar as características da inspeção de aplicativo do protocolo simples de transferência de correspondência estendido (ESMTP) no Firewall para todos os endereços de host da ferramenta de segurança. À revelia, a inspeção do protocolo ESMTP é permitida para todas as conexões que passam com os Firewall de Cisco. Isto significa que os comandos all emitidos entre gateways do correio através da porta TCP 25, assim como os cabeçalhos da mensagem individuais, estão analisados para aderir restritamente às especificações da solicitação para comentários (RFC) que incluem RFC 821, 1123, e 1870. Há

uns valores padrão definidos para o número máximo de receptores e de tamanhos de mensagem que puderam causar edições com entrega a e de seu ESA. Estes padrões específicos da configuração são esboçados aqui (tomado da ferramenta de consulta do comando cisco).

O comando inspect esmtp inclui a funcionalidade fornecida previamente pelo comando **smtp dos reparares**, e fornece o suporte adicional para alguns comandos ESMTP. A inspeção de aplicativo ESMTP adiciona o apoio para oito comandos ESMTP, incluindo o **AUTH**, **EHLO**, **ETRN**, **AJUDA**, **SAML**, **ENVIA-O**, **SOML** e **VRFY**. Junto com o apoio para sete comandos do RFC 821 (**DATA**, **HELO**, **CORREIO**, **NOOP**, **PARADO**, **RCPT**, **RSET**), a ferramenta de segurança apoia um total de 15 comandos S TP. O outro ESMTP comanda, como o **ATRN**, **STARTLS**, **ONEX**, **VERBO**, **CHUNKING**, e extensões privadas e não é apoiado. Os comandos Unsupported são traduzidos em Xs, que são rejeitados pelo servidor interno. Isto conduz a uma mensagem tal como um **desconhecido de 500 comandos: XXX**. Os comandos incompletos são rejeitados.

O comando inspect esmtp muda os caráteres no banner do SMTP do server aos asteriscos à exceção do "2", "0", caráteres de "0". Os caráteres da tecla semelhante a tecla ENTER (CR) e da LINE FEED (LF) são ignorados. Com a inspeção de SMTP permitida, uma sessão usada para o S TP interativo espera um comando válido e a máquina de estado do esmtp do Firewall mantém os estados corretos para a sessão se estas regras não são observadas:

- Os comandos S TP devem ser pelo menos quatro caráteres de comprimento.
- Os comandos S TP devem ser terminados com tecla semelhante a tecla ENTER e alimentação de linha.
- Os comandos S TP devem esperar uma resposta antes de emitir a resposta seguinte.

Um servidor SMTP responde aos pedidos do cliente com códigos numéricos da resposta e cordas compreensíveis para o utilizador opcionais. A inspeção de aplicativo S TP controla e reduz os comandos que o usuário pode usar, assim como as mensagens que o server retorna. A inspeção de SMTP executa três tarefas preliminares:

- Restringe pedidos S TP a sete comandos básicos S TP e a oito comandos estendidos.
- Monitora a sequência de comando response S TP.
- Gerencie uns circuitos de auditoria. O registro de exame 108002 é gerado quando um caractere inválido encaixado no endereço do correio é substituído. Para mais informação, veja o RFC 821.

Uma inspeção de SMTP monitora a sequência do comando e da resposta para as seguintes assinaturas anômalas:

- Comandos truncados.
- Terminação incorreta do comando (não terminada com <CR><LR>).
- Se a relação PHY para a assinatura de PCI Express (TUBULAÇÃO) é encontrada como um parâmetro a um **CORREIO** de ou a um **RCPT** para comandar, a sessão está fechada. Não é configurável pelo usuário.
- Transição inesperada pelo servidor SMTP.
- Para comandos desconhecidos, a ferramenta de segurança muda todos os caráteres no pacote ao **X.** neste caso, o server gerará um código de erro ao cliente. Devido à mudança no pacote, a soma de verificação TCP tem que ser voltada a calcular ou ajustado.
- Edição do córrego TCP.

A saída da serviço-**política da mostra inspeciona o ESMTP** fornece os valores da inspeção do padrão e suas ações correspondente.

```
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

Ocasionalmente, as mensagens corretamente não entregarão nem não receberão por Cisco ESA. Umas ou várias destas mensagens são vistas nos mail_logs do dispositivo de Cisco ESA:

- XXX MEADOS DE abortado mensagem
- Recebendo ICID abortado 21916 perdido
- Fim ICID 21916
- Erro de conexão: DCID: Domínio XXX: IP example.com: porta de 10.1.2.3: 25 detalhes: [Erro 60]
  A operação programada conecta para fora: razão de 10.10.10.1: erro de rede

Solução

Algumas destas configurações padrão poderiam impactar coisas como a entrega de mensagens codificada do Transport Layer Security (TLS), de campanhas da lista de endereços, e de Troubleshooting. Uma política melhor pôde mandá-lo utilizar o Firewall para inspecionar todo o tráfego restante do email que não passa primeiramente através da ferramenta de segurança, ao isentar todo o tráfego que tem. Este exemplo ilustra como ajustar a configuração padrão (notável previamente) para isentar a inspeção de aplicativo ESMTP para um único endereço de host da Segurança.

Você pode definir todo o tráfego a e do endereço interno de Cisco ESA para a referência em um mapa de classe modular da estrutura de política (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
```

Isto cria um mapa de classe novo para combinar especificamente ou o tráfego seleto a ser tratado 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 seção liga o mapa de classe novo de Cisco e desabilita as características da inspeção do 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
```

Igualmente note a indicação da tradução de endereços que pode ajudar a controlar o número de conexões (embrionárias) entrantes e entreabertas ao endereço. Isto é útil para combater o ataque de recusa de serviço (DoS), mas pode interferir com as taxas da entrega.

Formate para arrastar parâmetros do NAT e do [tcp (max_conns)] dos comandos static… [max_embryonic].
Este exemplo especifica limites de conexões de TCP do total dos 50 pés e de 100 tentativas entreabertas ou da conexão embriônica:

```
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
```