Contenu

Introduction

Ce document décrit comment dépanner les questions intermittentes et les connexions abandonnées pendant la réception et la livraison de la messagerie.

Conditions préalables

Cisco vous recommande de prendre connaissance des rubriques suivantes :

- Échange privé d'Internet de Cisco (PIX) ou version 7.x et ultérieures de l'appliance de sécurité adaptable (ASA)
- Appliance de sécurité du courrier électronique de Cisco (ESA)

Informations générales

Les passerelles d'email de Cisco ESA sont en soi des Pare-feu d'email. Ceci réalise une inversion le besoin d'un Pare-feu en amont, tel que Cisco PIX ou ASA, d'examiner le trafic de messagerie à et d'un ESA. On lui suggère de désactiver les configurations étendues d'inspection d'application du Simple Mail Transfer Protocol (ESMTP) sur le Pare-feu pour toutes les adresses d'hôte de dispositifs de sécurité. Par défaut, l'inspection de protocole ESMTP est activée pour toutes les connexions qui traversent les Pare-feu de Cisco. Ceci signifie que toutes les commandes émises entre les passerelles de messagerie par l'intermédiaire du port TCP 25, aussi bien que différentes en-têtes de message, sont analysées pour respecter rigoureusement aux caractéristiques du Request For Comments (RFC) qui incluent RFC 821, 1123, et 1870. Il y a des valeurs par défaut définies pour le nombre maximal de destinataires et de tailles de message qui pourraient entraîner des questions avec la livraison à et de votre ESA. Ces par défaut spécifiques de configuration sont tracés les grandes lignes ici (pris de l'utilitaire de recherche de commande Cisco).

La commande d'**esmtp d'examiner** inclut la fonctionnalité précédemment fournie par la commande de **SMTP de fixup**, et fournit le support supplémentaire pour des commandes certain ESMTP. L'inspection d'application ESMTP ajoute le soutien de huit commandes ESMTP, y compris

AUTHENTIQUE, EHLO, ETRN, AIDE, SAML, L'ENVOIE, SOML et VRFY. Avec le soutien de sept commandes RFC 821 (DONNÉES, HÉLICOPTÈRE, MESSAGERIE, NOOP, QUITTÉ, RCPT, ENSEMBLE DE RÉFÉRENCE), les dispositifs de sécurité prennent en charge un total de 15 commandes de SMTP. L'autre ESMTP commande, comme ATRN, STARTLS, ONEX, VERBE, CHUNKING, et extensions privées et n'est pas pris en charge. Des commandes non vérifiées sont traduites dans Xs, qui sont rejetées par le serveur interne. Ceci a comme conséquence un message tel que l'inconnu de 500 commandes : XXX. Des commandes inachevées sont jetées.

La commande d'esmtp d'examiner change les caractères dans la bannière de SMTP de serveur aux astérisques excepté le "2", "0", des caractères de "0". Des caractères de retour chariot (CR) et de retour à la ligne (LF) sont ignorés. L'inspection de SMTP étant activé, une session utilisée pour le SMTP interactif attend une commande valide et l'ordinateur d'état d'esmtp de Pare-feu garde les états corrects pour la session si on n'observe pas ces règles :

- Les commandes de SMTP doivent être au moins quatre caractères de longueur.
- Des commandes de SMTP doivent être terminées avec le retour chariot et retour à la ligne.
- Les commandes de SMTP doivent attendre une réponse avant d'émettre la prochaine réponse.

Un serveur SMTP répond aux demandes de client avec des codes numériques de réponse et des chaînes lisibles pour l'homme facultatives. L'inspection d'application de SMTP contrôle et réduit les commandes que l'utilisateur peut utiliser, aussi bien que les messages que le serveur renvoie. L'inspection de SMTP effectue trois tâches primaires :

- Limite des demandes de SMTP à sept commandes de base de SMTP et à huit commandes étendues.
- Surveille l'ordre de commande-réponse de SMTP.
- Génère une vérification rétrospective. L'enregistrement d'audit 108002 est généré quand un caractère incorrect inclus dans l'adresse de messagerie est remplacé. Le pour en savoir plus, voient RFC 821.

Une inspection de SMTP surveille l'ordre de commande et de réponse pour les signatures anormales suivantes :

- Commandes tronquées.
- Arrêt incorrect de commande (non terminé avec <CR><LR>).
- Si l'interface PHY pour la signature de PCI Express (CANAL) s'avère comme paramètre à une MESSAGERIE de ou à un RCPT pour commander, la session est fermée. Il n'est pas configurable par l'utilisateur.
- Transition inattendue par le serveur SMTP.
- Pour des commandes inconnues, les dispositifs de sécurité changent tous les caractères dans le paquet au X. dans ce cas, le serveur génèreront code d'erreur au client. En raison du changement du paquet, la somme de contrôle de TCP doit être recalculée ou ajustée.
- Retouche de flot de TCP.

La sortie du show service-policy examinent ESMTP fournit les valeurs par défaut d'inspection et leurs actions correspondantes.

```
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
```

Problème

De temps en temps, les messages correctement ne fourniront pas ou ne recevront pas par Cisco ESA. Un ou plusieurs de ces messages sont vus dans les mail_logs de périphérique de Cisco ESA :

- MID abandonné par message XXX
- Recevant ICID abandonné 21916 perdu
- Fin ICID 21916
- Erreur de connexion : DCID : Domaine XXX : IP example.com : port de 10.1.2.3 : 25 détails : [Erreur 60]
  L'exécution synchronisée relient : raison de 10.10.10.1 : erreur réseau

Solution

Certaines de ces valeurs par défaut pourraient affecter des choses comme la livraison des messages cryptés de Transport Layer Security (TLS), des campagnes de liste de diffusion, et du dépannage. Une meilleure stratégie pourrait vous faire utiliser le Pare-feu pour examiner tout les trafic restant d'email qui ne traverse pas d'abord les dispositifs de sécurité, tout en exemptant tout le trafic qui a. Cet exemple montre comment accorder la configuration par défaut (remarquable précédemment) pour exempter l'inspection d'application ESMTP pour un host address simple de Sécurité.

Vous pouvez définir tout les trafic à et de l'adresse interne de Cisco ESAs pour la référence dans un class-map modulaire du cadre de stratégie (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
```

Ceci crée un nouveau class-map spécifiquement pour apparier ou sélectionner le trafic à traiter différemment :

```
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
```

Cette section joint le nouveau class-map de Cisco et désactive les configurations d'inspection de protocole 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
```

Notez également la déclaration de traduction d'adresses qui peut aider à contrôler le nombre de connexions (embryonnaires) entrantes et entrouvertes à l'adresse. C'est utile pour combattre les attaques par déni de service (DOS), mais peut gêner des débits de la livraison.

Formatez pour traîner des paramètres des commandes NAT et STATIQUES… [TCP (les max_conns)] [max_embryonic].
Cet exemple spécifie des limites de 50 connexions TCP totales et 100 entrouverts ou des tentatives embryonnaires de connexion :

```
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
```