目次

概要

この資料にメールの受信および配信の間に断続的な問題および打ち切られた接続を解決する方法を記述されています。

前提条件

次の項目に関する知識があることが推奨されます。

- Cisco Private Internet Exchange （ PIX ）または適応性があるセキュリティ アプライアンス モデル (ASA) バージョン 7.x および それ 以上
- Cisco E メール セキュリティ アプライアンス (ESA)

背景説明

Cisco ESA 電子メール ゲートウェイは本来電子メール ファイアウォールです。 これはアップストリーム ファイアウォールのための必要を、Cisco PIX か ASA のような、ESA に出入してメール トラフィックを検査する否定します。 あらゆるセキュリティ アプライアンス モデル ホストアドレスのためのファイアウォールの Extended Simple Mail Transfer Protocol （ ESMTP ） アプリケーション インスペクション 機能をディセーブルにすることを提案します。 デフォルトで、ESMTP プロトコル インスペクションはすべての接続のためにそのパススルー Cisco ファイアウォール 有効に なります。 これは TCPポート 25 によってメールゲートウェイの間で、また個々のメッセージヘッダーが発行される RFC 821、1123、および 1870 を含む Request For Comments (RFC) 仕様に厳しく付着するために、すべてのコマンド分析されることを意味します。 ESA に出入して配信においての問題を引き起こすかもしれないメッセージサイズおよび受信者の最大数の定義されたデフォルト値があります。 これらの特定の設定 デフォルトはここに説明されています (Cisco コマンド 検索ツールから奪取 されて) 。

Inspect ESMTP コマンドは以前に **フィックスアップ smtp** コマンドによって提供される機能性が含まれいくつかの ESMTP コマンドに追加的支援を提供します。 ESMTP アプリケーション インスペクションは **AUTH**、**EHLO**、**ETRN**、**ヘルプ**、**SAML**、**送信**、**SOML** および **VRFY** を含む 8

つの ESMTP コマンドのためのサポートを、追加します。 7 つの RFC 821 コマンド（**DATA**、**ヘリコプター**、**メール**、**RCPT**、**RSET やめられる**）のためのサポートと共に **NOOP** セキュリティ アプライアンス モデルは 15 の SMTP コマンドの合計をサポートします。 他の ESMTP は、**ATRN** のような、**STARTLS**、**ONEX**、**動詞**、**チャンク**および個人の必要に応じた拡張を命じ、サポートされません。 内部サーバによって拒否されるサポートされていないコマンドは Xs に変換されます。 これは **500 コマンド未知数**のようなメッセージという結果に終ります: **XXX**. 不完全な コマンドは廃棄されます。

Inspect ESMTP コマンドは "2" を除いてアスタリスクにサーバ SMTP バナーの文字を、"0"、"0" 文字変更します。 キャリッジリターン（CR）および改行（LF）文字は無視されます。 有効に されて SMTP インスペクションが対話型 SMTP に使用するセッションは無効なコマンドを待ち、これらのルールが観察されない場合ファイアウォール ESMTP 状態マシンはセッションのための正しい状態を保存します:

- SMTP コマンドは長さが少なくとも 4 文字である必要があります。
- SMTP コマンドはキャリッジリターンおよびライン フィードと終える必要があります。
- SMTP コマンドは次の応答を発行する前に応答を待つ必要があります。

SMTP サーバは数字応答コードおよびオプションの人が読み取り可能なストリングとの Client 要求に応答します。 SMTP アプリケーション インスペクションは使用ユーザができる、またそのメッセージはサーバ戻りますコマンドを制御し、減らします。 SMTP インスペクションは 3 つのプライマリ タスクを行います:

- 7 つの基本的な SMTP コマンドおよび 8 つの拡張されたコマンドに SMTP 要求を制限します。
- SMTP コマンドレスポンス シーケンスを監視します。
- 監査証跡を生成します。 メール アドレスで組み込まれる無効の文字列が取り替えられるとき監査レコード 108002 は作成されます。 詳細については、RFC 821 を参照して下さい。

SMTP インスペクションは次の変則的なシグニチャのためのコマンドおよび応答シーケンスを監察します:

- 切捨てられたコマンド。
- 不正確なコマンド 終了（<CR><LR> と終わらない）。
- PCI Express 命じる**メール**からのまたは **RCPT** へのパラメータがセッション閉じると同時に（パイプ）シグニチャのための PHY インターフェイスがあれば。 それはユーザによって設定できません。
- SMTP サーバによる予想外遷移。
- 未知コマンドに関しては、セキュリティ アプライアンス モデルはクライアントに **X.**にパケットのすべての文字を、サーバ生成します工ラーコードをこの場合変更します。 パケットの変更が理由で、TCP チェックサムは計算し直されるか、または調節されなければなりません。
- TCP ストリーム編集。

show service ポリシー Inspect ESMTP の出力はデフォルト インスペクション値および対応するアクションを提供したものです。

```
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
```

問題

時折、メッセージは正しく提供されるか、または Cisco ESA によって受け取りません。 これらのメッセージの何れか一つ以上は Cisco ESA デバイス mail_logs で見られます:

- メッセージによって打ち切られる MID XXX
- 失われる打ち切られた ICID 21916 を受け取ります
- ICID 21916 終わり
- 接続エラー: DCID: XXX ドメイン: example.com IP: 10.1.2.3 ポート: 25 の詳細: [エラー 60] 時間を計られるオペレーションはインターフェイスします: 10.10.10.1 原因: ネットワークエラー

解決策

いくつかのこれらのデフォルト設定は Transport Layer Security （TLS）暗号化 された メッセージ、メーリングリスト キャンペーンおよびトラブルシューティングの配信のような事柄に影響を与える可能性があります。 よりよいポリシーは最初パススルー持っているセキュリティ アプライアンス モデル残りの電子メール トラフィックすべてを検査するのにファイアウォールを利用してもらうかもしれません、すべてのトラフィックを免除している間。 この例に単一 セキュリティ ホスト アドレスのための ESMTP アプリケーション インスペクションを免除するためにデフォルト 設定を（以前に注意される）調整する方法を説明されています。

モジュラ 政策の枠組（MPF） class-map の参照用の Cisco ESA の内部アドレスに出入してトラフィックすべてを定義できます:

```
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
```

これは適合するために新しい class-map か別様に扱われるべき選定されたトラフィックを生成します:

```
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
```

このセクションは Cisco 新しい class-map をリンクし、ESMTP プロトコル インスペクション 機能をディセーブルにします:

```
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
```

またアドレスへの着信およびハーフ オープン（萌芽期）接続の数の制御を助けることができるアドレス 変換文に注意して下さい。 これはサービス拒否不正侵入（DoS）を戦うために役立ちましたり、しかし配信率と干渉するかもしれません。

NAT および Static コマンドのパラメータを追跡するために…フォーマットして下さい[TCP（max_conns）] [max_embryonic]。
この例は 50 の総 TCP 接続および 100 つのハーフ オープンまたは初期接続試みの制限を規定 したものです:

```
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
```