ESAの一般的なHAT/RATエラーのトラブルシューティング

内容

はじめに

このドキュメントでは、Eメールセキュリティアプライアンス(ESA)のホストアクセステーブル(HAT)と受信者アクセステーブル(RAT)に関する一般的な問題を診断するための概要、設定ガイダンス、およびトラブルシューティングテクニックについて説明します。

概要

HAT

設定されたリスナーごとに、リモートホストからの着信接続を制御する規則のセットを定義する必要があります。たとえば、リモートホストを定義したり、リモートホストがリスナーに接続できるかどうかを定義したりできます。AsyncOSでは、HATを使用してリスナーへの接続を許可す

るホストを定義できます。

HATは、リスナーのリモートホストからの着信接続を制御する一連の規則を維持します。設定されたリスナーはすべて、独自の独立したHATを持ちます。HATは、パブリックリスナーとプライベートリスナーの両方に設定できます。

デフォルトでは、HATはリスナーのタイプに応じて異なるアクションを実行するように定義されています。

- パブリックリスナー：HATは、すべてのホストからの電子メールを受け入れるように設定されています。
- プライベートリスナー：HATは、指定したホストからの電子メールを中継し、その他すべてのホストを拒否するように設定されます。

HATルールは、送信者グループ、SenderBase Reputation Score(SBRS)、適用される外部脅威フィードソース、およびメールフローポリシーで構成されます。

送信者グループ

送信者グループとは、次の1つ以上によって識別される送信者のリストです。

- IPアドレス（IPv4またはIPv6）
- IP の範囲
- 特定のホスト名またはドメイン名
- IPレピュテーションサービスの「組織」分類
- IPレピュテーションスコア(IPRS)の範囲（またはスコアの欠如）
- DNSリストクエリ応答

SenderBase評価スコア

アプライアンスはIPレピュテーションサービスを照会して、IPレピュテーションスコアを決定できます。IPレピュテーションスコアは、IPレピュテーションサービスからの情報に基づいて、IPアドレス、ドメイン、または組織に割り当てられる数値です。

適用される外部脅威フィード(ETF)ソース

ETFフレームワークにより、ESAはTAXIIプロトコル経由で通信されるSTIX形式の外部脅威情報を使用できます。

外部の脅威情報を利用する機能は、組織にとって次のような利点があります。

- マルウェア、ランサムウェア、フィッシング攻撃、標的型攻撃などのサイバー脅威にプロアクティブに対応します。
- ローカルおよびサードパーティの脅威インテリジェンスソースを購読します。
- 有効性の向上

ESAでETFを使用するには、有効な機能キーが必要です。機能キーを取得する方法については、シスコの営業担当者またはCisco Global Licensing Operationsにお問い合わせください。

メール フロー ポリシー

メールフローポリシーを使用すると、SMTPカンバセーション中の送信者からリスナーへの電子メールメッセージのフローを制御または制限できます。SMTPカンバセーションを制御するには、メールフローポリシーで次のタイプのパラメータを定義します。

- 接続パラメータ（接続ごとの最大メッセージ数など）
- レート制限パラメータ（1時間あたりの最大受信者数など）
- カスタムSMTPコードと応答は、SMTPカンバセーション中に通信されます
- スパム対策検出の有効化/無効化
- ウイルス対策保護を有効/無効にする
- 暗号化（TLSなど）
- 認証と検証（DMARC、DKIM、SPFなど）

ねずみ

AsyncOSでは、各パブリックリスナーに対してRATを使用して、受信者アドレスの受け入れまたは拒否を管理します。受信者アドレスには次のものが含まれます。

- ドメイン
- 電子メールアドレス
- 電子メールアドレスのグループ

デフォルトでは、オープンリレーの作成を防ぐために、RATはすべての受信者を拒否します。

一般的な実装シナリオ

送信者を手動でブロックする

特定の送信者を送信者のIPアドレスでブロックするには、ブロックリスト送信者グループの下にIPアドレスの手動エントリを追加し、アクションが「Reject」または「TCP Refuse」に設定されていることを確認します。 設定手順については、「ESAで送信者IPを手動でブロックする」を参照してください。

HATへのIPアドレスのグループ/範囲の追加

隣接するIPアドレスは、192.0.2.0/24などのサブネット、192.0.2.10-20などのIPアドレス範囲、または192.0.2.などの部分的なIPアドレスとしてグループ化し、テーブルに追加できます。複数の非隣接IPアドレスを追加するには、次の手順を実行します。

GUI で次の手順を実行します。

1. Mail Policies > HAT Overviewの順に移動します (必要に応じて、適切なクラスタレベルを選択します) 。
2. 変更する送信者グループを選択し、Add Senderを選択します。
3. Senderフィールドに、適切なIP範囲(192.0.2.0/24など)、およびオプションのコメントを入力し、Submitを選択します。
4. Commit Changesをクリックして保存します。

CLI から、

1. 次のコマンドシーケンスを実行します。

   <#root>

   listenerconfig >> EDIT

2. 編集するリスナーの名前または番号を入力します。
3. コマンドシーケンスを実行し、編集する送信者グループ番号または名前を入力します。

   HOSTACCESS >> EDIT >> 1

4. newを選択し、追加する送信者のコンマ区切りリストを入力します。
5. 完了したら、commitを実行して変更を保存します。

トラブルシューティング

正しくない送信者グループと一致する送信者

ESAのメールログまたはセキュリティ管理アプライアンス(SMA)のメッセージトラッキングを確認し、着信接続ID(ICID)の次のエントリを確認します。

```
ICID 476946 ACCEPT SG WhiteList match nx.example SBRS None country United States
```

理由：接続ホストのDNS検証が送信者グループで有効になっており、接続ホストのPTRレコードがDNSに存在しないことが選択されています。

```
ICID 476946 ACCEPT SG WhiteList match not.double.verified.example SBRS None country United States
```

理由：送信側グループで接続ホストのDNS検証が有効になっており、接続ホストの逆DNSルックアップ(PTR)が正引きDNSルックアップ(A)と一致しません。

```
ICID 476946 ACCEPT SG WhiteList match serv.fail.example SBRS None country United States
```

理由：送信側グループで接続ホストのDNS検証が有効になっており、一時的なDNS障害が原因で接続ホストのPTRレコードの検索が失敗するように選択されています。

誤った送信者グループホスト設定

送信者グループとは、次の送信者によって識別される送信者のリストです。

- IPアドレス（IPv4またはIPv6）
- IP の範囲
- 特定のホスト名またはドメイン名
- IPレピュテーションサービスの「組織」分類
- IPレピュテーションスコア(IPRS)の範囲（またはスコアの欠如）
- DNSリストクエリ応答

送信者グループの下に誤って設定されたアドレスの例：部分的なホスト名に一致するESA送信者グループ。

HAT/RATの拒否は、「レピュテーションフィルタリングにより阻止される」と見

なされますか。

はい。送信者グループによって拒否され、メールフローポリシーで拒否アクションが指定されたメッセージは、'Stopped by Reputation Filtering'レポートカウンタでカウントされます。

注：このカウンタには、HATポリシー拒否およびSBRSベースの拒否を含めることができます。メールログで拒否理由を確認して、送信元を識別します。

RATテーブルによる拒否の確認

次に、ESAのメールログからのログ出力例を示します。

```
Thu Sep 18 09:10:14 2014 Info: MID 48445 ICID 15970 To: <user@example.com> "Rejected by RAT"
```

理由：特定のドメインはESA設定のRATで許可されていません。

拒否された接続に関する追加の送信者/受信者の情報をログに記録する方法

デフォルトでは、拒否された接続は、送信者のMTA IPアドレスだけをメールログに記録し、エンベロープ送信者またはエンベロープ受信者は記録しません。トラブルシューティングのために追加のロギングが必要な場合は、AsyncOSで遅延HAT拒否を有効にすることができます。

注意：この機能は追加のリソースを必要とするため、永続的には有効にしないことをお勧めします。

詳細については、HAT Delayed Rejection FAQを参照してください。

関連情報

- Cisco E メール セキュリティ アプライアンス：エンドユーザ ガイド
- シスコのテクニカルサポートとダウンロード

翻訳について
シスコは世界中のユーザにそれぞれの言語でサポート コンテンツを提供するために、機械と人による翻訳を組み合わせて、本ドキュメントを翻訳しています。ただし、最高度の機械翻訳であっても、専門家による翻訳のような正確性は確保されません。シスコは、これら翻訳の正確性について法的責任を負いません。原典である英語版（リンクからアクセス可能）もあわせて参照することを推奨します。