Traffic Anomaly Detector および Guard（Riverhead Networks）に関する FAQ

目次

概要

このドキュメントでは、Cisco Traffic Anomaly Detector および Guard（Riverhead Networks）に関するよくある質問（FAQ）について説明します。

ドキュメント表記の詳細は、『シスコ テクニカル ティップスの表記法』を参照してください。

Q. Cisco トラフィック異常探知器およびガードのためのデフォルトパスワードとは何か。

A. Cisco トラフィック異常探知器およびガードのためのデフォルトパスワードは admin/rhadmin です。

Q. "date 12012004" CLI コマンドを使用して 08062004 から 12012004 の先物期日に日付情報を変更しました。 SNMP OID rhZoneLastChangeTime によってゾーンにそれから日付変更をテストしました。 これは日付が日付に最後の変更された日付より先に変更されるとき以外うまく作動しました。 次に、CLI の遡 08062004 を

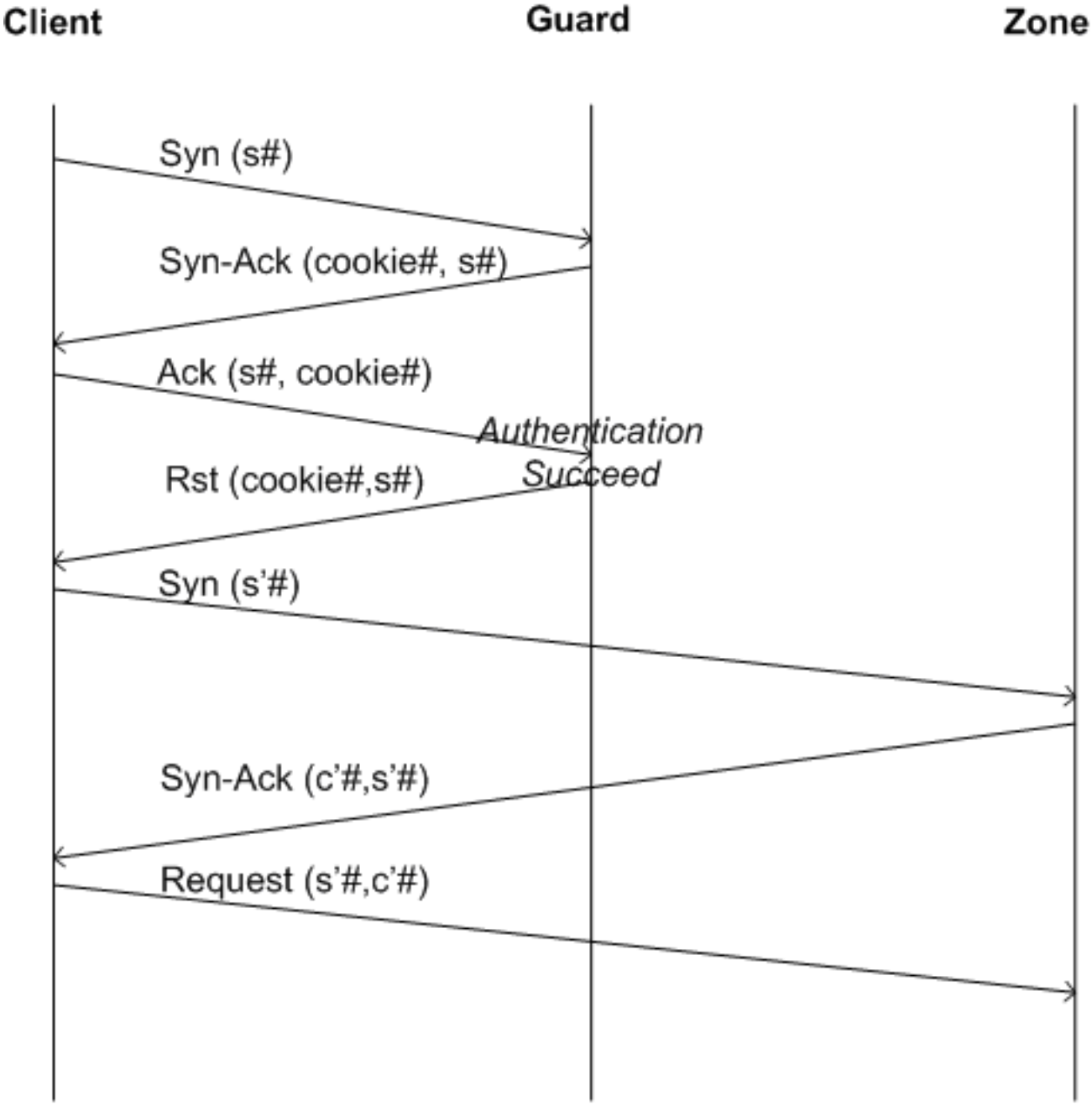
変更しました。 ただし、rhZoneLastChangeTime のために問い合わせるべき SNMP OID 応答は 12012004 に残りました（古い日付）。 リロードが、OID 応答正しい（最後の）日付変更を示した後。 これはバグですか。

A. これは Cisco バグ ID CSCuk52710 （登録ユーザのみ）です。 通常デバイスの時を逆方向に変更することを推奨しません。 これはいくつかのヒストリ データのオーバーラップという結果に終る場合があります。 この問題のための回避策は時間が逆方向に設定 される時はいつでも snmp-server を再起動することです:

```
admin@Guard-conf#no service snmp-server admin@Guard-conf#service snmp-server
```

これは SNMP キャッシュを消去し、要求者に更新されたデータを持って来ます。

Q. TCP Reset と TCP セーフ リセットの違いとは何か。



- **リセット:** RST パケットが受信される場合の接続するために再試行するすべての TCP アプリケーションのために適した（またはユーザが再接続することを可能にするため）。 RST パケ

ットの接続は切断され、タグは送信 されません。 リセット アルゴリズムのパケットフローについては図を参照して下さい。

- **セーフ リセット**: 上の方式がアプリケーション レベル対応を必要とする間、セーフ リセットは TCP スタック RFC 準拠性だけ必要としますが、3 第 2 遅延から最初の接続 セットアップ時間を追加します。 それはほとんどの自動 TCP プロトコルのために適しています (メールのような) 。 クライアント SYN への応答として、ガードはクッキーを保持する悪い承認番号が付いている ACK を送信 します。 クライアントが RFC 793 と対応である場合、悪い承認番号が含まれ、3 秒タイムアウトの後でオリジナル SYN を再送信する RST パケットと答えます。 ガードが悪い承認番号との RST パケットを受信するとき、接続を認証し、次の接続と干渉しません。 このソリューションの主要な警告はこれが対応 RFC ではないのにいくつかのファイアウォールが無言で悪番号を付けられた ACK を廃棄することです。 ガードが RST 無しで第 1 の 4 秒以内に同じ出典から第 2 Syn パケットを、第 2 SYN 中間受信すればソリューションをそのような場合提供する n 順序はリセット 方式で扱われると同様に扱われます。

Q. 「受け取るアップグレードが管理モジュールに接続できなかった後; システムは完全に機能していません: 拒否される接続はソケットにエラーメッセージ」書くことができません。 これはどのように解決すればよいですか。

A. に加えて; : エラーメッセージリブートするときこのエラー生成されます:

```
myguard@GUARDUS#reboot Are you sure? Type 'yes' to reboot yes sh: /sbin/reboot: Input/output
error myguard@GUARDUS# myguard@GUARDUS#show diagnostic-info Can't connect to managment module;
SYSTEM IS NOT FULLY OPERATIONAL: Connection refused Can't write to socket Management module is
busy. Please try again in 10 seconds Failed to get counters myguard@GUARDUS# myguard@GUARDUS#
Message from syslogd@GUARDUS at Sun Sep 19 17:38:51 2004 ... GUARD-US RHWatchdog: RHWatchdog:
subsystem failure - CM
```

このガードのファイル システム エラーのように見え。 FS エラーを解決し、ガードをリブートし、**fsck** が密接に処理するのを視聴するため。 シングル ユーザー モードに得る場合、**fsck** の手動実行を要求するために **fsck** を**- y/**コマンド発行して下さい。

Q. 既定のテンプレートを使用してゾーンを設定するとき、"show policies" コマンドを発行するときゾーンの下で HTTP ポリシー テンプレートを見つけることができません。 HTTP を除いてその他すべてのポリシー テンプレートを見ます。 どのようにそれを見つけることができますか。

A. デフォルトポリシーは **wr t** を発行するとき利用できます | HTTP を命じ、含んで下さい。 これは **policy-template http -1 10.0 enabled** と同じような何かを示します。 トラフィックの HTTP ポリシーは基づいていることしきい値形式に基づいているガードそして外観および Cisco トラフィック異常探知器。

Q. ルート ユーザ パスワードの回復を行う方法

A. **ルート ユーザ** パスワードの回復に関する説明に関しては [Cisco ガードおよびトラフィック異常探知器パスワード リカバリを](#)参照して下さい。

Q. Cisco 異常ガードにカスタム SSL 認証をインポートできますか。

A. いいえ、Cisco 異常ガード 自己署名 SSL 認証だけをサポートします。

Q. このエラーメッセージを受け取りました。 どのように問題を解決できますか。

RHWatchdog: RHWatchdog: Hardware Monitoring card reports HW errors.

A. 問題を解決するために電源を再置して下さい。

関連情報

- Cisco ガードおよび軽減アプライアンス 技術文書
- テクニカルサポートとドキュメント - Cisco Systems