Trafic Anomaly Detector et Guard (Riverhead Networks) - Forum Aux Questions

Contenu

Introduction

Ce document aborde les questions fréquemment posées (Foires aux questions) liées au Traffic Anomaly Detector de Cisco et à la protection (réseaux de Riverhead).

Pour plus d'informations sur les conventions utilisées dans ce document, reportez-vous à Conventions relatives aux conseils techniques Cisco.

Q. Quel est le mot de passe par défaut pour le Traffic Anomaly Detector et la protection de Cisco ?

A. Le mot de passe par défaut pour le Traffic Anomaly Detector et la protection de Cisco est **admin/rhadmin**.

Q. J'ai changé les informations de date de 08062004 à une future date de

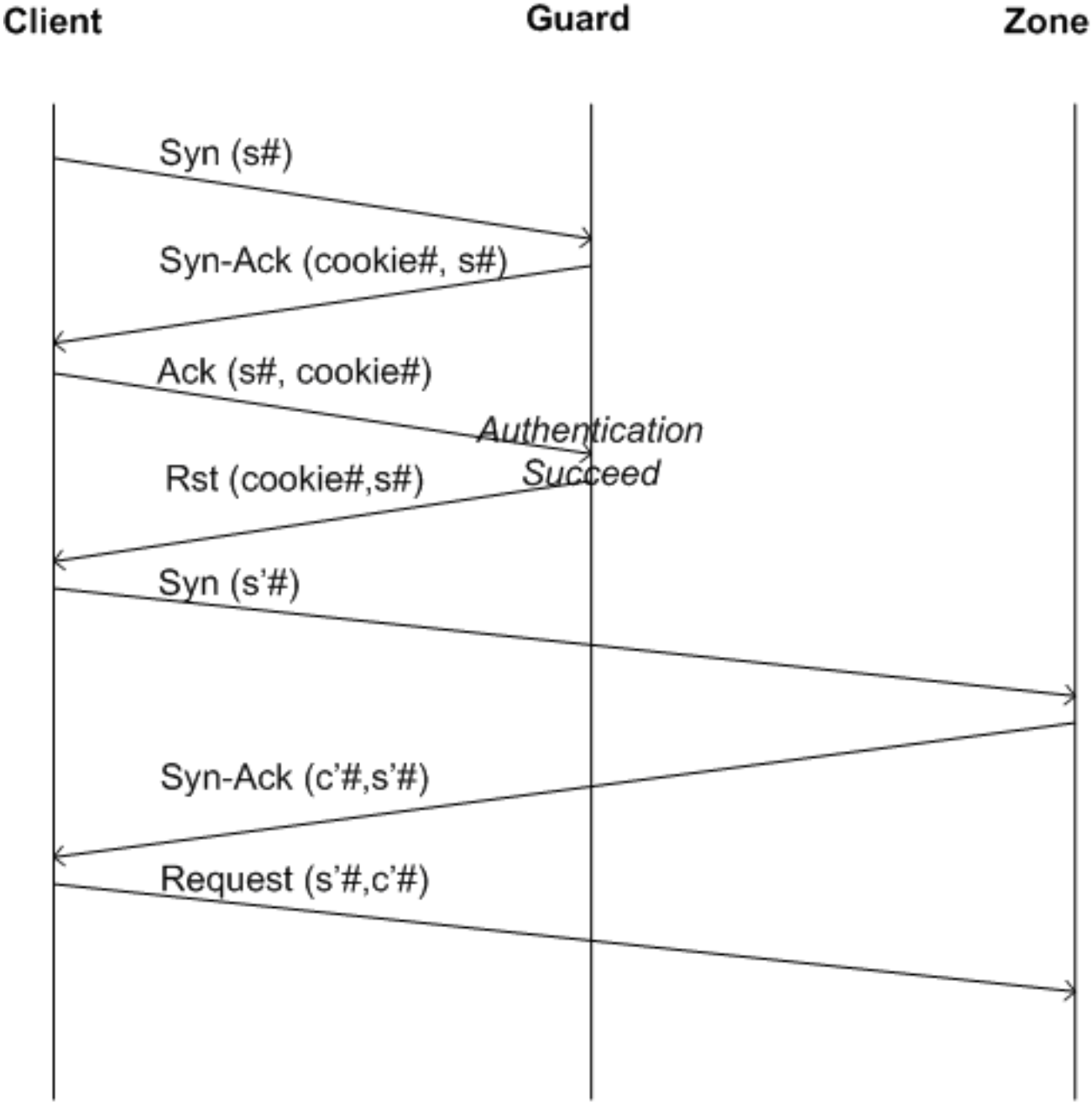
12012004 utilisant la « commande de la date 12012004" CLI. J'ai alors testé la modification de date à une zone par l'intermédiaire du rhZoneLastChangeTime SNMP OID. Ceci a fonctionné bien à moins que quand la date est changée à une date plus tôt que la dernière date changée. Ensuite, j'ai changé le remonter à 08062004 sur le CLI. Cependant, la réponse SNMP OID à questionner pour le rhZoneLastChangeTime est demeurée 12012004 (la vieille date). Après qu'une recharge, la réponse OID ait affiché (la dernière) modification correcte de date. Est-ce que c'est une bogue ?

A. C'est l'ID de bogue Cisco CSCuk52710 (clients enregistrés seulement). Il n'est pas généralement recommandé pour changer la période du périphérique vers l'arrière. Ceci peut avoir comme conséquence la superposition de quelques données d'historique. Un contournement pour ce problème est de redémarrer le serveur SNMP toutes les fois que l'heure est placée vers l'arrière :

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

Ceci efface le cache SNMP et apporte les données mises à jour au demandeur.

Q. Quelle est la différence entre la Réinitialisation TCP et la Coffre--remise de TCP ?



- **Remise :** Approprié à toutes les applications TCP qui relancent pour se connecter quand un paquet RST est reçu (ou permettre à l'utilisateur de rebrancher). La connexion est fermée avec un paquet RST et aucune balise n'est envoyée. Voir la figure pour l'écoulement de paquet de l'algorithme de remise.
- **Coffre--remise :** Tandis que la méthode ci-dessus exige la connaissance de niveau application, la coffre--remise exige seulement la conformité RFC de pile de TCP, mais ajoute un seconde retard 3 à la première fois de configuration de connexion. Il convient à la plupart des protocoles TCP automatiques (tels que la messagerie). Comme réponse à la synchronisation de client, la protection envoie un ACK avec un mauvais nombre d'accusé de réception qui tient un Témoin. Si le client est conforme avec RFC 793, il répond avec un paquet RST qui contient le mauvais nombre d'accusé de réception et retransmet la synchronisation d'origine après un 3-deuxième délai d'attente. Quand la protection reçoit le paquet RST avec le mauvais nombre d'accusé de réception, il authentifie la connexion et ne gêne pas la prochaine connexion. La mise en garde principale dans cette solution est que quelques Pare-feu relâchent silencieusement l'ACK mauvais-numéroté quoique ce ne soit pas RFC conforme. la commande n pour fournir une solution en pareil cas, si la protection reçoit

un deuxième paquet de synchronisation de la même source dans 4 secondes de la première, sans RST dans l'intervalle, la deuxième synchronisation est traitée de la même manière qu'elle est traitée dans la méthode de remise.

Q. Après qu'une mise à jour que je reçois « ne puisse pas se connecter au module de gestion ; LE SYSTÈME N'EST PAS COMPLÈTEMENT OPÉRATIONNEL : La connexion refusée ne peut pas écrire message d'erreur à socket ». Comment résoudre ce problème ?

A. En plus du `ne peut pas se connecter au module de gestion ; LE SYSTÈME N'EST PAS COMPLÈTEMENT OPÉRATIONNEL : La connexion refusée ne peut pas écrire au` message d'erreur de `socket`, cette erreur est générée quand vous redémarrez :

```
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
```

Ceci ressemble à une erreur de système de fichiers sur la protection. Afin de résoudre les erreurs FS, redémarrez la protection et observez le processus de **fsck** étroitement. Si vous entrez dans le mode de seul utilisateur, émettez le **fsck - y/**commande de demander une série manuelle de **fsck**.

Q. Quand je configure une zone utilisant le modèle par défaut, je ne peux pas trouver le modèle de stratégie de HTTP sous la zone quand j'émets la commande « de stratégies d'exposition ». Je vois chaque autre modèle de stratégie excepté le HTTP. Comment est-ce que je peux le trouver ?

A. La stratégie par défaut est disponible quand vous émettez le **wr t |** commandez et incluez le HTTP. Ceci t'affiche quelque chose semblable au **HTTP de stratégie-modèle -1 10.0 activés**. Le Traffic Anomaly Detector et la protection de Cisco regarde alors le trafic qui est basé sur la forme de seuil que la stratégie de HTTP est basée en fonction.

Q. Comment est-ce que j'exécute la reprise de mot de passe d'utilisateur de base ?

A. Référez-vous à la reprise de mot de passe de protection et de Traffic Anomaly Detector de Cisco pour des instructions sur la reprise de mot de passe d'**utilisateur de base**.

Q. Est-ce que je peux importer les Certificats faits sur commande SSL à la protection d'anomalie de Cisco ?

A. Non, protection d'anomalie de Cisco prend en charge seulement le certificat ssl auto-signé.

Q. J'ai reçu ce message d'erreur. Comment est-ce que je peux résoudre le problème ? **`RHWatchdog: RHWatchdog: Hardware Monitoring card reports HW errors.`**

A. Réinsérez le bloc d'alimentation pour résoudre le problème.

Informations connexes

- Cisco documentation technique d'appareils gardent et de réductions
- Support et documentation techniques - Cisco Systems