Часто задаваемые вопросы по обнаружению и защите от аномалий трафика (для сетей Riverhead)

Содержание

Введение

Этот документ обращается к большинству часто задаваемых вопросов (часто задаваемые вопросы), отнесенные к средству обнаружения аномального трафика Cisco и Защите (сети Riverhead).

Более подробную информацию о применяемых в документе обозначениях см. в описании условных обозначений, используемых в технической документации Cisco.

Вопрос. . Каков пароль по умолчанию для средства обнаружения аномального трафика Cisco и Защиты?

О. Пароль по умолчанию для средства обнаружения аномального трафика Cisco и Защиты является **admin/rhadmin**.

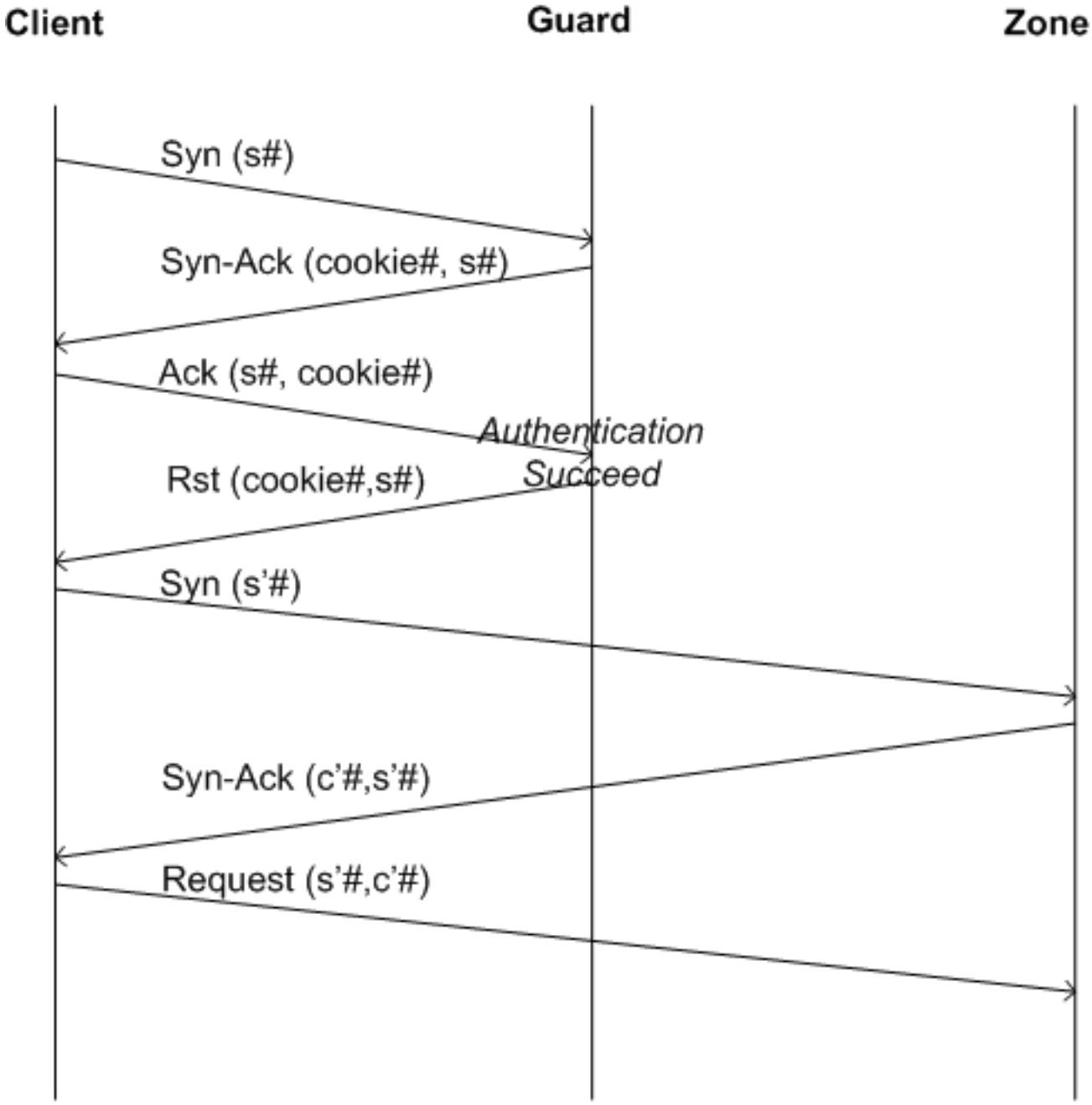
Вопрос. . Я изменил информацию о дате от 08062004 до будущей даты 12012004 использований "даты 12012004" команды CLI. Я тогда протестировал изменение даты к зоне через последнее изменение поясного времени rh SNMP OID. Это работало хорошо кроме тех случаев, когда дата изменена на дату ранее, чем последняя измененная дата. Затем, я изменил дату назад назад на 08062004 на CLI. Однако ответ SNMP OID для запроса для rhZoneLastChangeTime остался 12012004 (старая дата). После повторной загрузки ответ OID показал корректное (последнее) изменение даты. Это неполадка?

O. Это - идентификатор ошибки Cisco CSCuk52710 (только зарегистрированные клиенты). Обычно не рекомендуется изменить время устройства назад. Это может привести к наложению некоторой предыстории. Обходной путь для этой проблемы должен перезапустить snmp-server каждый раз, когда время установлено назад:

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

Это очищает кэш SNMP и приносит обновленные данные к запрашивающей стороне.

Вопрос. . Каково различие между Безопасным Сбросом TCP и Сбросом TCP?



- **Сброс:** Подходящий для всех приложений TCP, которые повторяют для соединения, когда пакет RST получен (или позволяют пользователю воссоединиться). Соединение закрыто с пакетом RST, и никакая метка не передается. Посмотрите рисунок для потока пакетов алгоритма Сброса.
- **Безопасный сброс:** В то время как вышеупомянутый метод требует осведомленности уровня приложения, безопасный сброс требует только соответствия RFC стека TCP, но добавляет 3--секундную задержку к первому разу настройки подключения. Это подходит для большинства автоматических протоколов TCP (таких как почта). Как ответ на клиентский SYN, Защита передает ACK с плохим номером подтверждения, который держит cookie. Если клиент совместим с RFC 793, он отвечает с пакетом RST, который содержит плохой номер подтверждения и повторно передает исходный SYN после 3--секундного таймаута. Когда Защита получает пакет RST с плохим номером подтверждения, это аутентифицирует соединение и не вмешивается в следующее соединение. Основное предупреждение в этом решении состоит в том, что некоторые межсетевые экраны тихо отбрасывают плохо пронумерованный ACK даже при том, что это не RFC-совместимый. n заказ предоставить решение в таких случаях, если Защита

получает второй SYN - пакет от того же источника в течение 4 секунд после первого без промежуточного RST, второй SYN рассматривается таким же образом, как это рассматривается в методе Сброса.

Вопрос. . После обновления я получаю, "Не может соединиться с модулем управления; СИСТЕМА НЕ FULL В РАБОЧЕМ СОСТОЯНИИ: Соединение отказалось, не Может записать для снабжения сокетом" сообщения об ошибках. Как это исправить?

O. В дополнение к ; FULL : , сообщение , эта ошибка генерируется, когда вы перезагружаете:

```
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
```

Это похоже на ошибку файловой системы на защите. Для решения ошибок FS перезагрузите защиту и смотрите **тщательная обработка FSCK**. Если вы входите в однопользовательский режим, выполняете **fsck-y /** команда для запроса ручного выполнения **fsck**.

Вопрос. . Когда я настраиваю Зону с помощью шаблона по умолчанию, я неспособен найти шаблон политики HTTP под зоной, когда я выхожу, "показывают политику" команда. Я вижу любой шаблон политики за исключением HTTP. Как я могу найти его?

O. Когда вы выполняете **команду wr t |** и включаете HTTP, политика по умолчанию доступна. Это показывает вам, что-то подобное **http шаблона политики-1 10.0 включило**. Средство обнаружения аномального трафика Cisco и Защита тогда посмотрели на трафик, который основывается на пороговой форме, на которой основывается политика HTTP.

Вопрос. . Как я выполняю восстановление пароля пользователя маршрута?

O. См. Cisco Guard и Восстановление пароля Средства обнаружения аномального трафика для инструкций по восстановлению пароля **пользователя маршрута**.

Вопрос. . Я могу импортировать пользовательские сертификаты SSL к Защите Аномалии Cisco?

O. Нет, Защита Аномалии Cisco только поддерживает самоподписанный сертификат SSL.

Вопрос. . Я получил это сообщение об ошибках. Как я могу решить вопрос?

RHWatchdog: RHWatchdog: Hardware Monitoring card reports HW errors.

O. Переустановите источник питания для решения вопроса.

Дополнительные сведения

- Cisco Guard и техническая документация понижающих устройств
- Cisco Systems – техническая поддержка и документация