Introduction

The RX/RE release Version 4.3.5 is a major release, enabling the RX to meet several new DDOS attacks observed recently on the Internet.

This release requires rView 4.3.1 and we recommend that all RX/RE users to upgrade their systems immediately.

Version 4.3.5 has several new DDOS algorithms providing better filtering against new TCP and UDP random attacks. In addition, Version 4.3.5 introduced a number of new user adjustable screens. This Release Note explains how to use these adjustments effectively.

These adjustments must be made carefully. The adjustments allow the RX/RE user to tailor the DDOS filter to their specific network environment, which when adjusted correctly, will enhance the filtering effectiveness of the device. On the other hand, if these adjustments were not set correctly, they can cause excessive false positive or false negative, making the entire system ineffective.

Key Version 4.3.5 Features Summary

- The <Interface Configuration> Menu has been expanded. The new menu now has:
  1. Interface Config Tab: This is the standard Filter/Monitor/Software Bypass configuration tab.
  2. TCP SYN Rate Config Tab: This tab was introduced in version 4.1.2. Based on operating experience, more detail configuration information is included in this Release Note.
  3. Source IP Whitelist Tab: Also a feature introduced in 4.1.2.
  5. Filter Sensitivity Tab: A new feature allowing filtering to start at an earlier time.
- In addition, in version 4.3.5, the RX will no longer accept UDP traffic to destination Port 80. This feature is “hard coded”. In future RX/rView releases, the user will have the option to turn on or off this UDP port 80 block.
- Note: The <Traffic Capture> feature displayed in rView 4.3.1 has not been activated yet. This will be enabled in the next RX release.

TCP SYN Rate Configuration Details

The TCP SYN rate engine is an effective tool defending a large number of different application level attacks. These attacks include certain variations of HTTP attacks, CC attacks, P2P attacks and many others. The TCP SYN Rate engine is very flexible, it examines client behavior instead of server behavior, and therefore will not produce false alarms during busy hours.

We shall illustrate how the TCP SYN Rate engine work with a HTTP attack example.

A HTTP attack starts by opening a TCP connection, and then executes a valid HTTP GET request to a specific page on the Victim's server. When the connection and HTTP GET request is repeated quickly,
and by multiple BOTs, it overwhelms the HTTP server and causes it to crash.

However, HTTP requests have two major types:

a) One HTTP request within a single TCP connection; this is supported by HTTP 1.0 and 1.1 versions
b) Multiple requests within a single TCP connection; this is supported by HTTP 1.1 only.

An Example Of An HTTP Attack

Today, nearly all HTTP attacks uses technique a), which process one HTTP request within a single TCP connection. This is also how most lab test software generate a HTTP attack. However, a few sophisticated attacks use technique b), which can cause more damages to the victim with fewer attacking BOTs and less attack bandwidth. For RioRey, attack type a) is considered a TCP SYN rate attack while attack type b) is considered a HTTP attack.

To execute HTTP attack using technique a):

i) The attacker starts a TCP connection by generating a TCP SYN packet
ii) It then sends an ACK and a GET command such as:

```
GET / HTTP/1.1
Host: www.ddosvictim.com...
```

iii) The attacker would then repeat steps i and ii frequently to keep the victim server busy.

In this type of attack, the attacker needs to generate attack packets at a high rate.

For this attack to work, the attacking BOT must issue a TCP SYN BEFORE every HTTP GET is generated. Therefore, often, an HTTP attack using this technique also causes a SYN RATE flood of the same rate of HTTP GET request.

Since a TCP SYN comes before every HTTP GET request, RioRey detects this excessive SYN rate request quickly, and will reject all TCP connection from this particular attacking BOT. This is a very effective method, because SYN rate limiting not only handles HTTP attacks, it also handles many variation of TCP connection based application attacks.

How To Set TCP Limits

To use the SYN RATE Limit properly, the SYN RATE Limits must be set correctly. SYN RATE in the RX is defined as the SYN per minute between a pair of IP address, therefore, it looks at the client behavior closely, and not the server.

The RioRey SYN RATE algorithm examines each client independently whether there is one client or 1000 clients connected to a server. Using our method, the type of application defines the active SYN RATE, and not the number of clients connecting to a server. For example, for normal web access, SYN RATE per client IP would be about 10 or so SYNs per minute. This rate is dependent upon the application and does not change during busy-hour or not-busy-hour for the network. Different applications will have different SYN rates per client.

There are two sets of tools to help you set the SYN RATE levels properly. First, the SYN RATE Config screen has a recommended level based on the current traffic it observes on the network. This is a conservative estimate, and is only based on the clients on the network at this moment.

Secondly, the TCP SYN Rate Config screen contains detail SYN rate statistics. You can use these statistics to make a more precise decision.

Setting Method I

Use the recommended settings on the SYN Rate Config Screen. The following diagram shows how this
is done. The two suggested levels are conservative, and safe. So they are good beginning levels to use until you have more experience working with the system.

![Figure 1. Example of a TCP SYN Rate Configuration screen](image)

It is also good initially to set the SYN Block Minute to 5 minutes, so any setting mistakes can recover quickly.

### Setting Method 2

When you have more experience with the system, you can set a much better settings for SYN RATE limit that can block most TCP application floods.

To set the SYN RATE levels, observe the network under normal operating conditions. The RX will report to you the SYN RATE per minute on your network. You will see a cluster of IPs around the normal SYN RATE for your application.

Using figure 1 as an example, You can see the following characteristics:

1. most of the applications inside this network generates less than 20 SYNs per minute
2. a few applications exist that generates SYNs up to 250 SYNs per minute
3. the top entry in “IP that contributes most SYNs” are two IPs with 605 SYNs per minute. This group contributed 1,210 total SYNs in a minute. But 605 is not the busiest IP. Since this list accounts for only 32% of all SYNs, there are still 68% of SYNs not included in the list.
4. the source (client IP) with Max SYN count is 1,100 SYNs per minute, but at 1,100 SYNs per minute, it did not make it into the “IP that contributes most SYNs” -- (1,100 is less than 1,210!)
5. using data from points 3 and 4 above, we can deduce that there are a lot of IPs sending SYN at rates between 605 and 1,100.
6. therefore, after observing the regular good traffic for a while, if the “SYN Count by most busy IP” stays around 1,100, then the “Per IP SYN Rate Limit” should be set about 10% (or a minimum of 10 SYNs per minute) above the 1,100 observed. Therefore, in this case, we should set the “Per IP
SYN Rate Limit" to: 1,100+110 = 1,210.

7. The “Max SYN Rate” should be set at 10% (or a minimum of 10) above the “Per IP SYN Rate Limit”, and therefore, in this case, 1,210 + 121 = 1,331.

8. Once set, observe good applications and make sure that there are no issues with good users.

Important Notes About SYN RATE Settings

- “Per IP SYN Rate Limit” limits a source IP to send no more SYNs per minute than what is specified in this entry. If this entry is set at 1,210, then if a source IP sends 1,211 SYNs in a minute, only the first 1,210 will pass through and 1 SYN will be dropped. This will be reported as 1 SYN dropped in the Attacker display, and the SYN RATE alarm will be raised to level 3.

- If “Per IP SYN Rate Limit” is set to 0 (zero), then this rate limit feature will be disabled.

- However, if any source IP sends SYNs at rate higher than what is specified in “Max SYN Rate”, this source IP will be blocked. All SYNs from this IP will be dropped and displayed in the Attacker display. The SYN RATE alarm will be set to level 6.

- If “Max SYN Rate” is set to 0 (zero), this check will be disabled and no source IP will be blacklisted.

- An IP address will stay in the Attacker list for the duration specified in “SYN Block Minutes” input.

- A blocked IP is not a Blacklisted IP (below). Attacker listed IP is only blocked for a duration defined in “SYN Block Minutes”. A Blacklisted user is definable, and blocked forever.

Source IP Whitelist

Source IP Whitelist is used to prevent certain IP from any blocking. For example, any trusted source IP such as network management IP, special trusted data upload/download sources etc. should be white listed to prevent accidental blocking.

Also, since some of these special sites may have high SYN rate access especially for upload/download applications; excluding these special high SYN Rate IP allow you to lower the SYN rate limit to a lower value. The lower the SYN rate limit value is, the better protection you have in your system.

When an IP in Source Whitelist generates SYN rate higher than the limit settings, the offending white listed IP will still be displayed in the Attacker list, but in gray instead of black. This indicates that the specific IP is not filtered.

The user can copy addresses from the Attacker display list and paste into the Whitelist to permanently unblock an IP address.

![Source IP Whitelist example](image)

Source IP Blacklist

Source IP Blacklist is used to block certain known bad IP address. The user can copy addresses from the Attacker display list and paste into the Blacklist for permanent blocking.
Filter Sensitivity

The RX assigns six levels of confidence when analyzing an attack.

Level 1 means an attack has been identified, but with little differentiation of good and bad traffic.

Level 2 means an improved level of differentiation of good and bad traffic.

Level 3 means all good traffic are identified, but there could be some bad traffic identified as good.

Level 4, 5 and 6 are various levels of improved attack traffic identification, where by level 6, the RX should identify 100% of good traffic and nearly 100% of the attacking traffic.

Normally, the RX is set to start filtering at level 3 to avoid dropping good traffic. However, for clients where they cannot tolerate the burst of bad traffic in the early analyze process, the user can select to start filtering at an earlier level. This is adjusted in the screen below.

Summary

Version 4.3.5 adjustments must be made carefully. The adjustments allow the RX/RE user to tailor the DDOS filter to their specific network environment, which when adjusted correctly, will enhance the filtering effectiveness of the device. On the other hand, if these adjustments were not set correctly, they can cause excessive false positive or false negative, making the entire system ineffective.