“Network Hygiene Pays Off”
The Business Case for IP Source Address Verification

Joao Luis Silva Damas
Daniel Karrenberg

Document ID: ripe-432
Date: 9 Mai 2008

Introduction

IP source address verification completely prevents a class of prevalent reflector-type DDoS attacks, helps to track down attacking hosts and simplifies some network management tasks. Yet a significant number of ISPs do not deploy it at the edge of their networks. Common wisdom seems to be that doing so would be expensive and would only help the "other guy" who is being attacked. This memo tries to contrast this common wisdom with some facts.

What is BCP 38

BCP 38 is a "Best Current Practice" document of the IETF. BCP 38, RFC 2827, is intended to limit the impact of distributed denial of service attacks, by:

- Denying access to the network to traffic with spoofed addresses
- Helping to ensure that traffic is traceable to its correct source network

As a side effect of protecting the Internet against such attacks, the network implementing the solution also protects itself from this and other attacks, such as management access to networking equipment by using spoofed addresses. BCP 84, RFC3704, has updated BCP 38.

No Confidence in IP Source Addresses is Bad

Suppose you need to investigate some unusual traffic flows or you just plain want to analyze current traffic load. If you do not do BCP 38 there is absolutely nothing you can get to know about the source of a packet from the packet alone. You cannot trust the source address at all. They packet could have entered your network *anywhere*. Can that be good?

Suppose someone launches an attack on one of your customers with packets that appear to come from another customer. The victim will likely request that you take action and stop the harmful traffic that appears to originate from another customer of yours. If you do not use BCP 38, you would have to tell the victim that this traffic could come from anywhere, and that you cannot determine quickly where the traffic is actually coming from.

Someone Can Pretend to be You

If you do not do BCP 38 an attacker can even launch an attack with packets that appear to be coming from one of the machines you operate yourself. Imagine the reaction of a customer that gets attacked by such packets. Are they going to trust you when you explain it is not really you? What will they think if you tell them that your network operating practices allow such masquerading? Imagine the cost of that.

Good Practice is Not Hard

It is not hard to prevent such a scenario. You simply have to:

- Do BCP 38 towards your customers
- Drop all packets with internal source addresses, that come in from external peerings

Once you have done that you *know* exactly who has sent a packet with an internal source address and you also know that any packet with an external source address must have come in via one of the external peerings.

Do keep in mind that some multihoming customers may require special configuration efforts.

However, these efforts are neither impossible nor very costly if implemented well. Our how-to documents explain the technical details. Since large classes of customers cannot be multihomed to start with, you can gain a lot by starting to do BCP 38 for them.

Doing BCP 38 Helps A Lot and Builds Confidence

Doing BCP 38 helps a lot with analyzing anomalies and makes understanding normal traffic load much more reliable.

In case any attacks or anomalies do happen, you can determine whether the source is within your own network or is a customer with confidence, simply by looking at the traffic itself! The decision about any countermeasures can be made very quickly and without involving any specialised analysis.

In case the source of the attack traffic is external, you can state that with confidence to your customers, and take action.

Reflector Attacks Cannot Happen Between Customers

If you do not do BCP 38, one customer can attack another with a DoS reflector attack. Consider your responsibility and possible liability if this were possible. If you do BCP 38, your customers cannot do this to each other. Any reflector attack traffic has to come from outside your network, thus be outside your direct responsibility.

Doing BCP 38 is Good Publicity

Showing that you operate your network responsibly and safely is good publicity; stating that you do BCP 38 is helps with that. Showing responsibility for operating safely discourages regulation and legislation of operating practices. Consider the difficulty to convince policy makers that enabling users to lie about their "caller-ID" is your normal operating practice.

Consider All Costs

When considering the cost of implementing BCP 38 in your network, also consider the costs of not doing so, together with the costs for implementation of BCP 38 itself. The savings in the network management area and in mitigation of DoS attacks may well outweigh the implementation costs. The added good publicity and confidence in good operating practices should not be neglected either.