Cisco IP Version 4 Source Guard
draft-baker-sava-cisco-ip-source-guard-00

Abstract

As requested in the SAVA discussions, this document describes Cisco’s IP Source Guard feature.
Table of Contents

1. Introduction .................................................. 3
2. IP Source Guard ................................................ 3
   2.1. Intended use of IP Source Guard ......................... 4
   2.2. Pitfalls of IP Source Guard .............................. 4
3. IANA Considerations .......................................... 5
4. Security Considerations ....................................... 5
5. Acknowledgements .............................................. 5
6. Informative References ....................................... 5
Author’s Address .................................................. 5
Intellectual Property and Copyright Statements .................. 7
1. Introduction

As requested in the SAVA discussions, this document describes Cisco’s IP Source Guard feature. This is a feature intended to implement BCP 38 [RFC2827] for IPv4 [RFC0791] in a switched LAN environment. It is referred to in [I-D.baker-sava-operational], which describes existing implementations of BCP 38 in real networks.

For IPR purposes, this document is coded as "no derivative works", which implies "not to be published as an RFC". The reason is that it describes a specific feature of a specific set of products, not for the purpose of setting a standard, but for the purpose of describing existing practice. This is an input to the process, not an output. Also, the proper place to find documentation of vendor features is the vendor’s web site (in this case, [IPSRCGRD]), not an IETF RFC. That said, we are happy to discuss the feature with anyone that is interested.

2. IP Source Guard

IP Source Guard provides source IPv4 address filtering on a Layer 2 port to prevent a malicious host from impersonating a legitimate host by assuming the legitimate host’s IPv4 address. The feature uses dynamic DHCP snooping and static IPv4 source binding to match IPv4 addresses to hosts on untrusted Layer 2 ports, including both access and trunk ports.

Initially, all IPv4 traffic on the protected port is blocked except for DHCP packets. After a client receives an IPv4 address from the DHCP server, or after a static IPv4 source binding is configured by the administrator, all traffic with that IPv4 source address is permitted from that client. Traffic from other hosts is denied. This filtering limits a host’s ability to attack the network by claiming a neighbor host’s IPv4 address. IPv4 Source Guard is a port-based feature that automatically creates an implicit port access control list (PACL).

As described, the feature is clearly one implemented on an IP or Ethernet switch intended for use in a SOHO, corporate, or access network. It is not, at this writing, supported on Cisco routers, nor is it something one would expect to be implemented on a host. Interoperability is not a requirement per se; if the DHCP client and server are interoperable with each other, spoofing is adequately eliminated.
2.1. Intended use of IP Source Guard

In the IPv4 architecture, it is legal to have more than one IP address on a host, and there are systems (including routers and some hosts) that routinely send datagrams using a source IP address that differs from the interface’s primary IP address. However, in the general case, a host has one address for each interface, and in the general case, a host has one interface. It is this case that the IP Source Guard feature addresses. By dropping all IPv4 datagrams from such hosts that use a different address than the one assigned, the feature severely limits a network’s ability to introduce spoofed source addresses to the Internet.

One could argue that this done not help the local network, but one would be wrong. An attack that happens elsewhere in the Internet can and does happen on the local LAN and in the IP network that a host resides in. Hence, while the degree may not be the same, eliminating address spoofing remains the first step in removing several classes of attacks from one’s network, and is therefore a good idea.

2.2. Pitfalls of IP Source Guard

IP Source Guard assumes that some ports on a switch - those whose single interface has one address - are "protected" and others are not. "Others" include systems with multiple interfaces, which might as a result receive a datagram through one interface and respond to it ("from" the IP of that interface) on the other, for which this capability is obviously problematic. "Others" also includes routers, prefix-based NATs, and others, which may originate traffic from a variety of addresses that are not within the local prefix.

The problem on a router interface should be obvious: a router forwards datagrams sent by other systems, which carry the source address of their originators. If this feature is applied to a router interface, the data it is forwarding will be discarded, nullifying its usefulness without advising either the network or its users of the fact - a clear violation of the End-to-End principle.

The problem on other varieties of devices - NATs that use multiple addresses, hosts that have "primary" and "secondary" addresses, and hosts with multiple LAN interfaces - is of the same nature. The system will be prevented from carrying out an intended function when using an address other than the one that the switch is enforcing the use of.
3. IANA Considerations

This memo adds no new IANA considerations.

Note to RFC Editor: This section will have served its purpose if it correctly tells IANA that no new assignments or registries are required, or if those assignments or registries are created during the RFC publication process. From the author’s perspective, it may therefore be removed upon publication as an RFC at the RFC Editor’s discretion.

4. Security Considerations

IP Source Guard is intended to contribute to the security of an IPv4 network by reducing the probability that an end system can inject data into the network that appears to be from a different interface or system. Obvious weaknesses, as discussed in Section 2.1, include any system that might legitimately send datagrams from an address other than that of an interface.

5. Acknowledgements

6. Informative References

[I-D.baker-sava-operational]

[IPSRCGRD]


Author’s Address

Fred Baker
Cisco Systems
Santa Barbara, California 93117
USA

Phone: +1-408-526-4257
Fax: +1-413-473-2403
Email: fred@cisco.com