Knowledge Base Article PG8762

PolicyGuru® Meta-Policy Controller

ENUM Requests and Source Number in Firewall Policy

Synopsis

Each Rule in a PolicyGuru® Solution Firewall Policy specifies the source(s), destination(s), and direction of calls to which the Rule applies, and the call-control action to be taken if a call matches the rule. The PolicyGuru ENUM Server compares the source and destination values in the policy rules with the source and destination values the SBC sends in the ENUM request and returns an ENUM response to the SBC that dictates the call-control action for that call: allow the call as originally routed, redirect the call to an alternate destination, or block the call.

For the source number in the ENUM request, the SBC may send the value from either the P-Asserted Identity (PAI) header or the FROM header:

- P-Asserted Identity (PAI)—The billing number for the line.
- FROM—The Caller ID.

Both header values are valid for use in whitelists and blacklists in PolicyGuru Firewall Rules. The PolicyGuru Solution executes policy on the source number that the SBC sends. MSSV analysts will ensure that the appropriate source number is added to the managed white and blacklists.

The purpose of this article is to provide additional information on the two types of source headers and how those sources can be used in policy.

More Information

For calls from mobile phones or consumer landlines, the PAI and FROM header values are expected to match. However, on calls from business phone lines, the PAI is the company’s billing number, while the FROM (Caller ID) is typically, but not always, the calling employee’s DID. Caller ID is usually, but not always, the number displayed on the receiving device. For example, contact center agents generally see PAI if it is available.

The FROM header is populated for all calls, while PAI is only present on inbound calls to an organization's toll-free numbers if the organization subscribes to ANI from the carrier. However, even if the organization subscribes to ANI from the carrier, PAI may not be present on all calls.

The Oracle SBC’s default behavior for ENUM requests is as follows: If the PAI header in the SIP Invite is populated, the SBC populates the ENUM source parameter with the PAI value. If the PAI header does not contain data, the SBC populates the ENUM source parameter with the value in the FROM header.

Since the FROM and PAI header are expected to match on calls from mobile phones and consumer landlines, PAI may be a key attribute in identifying the true source of spoofed calls when the FROM and PAI headers do not match. In these cases, the MSSV team can implement policies to mitigate the spoofed calls. For example:

- Attacks in which the caller is spoofing the attacked organization’s own DIDs.
- A TDoS attack in which the attacker is spoofing multiple Caller IDs.

If the SBC sends PAI for a call from a business phone line, it is possible that an individual caller's Caller ID will not be available. In this case, it may not be possible to block an individual caller in the organization; however, this is an unlikely scenario. The most common reason for blocking an individual caller is to mitigate fraudulent, abusive, or harassing calls. Employees are extremely unlikely to carry out this behavior at their place of work on an employer-provided telephone, for fear that their employer will take action when they find out. SecureLogix has offered managed services to Fortune 500 companies for nearly 20 years and has never seen this scenario. Also, whitelisting the PAI of known business partners can be used to ensure that valued calls are not unintentionally impacted.

Conclusion

The PolicyGuru Solution fully supports both PAI and FROM as the source number in ENUM requests. MSSV analysts manage the customer's policy and tailor the phone numbers in the whitelists and blacklists used in policy to match the header values received. All of the benefits of the SecureLogix MSSV are fully provided, regardless of which header value the SBC sends in an ENUM request.

Last Update: 12/21/2018

SecureLogix Corporation

13750 San Pedro, Suite 820 • San Antonio, Texas 78232
(210) 402-9669 • securelogix.com

Support (877) SLC-4HELP • EMAIL support@securelogix.com • support.securelogix.com