Does SenderBase Function Correctly behind NAT?

Document ID: 118061

Contributed by Scott Roeder and Robert Sherwin, Cisco TAC Engineers.
Jul 24, 2014

Contents

Introduction

This document describes SenderBase and its functionality behind Network Address Translation (NAT).

Does SenderBase function correctly behind NAT?

SenderBase is an IP−based reputation service that assigns SenderBase Reputation Service (SBRS) scores to IP addresses. SenderBase scores range from −10 to +10, reflecting the likelihood that a sending IP address is trying to send spam. Highly negative scores indicate senders who are very likely to be sending spam; highly positive scores indicate senders who are unlikely to be sending spam.

The SMTP listener in a Cisco Email Security Appliance (ESA) does SBRS score queries using DNS queries based on the IP address of the incoming TCP connection. If the IP address that the email appliance sees is the "real" address of the sender, then SBRS will function perfectly. However, if the NAT or Network Address and Port Translation (NAPT) device performs a NAT or NAPT function on the address of the email sender, then SBRS will not work for the sendergroups. In this case the incoming reply function can be used to get the correct IP address. Please see the user guide how to set up the incoming relay function.

Most enterprises using NAT do so to hide internal addresses from the Internet (or because they do not have sufficient IP addresses to operate without a NAT or NAPT function). In those cases, SenderBase works successfully, because the IP address of the external sender is not modified in any way.

Some enterprises with more complex network topologies do network address translation or proxy connections towards the inside of their networks. In those cases, SenderBase queries will not work properly and should be disabled on the incoming listener. (From the CLI, ***listenerconfig> edit > setup***.)

If you have any doubt whether the addresses are being converted or not or whether connections are being proxied, simply examine the mail_logs file (use a CLI command such as ***tail mail_logs***). This shows you each incoming connection to each listener, and you will quickly be able to see whether the IP addresses the ESA sees are from the general Internet or not.

Note: Be careful to look only at connections to public, inbound, listener.

Related Information

- ***Cisco Email Security Appliance User Guides***
- ***Technical Support & Documentation − Cisco Systems***