SPF Configuration and Best Practices

Contents

Introduction

This document describes different scenarios with Sender Policy Framework (SPF) on the Cisco Email Security Appliance (ESA).

Prerequisites

Cisco recommends that you know these topics:

- Cisco ESA
- All versions of AsyncOS

What is SPF?

Sender Policy Framework (SPF) is a simple email validation system designed to detect email spoofing by providing a mechanism to allow receiving mail exchangers to check that incoming mail from a domain is being sent from a host authorized by that domain's administrators. The list of authorized sending hosts for a domain is published in the Domain Name System (DNS) records for that domain in the form of a specially formatted TXT record. Email spam and phishing often use forged sender addresses, so publishing and checking SPF records can be considered anti-spam techniques.

Will there be much performance impact on the ESAs?

From the CPU prospect, there will not be a huge performance impact. However, enabling SPF verification will increase the number of DNS queries and DNS traffic. For every message, the ESA might have to initiate 1-3 SPF DNS queries and this will result in expiring DNS cache earlier than before. Therefore, the ESA will generate more queries for the other processes as well.

In addition to the previous information, the SPF record will be a TXT record that may be larger than the normal DNS records and could cause some extra DNS traffic.

How do you enable the SPF?

These instructions are from Advance User Guide on setting up SPF verification:

To enable SPF/System Independent Data Format (SIDF) on the default mail flow policy:

1. Click **Mail Policies > Mail Flow Policy**.
2. Click **Default Policy Parameters**.
3. In the default policy parameters, view the **Security Features** section.
4. In the SPF/SIDF Verification section, click **Yes**.
5. Set the level of conformance (the default is SIDF-compatible). This option allows you to determine which standard of SPF or SIDF verification to use. In addition to SIDF conformance, you can choose SIDF-compatible, which combines SPF and SIDF. Conformance levels details are available within the *End-User Guide.*
6. If you choose a conformance level of SIDF-compatible, configure whether the verification downgrades a **Pass** result of the PRA identity to **None** if there are Resent-Sender: or Resent-From: headers present in the message. You might choose this option for security purposes.
7. If you choose a conformance level of SPF, configure whether to perform a test against the HELO identity. You might use this option to improve performance by disabling the HELO check. This can be useful because the spf-passed filter rule checks the PRA or the MAIL FROM Identities first. The appliance only performs the HELO check for the SPF conformance level.

To take action on SPF verification results, please add content filter(s):

1. Create a spf-status content filter for each type of SPF/SIDF verification. Use a naming convention to indicate the type of verification. For example, use **SPF-Passed** for messages that pass SPF/SIDF verification, or **SPF-TempErr** for messages that were not passed due to a transient error during verification. For information about creating a spf-status content filter, see the spf-status Content Filter Rule in the GUI.
2. After you process some SPF/SIDF-verified messages, click **Monitor > Content Filters** to see how many messages triggered each of the SPF/SIDF-verified content filters.

What does "Helo Test" on and off mean? What will happen if the Helo test fails from a certain domain?

If you choose a conformance level of SPF, configure whether to perform a test against the HELO identity. You might use this option to improve performance by disabling the HELO check. This can be useful because the spf-passed filter rule checks the PRA or the MAIL FROM Identities first. The appliance only performs the HELO check for the SPF conformance level.

Valid SPF Records

To pass the SPF HELO check, ensure that you include an SPF record for each sending MTA (separate from the domain). If you do not include this record, the HELO check will likely result in a **None** verdict for the HELO identity. If you notice that SPF senders to your domain return a high number of **None** verdicts, these senders may not have included an SPF record for each sending MTA.

The message will be delivered if there are no Message/Content Filters configured. Again, you can take certain actions using Message/content filters for every SPF/SIDF verdict.

What is the best way to enable it for only one external domain?

To enable the SPF for a certain domain, you might need to define a new sender group with a mail flow policy that has SPF enabled; then create filters as mentioned previously.

Can you enable an SPF check for suspected Spam?

The Cisco Anti-Spam considers quite a lot of factors while calculating spam scores. Having a verifiable SPF record may reduce the spam score but there is still a chance of getting those messages caught as suspected spam.

The best possible solution would be to Allowlist the sender IP address OR create a message filter to skip spam check with multiple conditions (remote-ip, mail-from, X-skipspamcheck header, etc.). The header can be added by the sending server to identify one type of messages from others.

Related Information

- **Cisco Email Security Appliance - End-User Guides**
- **Email Authentication Best Practises - Deplying SPF/DKIM/DMARC**
- **Technical Support & Documentation - Cisco Systems**