Sender Domain Reputation Filtering

This chapter contains the following sections:

Overview of Sender Domain Reputation Filtering

Cisco Talos Sender Domain Reputation (SDR) is a cloud service that provides a reputation verdict for email messages based on the domains provided in the email envelope and header. Examples may include domains from - HELO/EHLO strings, envelope and header "From" addresses, "Reply-to" addresses, and "List-Unsubscribe" headers.

The domain-based reputation analysis enables a higher spam catch rate by looking beyond the reputation of shared IP addresses, hosting or infrastructure providers, and derives verdicts based on features that are associated with fully qualified domain names (FQDNs) and other sender information in the Simple Mail Transfer Protocol (SMTP) conversation and message headers.

The Sender Domain Age option is replaced with Sender Maturity from AsyncOS 14.2.x release onwards. Sender Maturity is an important feature to establish sender reputation. Sender Maturity is automatically generated for spam classification based on multiple sources of information and can differ from “Whois-based domain age.” Sender Maturity is set to a limit of 30 days, and beyond this limit, a domain is considered mature as an email sender, and no further details are provided.

From this release onwards, an additional Sender Domain Reputation check is performed after the sender header of the message is received. Messages with a Threat Level that matches the configured SDR reject level (in your email gateway) are rejected.

Note From this release onwards, the 'SDR Domain Age' configured filters are automatically updated to the 'SDR Sender Maturity' filters. The filters with an invalid value for Sender Maturity are marked as 'inactive' after the upgrade. Make sure you review and modify the message and content filters accordingly.

Note The Sender Maturity functionality uses the current time of your email gateway to display the Sender Maturity information in the logs and to match the required filter conditions. Make sure your email gateway is configured with the correct time based on your time zone.

After you upgrade to AsyncOS 14.2.x release, the legacy SDR verdicts in the content or message filters, reporting, and message tracking are replaced with the new SDR verdicts as follows:

- Untrusted
- Questionable
- Neutral
- Favorable
- Trusted
- Unknown

For more information about the recommended actions, you can take for each new SDR verdict, see SDR Verdicts, on page 2.

For more information, see the Cisco Talos Sender Domain Reputation (SDR) white paper in the Security Track of the Cisco Customer Connection program at http://www.cisco.com/go/ccp.

Note

- You must create a Cisco Customer Connection account to access the SDR white paper.
- Like Cisco IPAS disputes, submit SDR disputes by opening a support request with the Cisco Technical Assistance Center (TAC).

SDR Verdicts

The following table lists the SDR verdict names, descriptions, and recommended actions:

Table 1: SDR Verdicts

Verdict Name	Description	Recommended Action
Untrusted	The worst reputation verdict. Safest recommended blocking threshold. Expect to see false-negatives (FN) if the blocking threshold is set to only this verdict, which prioritizes delivery over security.	Block the message.
Questionable	This verdict has a low and relatively safe false-positive (FP) rate and might not be safe for all organizations. Not blocking on this verdict prioritizes delivery over security, but it results in false-negatives.	Scan the message with the other engines configured on your email gateway. Block only after review. For more information, see Tuning Sender Domain Reputation Policy , on page 5.
Neutral	The most common verdict, assigned to legitimate and mixed-use domains, associated with weak indicators that prevent a favorable verdict.	Scan the message with the other engines configured on your email gateway.
Favorable	The sender is using a fair domain that is not a new domain. The sender is following sender best practices, including, but not limited to using SPF, DKIM-signing, employing DMARC, and not sending spam.	Scan the message with the other engines configured on your email gateway.
Trusted	A rare verdict that indicates the sender is using a certified domain, where messages are authenticated by DKIM (aligned on the “From:” header domain).	Allow the message. For more information on how to bypass subsequent engines , use Message Filter rules such as "skip-spamcheck," "skip-viruscheck," and so on, see the “Message Filter Actions” section in the Using Message Filters to Enforce Email Policies.
Unknown	The sender is using domains that SDR does not recognize or cannot use to establish a reputation.	Scan the message with the other engines configured on your email gateway.

How to Filter Messages based on Sender Domain Reputation

Steps	Do This	More Information
Step 1	Enable SDR filtering on Cisco Email Security Gateway. **Note** After you upgrade to AsyncOS 12.0, SDR queries are enabled by default.	Enabling Sender Domain Reputation Filtering on Email Gateway, on page 4
Step 2	[Optional] Perform a review of the SDR configuration in your email gateway to establish an appropriate SDR policy	Tuning Sender Domain Reputation Policy , on page 5
Step 3	Configure a message or content filter to handle messages based on SDR.	Configuring Message or Content Filter for Handling Messages based on Sender Domain Reputation, on page 6
Step 4	Attach the content filter that you configured to filter messages based on SDR to an incoming mail policy.	Attaching Content Filter to Incoming Mail Policy, on page 10

Enabling Sender Domain Reputation Filtering on Email Gateway

Note After you upgrade to AsyncOS 12.0, SDR queries are enabled by default.

Procedure

Step 1 Go to **Security Services > Domain Reputation**.

Step 2 Click **Enable**.

Step 3 Check **Enable Sender Domain Reputation Filtering**.

Step 4 (Optional) Check **Include Additional Attributes** if you want the SDR service to check for SDR based on additional attributes of the message.

If you enable this option, the following additional attributes of the message are included in the SDR check to improve the efficacy:

- Username part of the email address present in the `'Envelope From:,'` `'From:,'` and `'Reply-To:'` headers.
- Display name in the `'From:'` and `'Reply-To:'` headers.

Step 5 (Optional) Enter the number of elapsed seconds before the SDR query times out.

Note Modifying the SDR query timeout value may impact the performance of mail processing.

Step 6 (Optional) Check **Match Domain Exception List based on Domain in Envelope From**: if you want the email gateway to skip the SDR check based on the domain in the Envelope From: header only.

Step 7 Move the **Range Slider** to choose the required SDR verdict range to accept or reject messages at the SMTP conversation level.

Note After you upgrade to AsyncOS 14.x and later, the range slider by default points to the Untrusted verdict. All messages with the Untrusted verdict are dropped at the SMTP conversation level.

Note You cannot select the Favorable verdict to reject messages because the verdict indicates that the sender uses a certified domain.

Step 8 Click **Submit** .

Step 9 (Optional) Click **I Agree** if you want to accept the SDR Include Additional Attributes Agreement message.

Note The SDR Include Additional Attributes Agreement message appears only when you select the Include Additional Attributes option.

Step 10 Click **Commit** to commit your changes.

What to do next

Review the SDR configuration in your email gateway to establish an appropriate SDR policy. See Tuning Sender Domain Reputation Policy , on page 5.

Tuning Sender Domain Reputation Policy

SDR recommends default behaviors for each verdict. However, if optimal tuning of false-positives and false-negatives is essential to your organization, follow the given steps to tune the SDR policy based on your security requirements.

Procedure

Step 1 Enable SDR on your email gateway without configuring any SDR policy actions for 10 days.

Step 2 Use the Message Tracking functionality to review messages based on the SDR verdict.

For more information, see Displaying Sender Domain Reputation Details in Message Tracking, on page 10. You can search for messages that received a verdict of 'Untrusted' or 'Questionable.'

Step 3 Review the messages obtained from the Message Tracking search (performed in step 2) for any false positives or false negatives.

False positives are messages that require to be delivered to the recipient’s mailbox but received a verdict of 'Questionable' or especially 'Untrusted.' False-negatives are messages that have not received an 'Untrusted' verdict but are expected to be blocked based on the message attributes related to SDR.

Step 4 [If false-positives are present because the message received an 'Untrusted' verdict] Open a support ticket with Cisco TAC before you proceed to configure SDR policy to block messages based on the 'Untrusted' verdict.

Note In most use-cases, Cisco Talos expects you to block messages with an 'Untrusted' verdict.

Step 5 Use the recommended safe 'Untrusted' threshold if false-positives are present in the messages that received a “Questionable” verdict.

Note If you do not use the 'Untrusted' threshold, you can block messages based on the more aggressive 'Questionable' threshold. For more information, see Configuring Message or Content Filter for Handling Messages based on Sender Domain Reputation, on page 6.

Note The 'Questionable' verdict is associated with large volume senders that send spam messages but might also deliver legitimate (mostly low-priority) bulk email. It is appropriate to block messages after review based on your security requirements.

Configuring Message or Content Filter for Handling Messages based on Sender Domain Reputation

You can use the ‘Domain Reputation’ message or content filter in any one of the following ways to filter messages based on SDR, and take appropriate actions on such messages:

- Sender Domain Verdict
- Sender Maturity
- Sender Domain Unscannable

Note The Sender Domain Age option is replaced with Sender Maturity from AsyncOS 14.2.x release onwards. Sender Maturity is already incorporated into the SDR verdict. It is generally not recommended to filter messages based on Sender Maturity, except for special use-cases.

Related Topics

- Tuning Sender Domain Reputation Policy , on page 5
- Filtering Messages based on Sender Domain Reputation using Message Filter, on page 7
- Filtering Messages based on Sender Domain Reputation using Content Filter, on page 8

Filtering Messages based on Sender Domain Reputation using Message Filter

Filtering Messages based on Sender Domain Verdict

Note The recommended blocking threshold is "Untrusted." For more information about SDR verdicts, see SDR Verdicts, on page 2 and for tuning SDR policy, see Tuning Sender Domain Reputation Policy , on page 5

Syntax:

```
drop_msg_based_on_sdr_verdict:
if sdr-reputation (['untrusted', 'questionable'], "<domain_exception_list>")
{drop();}
```

Where:

- `'drop_msg_based_on_sdr_verdict'` is the name of the message filter.
- `'sdr-reputation'` is the Domain Reputation message filter rule.
- `'untrusted','questionable'` is the range of the sender domain verdict used to filter messages based on SDR.
- `'domain_exception_list'` is the name of a domain exception list. If a domain exception list is not present it is displayed as "".
- `'drop'` is the action applied on the message.

Example

In the following message, if the SDR verdict is 'Unknown', the message is quarantined.

```
quarantine_unknown_sdr_verdicts:
if sdr-reputation (['unknown'], "")
{quarantine("Policy")}
```

Filtering Messages based on Sender Maturity

Note The Sender Domain Age option is replaced with Sender Maturity from AsyncOS 14.2.x release onwards. Sender Maturity is already incorporated into the SDR verdict. It is generally not recommended to filter messages based on Sender Maturity, except for special use-cases. Sender Maturity is set to a limit of 30 days, and beyond this limit, a domain is considered mature as an email sender, and no further details are provided.

Syntax:

```
<msg_filter_name>
if sdr-maturity (<'unit'>, <'operator'> <'actual value'>)
{<action>}
```

Where:

- `'sdr-maturity'` is the Sender Maturity message filter rule.
- `'unit'` is the number of 'days,' 'years,' 'months,' or 'weeks' option used to filter messages based on the sender maturity.

- `'operator'` are the following comparison operators used to filter messages based on the sender maturity:
  - – > (Greater than)
  - – >= (Greater than or equal to)
  - – < (Lesser than)
  - – <= (Lesser than or equal to)
  - – == (Equal to)
  - – != (Not equal to)
  - – Unknown
- `'actual value'` is the number used to filter messages based on the sender maturity.

Examples

In the following message, if the maturity of the sender domain is unknown, the message is dropped.

```
Drop_Messages_Based_On_SDR_Maturity: if (sdr-maturity ("unknown", "")) {drop();}
```

In the following message, if the maturity of the sender domain is less than one month, the message is dropped.

```
Drop_Messages_Based_On_SDR_Maturity: if (sdr-maturity ("months", <, 1, "")) { drop(); }
```

Filtering Messages based on Sender Domain Unscannable

Syntax:

```
<msg_filter_name>
if sdr-unscannable (<'domain_exception_list'>)
{<action>}
```

Where:

- `'sdr-unscannable'` is the Domain Reputation message filter rule.

  `'domain_exception_list'` is the name of a domain exception list. If a domain exception list is not present it is displayed as "".

Example

In the following message, if the message failed the SDR check, the message is quarantined.

```
Quarantine_Messages_Based_On_Sender_Domain_Unscannable: if (sdr-unscannable (""))
{quarantine("Policy");}
```

Filtering Messages based on Sender Domain Reputation using Content Filter

Before you begin

- (Optional) Create an address list that contains only domains. To create one, go to *Mail Policies* > *Address Lists* page in the web interface or use the `addresslistconfig` command in the CLI. For more information, see Mail Policies.

- (Optional) Create a Domain Exception List. For more information, see Creating Domain Exception List, on page 9.

Procedure

Step 1 Go to **Mail Policies** > **Incoming Content Filters**.

Step 2 Click **Add Filter**.

Step 3 Enter a name and description for the content filter.

Step 4 Click **Add Condition**.

Step 5 Click **Domain Reputation**.

Step 6 Choose any one of the following conditions to filter messages based on SDR:

- Select **Sender Domain Reputation Verdict** to choose a verdict range to filter messages based on the verdict received from the SDR service.

  Note The recommended blocking threshold is "Untrusted." For more information about SDR Verdicts, see SDR Verdicts, on page 2.

- Select **Sender Maturity**, choose the comparison operator, enter a number, and choose the time period to filter messages based on the maturity of the sender domain.

  Note The Sender Domain Age option is replaced with Sender Maturity from AsyncOS 14.2.x release onwards. Sender Maturity is already incorporated into the SDR verdict. It is generally not recommended to filter messages based on Sender Maturity, except for special use-cases. Sender Maturity is set to a limit of 30 days, and beyond this limit, a domain is considered mature as an email sender, and no further details are provided.

- Select **Sender Domain Reputation Unscannable** to filter messages that failed the SDR check.

Step 7 (Optional) Select the list of allow listed domains that you do not want the email gateway to filter messages based on SDR.

Step 8 Click **Add Action** to configure an appropriate action to take on messages based on SDR.

Step 9 Submit and commit your changes.

Creating Domain Exception List

A domain exception list consists of a list of addresses that contain only domains. You can use a domain exception list to skip the SDR check for all incoming messages, irrespective of the mail policies configured on your Cisco Email Security Gateway.

Note If you want to skip SDR content filter actions on incoming messages for specific mail policies, you need to select the domain exception list in the Domain Reputation content filter.

Criteria for using Domain Exception List

By default, to skip the SDR check, the domains in the `Envelope From:`, `From:`, and `Reply-To:` headers of the message must be the same and match the domain configured in the domain exception list. If you want to skip

the SDR check based on the domain in the Envelope From: header only, select the ‘Match Domain Exception List based on Domain in Envelope From:’ option in the Domain Reputation settings page.

Procedure

Step 1 Go to **Security Services > Domain Reputation**.

Step 2 Click **Edit Settings** under Domain Exception List.

Step 3 Select the required address list that contains domains only.

Step 4 Submit and commit your changes.

What to do next

You can also create a Domain Exception List using the `domainrepconfig` command in the CLI. For more information, see the *CLI Reference Guide for AsyncOS for Cisco Email Security Appliances*.

Attaching Content Filter to Incoming Mail Policy

You can attach the content filter that you configured to filter messages based on SDR to an incoming mail policy.

Procedure

Step 1 Go to **Mail Policies > Incoming Mail Policies**.

Step 2 Click the link below Content Filters.

Step 3 Make sure to select **'Enable Content Filters (Customize Settings).'**

Step 4 Select the content filter that you created for filtering messages based on SDR.

Step 5 Submit and commit your changes.

Sender Domain Reputation Filtering and Clusters

If you use centralized management, you can enable SDR filtering and mail policies at the cluster, group, and machine level.

Displaying Sender Domain Reputation Details in Message Tracking

You can use Message Tracking to view the message details based on SDR.

Before you begin

- Make sure that you enable the Message Tracking feature on the email gateway. To enable Message Tracking, go to **Security Services > Message Tracking** page in the web interface.

Note You can track messages based on SDR verdicts even when you do not configure SDR-based content or message filters in your email gateway.

Procedure

Step 1 Go to **Monitor > Message Tracking**.

Step 2 Click **Advanced**.

Step 3 Check **Sender Domain Reputation** under Message Event.

Step 4 Select the required SDR verdict(s) to view messages based on the verdict received from the SDR service.

Step 5 (Optional) Check **Unscannable** to view messages when the SDR check failed.

Step 6 (Optional) Select the required SDR threat categories to view messages based on the threat category.

Step 7 Click **Search**.

Viewing Alerts

The following table lists the system alert generated for SDR, including a description of the alert and the alert severity.

Component/Alert Name	Message and Description	Parameters
MAIL.IMH.SENDER_DOMAIN_LOOKUP_FAILURE_ALERTS	The SDR lookup failed. Reason - <$reason> Warning. Sent when a SDR query fails.	**'reason'** - The reason why the SDR query failed.

Viewing Logs

The SDR filtering information is posted to the Mail Logs. Most information is at the Info or Debug level.

Examples of SDR Filtering Log Entries

The SDR filtering information is posted to the Mail Logs. Most information is at the Info or Debug level.

- Sender Domain Reputation Request Timeout, on page 12
- Sender Domain Reputation General Errors, on page 12

Sender Domain Reputation Request Timeout

In this example, the log shows a message that was not filtered based on SDR because of a request timeout error when communicating with the SDR service.

```
Mon Jul 2 09:00:13 2018 Info: New SMTP ICID 4 interface Management (192.0.2.10) address
224.0.0.10 reverse dns host unknown verified no
Mon Jul 2 09:00:13 2018 Info: ICID 4 ACCEPT SG UNKNOWNLIST match ipr[none] ipr not enabled
 country not enabled
Mon Jul 2 09:00:13 2018 Info: Start MID 4 ICID 4
Mon Jul 2 09:00:13 2018 Info: MID 4 ICID 4 From: <sender1@example.com>
Mon Jul 2 09:00:13 2018 Info: MID 4 ICID 4 RID 0 To: <recipient1@example.com >
Mon Jul 2 09:00:13 2018 Info: MID 4 Message-ID '<000001cba32e$f24ff2e0$d6efd8a0$@com>'
Mon Jul 2 09:00:13 2018 Info: MID 4 Subject 'Message 001'
Mon Jul 2 09:00:13 2018 Info: MID 4 SDR: Message was not scanned for Sender Domain Reputation.
 Reason: Request timed out.
```

Solution

When an SDR request times out, the message is marked as unscannable, and the configured actions are applied to the message.

Sender Domain Reputation General Errors

In this example, the log shows a message that was not filtered based on SDR because of an unknown error.

```
Mon Jul 2 09:00:13 2018 Info: New SMTP ICID 4 interface Management (192.0.2.10) address
224.0.0.10 reverse dns host unknown verified no
Mon Jul 2 09:00:13 2018 Info: ICID 4 ACCEPT SG UNKNOWNLIST match ipr[none] ipr not enabled
 country not enabled
Mon Jul 2 09:00:13 2018 Info: Start MID 4 ICID 4
Mon Jul 2 09:00:13 2018 Info: MID 4 ICID 4 From: <sender1@example.com >
Mon Jul 2 09:00:13 2018 Info: MID 4 ICID 4 RID 0 To: <recipient1@example.com >
Mon Jul 2 09:00:13 2018 Info: MID 4 Message-ID '<000001cba32e$f24ff2e0$d6efd8a0$@com>'
Mon Jul 2 09:00:13 2018 Info: MID 4 Subject 'Test mail'
Mon Jul 2 09:00:13 2018 Info: MID 4 SDR: Message was not scanned for Sender Domain Reputation.
 Reason: Unknown error.
```

Solution

When an unknown error occurs, the message is marked as unscannable, and the configured actions are applied to the message.