ESAの送信者ドメインレピュテーションの設定 REFRESH In Progress 2024年4月

内容

はじめに

このドキュメントでは、Eメールセキュリティアプライアンス(ESA)の送信者ドメインレピュテーション(SDR)の設定について説明します。

前提条件

要件

次の項目に関する知識があることが推奨されます。

- ESAの概念
- ESA の設定

- メールフローポリシー、メッセージフィルタ、コンテンツフィルタ、グローバルドメインレピュテーションなどのSEG機能/機能に関する一般的な知識。

使用するコンポーネント

このドキュメントの情報は、AsyncOS for ESA 14.2以降に基づくものです。

このドキュメントの情報は、特定のラボ環境にあるデバイスに基づいて作成されたものです。このドキュメントで使用するすべてのデバイスは、クリアな（デフォルト）設定で作業を開始しています。本稼働中のネットワークでは、各コマンドによって起こる可能性がある影響を十分確認してください。

概要

1. SDRは、スパムフィッシング検出を改善する追加サービスとして開発されました。

2. SDRは複数のヘッダー値をキャプチャしてTalos Threat Intelligence Serverにアップロードし、大規模なTalosリソースが段階的なスケールで各メッセージの判定を行います。

3. 決定に含まれるヘッダー値は、次のとおりです。

- 封筒の差出人
- 変更前
- 返信先
- DMAR、DKIM、SPFの検証（設定されている場合）
- 電子メールアドレスの（ユーザ名）値は、オプションでFrom、Envelope-From、およびReply-Toヘッダーから送信されます
- 送信者IP
- FromヘッダーとReply-Toヘッダーに名前を表示します。

5. SDRスキャンは、すべてのインバウンドメッセージに対して実行されます。

6. SDRスキャンは、Simple Mail Transfer Protocol(SMTP)がメッセージを受け入れた直後に行われます。

7. SDRアクションは、最初のメールフローポリシー段階で、メッセージフィルタまたはコンテンツフィルタのオプションとともに実行できます。

8. 構成するコンポーネントは次のとおりです。

- ドメインレピュテーションサービスの有効化
- ドメイン例外リスト（オプション）
  - ドメイン例外リスト（グローバル）
  - メッセージ/コンテンツフィルタ固有のドメイン例外リスト。
  - メールフローポリシーを利用したドメイン修復によるグローバルアクション。
  - SMTPカンバセーションレベルでアクションを実行するドメインレピュテーションを使用したグローバルアクション。
- メッセージフィルタまたはコンテンツフィルタ

設定

ドメインレピュテーションサービスWebUIの有効化

SDRは、WebUIまたはCLIインターフェイスから有効にできます。

WebUI:

1. Mail Security Services > Domain Reputation > Enableの順に移動します。

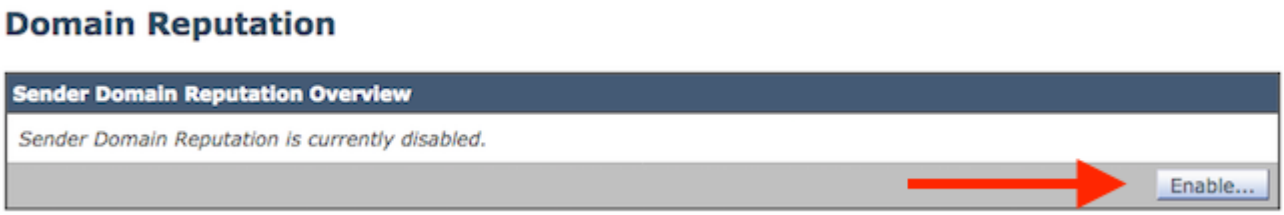
2. Enable Sender Domain Reputation Filteringの横にあるボックスをクリックします。

3. チェックしたデータにオプションのヘッダー値を含めて有効性を向上させる場合は、このボックス「追加属性を含む：（オプション）」を選択します。？(疑問符)をクリックして、詳細を確認してください。

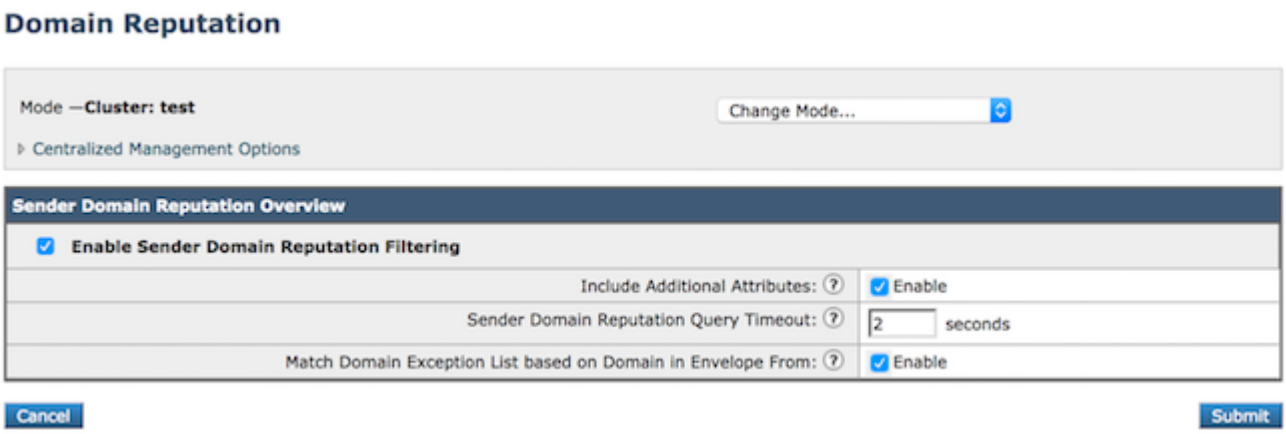
4. このボックスはSender Domain Reputation Query Timeoutを選択します。？(疑問符)をクリックして、詳細を確認してください。

5. 「Match Domain Exception List Based On Domain in Envelope From - Enabled」を選択します。

6. 図に示すように、Submit > Commitの順にクリックします。



送信者（ドメインレピュテーション）サービス



Security Services > Domain Reputation（セキュリティサービス）

ドメイン例外リスト

1. ドメイン例外リストは、受信メールフローに対する送信者ドメインレピュテーションスキャンをバイパスできます。

2. ドメイン例外リストは、メールフローに影響を与えるために異なる場所に適用できます。

3. グローバルアプリケーションは、スキャンされたすべてのメールに適用できます。

4. コンテンツ/メッセージフィルタ内のより詳細なアプリケーションは、設定されたフィルタにのみ影響を与える可能性があります。

5. ドメイン例外リストには、単純なオプションとより安全なオプションの両方を提供する2つのオプションがあります。

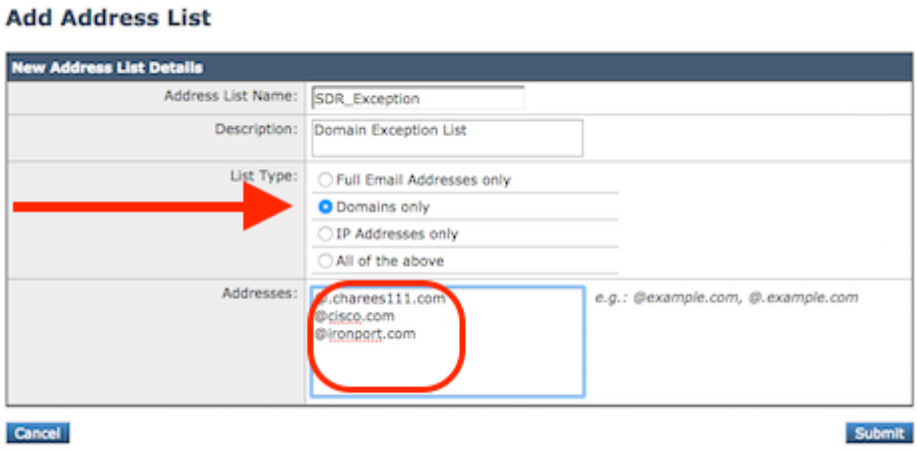
6. このドキュメントでは、ドメイン例外リストを使用するメッセージのSDRを正常にバイパスするためのオプションについて説明します。

7. [ドメイン例外リストの要件の説明]

アドレス一覧の作成

1. Mail Policies > Address List > Add Address List > Name > Description > List Type: Domains Onlyの順に移動します。
2. カンマ区切りを使用して各ドメイン名を追加します。

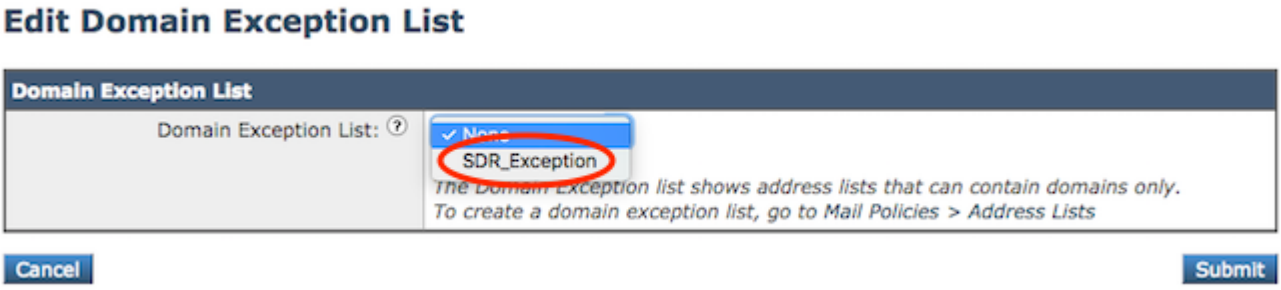
3. Submit をクリックし、図に示すようにCommit Changes をクリックします。



ドメイン例外リストに適用されるアドレスリスト

SDRグローバルドメイン例外リストへのアドレスリストの適用

1. Security Services > Domain Reputation > Domain Exception List > Edit Settings > Domain Exception Listの順に移動します（リストを選択します）。
2. Submit をクリックし、図に示すようにCommit Changes をクリックします。



ドロップダウンからアドレスリストを選択します。

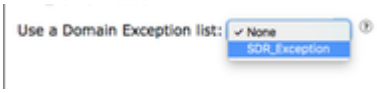
コンテンツ/メッセージフィルタへのアドレスリストの適用

受信コンテンツフィルタ：

1. Condition > URL Reputation > Threat Feeds Optionの順に移動します。

2. ドメインレピュテーションの条件。

3. ここをクリック：



ドメイン例外リストでは、ポリシーごとのアクションが許可されます。

メッセージ フィルタ

メッセージフィルタ内のドメイン例外リストアプリケーションは、条件内のオプションとして含まれます。

注：これらのサンプルには、条件全体の一部としてdomain_exception_listが含まれています。

---

1. sdr-reputation (['awful', 'poor', 'tained', 'weak', 'unknown', 'neutral', 'good'], domain_exception_list)
2. sdr-age("days", <, 5, domain_exception_list)
3. sdr-unscannable(domain_exception_list)

より包括的な説明とメッセージフィルタアプリケーションのサンプルについては、以下の見出しの下にある『ESA User Guides』を参照してください。

- ETFのドメインレピュテーションルール
- メッセージフィルタを使用する送信者ドメインレピュテーションに基づくメッセージのフィルタリング

SDR判定に対してアクションを実行するコンテンツフィルタの作成

1. SDRは受信メールフローに対してのみ有効です。
2. SDR条件名：Domain Reputation
3. 複数の条件を作成して、異なる結果を組み合わせることができます。
4. ドメインレピュテーション条件には、それぞれに複数のオプションを含む2つの異なるチェックが含まれます。

- 送信者ドメインレピュテーション
  - 送信者ドメインレピュテーション判定
  - 送信元ドメインの経過時間
  - 送信者ドメインレピュテーションのスキャン不能
- 外部の脅威フィード
  - ダウンロードされたコンテンツリストの脅威フィードを使用して、SDR用に収集され

た同じドメインヘッダーに対してスキャンできます。

注：ドメインレピュテーション条件に含まれるこれらのオプションは、選択ごとに異なるオプションに基づいて視覚的に変更できます。

---

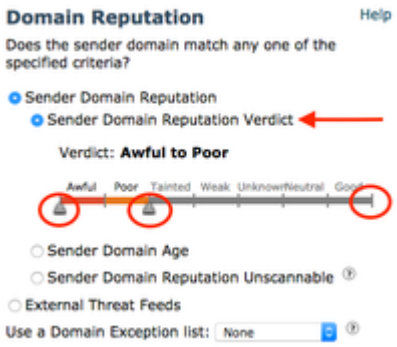
5. ドメインレピュテーション条件の最後のオプションは、ドメイン例外リストです。

6. アドレス一覧に関連付けられたドメイン例外リスト機能は、メッセージ処理のより詳細なメールポリシーレベルにリストを適用することによって、アクションの適用により多くの制御を追加します。

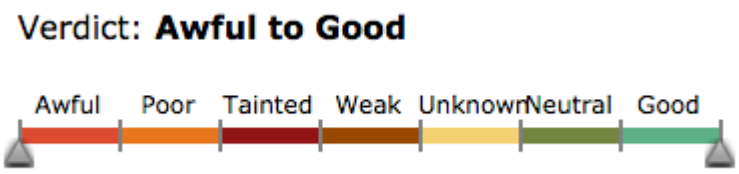
7. メールポリシー>受信コンテンツフィルタ>フィルタの追加>条件の追加>ドメインレピュテーションに移動します。

8. 条件1：送信者ドメインレピュテーション判定。

- ひどい、貧しい、汚れた、弱い、不明、中立、良い
- 三角形のスライディングマーカーを使用して、一致させる範囲を選択します。
- AwfulとPoorが推奨値です。
- 「Awful」と「Poor」に一致するメッセージには、「Spam」や「Malicious」などの追加のカテゴリ値が含まれていることがあります。これらの値は、メッセージトラッキングで確認できます。



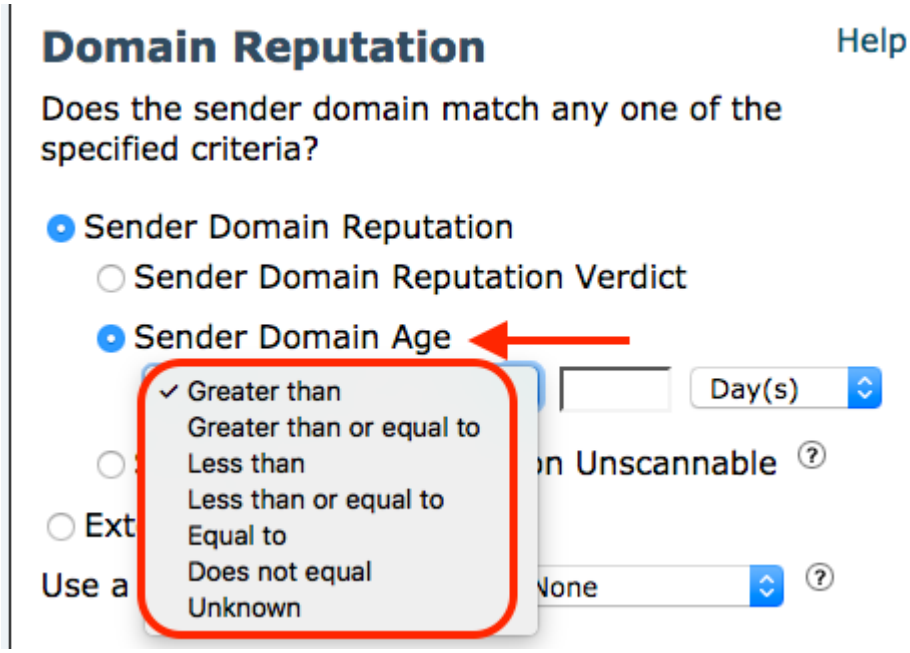
SDR判定可能な範囲スライドバー



SDR判定スライドバーの全表示

9. 条件2：送信者ドメインの保存期間。

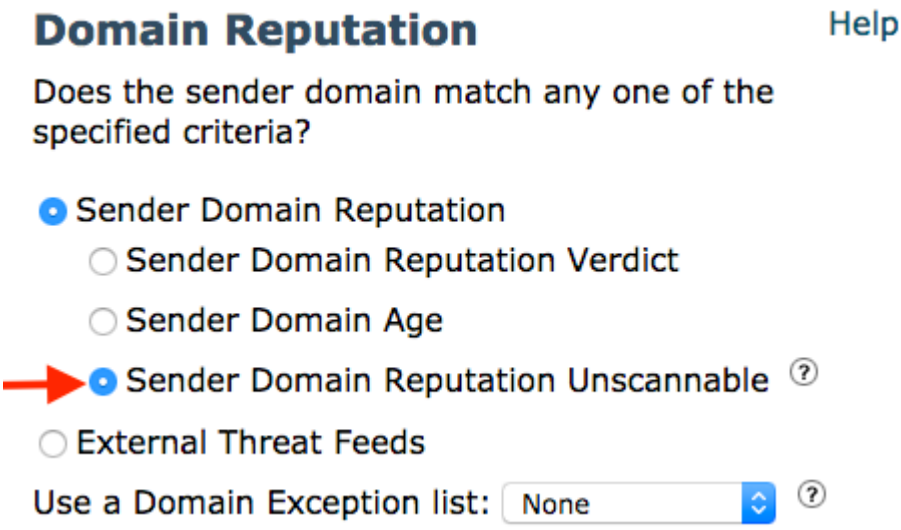
- ドメインの古さは、より多くのリスクまたは長く確立された信頼性に関連付けることができます。
- 10日未満のドメインの可能性はリスクが高くなる可能性があります。



送信者のドメインの経過時間。値が低いほど、リスクが高くなります。

10. 条件3：送信者ドメインレピュテーションがスキャン不能です。

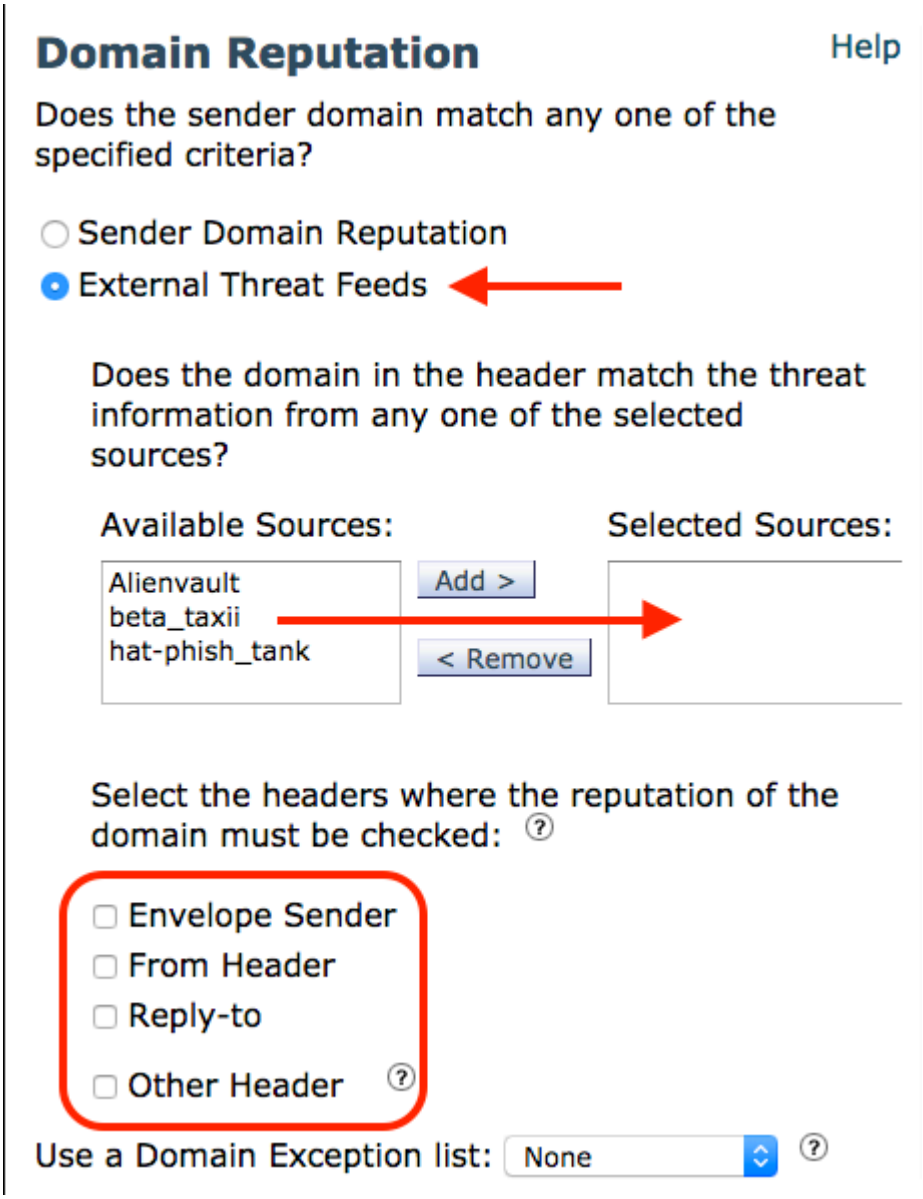
- 判定を取得できない場合に管理者がアクションを実行するオプションを提供します。



SDRスキャン不能

11. 条件4：外部の脅威フィード

- SDRスキャンに含まれるヘッダーは、カスタムダウンロードされたSTIX/TAXIIコンテンツでもスキャンできます。
- 外部脅威フィードについては、ここで詳しく説明します。 [外部脅威フィード。]

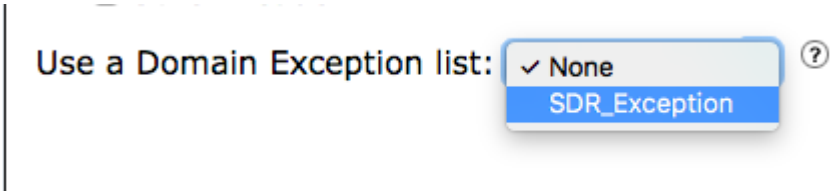


外部脅威フィードは、SDRと同じヘッダーのスキャンに使用できます。

- [Eメールセキュリティアプライアンスユーザガイド]

12. 条件5：ドメイン例外リストを使用する。

- コンテンツフィルタ内でドメイン例外リストを使用すると、グローバルリストよりも多くの制御が追加されます。



ドメイン例外リストでは、ポリシーごとのアクションが許可されます。

13. これらの条件と組み合わされた行動は、最小限から極端まで及び、管理者の望ましい結果に依存する可能性があります。

14. 人気の高いアクションの一部を次に示します。

- 検疫/検疫へのコピー
- [Drop]
- メッセージの件名または本文に免責事項または警告を追加します。
- メッセージトラッキングログに特定の単語、フレーズ、または値を生成するためのログエントリを作成します。

メッセージフィルタを使用したSDRの設定

1. ESAユーザガイドは、メッセージフィルタの構文、定義、および例に関する優れた情報源です。
2. ここに記載されている情報以外のメッセージフィルタに関するその他のコンテンツについては、ユーザガイドでこのヘッダーを検索してください。

- メッセージフィルタを使用した送信者ドメインレピュテーションに基づくメッセージのフィルタリング

3. 次の条件がSDRメッセージ・フィルタに関連付けられています。

- sdr-reputation (['awful', 'poor'] >>>この評価の値はすべてAwful、Poor、Tainted、Weak、Unknown、Neutral、Goodです。
- if sdr-reputation (['awful', 'poor'], "<domain_exception_list>") >>>これには、ドメイン例外リストの使用が含まれます
- sdr-age (<'unit'>, <'operator'> <'actual value'>) >>>の場合は、「operator」の定義についてユーザー・ガイドを参照してください。
  - (sdr-age ("unknown", "")) >>> unit =不明残りの値は「」に置き換えられます。
  - 例： (sdr-age ("months", <, 1, "")). >>> unit =日、月、年演算子= <（より小さい）。実績値= 1
- sdr-unscannable (<'domain_exception_list'>) >>>が表示された場合、メッセージの結果がスキャン不能になった場合。このサンプルには、ドメイン例外リストの条件も含まれています

。
- if (sdr-unscannable ("")) **>>>**このサンプルには例外リストは含まれていません。値は("")に置き換えられます

確認

このセクションでは、設定が正常に動作していることを確認します。

SDRサービスが有効になると、mail_logsとMessage TrackingにSDR：ログエントリが表示され始めます。

1. mail_logsには、収集されたSDRデータのスコアが含まれます。

2. スコアは、メールポリシーを決定する前に、メールフローの早い段階で決定されます。

3. 判定に対して行われるアクションは、メッセージフィルタおよびコンテンツフィルタのアクション時に発生します。

<#root>

xxx.com>

mail_logs sample including SDR verdict

```
Tue Dec 3 15:22:44 2019 Info: New SMTP ICID 5539460 interface Data 1 (10.10.10.170) address 55.1.x.y re
Tue Dec 3 15:22:44 2019 Info: ICID 5539460 ACCEPT SG Production_INBOUND match xxx1.xxx.com SBRS 2.5 cou
Tue Dec 3 15:22:44 2019 Info: ICID 5539460 TLS success protocol TLSv1.2 cipher ECDHE-RSA-AES128-GCM-SHA
Tue Dec 3 15:22:44 2019 Info: Start MID 3291517 ICID 5539460
Tue Dec 3 15:22:44 2019 Info: MID 3291517 ICID 5539460 From: <customer@xxx.com>
Tue Dec 3 15:22:44 2019 Info: MID 3291517 ICID 5539460 RID 0 To: <owner@xxx.com>
Tue Dec 3 15:22:44 2019 Info: MID 3291517 IncomingRelay(PROD_TO_BETA): Header Received found, IP 172.20
Tue Dec 3 15:22:44 2019 Info: MID 3291517 Message-ID '<mail>'
Tue Dec 3 15:22:44 2019 Info: MID 3291517 Subject "You\\'ve Been Nominated for inclusion with Who\\'s W
```

Tue Dec 3 15:22:44 2019 Info: MID 3291517 SDR: Domains for which SDR is requested: reverse DNS host: Not

Tue Dec 3 15:22:46 2019 Info: MID 3291517 SDR: Consolidated Sender Reputation: Awful, Threat Category: N

Tue Dec 3 15:22:46 2019 Info: MID 3291517 SDR: Tracker Header : 5Zrl76622ZDGPsS6cByUUXq7LTXXS3/wonoZb5cG

```
Tue Dec 3 15:22:46 2019 Info: MID 3291517 ready 10011 bytes from <owner@xxx.com>
```

```
Tue Dec 3 15:22:46 2019 Info: MID 3291517 Custom Log Entry: MF_URL_Category_all HIT
Tue Dec 3 15:22:46 2019 Info: MID 3291517 matched all recipients for per-recipient policy DEFAULT in th
Tue Dec 3 15:22:47 2019 Info: MID 3291517 interim verdict using engine: CASE spam positive
Tue Dec 3 15:22:47 2019 Info: MID 3291517 using engine: CASE spam positive
Tue Dec 3 15:22:47 2019 Info: MID 3291517 interim AV verdict using Sophos CLEAN
Tue Dec 3 15:22:47 2019 Info: MID 3291517 antivirus negative
Tue Dec 3 15:22:47 2019 Info: MID 3291517 AMP file reputation verdict : SKIPPED (no attachment in messa
Tue Dec 3 15:22:47 2019 Info: MID 3291517 using engine: GRAYMAIL negative
Tue Dec 3 15:22:47 2019 Info: MID 3291517 Custom Log Entry: SDR_Verdict_matched_Awful_Poor
Tue Dec 3 15:22:47 2019 Info: Start MID 3291519 ICID 0
```

4. 特定の判定の頻度または存在を確認するには、単純なgrepコマンドを使用します。

- >> grep "Sender Reputation: Awful" mail_logs
- >> grep "Sender Reputation: Poor" mail_logs

5. さらに、メールログの詳細は、CLIのfindeventコマンドをMID値とともに使用して取得できます。

```
xxx.com> grep "SDR: Domain Reputation.*Poor" mail_logs
Tue Dec 3 11:07:01 2019 Info: MID 3265844 SDR: Consolidated Sender Reputation: Poor, Threat Category: Sp
Tue Dec 3 12:57:28 2019 Info: MID 3277401 SDR: Consolidated Sender Reputation: Poor, Threat Category: Sp
```

```
xxx.com> grep "SDR: Domain Reputation.*Awful" mail_logs
Tue Dec 3 10:24:08 2019 Info: MID 3261075 SDR: Consolidated Sender Reputation: Awful, Threat Category: I
Tue Dec 3 15:18:27 2019 Info: MID 3291182 SDR: Consolidated Sender Reputation: Awful, Threat Category: I
```

トラブルシュート

このセクションでは、設定のトラブルシューティングに役立つ情報を紹介します。

1. SDRなし：mail_logsまたはMessage Tracking内にログが存在します。

- SDRログは、ACCEPT Mail Flow Policyを通過するメッセージに対して常に存在できます。
- このガイドの最初の手順に従って、サービスが有効になっていることを確認します。

2. SDRがタイムアウトしました：

- SDR用のCiscoクラウドサーバが開いていて、使用可能であることを確認します。
- v2.sds.cisco.com
- 非常に一般的なテストは、CLIからtelnetを使用して実行できます。

- バナーが表示されたら、基本的な到達可能性を確認できます。
    - CLI > telnet v2.sds.cisco.com 443 (これは、特定の時点のみを確認できます。)
- 他のサービスのログを確認して、インターネットベースのサービスに対する通信障害の可能性があるかどうかを判断します。
- CLI > displayalertsの順に選択して、通信障害の追加の兆候を確認します。
- 13.5より前のAsyncOSでは、SDRとURLフィルタリングはどちらもv2.sds.cisco.comを使用します。
    - URLフィルタリングCLIコマンド> websecuritydiagnosticsをチェックすると、ネットワークパスに遅延が含まれているかどうかを確認できます。
- Sender Domain Reputation Timeout Settingを確認して、値を1 ~ 10秒増やすことができるかどうかを判断します。Security Services > Domain Reputation > Edit > Sender Domain Reputation Query Timeout:2の順に移動します。

デフォルトは2秒で、最大設定は10秒です。

AsyncOSバージョン14以降の重要な更新

移行後も、ホスト名v2.sds.cisco.comは使用可能ですが、URLフィルタリングとSDRの両方に対して最適化できなくなります。

これらのホスト名とIPアドレスを、発信TCPポート443トラフィック用にファイアウォールで許可する必要があります。

ホスト名：

- serviceconfig.talos.cisco.com
- grpc.talos.cisco.com
- email-sender-ip-rep-grpc.talos.cisco.com

IPアドレス範囲：

- 146.112.62.0/24
- 146.112.63.0/24
- 146.112.255.0/24
- 146.112.59.0/24
- 2a04:e4c7:ffff::/48
- 2a04:e4c7:fffe::/48

これらは、IPレピュテーション、URLレピュテーション、およびカテゴリを取得し、サービスロ

グの詳細を送信するために使用されるCisco Talos Intelligence Servicesエンドポイントです。

関連情報

- ESAユーザガイド
- ESAリリースノート
- ESA CLIリファレンスガイド
- テクニカル サポートとドキュメント – Cisco Systems

翻訳について
シスコは世界中のユーザにそれぞれの言語でサポート コンテンツを提供するために、機械と人による翻訳を組み合わせて、本ドキュメントを翻訳しています。ただし、最高度の機械翻訳であっても、専門家による翻訳のような正確性は確保されません。シスコは、これら翻訳の正確性について法的責任を負いません。原典である英語版（リンクからアクセス可能）もあわせて参照することを推奨します。