SDR ändert sich in Ausnahmeliste für die Absenderdomäne für AsyncOS15.0 für Cisco Secure Email Gateway

Inhalt

[Einleitung](#)
[Voraussetzungen](#)
[Anforderungen](#)
[Verwendete Komponenten](#)
[Überblick](#)
[Konfigurieren](#)
[Überprüfung](#)
[Fehlerbehebung](#)
[Zugehörige Informationen](#)

Einleitung

In diesem Dokument wird eine wichtige Funktion zur Verbesserung der SDR-Einstellungsoption (Sender Domain Reputation) für Cisco Secure Email Gateway vorgestellt und erläutert. (SEG)

Beitrag von Chris Arellano, Cisco TAC Engineer.

Voraussetzungen

AsyncOS 15.0 und höher für Cisco Secure Email Gateway (SEG)

Allgemeine Kenntnisse über die SZR-Funktion.

Anforderungen

Aktivieren Sie den Absender-Domänenreputationsdienst, und erstellen Sie eine Adressliste mit der Option Nur Domäne.

Verwendete Komponenten

Absender-Domänenreputation.

Adressliste nur für Domäne.

Die Informationen in diesem Dokument beziehen sich auf Geräte in einer speziell eingerichteten Testumgebung. Alle Geräte, die in diesem Dokument benutzt wurden, begannen mit einer gelöschten (Nichterfüllungs) Konfiguration. Wenn Ihr Netzwerk in Betrieb ist, stellen Sie sicher, dass Sie die möglichen Auswirkungen aller Befehle kennen.

Überblick

Sender Domain Reputation für SEG ist ein Cloud-Service, der mehrere Senderwerte erfasst und daraus

Verdicts und Optionen ableitet, um entsprechende Maßnahmen zu ergreifen. Mit SDR können Einstellungen vertrauenswürdige Domänen mithilfe einer Adressliste umgehen, die auf die Domänenausnahmeliste angewendet wird.

Die SDR-Domänenausnahmeliste vor SEG 15.0 verfügte über 2 Optionen:

- Enabled = Übereinstimmung mit der Umschlag-From-Domäne zum Umgehen der SDR-Aktion
- Disabled = Match only if all of the following are present: Envelope-from + Friendly From + Reply-To + SPF + DKIM + DMARC .

Die neue 15.0-Änderung: Die Domänenausnahmeliste für SEG 15.0 und neuere Optionen:

- Enabled = Übereinstimmung mit der Umschlag-From-Domäne zum Umgehen der SDR-Aktion
- Disabled = Übereinstimmung, wenn die Domäne in einem der folgenden Werte vorhanden ist:
  - HALLO
  - RDNS
  - Umschlag von
  - Von
  - Antwort an

Konfigurieren

Im Mittelpunkt stehen nur die neuen Optionen der Domänenausnahmeliste. Die vollständige SDR-Einrichtung und -Konfiguration finden Sie im Benutzerhandbuch.

Navigieren Sie in der WebUI zu **Security Services** > **Domain Reputation**.

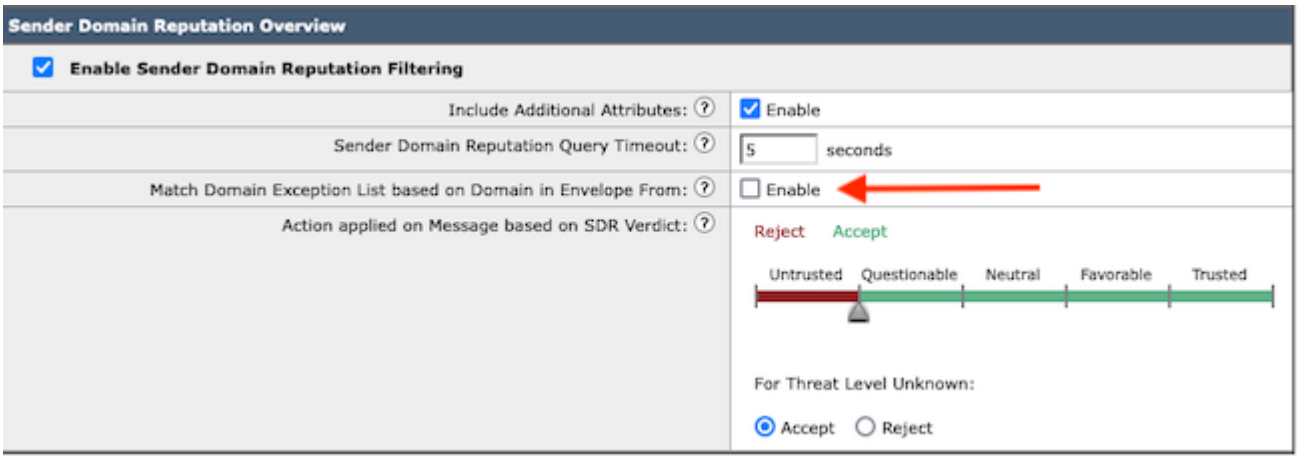
Die Option **Domänenausnahmeliste anhand des Domänennamenteils des Umschlags von zuordnen** ist standardmäßig aktiviert.

Wenn das zugehörige Informationssymbol **?** ausgewählt ist, wird die neue Option angezeigt.

Deaktivieren Sie diese Option, wenn Sie SDR überspringen möchten. Überprüfen Sie, ob Domänen in den Headern 'HELO:', 'RDNS:', 'Envelope From:', 'From:' und 'Reply-To:' der Nachricht mit den Domänen übereinstimmen, die in der Domänenausnahmeliste konfiguriert wurden.

> **Hinweis**: Standardmäßig werden SDR-Prüfungen nur basierend auf der Domäne im Header "Umschlag von:" übersprungen.

Wählen Sie **Globale Einstellungen bearbeiten**, um die Kontrollkästchen zu entfernen, wie in der Abbildung dargestellt:



Die Domänenausnahmeliste selbst ist eine Adressliste, die Domänennamen enthält.

Überprüfung

Um die korrekte Funktion mit der neuen Disable-Funktion zu überprüfen, benötigen Sie eine Testnachricht, die mit einem passenden Domänenwert in einem der 5 Header-Werte an die SEG gesendet wird.

Ein Beispielprotokoll, das eine Ausnahme in der globalen Ausnahmeliste angibt und in einer Mail Flow Policy abgeglichen wird, wird in der Anfangsphase in mail_logs angezeigt:

- Info: MID 14 SDR: Die MID 14 mit dem Domänennamen "**test1.com**" stimmt mit der **globalen** Domänenausnahmeliste "**SDR-TEST-1**" überein.

Ein Beispielprotokoll, das eine Ausnahme angibt, enthält sowohl den Domänen- als auch den Ausnahmelistennamen.

- Info: Die MID 16 mit dem Domänennamen "**test3.com**" stimmt mit der im **Filter** konfigurierten Domänenausnahmeliste "**SDR-TEST-3**" überein.

Fehlerbehebung

Treten Fragen zur Richtigkeit eines ausgewählten Message-Verdicts auf, werden die folgenden Werte dokumentiert und mit der Message-Tracking verglichen.

- Dokumentieren Sie die globalen **Domänenreputations-Einstellungen** > **Sicherheitseinstellungen** > **Domänenreputation**.
- Überprüfen Sie die zugeordnete Adressliste, die in den globalen Domänenreputations-Einstellungen konfiguriert wurde.
- Überprüfen Sie, ob die passende Mail Flow Policy verwendet wurde, basierend auf der Nachrichtenverfolgung.
- Überprüfen und notieren Sie Details zu Nachrichtenfiltern oder Inhaltsfiltern, für die Domänenausnahmelisten konfiguriert sind.

Erfassen Sie die Nachrichtenverfolgung, E-Mail-Protokolle und die ursprünglichen E-Mail-Header.

- Wenn die globale Ausnahme in einer Nachricht übereinstimmt, gibt es keine Protokolleinträge für die Domänenreputation, sondern nur eine Zeile, die die übereinstimmende Domäne angibt.
- Wenn die globale Ausnahmeliste in einer Nachricht nicht übereinstimmt, gibt es Protokolleinträge für die Domänenreputation, mit denen Werte verglichen werden sollen.
    - Info: MID 16 SDR: Domains for which SDR is requested: **reverse DNS host:** Not Present,

helo: testl.com, **env-from**: test2.com, **header-from**: te
st3.com, **Antwort an**: test5.com

- Die E-Mail-Header selbst enthalten alle 5 Werte einer einzelnen E-Mail, um sie mit den Einstellungen zu vergleichen.

Sobald alle Daten gesammelt wurden, überprüfen Sie, ob Übereinstimmungen vorliegen oder keine Übereinstimmungen vorliegen, um die ordnungsgemäße Funktion zu ermitteln.

Zugehörige Informationen

- Email Security - Einrichtungsleitfaden
- Cisco Secure Email Gateway Launch-Website für Support-Leitfäden

Informationen zu dieser Übersetzung

Cisco hat dieses Dokument maschinell übersetzen und von einem menschlichen Übersetzer editieren und korrigieren lassen, um unseren Benutzern auf der ganzen Welt Support-Inhalte in ihrer eigenen Sprache zu bieten. Bitte beachten Sie, dass selbst die beste maschinelle Übersetzung nicht so genau ist wie eine von einem professionellen Übersetzer angefertigte. Cisco Systems, Inc. übernimmt keine Haftung für die Richtigkeit dieser Übersetzungen und empfiehlt, immer das englische Originaldokument (siehe bereitgestellter Link) heranzuziehen.