CSC 6.x: Konfigurationsbeispiel für E-Mail-Reputation

Inhalt

Einführung

Dieses Dokument enthält eine Beispielkonfiguration zur Konfiguration der E-Mail-Reputation im Cisco Content Security and Control (CSC) Security Services Module (SSM).

Voraussetzungen

Anforderungen

Sie benötigen eine Security Plus-Lizenz, um diese Funktion nutzen zu können.

Verwendete Komponenten

Die Informationen in diesem Dokument basieren auf dem Cisco Content Security and Control SSM mit Softwareversion 6.3.

Die Informationen in diesem Dokument wurden von den Geräten in einer bestimmten Laborumgebung erstellt. Alle in diesem Dokument verwendeten Geräte haben mit einer leeren (Standard-)Konfiguration begonnen. Wenn Ihr Netzwerk in Betrieb ist, stellen Sie sicher, dass Sie die potenziellen Auswirkungen eines Befehls verstehen.

Konventionen

Weitere Informationen zu Dokumentkonventionen finden Sie in den Cisco Technical Tips Conventions (Technische Tipps zu Konventionen von Cisco).

Hintergrundinformationen

Die E-Mail-Reputation ist eine Technologie, die die Spam-E-Mails reduziert. Durch die Aktivierung dieser Funktion überprüft CSC SSM, ob es sich bei dem Urheber der E-Mail um eine in der Blacklist angegebene Adresse handelt. Es unterhält eine Liste von Datenbanken, die alle IP-Adressen enthalten, die die Spam-Nachrichten ausgeben. Wenn festgestellt wird, dass eine E-Mail einen Urheber von dieser Liste hat, wird diese E-Mail als Spam betrachtet und verworfen.

Die Service-Level, die von dieser E-Mail-Reputationstechnologie (ERS) angeboten werden, sind im Wesentlichen zwei Typen. Diese Dienste basieren hauptsächlich auf der Authentizität der Quell-IP-Adressen.

- ERS Standard - Enthält die bekannten Quellen von Spam
- ERS Advanced: Enthält die bekannten Quellen und die vermuteten Quellen.

Wenn eine IP-Adresse der ERS Standard-Datenbank hinzugefügt wird, wird sie als Spam-Quelle bezeichnet. In seltenen Fällen beobachten Sie eine IP-Adresse, die aus dieser Liste entfernt wurde. ERS Standard enthält die Liste der IP-Adressen, die konsistent Spam generieren.

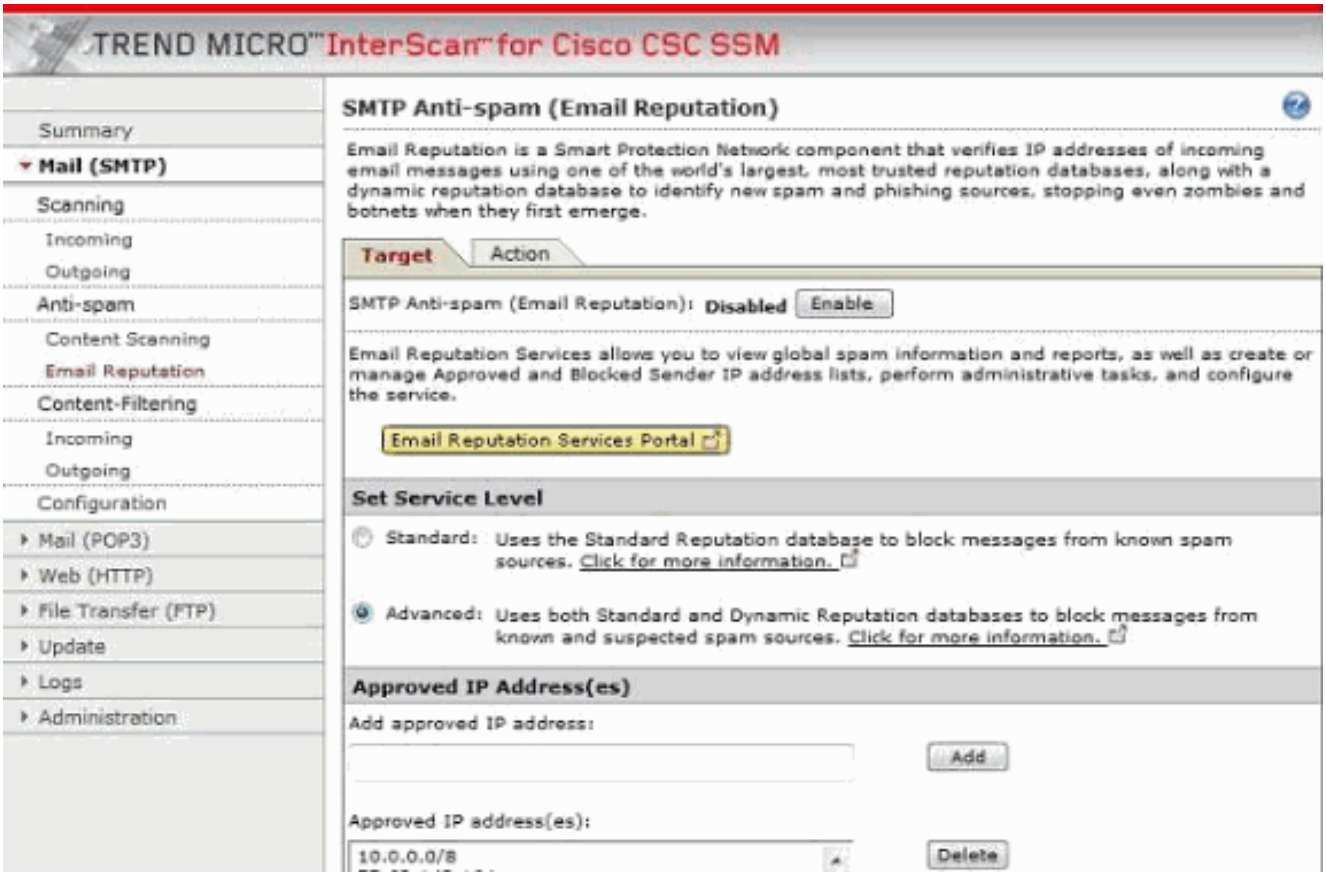
ERS Advanced enthält eine Liste von IP-Adressen, die entfernt werden sollen, wenn festgestellt wird, dass sie keinen Spam mehr erzeugen. Ein gehackter Mail-Server kann beispielsweise bei einer Gefährdung in dieser Datenbank aufgelistet werden. Wenn die Wiederherstellung der Normalität abgeschlossen ist, wird sie aus dieser Datenbank entfernt.

Konfigurieren

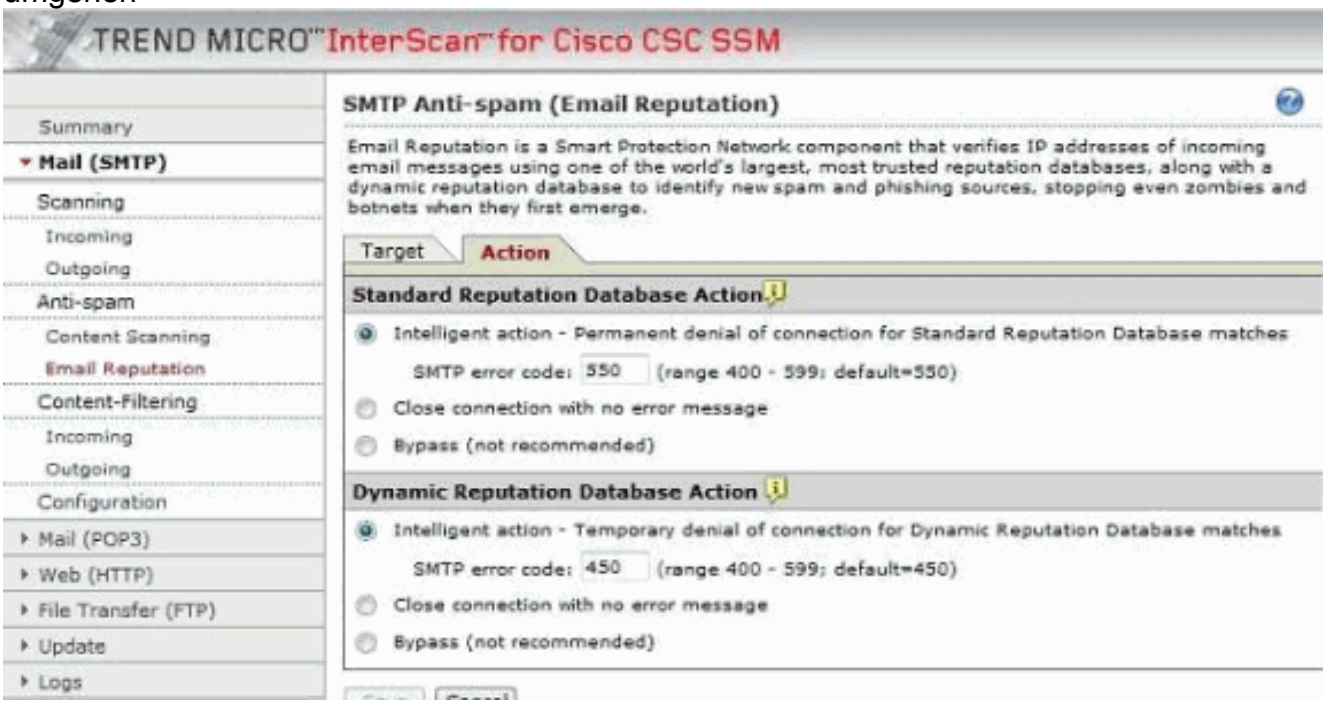
In diesem Abschnitt erhalten Sie Informationen zum Konfigurieren der in diesem Dokument beschriebenen Funktionen.

Hinweis: Verwenden Sie das Command Lookup Tool (nur registrierte Kunden), um weitere Informationen zu den in diesem Abschnitt verwendeten Befehlen zu erhalten.

1. Wählen Sie **Mail (SMTP) > Anti-Spam > Email Reputation aus**. Ein neues Fenster wird geöffnet.
2. Klicken Sie auf der Registerkarte Ziel auf **Aktivieren**, um diese E-Mail-Reputationsfunktion zu aktivieren.
3. Wählen Sie **Erweitert** als Servicelevel aus.
4. Geben Sie im Feld Approved IP Addresses (Genehmigte IP-Adressen) den Bereich der IP-Adressen an, die nicht gescannt werden
   sollen.



5. Geben Sie auf der Registerkarte Aktion die Art der Aktion an, die auf Ihrer Sicherheitsrichtlinie basiert. Diese drei Aktionen sind verfügbar:Verbindung mit Fehlermeldung schließenVerbindung schließen ohne FehlermeldungVerbindung umgehen



Überprüfen

Für diese Konfiguration ist derzeit kein Überprüfungsverfahren verfügbar.

Fehlerbehebung

Dieser Abschnitt enthält Informationen zur Fehlerbehebung in Ihrer Konfiguration.

E-Mails von einigen Domänen konnten nicht empfangen werden

Problem:

Das Problem ist, dass die E-Mails nicht von bestimmten Domänen aus empfangen werden können. Es scheint, dass das CSC-Modul die E-Mails blockiert. Wenn Sie das Modul umgehen, funktioniert alles in Ordnung. Diese Fehlermeldung wird angezeigt: `2012/06 14:33:00 GMT+00:00 NRS 174.37.94.181 RBL-Fail QIL-NA RejectWithErrorCode-550 NA 0 NA 0 NA NA 0 NA NA NA NA`

Lösung:

Um dieses Problem zu beheben, konfigurieren Sie die E-Mail-Reputationsfunktion ordnungsgemäß.

Zugehörige Informationen

- Unterstützung für Cisco ASA Content Security and Control (CSC) Security Services Module
- Technischer Support und Dokumentation - Cisco Systems