Best Practice-Leitfaden für Anti-Spam-, Anti-Virus-, Graymail- und Outbreak-Filter

Inhalt

Übersicht

Die überwiegende Mehrheit der Bedrohungen, Angriffe und Ärgernisse, mit denen Unternehmen per E-Mail konfrontiert sind, sind Spam, Malware und kombinierte Angriffe. Die E-Mail Security Appliance (ESA) von Cisco umfasst verschiedene Technologien und Funktionen, um diese Bedrohungen am Gateway abzuwehren, bevor sie in das Unternehmen eindringen. In diesem Dokument werden Best Practice-Ansätze zur Konfiguration von Anti-Spam-, Anti-Virus-, Graymail- und Outbreak-Filtern sowohl für den ein- als auch den ausgehenden E-Mail-Fluss beschrieben.

Anti-Spam

Der Anti-Spam-Schutz bietet Schutz vor einer Vielzahl bekannter Bedrohungen, darunter Spam, Phishing- und Zombie-Angriffe sowie schwer zu erkennende, kurzlebige E-Mail-Bedrohungen wie "419"-Scams. Darüber hinaus erkennt der Anti-Spam-Schutz neue und neue kombinierte Bedrohungen wie Spam-Angriffe, die schädliche Inhalte über eine Download-URL oder eine ausführbare Datei verbreiten.

Cisco Email Security bietet die folgenden Anti-Spam-Lösungen:

- IronPort Anti-Spam-Filterung (IPAS)

- Cisco Intelligent Multi-Scan Filtering (IMS)

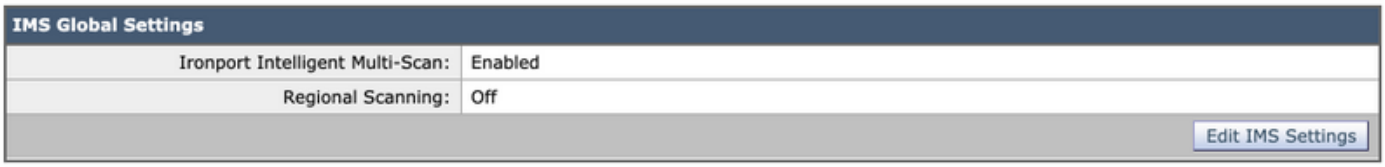
Sie können beide Lösungen auf Ihrer ESA lizenzieren und aktivieren, jedoch nur eine in einer bestimmten E-Mail-Richtlinie. Für die Zwecke dieses Dokuments mit bewährten Verfahren wird die IMS-Funktion verwendet.

Feature-Schlüssel überprüfen

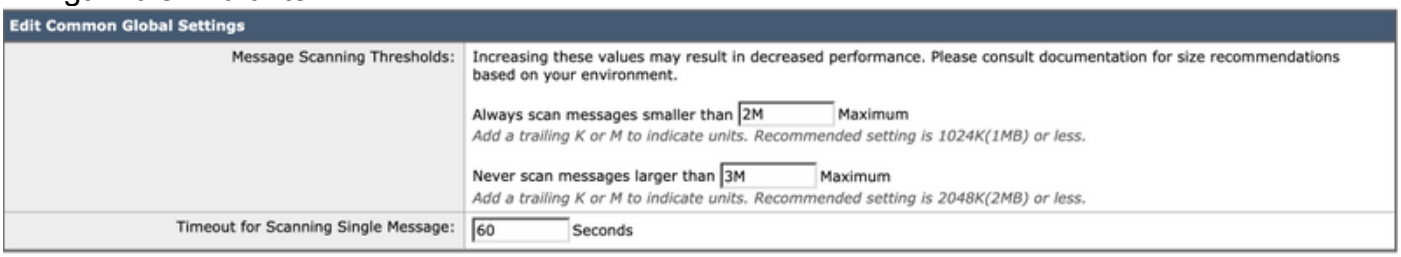
- Navigieren Sie auf der ESA zu **Systemverwaltung > Feature Keys (Funktionstasten).**
- Suchen Sie nach der Lizenz für intelligentes Mehrfach-Scannen, und stellen Sie sicher, dass diese aktiviert ist.

Globale Aktivierung von IMS (Intelligent Multi Scan)

- Ein die ESA, navigieren an **Sicherheit Services> IMS und Graymail**
- Klicken die **Aktivieren**auf **globalen IMS-Einstellungen**:



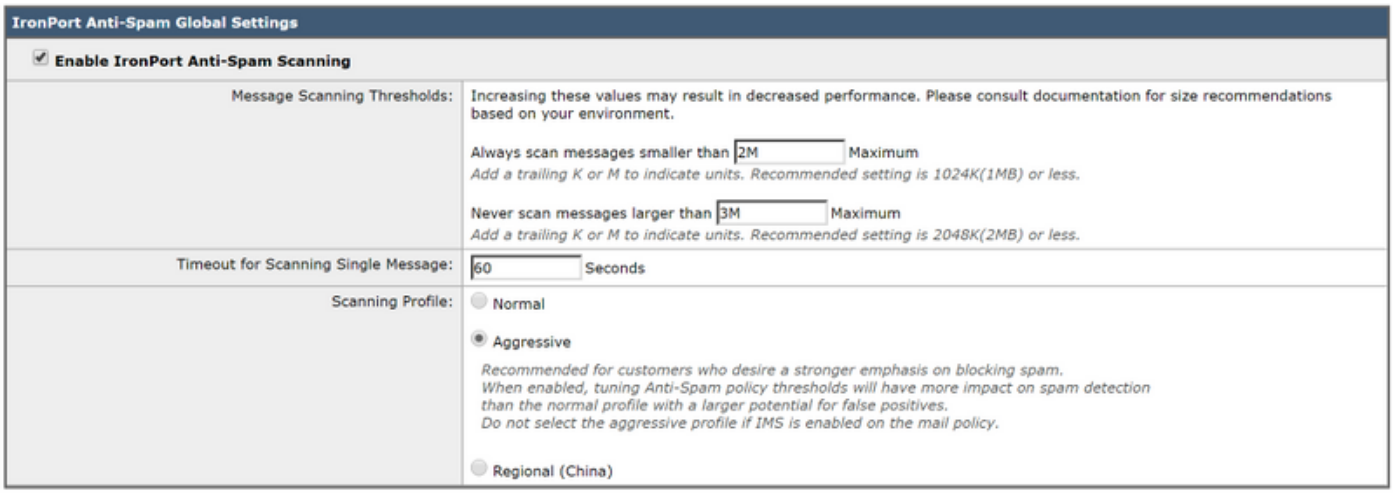
- Suchen Sie nach **allgemeinen globalen Einstellungen** und Klicken Sie auf **Globale Einstellungen bearbeiten.**
- Hier Sie können konfigurieren mehrere Einstellungen. Die empfohlen Einstellungen sind gezei gt in die Bild unten:



- Klicken Sie auf **Senden**und **Bestätigen Sie Ihre Änderungen.**

Wenn Sie kein IMS-Lizenzabonnement besitzen:

- Navigieren Sie zu **Sicherheitsdienste > IronPort Anti-Spam.**
- Klicken die **Aktivieren**auf **IronPort Anti-Spam - Übersicht**
- Klicken Sie auf **Globale Einstellungen bearbeiten.**
- Hier Sie können konfigurieren mehrere Einstellungen. Die empfohlen Einstellungen sind gezei gt in die Bild unten:

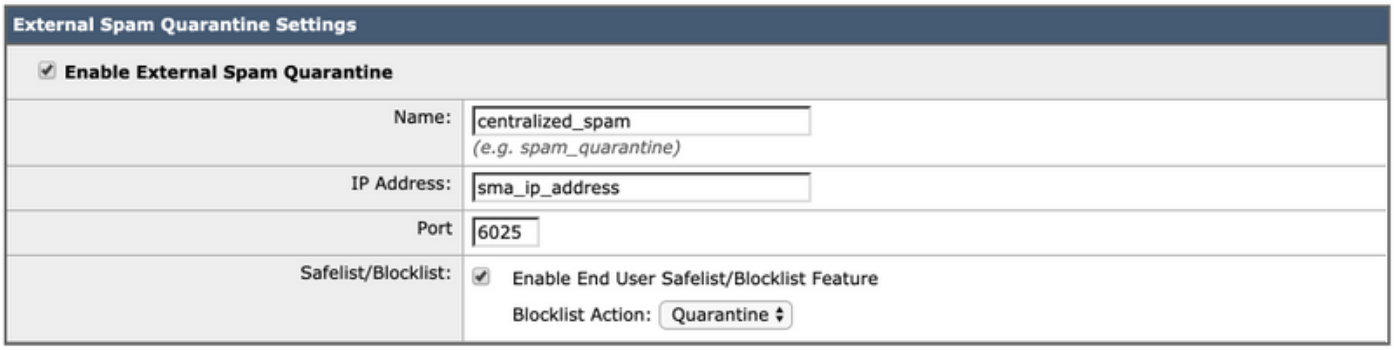


- Cisco empfiehlt, **Aggressive** Scanning Profile für einen Kunden auszuwählen, der eine starke Betonung auf der Blockierung von Spam legen möchte.
- Klicken Sie auf **Senden**und **Bestätigen Sie Ihre Änderungen**

Zentrale Spam-Quarantäne aktivieren

Da Anti-Spam die Option hat, in Quarantäne zu verschicken, ist es wichtig, sicherzustellen, dass die Spam-Quarantäne eingerichtet ist:

- Navigieren Sie zu **Sicherheitsdienste > Spam Quarantine.**
- Klickening die **Konfigurieren**Schaltfläche werden nehmen Sie an die Follschuldig Seite.
- Hier Sie können aktivieren die Quarantäne von Überprüfung die **aktivieren**Box und Punkte Qu arantäne an sein zentralisiert auf SicherheitManagement AAppliance (SMA) vonFüllung in SMA**Name**und **IP Adresse.** Die empfohlen Einstellungen sind gezeigt unt en:



- Klicken Sie auf **Senden**und **Bestätigen Sie Ihre Änderungen**

Weitere Informationen zum Einrichten und Zentralisieren von Quarantänen finden Sie im Dokument Best Practices:
[Best Practices für die Einrichtung von zentralisierten Richtlinien, Virus- und Outbreak-Quarantänen und die Migration von der ESA zur SMA]

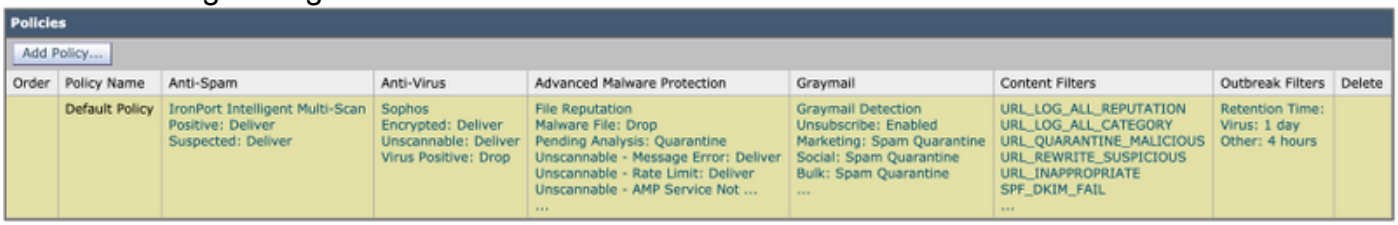
Anti-Spam in-Richtlinien konfigurieren

Einmal Intelligent Multi - Scannen hat wurden konfiguriert global , Sie können Jetzt anwenden Intelligent Multi - Scannen an Post Richtlinien:

- Navigieren Sie zu **Mail-Policys > Mail-Policys für eingehende E-Mails.**
- Die Richtlinien für eingehende E-Mails verwenden standardmäßig IronPort Anti-Spam-

Einstellungen.

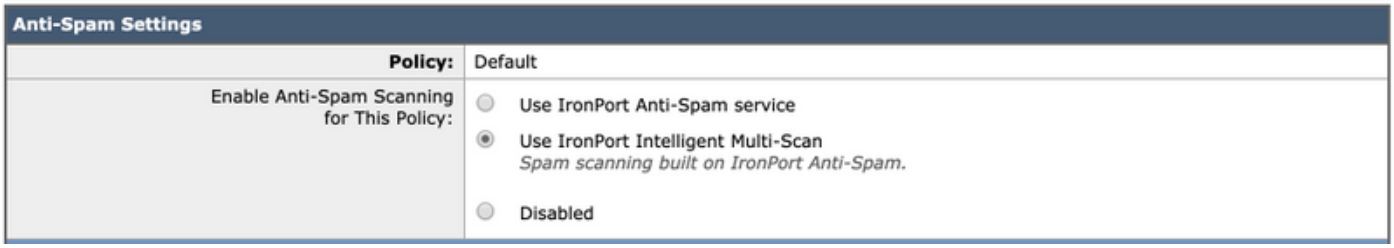
- Durch Klicken auf den blauen Link unter **Anti-Spam** können für diese Policy benutzerdefinierte Anti-Spam-Einstellungen verwendet werden.
- Unten sehen Sie ein Beispiel, das die Standardrichtlinie mit benutzerdefinierten Anti-Spam-Einstellungen zeigt:



Passen Sie die Anti-Spam-Einstellungen für eine Richtlinie für eingehende E-Mails an, indem Sie auf den blauen Link unter **Anti-Spam** für die Richtlinie klicken, die Sie anpassen möchten.

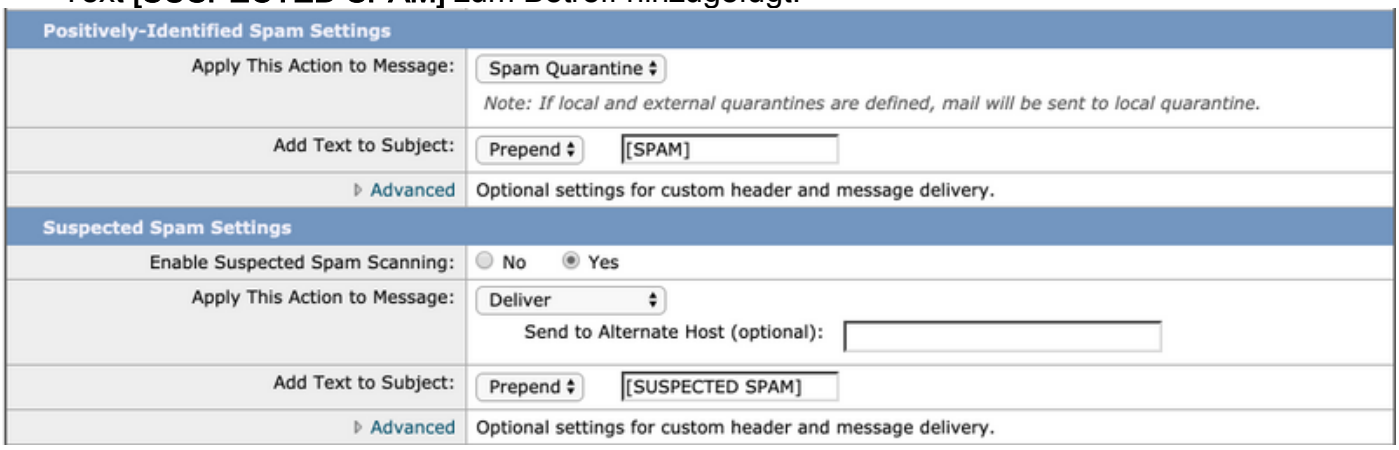
Hier Sie können auswählen die Anti-
SPause Scannen Option Sie Wunsch an aktivieren für diese Policy.

- für die Zweck von diese beste ÜbungEis Dokument, klicken die Funk Schaltfläche Nächste an Verwenden **Intelligentes Mehrfach-Scannen:**

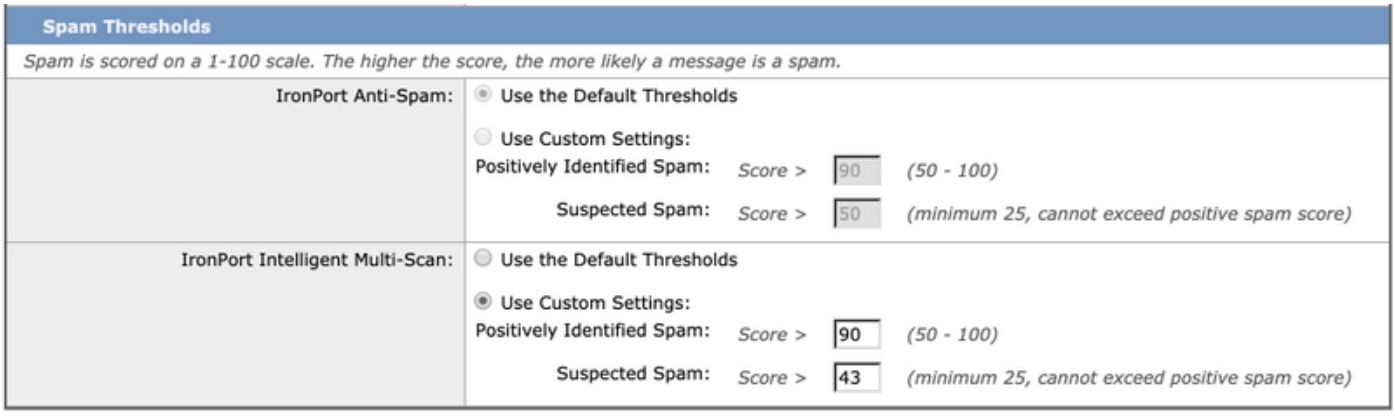


Die nächsten beiden Abschnitte enthalten **Einstellungen für Spam-verdächtig** und **Einstellungen für Spam-verdächtig:**

- Die empfohlene Best Practice besteht darin, die **Quarantäneaktion** für die Einstellung **positiv identifizierter Spam** mit dem vorangestellten Text **[SPAM]** zu konfigurieren, der dem Betreff und dem Betreff hinzugefügt wurde.
- Anwenden auf "**Zustellen**" als Aktion für **verdächtige Spam-Einstellungen** mit vorangestelltem Text **[SUSPECTED SPAM]** zum Betreff hinzugefügt:



- Sie können die **Spam-Schwellenwerteinstellung** ändern, und es wird empfohlen, die Punktzahl für **positiv identifizierte Spam** auf **90** und die Punktzahl für **Spam-verdächtig** auf **43** anzupassen:



- Klicken Sie auf **Sendenund** **Bestätigen Sie Ihre Änderungen**

Antivirus

Der Virenschutz wird über zwei Engines von Drittanbietern bereitgestellt - Sophos und McAfee. Diese Engines filtern alle bekannten schädlichen Bedrohungen, löschen sie, reinigen oder unter Quarantäne stellen.

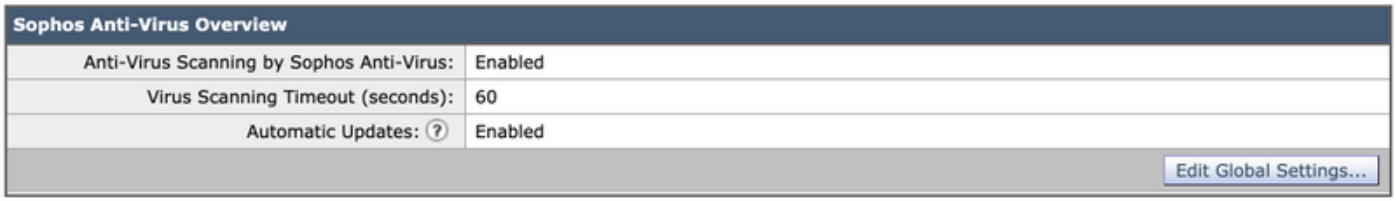
Überprüfen der Funktionstasten

So überprüfen Sie, ob beide Feature-Schlüssel aktiviert und aktiv sind:

- Gehen Sie zu **Systemverwaltung > Feature Keys.**
- Stellen Sie sicher, dass **Sophos Anti-Virus-** und **McAfee-**Lizenzen aktiv sind.

Anti-Virus-Scanning aktivieren

- Navigieren an **Sicherheit Services> Anti-Virus - Sophos**
- Klicken die **Aktivieren**-Taste.
- Vergewissern Sie sich, dass **Automatische Aktualisierung aktiviert** ist und die Aktualisierung der Sophos Anti-Virus-Dateien einwandfrei funktioniert. Klicken Sie ggf. auf **Jetzt aktualisieren**, um die Dateiaktualisierung sofort zu starten:



- Klicken Sie auf **Sendenund** **Bestätigen Sie Ihre Änderungen.**

Wenn die McAfee-Lizenz ebenfalls aktiv ist, navigieren Sie zu an **Sicherheit Services> Anti-Virus - McAfee**

- Klicken die **Aktivieren**-Taste.

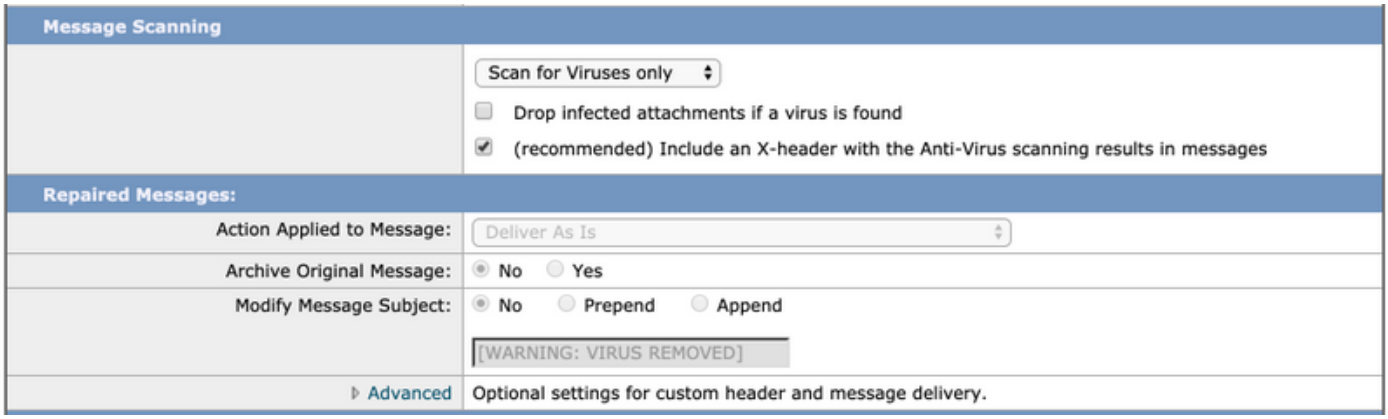
- Vergewissern Sie sich, dass **Automatische Aktualisierung aktiviert** ist und die McAfee Anti-Virus-Dateiaktualisierung einwandfrei funktioniert. Klicken Sie ggf. auf **Jetzt aktualisieren**, um die Dateiaktualisierung sofort zu starten.
- Klicken Sie auf **Sendenund** **Bestätigen Sie Ihre Änderungen**

Anti-Virus in Mail-Richtlinien konfigurieren

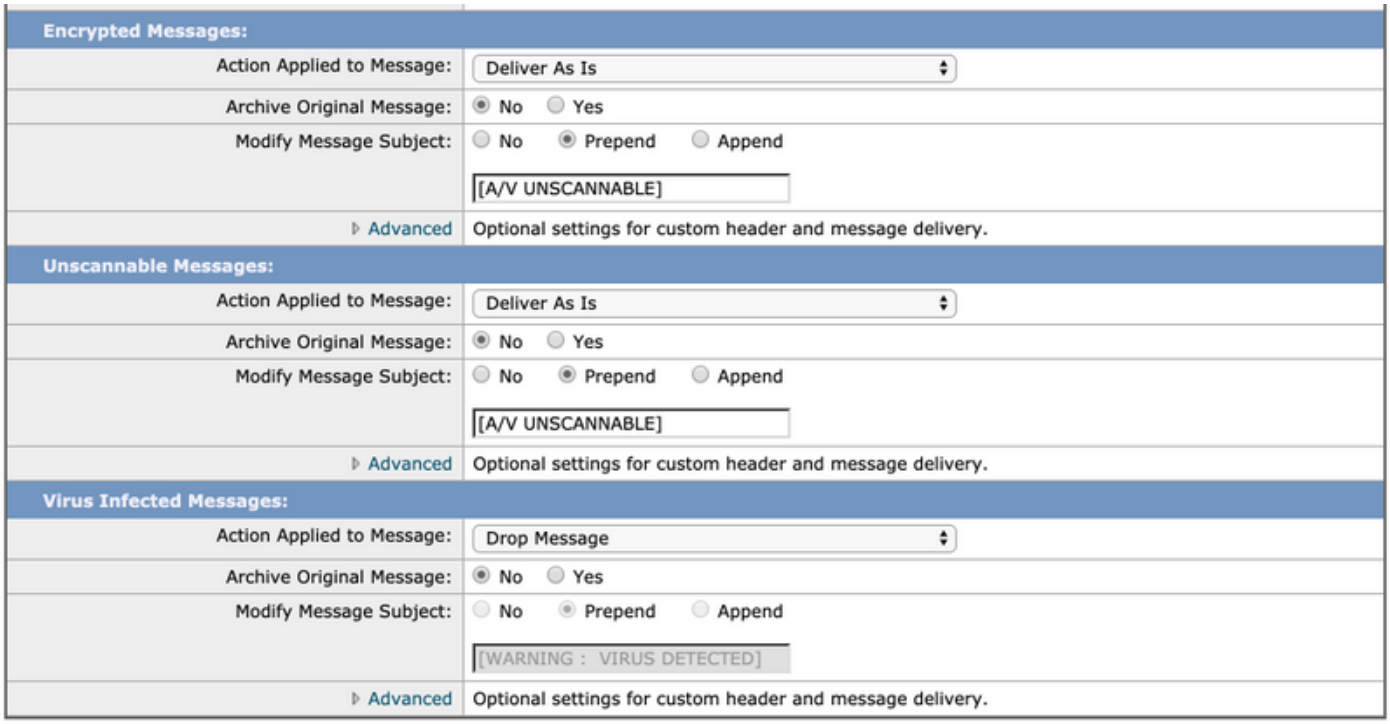
Für Richtlinien für eingehende E-Mails wird Folgendes empfohlen:

- Navigieren Sie zu **Mail-Policys > Mail-Policys für eingehende E-Mails.**
- Passen Sie die **Anti-Virus-**Einstellungen für eine Richtlinie für eingehende E-Mails an, indem Sie auf den blauen Link unter Anti-Virus für die Richtlinie klicken, die Sie anpassen möchten.
- Hier Sie können auswählen die Anti-
  Virus Scannen Option Sie Wunsch an aktivieren für diese Policy.
- für die Zweck von dieseest pRackeEis -Dokument wählen Sie **McAfee** und **Sophos Anti-Virus aus**:

- Wir versuchen nicht, eine Datei zu reparieren. Die Nachrichtenprüfung besteht also **nur** nach **Viren suchen**:



- Die empfohlene Aktion für **verschlüsselte** und **nicht scanbare Nachrichten** ist **wie besehen** mit einer modifizierten Betreffzeile bereitzustellen.
- Die empfohlene Richtlinie für Antivirus ist **Drop** all **virus-infizierte Nachrichten**, wie in der Abbildung unten gezeigt:



- Klicken Sie auf **Senden**und **Bestätigen Sie Ihre Änderungen**

Eine ähnliche Richtlinie wird für Richtlinien für ausgehende E-Mails empfohlen. Es wird jedoch nicht empfohlen, die Betreffzeile für ausgehende E-Mails zu ändern.

Graymail

Die Graymail-Management-Lösung der E-Mail Security Appliance besteht aus zwei Komponenten: eine integrierte Graymail Scan-Engine und einen Cloud-basierten Unsubscribe Service. Die Graymail-Management-Lösung ermöglicht Unternehmen, mithilfe der integrierten Graymail-Engine Gramail-Nachrichten zu identifizieren und entsprechende Richtlinienkontrollen anzuwenden. Endbenutzer können so mithilfe des Unsubscribe-Dienstes auf einfache Weise unerwünschte Nachrichten abbestellen.

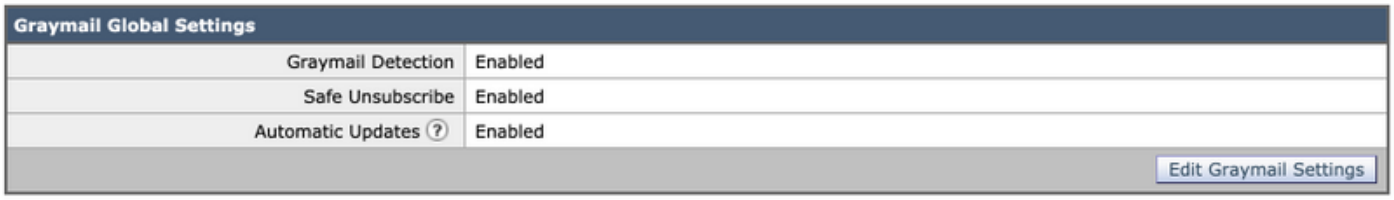
Graymail-Kategorien umfassen Marketing-E-Mails, E-Mails in sozialen Netzwerken und E-Mails in großen Mengen. Zu den erweiterten Optionen gehören das Hinzufügen eines benutzerdefinierten Headers, das Senden an einen alternativen Host und das Archivieren der Nachricht. Für diese Best Practice aktivieren wir Graymail's Safe Unsubscribe-Funktion für die Standard-Mail-Richtlinie.

Feature-Schlüssel überprüfen

- Navigieren Sie auf der ESA zu **Systemverwaltung > Feature Keys (Funktionstasten).**
- Suchen Sie nach **Graymail Safe Unsubscription** und stellen Sie sicher, dass es aktiviert ist.

Aktivieren von Graymail- und Safe Unsubscribe-Diensten

- Ein die ESA, navigieren an **Sicherheit Services> IMS und Graymail**
- Klicken die **Graymail-Einstellungen bearbeiten**Schaltfläche **"Globale Graymail-Einstellungen"**
- Wählen Sie alle Optionen aus: **Graymail-Erkennung aktivieren**, **Abgesichertes Abmelden aktivieren** und **Automatische Aktualisierungen aktivieren**:



- Klicken Sie auf **Sendenund** **Bestätigen Sie Ihre Änderungen**

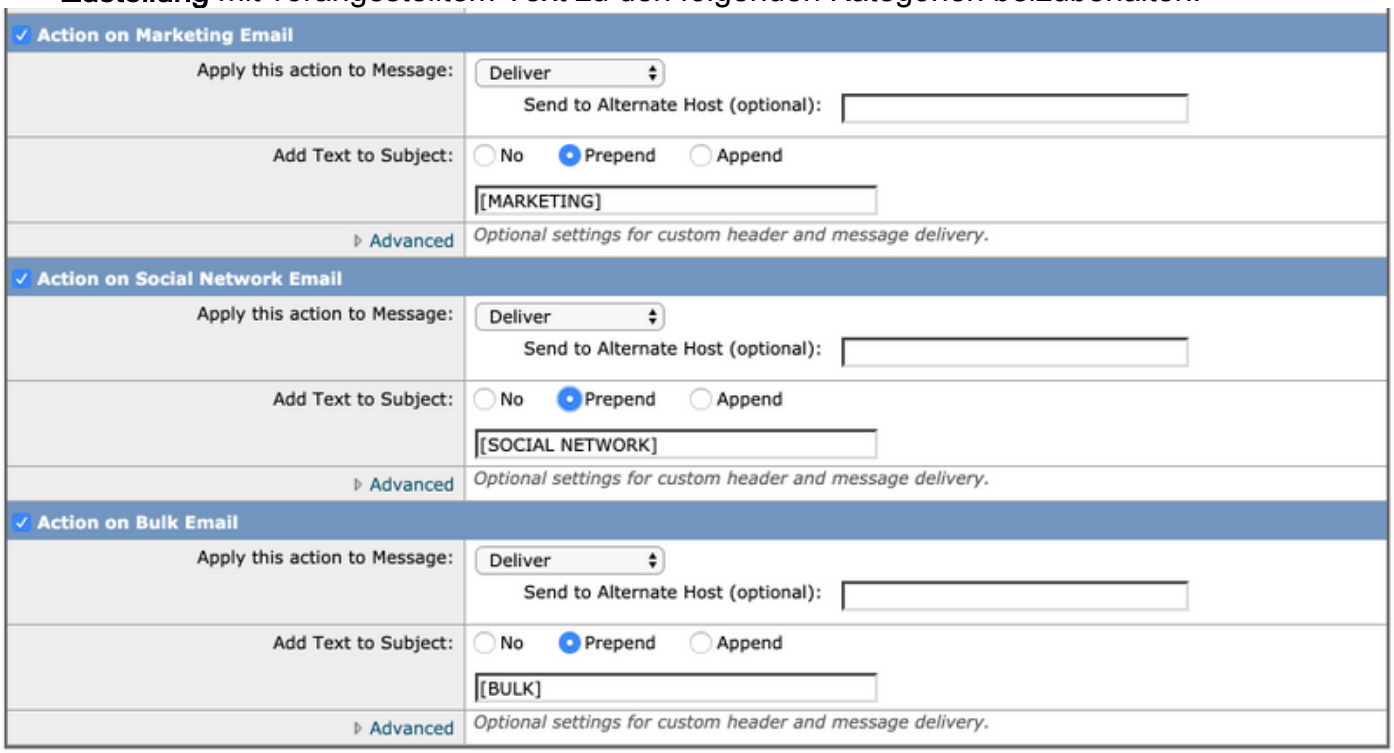
Konfigurieren von Graymail und Safe Unsubscribe in Richtlinien

Einmal Graymail und Abbestellen hat wurden konfiguriert global , Sie können Jetzt Diese Services anwenden an Post Richtlinien.

- Navigieren Sie zu **Mail-Policys > Mail-Policys für eingehende E-Mails.**
- Wenn Sie unter **Graymail** auf den blauen Link klicken, können für diese Richtlinie benutzerdefinierte Graymail-Einstellungen verwendet werden.
- Hier Sie können auswählen GraymailOptionen Sie Wunsch an aktivieren für diese Policy.
- für die Zweck von diese Beste pRackeEis Dokument, klicken die Funk Schaltfläche Nächste So **aktivieren Sie die Graymail-Erkennung für diese Richtlinie** und **aktivieren Sie Graymail Unsubscribing für diese Richtlinie**:

Die nächsten drei Abschnitte enthalten **Action on Marketing Email Settings**, **Action on Social Network Email Settings** and **Action on Bulk Email Settings**.

- Die empfohlene Best Practice besteht darin, alle diese Funktionen zu aktivieren und als **Zustellung** mit vorangestelltem Text zu den folgenden Kategorien beizubehalten:



- Klicken Sie auf **Senden**und **Bestätigen Sie Ihre Änderungen**

Für die Richtlinie für ausgehende E-Mails sollte **Graymail** im **deaktivierten** Zustand bleiben.

Outbreak-Filter

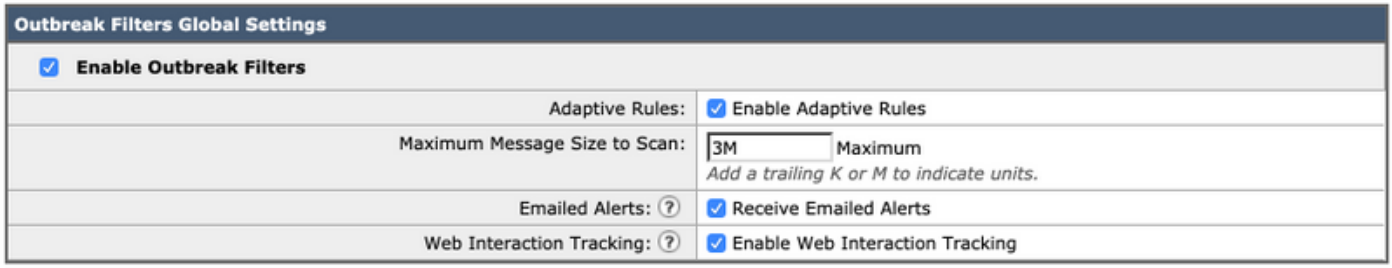
Outbreak-Filter kombinieren Auslöser in der Anti-Spam-Engine, URL-Scanning- und Erkennungstechnologien und mehr, um Elemente korrekt zu kennzeichnen, die nicht in die tatsächliche Spam-Kategorie fallen - z. B. Phishing-E-Mails und Spam-E-Mails, und behandeln diese entsprechend mit Benutzerbenachrichtigungen oder Quarantäne.

Feature-Schlüssel überprüfen

- Navigieren Sie auf der ESA zu **Systemverwaltung > Feature Keys (Funktionstasten).**
- Suchen Sie nach **Outbreak-Filtern**, und stellen Sie sicher, dass diese aktiv ist.

Outbreak-Filter-Service aktivieren

- Ein die ESA, navigieren an **Sicherheit Services> Outbreak-Filter**
- Klicken die **Aktivieren**unter **Übersicht über Outbreak-Filter**
- Hier Sie können konfigurieren mehrere Einstellungen. Die empfohlen Einstellungen sind gezei gt in die Bild unten:

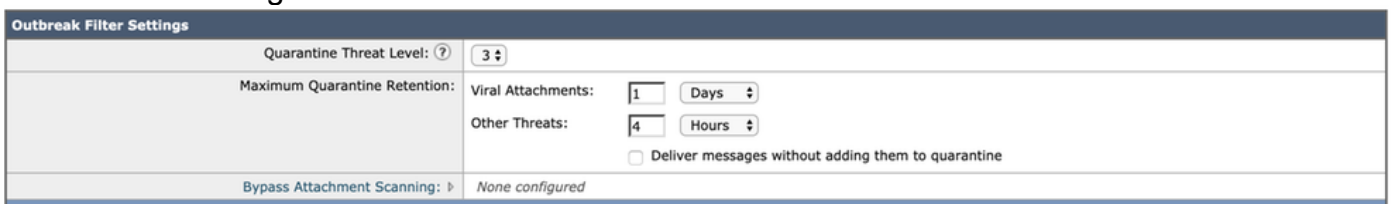


- Klicken Sie auf **Senden**und **Bestätigen Sie Ihre Änderungen.**

Konfigurieren von Outbreak-Filtern in Richtlinien

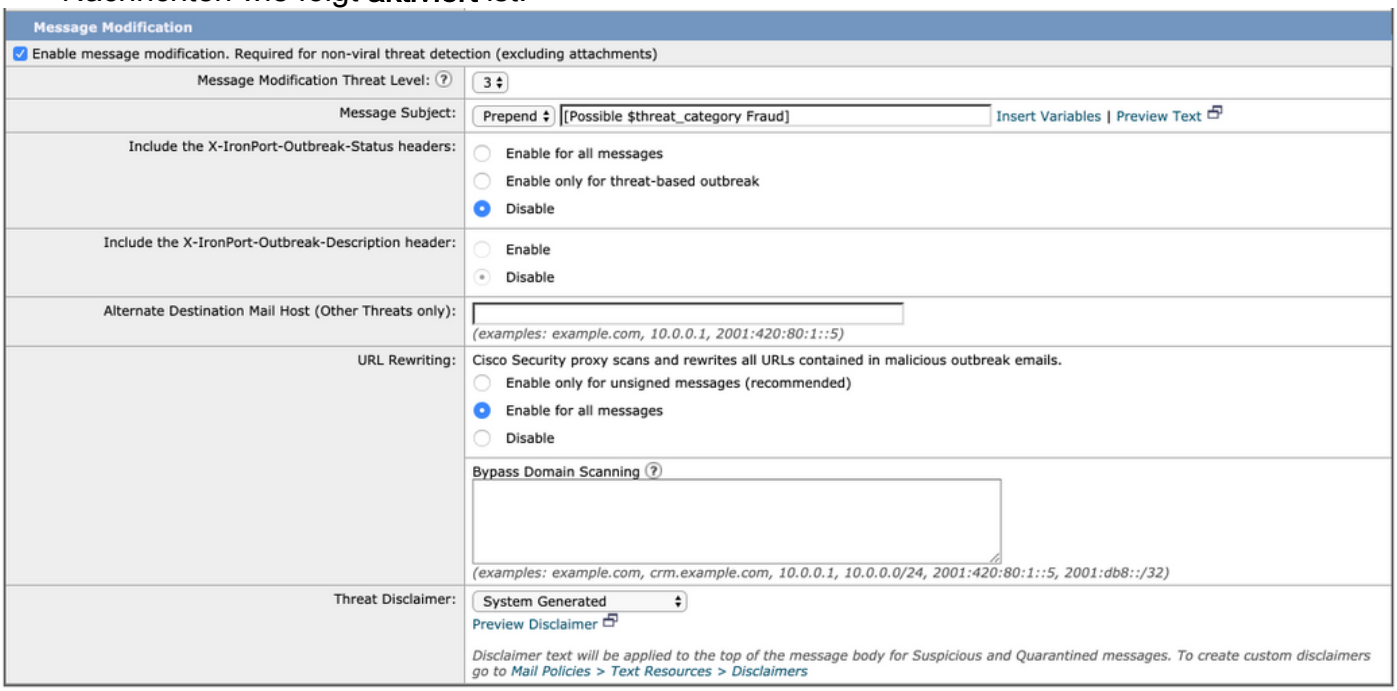
Nach Outbreak-Filtern hat wurden konfiguriert global , Sie können Jetzt Diese Funktion anwenden auf Post Richtlinien.

- Navigieren Sie zu **Mail-Policys > Mail-Policys für eingehende E-Mails.**
- Wenn Sie unter **Outbreak-Filter** auf den blauen Link klicken, können für diese Richtlinie benutzerdefinierte Outbreak-Filtereinstellungen verwendet werden.
- für die Zweck von diese beste ÜbungEis Dokument behalten wir die Outbreak-Filtereinstellungen mit Standardwerten bei:



- Outbreak-Filter können URLs umschreiben, wenn sie als schädlich, verdächtig oder phishing eingestuft werden. Wählen Sie **Nachrichtenmodifizierung aktivieren** aus, um URL-basierte Bedrohungen zu erkennen und umzuschreiben.

- Vergewissern Sie sich, dass die Option **URL Rewriting** (URL-Umschreibung) für alle Nachrichten wie folgt **aktiviert** ist:



- Klicken Sie auf **Senden**und **Bestätigen Sie Ihre Änderungen**

Die Richtlinie für ausgehende E-Mails sollte **Outbreak-Filter** im **deaktivierten** Zustand beibehalten.

Schlussfolgerung

Dieses Dokument beschreibt die Standard- oder Best Practice-Konfigurationen für Anti-Spam-, Anti-Virus-, Graymail- und Outbreak-Filter in der E-Mail Security Appliance (ESA). Alle diese Filter sind sowohl für eingehende als auch für ausgehende E-Mail-Richtlinien verfügbar, und Konfiguration und Filterung werden für beide empfohlen. Der Großteil des Schutzes ist für eingehende E-Mails vorgesehen, während das Filtern des ausgehenden Datenverkehrs Schutz vor weitergeleiteten E-Mails oder internen bösartigen Angriffen bietet.