

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

Inhalt

[Übersicht](#)

[Anti-Spam](#)

[Feature-Schlüssel überprüfen](#)

[Globale Aktivierung von IMS \(Intelligent Multi Scan\)](#)

[Zentrale Spam-Quarantäne aktivieren](#)

[Anti-Spam in-Richtlinien konfigurieren](#)

[Antivirus](#)

[Überprüfen der Funktionstasten](#)

[Anti-Virus-Scanning aktivieren](#)

[Anti-Virus in Mail-Richtlinien konfigurieren](#)

[Graymail](#)

[Feature-Schlüssel überprüfen](#)

[Aktivieren von Graymail- und Safe Unsubscribe-Diensten](#)

[Konfigurieren von Graymail und Safe Unsubscribe in Richtlinien](#)

[Outbreak-Filter](#)

[Feature-Schlüssel überprüfen](#)

[Outbreak-Filter-Service aktivieren](#)

[Konfigurieren von Outbreak-Filtern in Richtlinien](#)

[Schlussfolgerung](#)

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 **Aktivierenauf globalen IMS-Einstellungen:**

IMS Global Settings	
Ironport Intelligent Multi-Scan:	Enabled
Regional Scanning:	Off
Edit IMS Settings	

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

Edit Common Global Settings	
Message Scanning Thresholds:	<p>Increasing these values may result in decreased performance. Please consult documentation for size recommendations based on your environment.</p> <p>Always scan messages smaller than <input type="text" value="2M"/> Maximum <i>Add a trailing K or M to indicate units. Recommended setting is 1024K(1MB) or less.</i></p> <p>Never scan messages larger than <input type="text" value="3M"/> Maximum <i>Add a trailing K or M to indicate units. Recommended setting is 2048K(2MB) or less.</i></p>
Timeout for Scanning Single Message:	<input type="text" value="60"/> Seconds

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

Wenn Sie kein IMS-Lizenzabonnement besitzen:

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

IronPort Anti-Spam Global Settings	
<input checked="" type="checkbox"/> Enable IronPort Anti-Spam Scanning	
Message Scanning Thresholds:	<p>Increasing these values may result in decreased performance. Please consult documentation for size recommendations based on your environment.</p> <p>Always scan messages smaller than <input type="text" value="2M"/> Maximum Add a trailing K or M to indicate units. Recommended setting is 1024K(1MB) or less.</p> <p>Never scan messages larger than <input type="text" value="3M"/> Maximum Add a trailing K or M to indicate units. Recommended setting is 2048K(2MB) or less.</p>
Timeout for Scanning Single Message:	<input type="text" value="60"/> Seconds
Scanning Profile:	<p><input type="radio"/> Normal</p> <p><input checked="" type="radio"/> Aggressive Recommended for customers who desire a stronger emphasis on blocking spam. When enabled, tuning Anti-Spam policy thresholds will have more impact on spam detection than the normal profile with a larger potential for false positives. Do not select the aggressive profile if IMS is enabled on the mail policy.</p> <p><input type="radio"/> Regional (China)</p>

- 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**.
- Klickend die **Konfigurieren** Schaltfläche werden Sie an die Follschuldige Seite.
- Hier Sie können aktivieren die Quarantäne von Überprüfung die **aktivieren** Box und Punkte Quarantäne an sein zentralisiert auf SicherheitManagement AAppliance (SMA) von Füllung in SMA Name und **IP Adresse**. Die empfohlen Einstellungen sind gezeigt unten:

External Spam Quarantine Settings	
<input checked="" type="checkbox"/> Enable External Spam Quarantine	
Name:	<input type="text" value="centralized_spam"/> <small>(e.g. spam_quarantine)</small>
IP Address:	<input type="text" value="sma_ip_address"/>
Port:	<input type="text" value="6025"/>
Safelist/Blocklist:	<input checked="" type="checkbox"/> Enable End User Safelist/Blocklist Feature Blocklist Action: <input type="text" value="Quarantine"/>

- 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:

Order	Policy Name	Anti-Spam	Anti-Virus	Advanced Malware Protection	Graymail	Content Filters	Outbreak Filters	Delete
	Default Policy	IronPort Intelligent Multi-Scan Positive: Deliver Suspected: Deliver	Sophos Encrypted: Deliver Unscannable: Deliver Virus Positive: Drop	File Reputation Malware File: Drop Pending Analysis: Quarantine Unscannable - Message Error: Deliver Unscannable - Rate Limit: Deliver Unscannable - AMP Service Not ...	Graymail Detection Unsubscribe: Enabled Marketing: Spam Quarantine Social: Spam Quarantine Bulk: Spam Quarantine ...	URL_LOG_ALL_REPUTATION URL_LOG_ALL_CATEGORY URL_QUARANTINE_MALICIOUS URL_REWRITE_SUSPICIOUS URL_INAPPROPRIATE SPF_DKIM_FAIL ...	Retention Time: Virus: 1 day Other: 4 hours	

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**:

Anti-Spam Settings	
Policy:	Default
Enable Anti-Spam Scanning for This Policy:	<input type="radio"/> Use IronPort Anti-Spam service <input checked="" type="radio"/> Use IronPort Intelligent Multi-Scan <i>Spam scanning built on IronPort Anti-Spam.</i> <input type="radio"/> Disabled

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:

Positively-Identified Spam Settings	
Apply This Action to Message:	Spam Quarantine <i>Note: If local and external quarantines are defined, mail will be sent to local quarantine.</i>
Add Text to Subject:	Prepend [SPAM]
Advanced	Optional settings for custom header and message delivery.
Suspected Spam Settings	
Enable Suspected Spam Scanning:	<input type="radio"/> No <input checked="" type="radio"/> Yes
Apply This Action to Message:	Deliver Send to Alternate Host (optional):
Add Text to Subject:	Prepend [SUSPECTED SPAM]
Advanced	Optional settings for custom header and message delivery.

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

Spam Thresholds	
Spam is scored on a 1-100 scale. The higher the score, the more likely a message is a spam.	
IronPort Anti-Spam:	<input checked="" type="radio"/> Use the Default Thresholds <input type="radio"/> Use Custom Settings: Positively Identified Spam: Score > <input type="text" value="90"/> (50 - 100) Suspected Spam: Score > <input type="text" value="50"/> (minimum 25, cannot exceed positive spam score)
IronPort Intelligent Multi-Scan:	<input type="radio"/> Use the Default Thresholds <input checked="" type="radio"/> Use Custom Settings: Positively Identified Spam: Score > <input type="text" value="90"/> (50 - 100) Suspected Spam: Score > <input type="text" value="43"/> (minimum 25, cannot exceed positive spam score)

- Klicken Sie auf **Senden** und **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:

Sophos Anti-Virus Overview	
Anti-Virus Scanning by Sophos Anti-Virus:	Enabled
Virus Scanning Timeout (seconds):	60
Automatic Updates: (?)	Enabled
Edit Global Settings...	

Current Sophos Anti-Virus files			
File Type	Last Update	Current Version	New Update
Sophos Anti-Virus Engine	Wed Nov 6 10:04:30 2019	3.2.07.377.1_5.68	Not Available
Sophos IDE Rules	Wed Nov 6 12:03:56 2019	2019110602	Not Available
No updates in progress.			Update Now

- Klicken Sie auf **Senden** und **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 **Senden** und **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**:

Anti-Virus Settings	
Policy:	DEFAULT
Enable Anti-Virus Scanning for This Policy:	<input checked="" type="radio"/> Yes <input checked="" type="checkbox"/> Use McAfee Anti-Virus <input checked="" type="checkbox"/> Use Sophos Anti-Virus <input type="radio"/> No

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

Message Scanning	
	Scan for Viruses only <input type="button" value="v"/> <input type="checkbox"/> Drop infected attachments if a virus is found <input checked="" type="checkbox"/> (recommended) Include an X-header with the Anti-Virus scanning results in messages
Repaired Messages:	
Action Applied to Message:	<input type="text" value="Deliver As Is"/>
Archive Original Message:	<input checked="" type="radio"/> No <input type="radio"/> Yes
Modify Message Subject:	<input checked="" type="radio"/> No <input type="radio"/> Prepend <input type="radio"/> Append
	<input type="text" value="[WARNING: VIRUS REMOVED]"/>
Advanced	Optional settings for custom header and message delivery.

- 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:

Encrypted Messages:	
Action Applied to Message:	Deliver As Is
Archive Original Message:	<input checked="" type="radio"/> No <input type="radio"/> Yes
Modify Message Subject:	<input type="radio"/> No <input checked="" type="radio"/> Prepend <input type="radio"/> Append
	[A/V UNSCANNABLE]
▶ Advanced	Optional settings for custom header and message delivery.
Unscannable Messages:	
Action Applied to Message:	Deliver As Is
Archive Original Message:	<input checked="" type="radio"/> No <input type="radio"/> Yes
Modify Message Subject:	<input type="radio"/> No <input checked="" type="radio"/> Prepend <input type="radio"/> Append
	[A/V UNSCANNABLE]
▶ Advanced	Optional settings for custom header and message delivery.
Virus Infected Messages:	
Action Applied to Message:	Drop Message
Archive Original Message:	<input checked="" type="radio"/> No <input type="radio"/> Yes
Modify Message Subject:	<input type="radio"/> No <input checked="" type="radio"/> Prepend <input type="radio"/> Append
	[WARNING : VIRUS DETECTED]
▶ Advanced	Optional settings for custom header and message delivery.

- 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**:

Graymail Global Settings	
Graymail Detection	Enabled
Safe Unsubscribe	Enabled
Automatic Updates [?]	Enabled

[Edit Graymail Settings](#)

- Klicken Sie auf **Senden** und **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 an Post Richtlinien.

- Navigieren Sie zu **Mail-Policies > Mail-Policies 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 Graymail Optionen 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:**

Graymail Settings	
Policy:	DEFAULT
Enable Graymail Detection for This Policy:	<input checked="" type="radio"/> Yes <input type="radio"/> No
Enable Graymail Unsubscribing for This Policy:	<input checked="" type="radio"/> Yes <input type="radio"/> No
	Perform this action for: <input checked="" type="radio"/> All Messages (Recommended) <input type="radio"/> Unsigned Messages

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:

✓ Action on Marketing Email	
Apply this action to Message:	Deliver <input type="text" value="↓"/> Send to Alternate Host (optional): <input type="text"/>
Add Text to Subject:	<input type="radio"/> No <input checked="" type="radio"/> Prepend <input type="radio"/> Append <input type="text" value="[MARKETING]"/>
Advanced	<i>Optional settings for custom header and message delivery.</i>
✓ Action on Social Network Email	
Apply this action to Message:	Deliver <input type="text" value="↓"/> Send to Alternate Host (optional): <input type="text"/>
Add Text to Subject:	<input type="radio"/> No <input checked="" type="radio"/> Prepend <input type="radio"/> Append <input type="text" value="[SOCIAL NETWORK]"/>
Advanced	<i>Optional settings for custom header and message delivery.</i>
✓ Action on Bulk Email	
Apply this action to Message:	Deliver <input type="text" value="↓"/> Send to Alternate Host (optional): <input type="text"/>
Add Text to Subject:	<input type="radio"/> No <input checked="" type="radio"/> Prepend <input type="radio"/> Append <input type="text" value="[BULK]"/>
Advanced	<i>Optional settings for custom header and message delivery.</i>

- 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 gezeigt in die Bild unten:

Outbreak Filters Global Settings	
<input checked="" type="checkbox"/> Enable Outbreak Filters	
Adaptive Rules:	<input checked="" type="checkbox"/> Enable Adaptive Rules
Maximum Message Size to Scan:	<input type="text" value="3M"/> Maximum <small>Add a trailing K or M to indicate units.</small>
Emailed Alerts: (?)	<input checked="" type="checkbox"/> Receive Emailed Alerts
Web Interaction Tracking: (?)	<input checked="" type="checkbox"/> Enable Web Interaction Tracking

- 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 Übung Eis Dokument behalten wir die Outbreak-Filtereinstellungen mit Standardwerten bei:

Outbreak Filter Settings	
Quarantine Threat Level: (?)	<input type="text" value="3"/>
Maximum Quarantine Retention:	Viral Attachments: <input type="text" value="1"/> <input type="text" value="Days"/> Other Threats: <input type="text" value="4"/> <input type="text" value="Hours"/> <input type="checkbox"/> Deliver messages without adding them to quarantine
Bypass Attachment Scanning: ▶	None configured

- 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:

Message Modification	
<input checked="" type="checkbox"/> Enable message modification. Required for non-viral threat detection (excluding attachments)	
Message Modification Threat Level: ?	3
Message Subject:	Prepend [Possible \$threat_category Fraud] Insert Variables Preview Text
Include the X-IronPort-Outbreak-Status headers:	<input type="radio"/> Enable for all messages <input type="radio"/> Enable only for threat-based outbreak <input checked="" type="radio"/> Disable
Include the X-IronPort-Outbreak-Description header:	<input type="radio"/> Enable <input checked="" type="radio"/> Disable
Alternate Destination Mail Host (Other Threats only):	<input type="text"/> <small>(examples: example.com, 10.0.0.1, 2001:420:80:1::5)</small>
URL Rewriting:	Cisco Security proxy scans and rewrites all URLs contained in malicious outbreak emails. <input type="radio"/> Enable only for unsigned messages (recommended) <input checked="" type="radio"/> Enable for all messages <input type="radio"/> Disable
	Bypass Domain Scanning ? <input type="text"/> <small>(examples: example.com, crm.example.com, 10.0.0.1, 10.0.0.0/24, 2001:420:80:1::5, 2001:db8::/32)</small>
Threat Disclaimer:	System Generated Preview Disclaimer <small>Disclaimer text will be applied to the top of the message body for Suspicious and Quarantined messages. To create custom disclaimers go to Mail Policies > Text Resources > Disclaimers</small>

- 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 bössartigen Angriffen bietet.