Guida alle best practice per i filtri antispam, antivirus, di posta grigia ed epidemie

Sommario

Panoramica

La maggior parte delle minacce, degli attacchi e dei disturbi affrontati da un'organizzazione tramite la posta elettronica si presenta sotto forma di spam, malware e attacchi misti. Cisco Email Security Appliance (ESA) include diverse tecnologie e funzionalità per bloccare queste minacce sul gateway prima che entrino nell'organizzazione. In questo documento vengono descritti gli approcci best practice per configurare i filtri antispam, antivirus, di posta grigia ed epidemie sul flusso di posta in entrata e in uscita.

Antispam

La protezione antispam risolve una vasta gamma di minacce note, tra cui spam, phishing e attacchi zombie, oltre a minacce e-mail di breve durata, difficili da rilevare, di volume ridotto, come le truffe "419". Inoltre, la protezione antispam identifica minacce miste nuove ed in evoluzione, come gli attacchi di spam che distribuiscono contenuti dannosi tramite un URL di download o un eseguibile.

Cisco Email Security offre le seguenti soluzioni anti-spam:

- IronPort Anti-Spam Filtering (IPAS)

- Cisco Intelligent Multi-Scan Filtering (IMS)

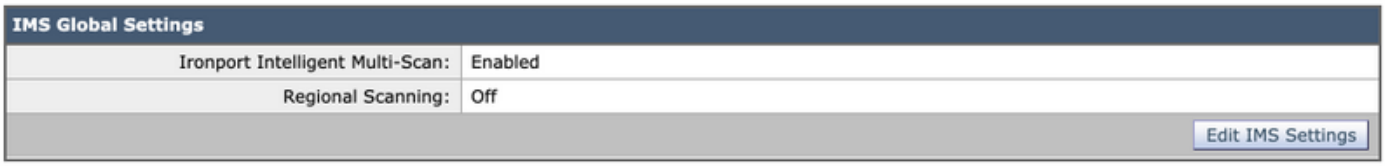
Èpossibile concedere in licenza entrambe le soluzioni, ma solo una può essere utilizzata in una particolare policy di posta. Ai fini di questo documento, verrà utilizzata la funzionalità IMS.

Verifica chiave funzionalità

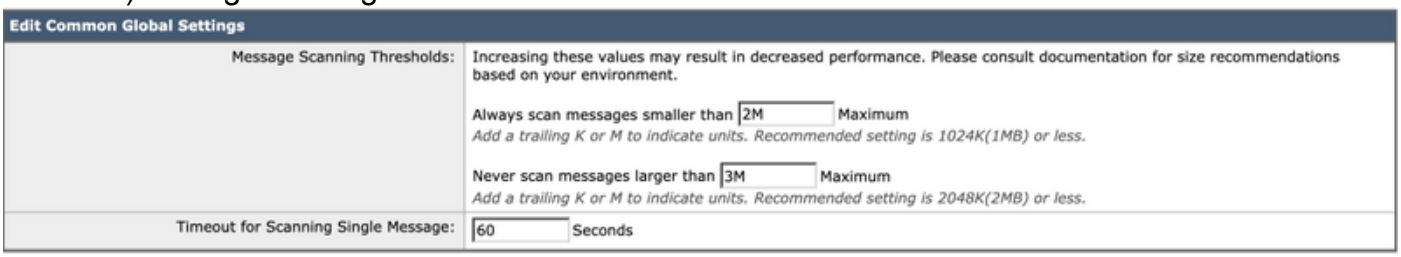
- Sull'ESA, selezionare **System Administration > Feature Keys (Amministrazione sistema > Chiavi funzione)**
- Cercare la licenza Intelligent Multi-Scan e verificare che sia attiva.

Abilita IMS (Intelligent Multi-Scan) a livello globale

- On OSPF (Open Shortest Path First) ESA, navigare a **Sicurezza Servizi> IMS e Graymail**
- Clic OSPF (Open Shortest Path First) **Attiva**in **Impostazioni globali IMS**:



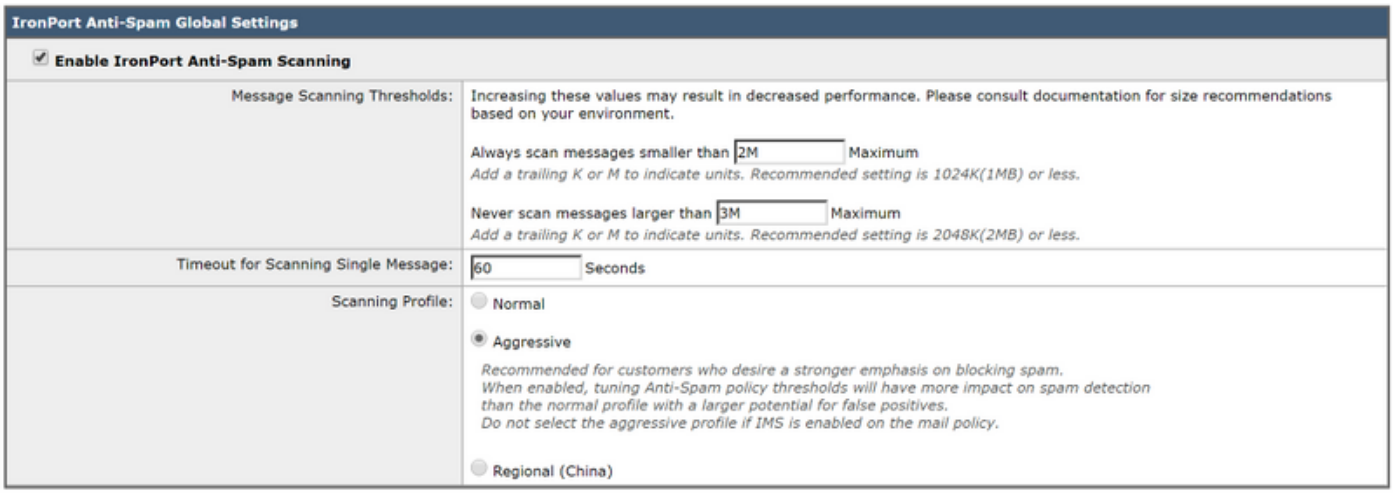
- Cerca **impostazioni globali comuni** e fare clic su **Modifica impostazioni globali**
- Qui tu può configurazione multiplo impostazioni. OSPF (Open Shortest Path First) consigliato impostazioni sono visualizzato in OSPF (Open Shortest Path First) immagine di seguito:



- Fare clic su **Submit (Invia).**e **Conferma modifiche.**

Se non si dispone di una sottoscrizione di licenza IMS:

- Selezionare **Security Services > IronPort Anti-Spam**
- Clic OSPF (Open Shortest Path First) **Attiva**pulsante sulla **panoramica di IronPort Anti-Spam**
- Fare clic su **Modifica impostazioni globali**
- Qui tu può configurazione multiplo impostazioni. OSPF (Open Shortest Path First) consigliato impostazioni sono visualizzato in OSPF (Open Shortest Path First) immagine di seguito:

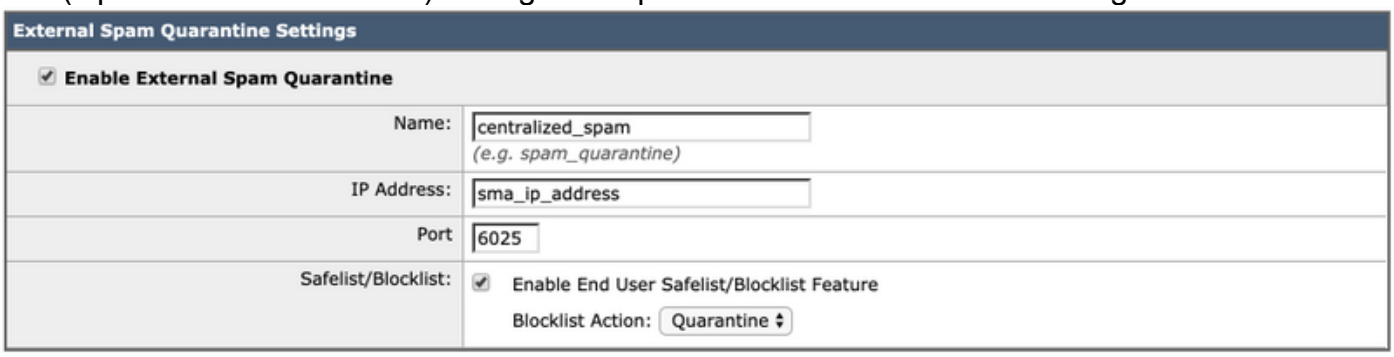


- Cisco consiglia di selezionare il profilo di scansione **aggressiva** per i clienti che desiderano porre l'accento sul blocco della posta indesiderata.
- Fare clic su **Submit (Invia)**.e **Conferma modifiche**

Abilita quarantena della posta indesiderata centralizzata

Dal momento che la funzionalità Protezione da posta indesiderata può essere impostata per essere messa in quarantena, è importante assicurarsi che tale funzionalità sia configurata:

- Passare a **Servizi di sicurezza > Quarantena posta indesiderata**
- Clicre OSPF (Open Shortest Path First) **Configurazione**pulsante sarà prendere tu a OSPF (Open Shortest Path First) piegaredebitore pagina.
- Qui tu può attivare OSPF (Open Shortest Path First) quarantena da controllo OSPF (Open Shortest Path First) **attivare**scatola e punto ths quarantena a essere centralizzato on a) SicurezzaGestione AAppliance (SMA) dariempimento in SMA**Nome**e **IP indirizzo.** OSPF (Open Shortest Path First) consigliato impostazioni sono visualizzato di seguito:



- Fare clic su **Submit (Invia)**.e **Conferma modifiche**

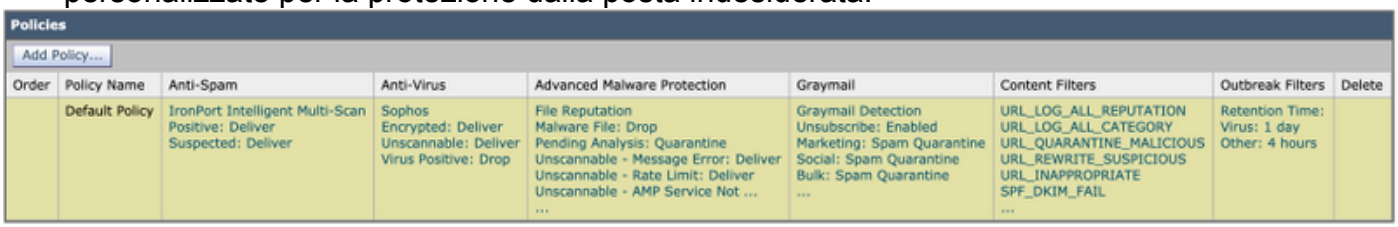
Per ulteriori informazioni sull'impostazione e la centralizzazione delle quarantene, fare riferimento al documento sulle best practice:
[Procedure ottimali per la configurazione centralizzata di quarantene per virus ed epidemie e per la migrazione da ESA a SMA]

Configura protezione da posta indesiderata nei criteri

Una volta Intelligente Multiplo - Scansione ha è stato configurato globalmente , tu può ora applicare Intelligente Multiplo - Scansione a posta criteri:

- Passare a **Criteri posta > Criteri posta in arrivo**

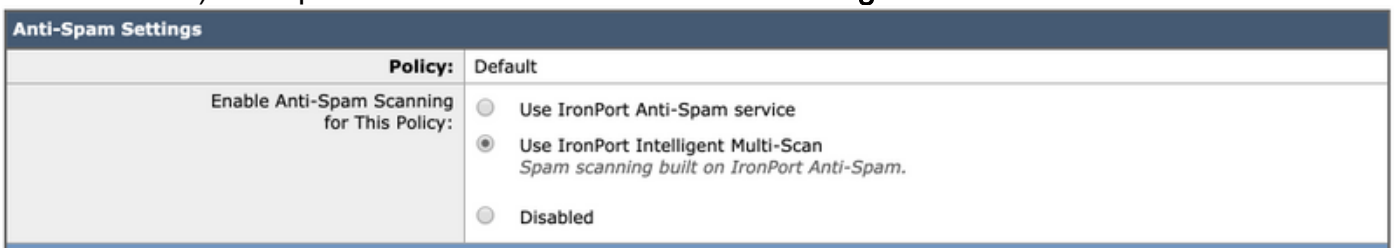
- Per impostazione predefinita, i criteri della posta in arrivo utilizzano le impostazioni di protezione da posta indesiderata IronPort.
- Se si fa clic sul collegamento blu in **Protezione antispam**, sarà possibile utilizzare le impostazioni personalizzate della protezione antispam per il criterio specifico.
- Di seguito è riportato un esempio che mostra i criteri predefiniti utilizzando le impostazioni personalizzate per la protezione dalla posta indesiderata:



Personalizzare le impostazioni della protezione dalla posta indesiderata per un criterio Posta in arrivo facendo clic sul collegamento blu in **Protezione dalla posta indesiderata** per il criterio che si desidera personalizzare.

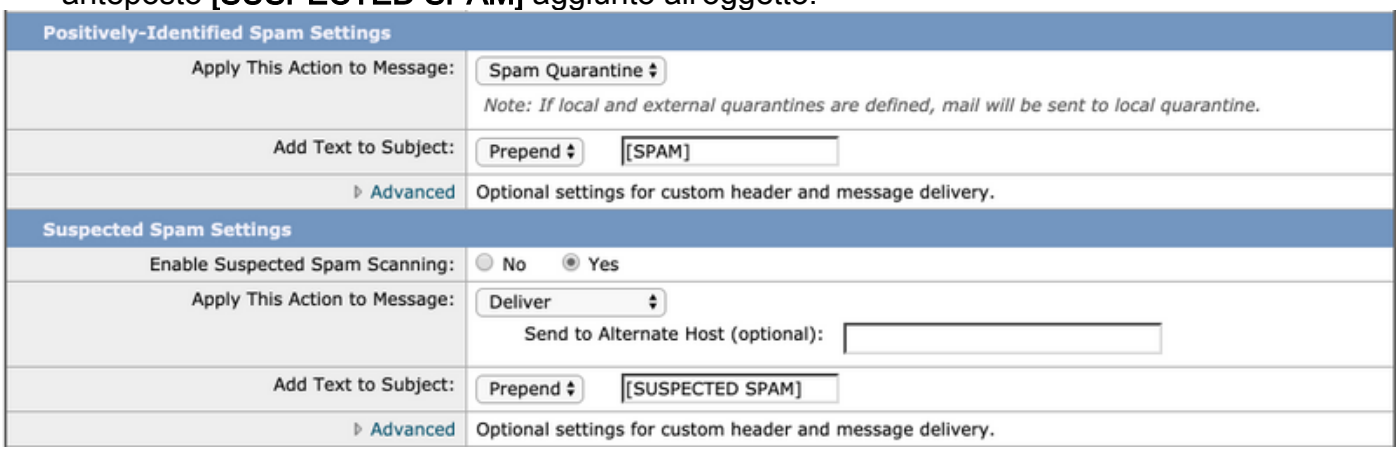
Qui tu può selezionare OSPF (Open Shortest Path First) Anti-
Spam Scansione opzione tu desiderio a attivare per questo policy.

- Per OSPF (Open Shortest Path
  First) scopi di questo migliore praticareghiaccio documento, fare clic OSPF (Open Shortest Path First) radio pulsante avanti a Utilizzo **IronPort Intelligent Multi-Scansione:**



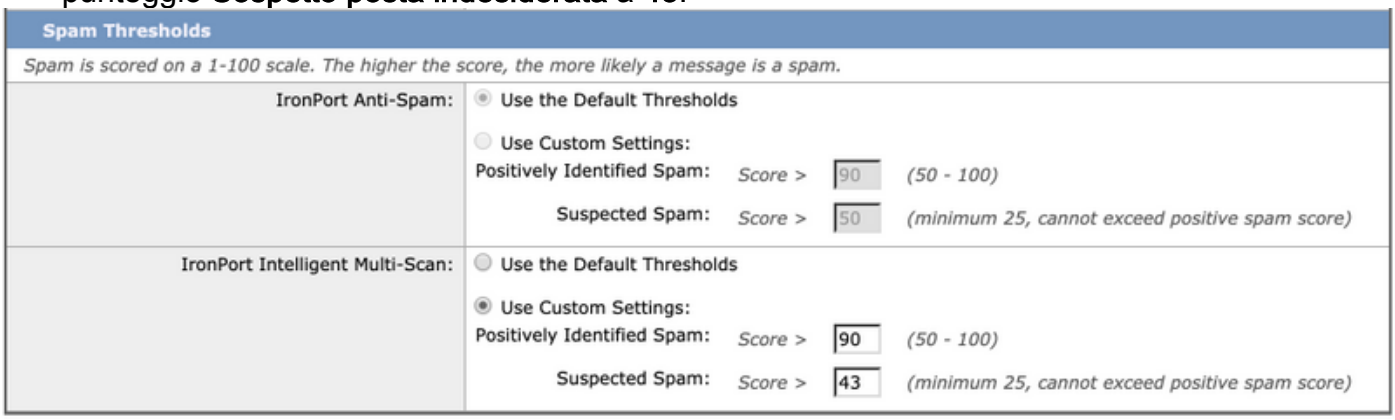
Le due sezioni successive includono **Impostazioni di posta indesiderata identificate in modo positivo** e **Impostazioni di posta indesiderata sospetta:**

- La procedura consigliata consiste nel configurare l'azione di **quarantena** sull'impostazione **Spam identificata positivamente** con il testo preceduto **[SPAM]** aggiunto all'oggetto e
- Applica a **recapita** come azione per **le impostazioni di posta indesiderata** con il testo anteposto **[SUSPECTED SPAM]** aggiunto all'oggetto:



- Èpossibile modificare l'impostazione della **soglia** della **posta indesiderata**; le impostazioni consigliate sono la personalizzazione del punteggio **Identificato in modo positivo** a **90** e del

punteggio **Sospetto posta indesiderata** a **43**:



- Fare clic su **Submit (Invia)**.e **Conferma modifiche**

Antivirus

La protezione antivirus è fornita da due motori di terze parti, Sophos e McAfee. Questi motori filtreranno tutte le minacce maligne conosciute, rilasciandole, pulendole o mettendole in quarantena come configurato.

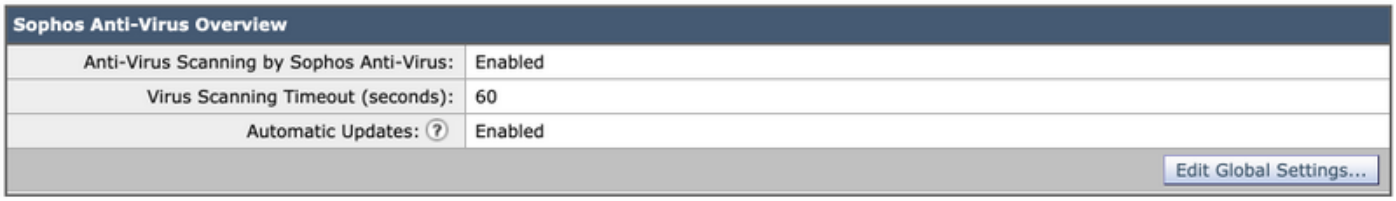
Verifica tasti funzione

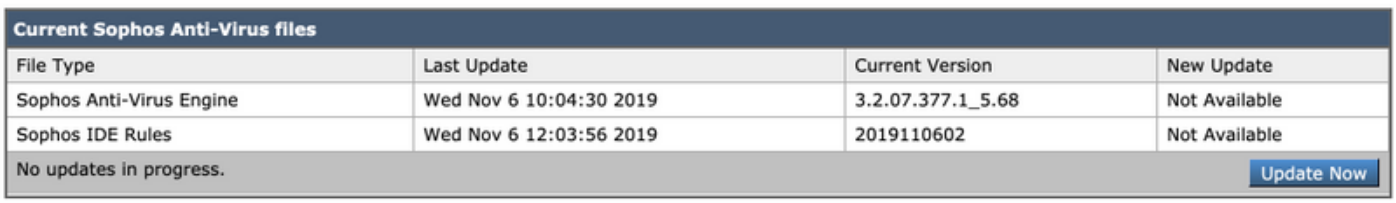
Per verificare che entrambe le chiavi di funzionalità siano attivate:

- Selezionare **Amministrazione sistema > Tasti funzione**
- Accertarsi che le licenze **Sophos Anti-Virus** e **McAfee** siano attive.

Abilita scansione antivirus

- Naviga a **Sicurezza Servizi> Antivirus - Sophos**
- Clic OSPF (Open Shortest Path First) **Attiva**pulsante.
- Verificare che l'opzione **Aggiornamento automatico** sia **attivata** e che l'aggiornamento dei file antivirus Sophos funzioni correttamente. Se necessario, fare clic su **Aggiorna ora** per avviare immediatamente l'aggiornamento del file:





- Fare clic su **Submit (Invia)**.e **Conferma modifiche.**

Se è attiva anche la licenza McAfee, selezionare a **Sicurezza Servizi> Antivirus - McAfee**

- Clic OSPF (Open Shortest Path First) **Attiva**pulsante.

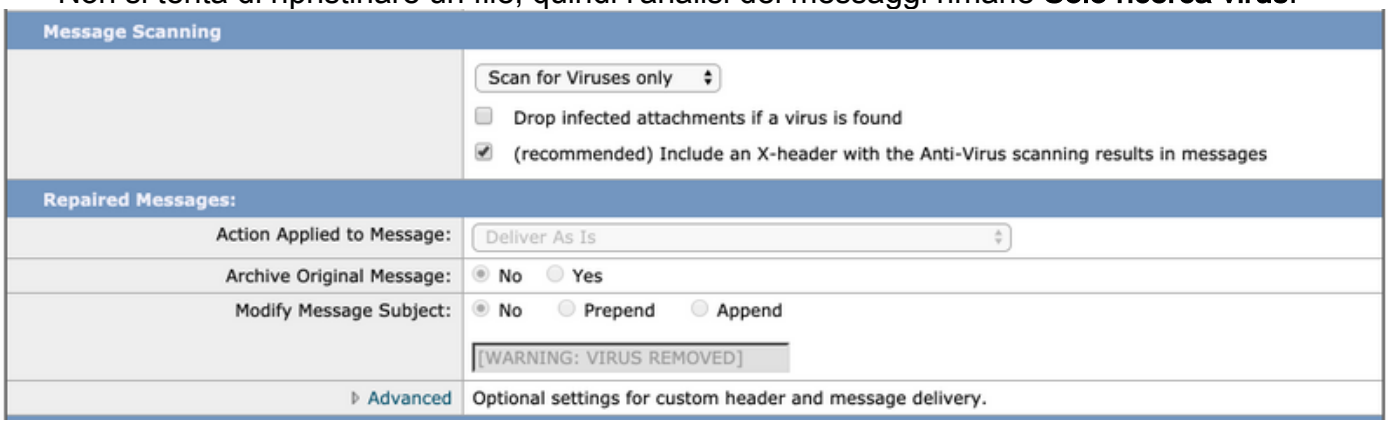
- Verificare che **Aggiornamento automatico** sia **abilitato** e che l'aggiornamento dei file di McAfee Anti-Virus funzioni correttamente. Se necessario, fare clic su **Aggiorna ora** per avviare immediatamente l'aggiornamento del file.
- Fare clic su **Submit (Invia).**e **Conferma modifiche**

Configurare antivirus nei criteri di posta elettronica

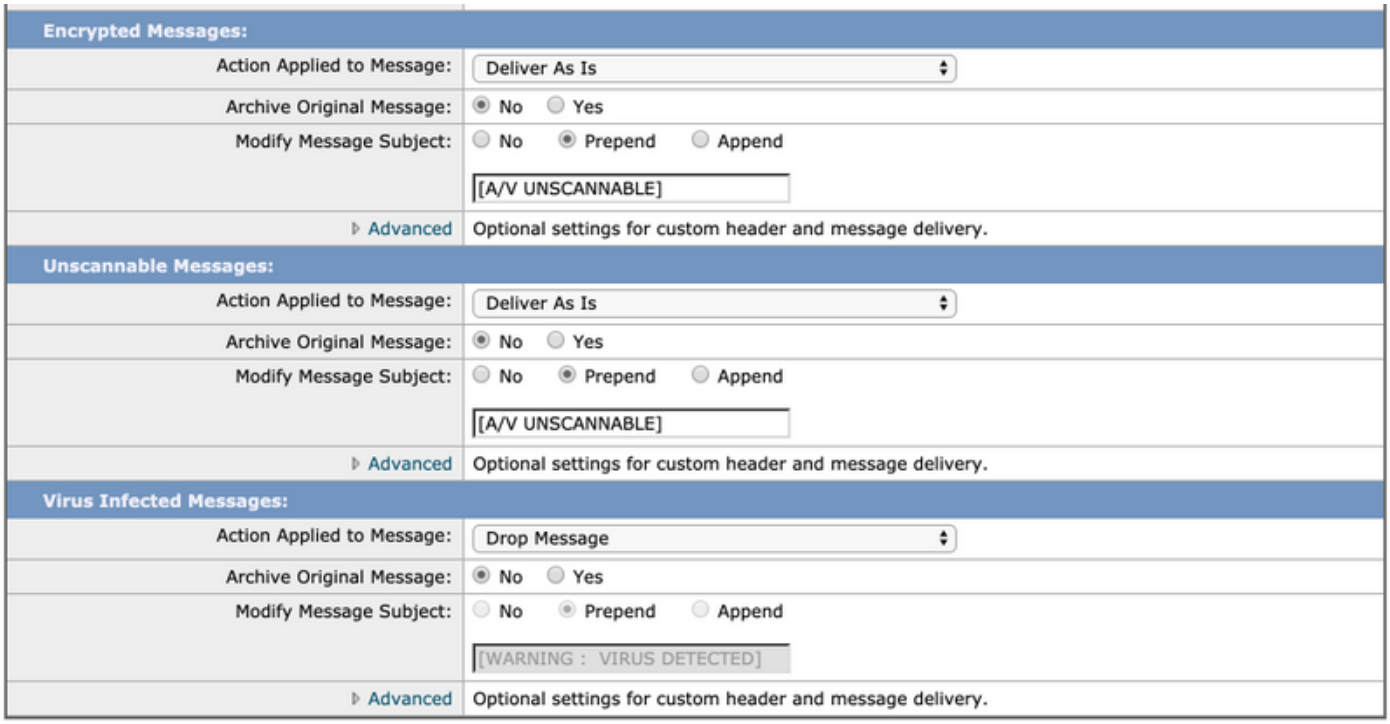
In un criterio Posta in arrivo è consigliabile eseguire le operazioni seguenti:

- Passare a **Criteri posta > Criteri posta in arrivo**
- Personalizzare le impostazioni **antivirus** per un criterio posta in arrivo facendo clic sul collegamento blu in Antivirus per il criterio che si desidera personalizzare.
- Qui tu può selezionare OSPF (Open Shortest Path First) Anti-Virus Scansione opzione tu desiderio a attivare per questo policy.
- Per OSPF (Open Shortest Path First) scopi di questa bconfigurarescattoghiaccio selezionare **McAfee** e **Sophos Anti-Virus**:

- Non si tenta di ripristinare un file, quindi l'analisi dei messaggi rimane **Solo ricerca virus**:



- L'azione consigliata per i **messaggi crittografati** e **non scansionabili** è **recapitare** il messaggio così com'è modificando l'oggetto.
- Il criterio consigliato per Antivirus è **Elimina** tutti i **messaggi infetti da virus**, come mostrato nell'immagine seguente:



- Fare clic su **Submit (Invia)**.e **Conferma modifiche**

Un criterio simile è consigliato per i criteri Posta in uscita, tuttavia si sconsiglia di modificare l'oggetto della posta in uscita.

Graymail

La soluzione di gestione delle e-mail di Greymail Security Appliance è costituita da due componenti: un motore di scansione della posta grigia integrato e un servizio Unsubscribe basato su cloud. La soluzione di gestione della posta grigia consente alle organizzazioni di identificare la posta grigia utilizzando il motore di posta grigia integrato e di applicare i controlli di policy appropriati e fornire un meccanismo semplice agli utenti finali per annullare la sottoscrizione ai messaggi indesiderati utilizzando il servizio di annullamento della sottoscrizione.

Le categorie di posta grigia includono marketing, social network e posta elettronica in blocco. Le opzioni avanzate includono l'aggiunta di un'intestazione personalizzata, l'invio a un host alternativo e l'archiviazione del messaggio. Per questa procedura ottimale, abiliteremo la funzione di annullamento della sottoscrizione sicura di Graymail per il criterio di posta predefinito.

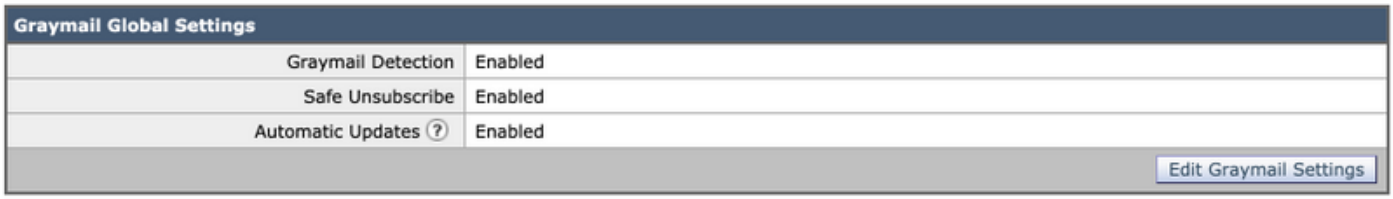
Verifica chiave funzionalità

- Sull'ESA, selezionare **System Administration > Feature Keys (Amministrazione sistema > Chiavi funzione)**
- Cercare **Greymail Safe Unsubscription** e assicurarsi che sia attivo.

Abilita i servizi di posta grigia e di cancellazione sicura dell'iscrizione

- On OSPF (Open Shortest Path First) ESA, navigare a **Sicurezza Servizi> IMS e Graymail**
- Clic OSPF (Open Shortest Path First) **Modifica impostazioni posta grigia**pulsante in **Impostazioni globali di Graymail**
- Selezionare tutte le opzioni - **Attiva rilevamento posta grigia**, **Attiva annullamento sicuro**

sottoscrizione e **Attiva aggiornamenti automatici**:



- Fare clic su **Submit (Invia)**.e **Conferma modifiche**

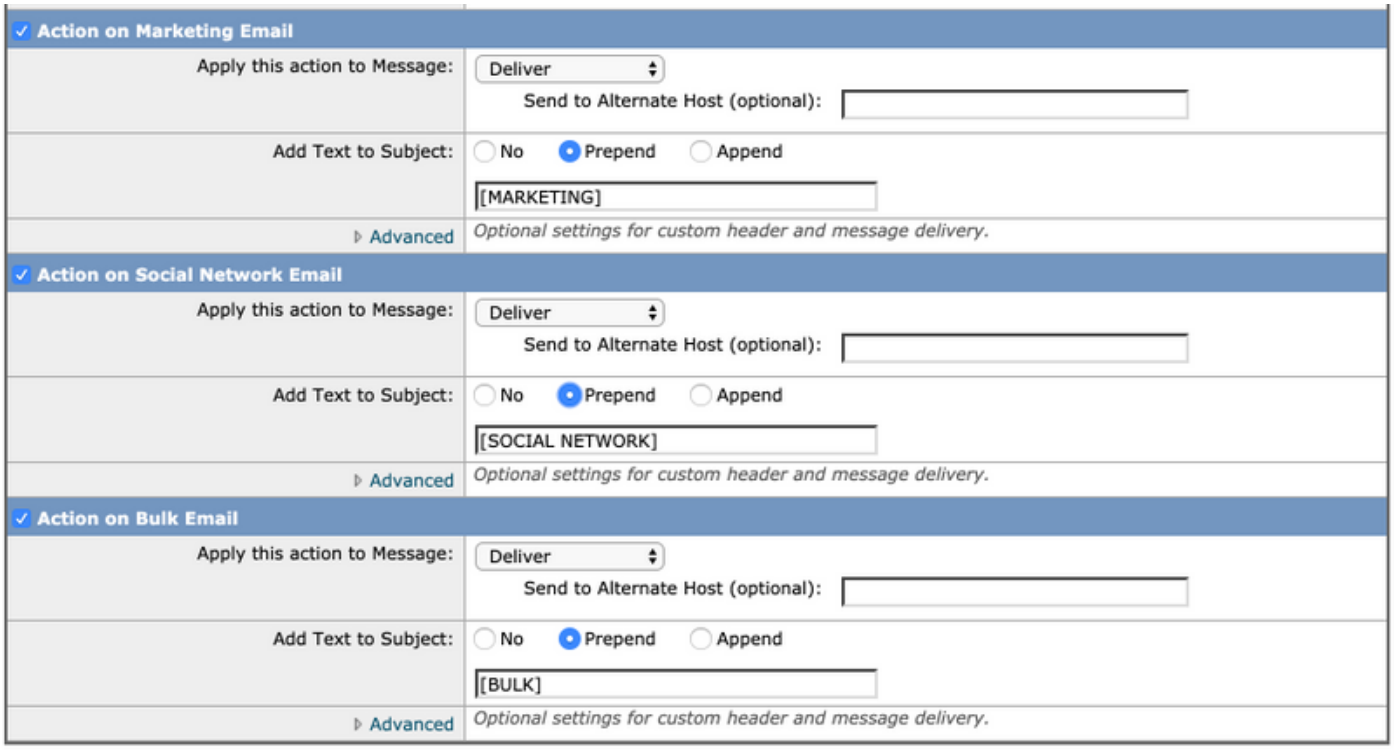
Configura la posta grigia e l'annullamento sicuro della sottoscrizione nei criteri

Once, Greymail e l'annullamento sicuro dell'iscrizione ha è stato configurato globalmente , tu può ora applica questi servizi a posta politiche.

- Passare a **Criteri posta > Criteri posta in arrivo**
- Se si fa clic sul collegamento blu in **Greymail**, per quel particolare criterio sarà possibile usare le impostazioni di Greymail personalizzate.
- Qui tu può selezionare Graymailopzioni tu desiderio a attivare per questo policy.
- Per OSPF (Open Shortest Path First) scopi di questo p ottimalescattoghiaccio documento, fare clic OSPF (Open Shortest Path First) radio pulsante avanti per **abilitare il rilevamento della posta grigia per questo criterio** e **abilitare l'annullamento della sottoscrizione della posta grigia per questo criterio**:

Le tre sezioni successive includono **Azione sulle impostazioni di posta elettronica di marketing**, **Azione sulle impostazioni di posta elettronica dei social network** e **Azione sulle impostazioni di posta elettronica di massa**.

- La migliore pratica raccomandata è di abilitarli tutti e rimanere l'azione come **Consegna** con testo preceduto aggiunto al soggetto in relazione alle categorie come mostrato di seguito:



- Fare clic su **Submit (Invia)**.e **Conferma modifiche**

La condizione **Graymail** dei criteri della posta in uscita deve rimanere **disabilitata**.

Filtri epidemie

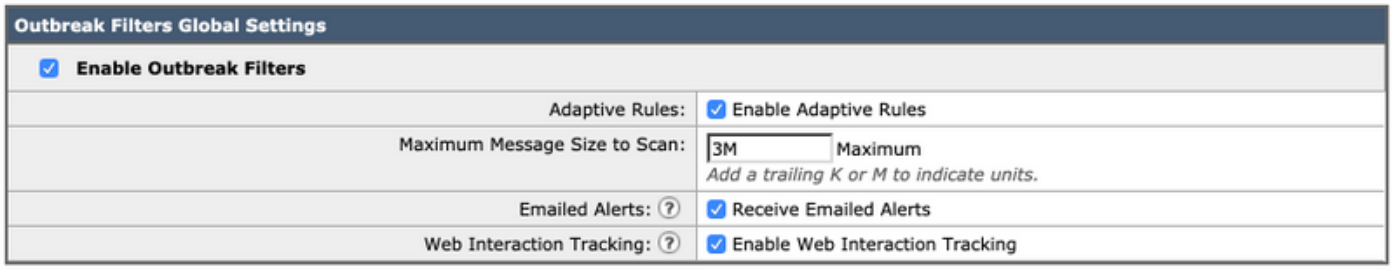
I filtri epidemie combinano trigger nel motore antispam, tecnologie di scansione e rilevamento degli URL e altro ancora per etichettare correttamente gli elementi che non rientrano nella vera categoria di posta indesiderata, come ad esempio le e-mail di phishing e di truffa, e li gestiscono in modo appropriato con le notifiche degli utenti o la quarantena.

Verifica chiave funzionalità

- Sull'ESA, selezionare **System Administration > Feature Keys (Amministrazione sistema > Chiavi funzione)**
- Cercare **i filtri epidemie** e verificare che sia attivo.

Abilita il servizio Filtri epidemie

- On OSPF (Open Shortest Path First) ESA, navigare a **Sicurezza Servizi> Filtri epidemie**
- Clic OSPF (Open Shortest Path First) **Attiva**pulsante **Panoramica dei filtri epidemie**
- Qui tu può configurazione multiplo impostazioni. OSPF (Open Shortest Path First) consigliato impostazioni sono visualizzato in OSPF (Open Shortest Path First) immagine di seguito:

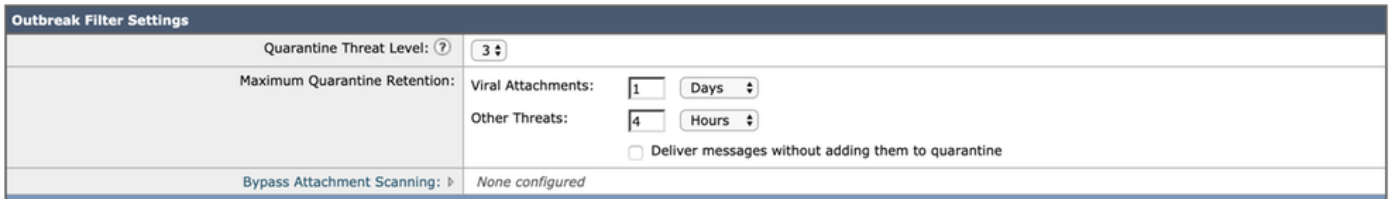


- Fare clic su **Submit (Invia)**.e **Conferma modifiche.**

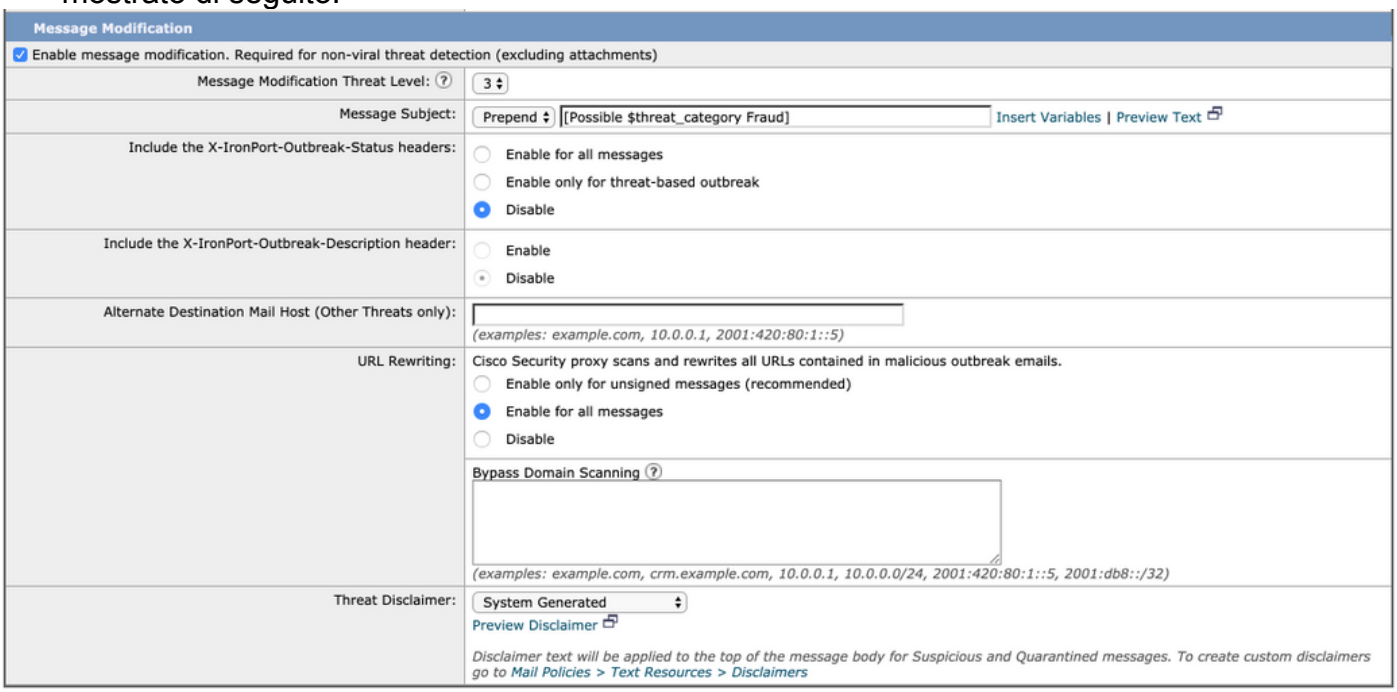
Configurare i filtri epidemie nei criteri

Filtri epidemie una sola volta ha è stato configurato globalmente , tu può ora applica questa funzionalità a posta politiche.

- Passare a **Criteri posta > Criteri posta in arrivo**
- Se si fa clic sul collegamento blu in **Filtri epidemie**, sarà possibile usare le impostazioni personalizzate dei filtri epidemie per quel criterio specifico.
- Per OSPF (Open Shortest Path First) scopi di questo migliore praticareghiaccio , le impostazioni del filtro epidemie vengono mantenute con i valori predefiniti:



- I filtri epidemie possono riscrivere gli URL se vengono considerati dannosi, sospetti o phishing. Selezionare **Abilita modifica messaggi** per rilevare e riscrivere le minacce basate su URL.
- Verificare che l'opzione **URL Rewriting** (Riscrittura URL) sia **Abilita** per tutti i messaggi, come mostrato di seguito:



- Fare clic su **Submit (Invia)**.e **Conferma modifiche**

Nei criteri di posta in uscita **i filtri epidemie** devono rimanere **disabilitati**.

Conclusioni

Questo documento ha lo scopo di descrivere le configurazioni predefinite, o best practice, per i filtri antispam, antivirus, grigi ed epidemie di Email Security Appliance (ESA). Tutti questi filtri sono disponibili sia nei criteri della posta in arrivo che in uscita, e la configurazione e il filtro sono consigliati su entrambi - mentre la maggior parte della protezione è per il traffico in entrata, il filtro del flusso in uscita fornisce protezione dai messaggi inoltrati o da attacchi dannosi interni.