Consenti a un mittente attendibile di ignorare la protezione dalla posta indesiderata

Sommario

Introduzione

In questo documento vengono descritti i dettagli che permettono a un mittente attendibile di ignorare la scansione antispam e i diversi metodi che è possibile scegliere allo stesso modo sul gateway di posta elettronica sicuro (in precedenza Email Security Appliance).

Aggiunta di nome host mittente/indirizzo IP nel gruppo di mittenti ALLOWED_LIST

Aggiungere mittenti attendibili al gruppo di mittenti ALLOWED_LIST perché questo gruppo di mittenti utilizza il criterio del flusso di posta $TRUSTED. I membri del gruppo di mittenti ALLOWED_LIST non sono soggetti a limitazioni di velocità e il contenuto di tali mittenti non viene analizzato dal motore antispam ma viene comunque analizzato da Anti-Virus.

> **Nota:** Con la configurazione predefinita, la scansione antivirus è abilitata ma la funzione Anti-Spam è disattivata.

Per consentire a un mittente di ignorare la scansione della posta indesiderata, aggiungere il mittente al gruppo di mittenti ALLOWED_LIST nella tabella di accesso all'host (HAT). È possibile configurare l'HAT tramite la GUI o la CLI.

Dall'interfaccia grafica

1. Selezionare la scheda **Mail Policies** (Criteri di posta).
2. Nella sezione **Tabella di accesso host**, selezionare **Panoramica HAT**.
3. A destra, assicurarsi che il listener **InboundMail** sia selezionato.
4. Dalla colonna **Gruppo mittenti**, selezionare **ALLOWED_LIST**.
5. Selezionare il pulsante **Aggiungi mittente** nella metà inferiore della pagina.
6. Immettere l'indirizzo IP o il nome host che si desidera ignorare nel primo campo.

Dopo aver aggiunto le voci, selezionare il pulsante **Invia**. Ricordarsi di selezionare il pulsante

Commit modifiche per salvare le modifiche.

Dalla CLI

```
example.com> listenerconfig
Currently configured listeners:
1. InboundMail (on PublicNet, 172.19.1.80) SMTP TCP Port 25 Public
2. OutboundMail (on PrivateNet, 172.19.2.80) SMTP TCP Port 25 Private
Choose the operation you want to perform:
- NEW - Create a new listener.
- EDIT - Modify a listener.
- DELETE - Remove a listener.
- SETUP - Change global settings.
[]> edit
Enter the name or number of the listener you wish to edit.
[]> 1
Name: InboundMail
Type: Public
Interface: PublicNet (172.19.1.80/24) TCP Port 25
Protocol: SMTP
Default Domain:
Max Concurrency: 1000 (TCP Queue: 50)
Domain Map: Disabled
TLS: No
SMTP Authentication: Disabled
Bounce Profile: Default
Use SenderBase For Reputation Filters and IP Profiling: Yes
Footer: None
LDAP: Off

Choose the operation you want to perform:
- NAME - Change the name of the listener.
- INTERFACE - Change the interface.
- LIMITS - Change the injection limits.
- SETUP - Configure general options.
- HOSTACCESS - Modify the Host Access Table.
- RCPTACCESS - Modify the Recipient Access Table.
- BOUNCECONFIG - Choose the bounce profile to use for messages injected on this
listener.
- MASQUERADE - Configure the Domain Masquerading Table.
- DOMAINMAP - Configure domain mappings.
[]> hostaccess
Default Policy Parameters
=========================
Allow TLS Connections: No
Allow SMTP Authentication: No
Require TLS To Offer SMTP authentication: No
Maximum Concurrency Per IP: 1,000
Maximum Message Size: 100M
Maximum Messages Per Connection: 1,000
Maximum Recipients Per Message: 1,000
Maximum Recipients Per Hour: Disabled
Use SenderBase For Flow Control: Yes
Spam Detection Enabled: Yes
Virus Detection Enabled: Yes
There are currently 4 policies defined.
There are currently 5 sender groups.
Choose the operation you want to perform:
- NEW - Create a new entry.
- EDIT - Modify an entry.
- DELETE - Remove an entry.
```

```
- MOVE - Move an entry.
- DEFAULT - Set the defaults.
- PRINT - Display the table.
- IMPORT - Import a table from a file.
- EXPORT - Export the table to a file.
- CLEAR - Remove all entries.
[]> edit
1. Edit Sender Group
2. Edit Policy
[1]> 1
Currently configured HAT sender groups:
1. ALLOWED_LIST (My trusted senders have no anti-spam scanning or rate limiting)
2. BLOCKED_LIST (Spammers are rejected)
3. SUSPECTLIST (Suspicious senders are throttled)
4. UNKNOWNLIST (Reviewed but undecided, continue normal acceptance)
5. (no name, first host = ALL) (Everyone else)
Enter the sender group number or name you wish to edit.
[]> 1

Choose the operation you want to perform:
- NEW - Add a new host.
- DELETE - Remove a host.
- MOVE - Reorder the hosts.
- POLICY - Change the policy settings and options.
- PRINT - Display the current definition.
- RENAME - Rename this sender group.
[]> new
Enter the hosts to add. CIDR addresses such as 10.1.1.0/24 are allowed. IP
address ranges such as 10.1.1.10-20 are allowed. IP subnets such as 10.2.3. are
allowed. Hostnames such as crm.example.com are allowed. Partial hostnames such
as .example.com are allowed.
Ranges of SenderBase Reputation scores such as SBRS[7.5:10.0] are allowed.
SenderBase Network Owner IDs such as SBO:12345 are allowed.
Remote blocklist queries such as dnslist[query.blocklist.example] are allowed.
Separate multiple hosts with commas
[]>
```

Ricordarsi di usare il comando **commit** per salvare le modifiche.

Rivedere la funzionalità di scansione di antispam e antivirus nel criterio Flusso di posta attendibile

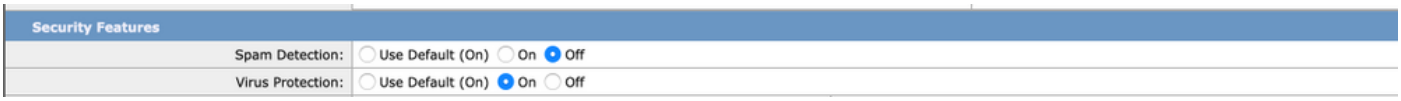
Per il mittente attendibile, per impostazione predefinita verrà definito un criterio flusso di posta denominato Presente attendibile. Il criterio Flusso di posta attendibile avrà un comportamento di connessione Accetto (simile al comportamento di altri criteri Flusso di posta per i messaggi in arrivo).

Quando un mittente è considerato attendibile per i requisiti aziendali, possiamo scegliere di disabilitare i controlli antivirus e antispam. Ciò aiuterà a ridurre il carico di elaborazione aggiuntivo su entrambi i motori di scansione durante la scansione dei messaggi di posta elettronica che non provengono da fonti attendibili.

> **Nota:** I motori antispam e antivirus sono disabilitati e non eseguiranno alcuna scansione relativa a spam o virus per i messaggi e-mail in arrivo in ESA. Questa operazione deve essere eseguita solo se si è totalmente certi che ignorare le scansioni per questi mittenti attendibili non comporta alcun rischio.

L'opzione da cui è possibile disabilitare i motori è disponibile nella scheda delle funzionalità di protezione in Criteri di flusso di posta. Il percorso per lo stesso è **GUI > Mail Policies > Mail Flow Policies**. Fare clic sul **criterio di flusso TRUSTEDMail** e scorrere verso il basso fino a **Funzionalità di sicurezza** nella pagina successiva.

Assicuratevi di eseguire il commit delle modifiche dopo aver apportato le modifiche desiderate.



Aggiungi un mittente attendibile all'elenco indirizzi attendibili

Gli elenchi di sicurezza e gli elenchi di blocco degli utenti finali vengono creati dagli utenti finali e archiviati in un database controllato prima dell'analisi della posta indesiderata. Ogni utente finale può identificare domini, sottodomini o indirizzi di posta elettronica che desidera vengano sempre considerati come posta indesiderata o non come posta indesiderata. Se l'indirizzo di un mittente fa parte di un elenco indirizzi attendibili degli utenti finali, l'analisi della posta indesiderata viene ignorata

Questa configurazione consentirà all'utente finale di mettere in vendita un mittente attenendosi ai requisiti previsti per l'esenzione delle scansioni antispam. La scansione antivirus e altre scansioni nella pipeline della posta elettronica non verranno modificate da questa configurazione e continueranno come da configurazione nei criteri di posta. Questa configurazione ridurrà il coinvolgimento dell'amministratore ogni volta che un utente finale deve esentare un mittente dall'analisi della posta indesiderata.

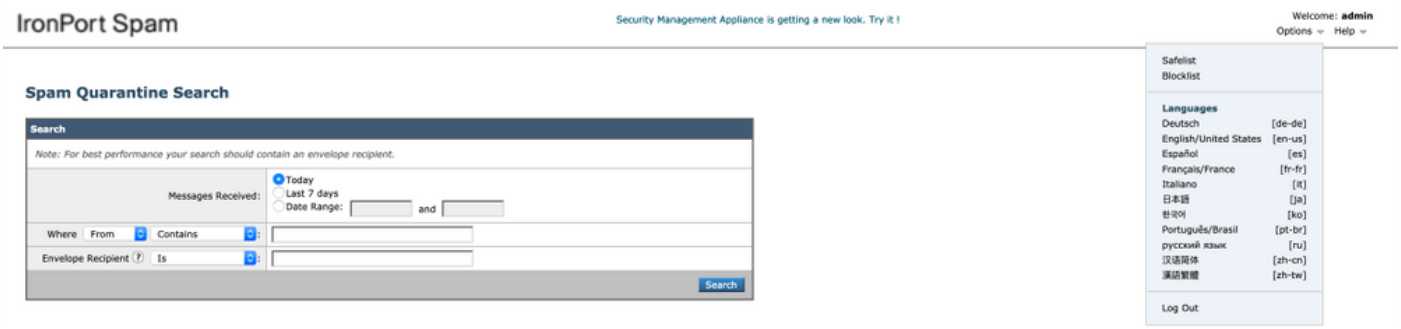
Per l'elenco indirizzi attendibili, è obbligatorio che l'accesso quarantena per l'utente finale sia abilitato per gli utenti finali e che l'elenco indirizzi attendibili/blocco per l'utente finale sia abilitato (sia in ESA che in SMA). In questo modo possono accedere al portale per la quarantena della posta indesiderata e, insieme al **rilascio/eliminazione** delle e-mail in quarantena, possono anche **aggiungere/eliminare** mittenti nell'elenco indirizzi attendibili.

L'accesso **alla quarantena per l'utente finale** può essere abilitato come indicato di seguito:

ESA: Selezionare **GUI > Monitoraggio > Quarantena posta indesiderata**. Archiviare il pulsante **di opzione** per **Accesso quarantena utente finale**. Selezionare il metodo di autenticazione per l'accesso in base ai requisiti (Nessuno/LDAP/SAML/IMAP o POP). Inviare il messaggio, abilitare elenco indirizzi attendibili/elenco indirizzi attendibili utente.

SMA: Selezionare **GUI > Centralized Services > Spam Quarantine (Quarantena posta indesiderata).** Archiviare il pulsante **di opzione** per **Accesso quarantena utente finale**. Selezionare il metodo di autenticazione per l'accesso in base ai requisiti (Nessuno/LDAP/SAML/IMAP o POP). Inviare il messaggio, abilitare elenco indirizzi attendibili/elenco indirizzi attendibili utente.

Una volta abilitato, quando un utente finale accede al portale di quarantena della posta indesiderata sarà in grado di **aggiungere/modificare il** proprio elenco di sicurezza, a scelta, dalle opzioni a discesa in alto a destra.



Mittenti attendibili con criteri di posta in arrivo

Èinoltre possibile aggiungere un mittente attendibile nei criteri della posta in arrivo e disattivare le analisi **antivirus/antispam** in base ai requisiti. È possibile creare un nuovo criterio di posta personalizzato con un nome, ad esempio **Mittenti attendibili/Mittenti attendibili** e così via, a seconda delle esigenze e quindi aggiungere i dettagli del mittente, ad esempio i nomi di dominio o gli indirizzi di posta elettronica del mittente, a questo criterio personalizzato.

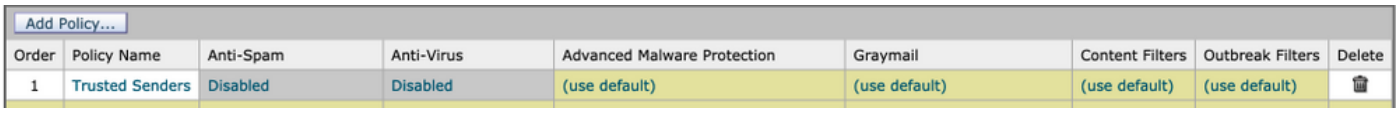
Una volta inviata la policy dopo l'aggiunta richiesta, è possibile fare clic sulle colonne **Antispam** o **Antivirus** e nella pagina successiva selezionare **Disabilita**.

Con questa configurazione, i domini dei mittenti attendibili o gli indirizzi di posta elettronica aggiunti a questo criterio di posta elettronica saranno esentati dalle analisi Antispam o Antivirus.

> **Nota:** I motori antispam e antivirus sono disabilitati e ignorano qualsiasi analisi relativa a spam o virus per i messaggi e-mail in arrivo nell'ESA elaborata tramite questo criterio di posta personalizzato. Questa operazione deve essere eseguita solo se si è totalmente certi che ignorare le scansioni per questi mittenti attendibili non comporta alcun rischio.

Il criterio di posta personalizzato può essere creato dalla **GUI ESA > Criteri di posta > Criteri di posta in arrivo > Aggiungi criterio**. Immettere il nome del criterio come da scelta, quindi selezionare **Aggiungi utente**. Selezionare il pulsante di opzione per i **Mittenti seguenti.** Aggiungere il dominio o gli indirizzi di posta elettronica richiesti nella casella e fare clic su **OK**.

Creazione di criteri post-posta, è possibile scegliere di disabilitare le analisi antivirus e antispam in base ai requisiti aziendali. Di seguito è riportato un esempio di schermata:



Informazioni correlate

- [Cisco Email Security Appliance - Guide per l'utente]
- [Documentazione e supporto tecnico – Cisco Systems]