Configurazione della configurazione Gold di Cloud Gateway

Sommario

Introduzione

Questo documento descrive un'analisi approfondita della configurazione Gold fornita per Cisco Secure Email Cloud Gateway.

Prerequisiti

Requisiti

Cisco raccomanda la conoscenza dei seguenti argomenti:

- Cisco Secure Email Gateway o Cloud Gateway, sia per l'amministrazione dell'interfaccia utente che della CLI
- Cisco Secure Email e Web Manager, amministrazione a livello di interfaccia utente
- I clienti Cisco Secure Email Cloud possono richiedere l'accesso CLI; vedere: Accesso CLI (Command Line Interface)

Componenti usati

Le informazioni di questo documento provengono dalla configurazione ottimale e dai consigli sulle best practice per i clienti e gli amministratori di Cisco Secure Email Cloud.

Le informazioni discusse in questo documento fanno riferimento a dispositivi usati in uno specifico ambiente di emulazione. Su tutti i dispositivi menzionati nel documento la configurazione è stata ripristinata ai valori predefiniti. Se la rete è operativa, valutare attentamente eventuali conseguenze derivanti dall'uso dei comandi.

Prodotti correlati

Il presente documento si applica anche a:

- Hardware locale o appliance virtuale Cisco Secure Email Gateway
- Hardware e appliance virtuale locale Cisco Secure Email e Web Manager

Quarantene

Le quarantene vengono configurate e gestite su Email e Web Manager per i clienti Cisco Secure Email Cloud. Accedere a Email e Web Manager per visualizzare le quarantene:

- ACQUISIZIONE_ACCOUNT
- ANTI_SPOOF
- ALLEGATI_BLOCCO
- BLOCKLIST
- DKIM_FAIL

- DMARC_QUARANTINE
- DMARC_RIFIUTA
- E-MAIL_FALSA
- CONTENUTO_INAPPROPRIATO
- MACRO
- OPEN_RELAY
- DATI_SDR
- SPF_HARDFAIL
- SPF_SOFTFAIL
- TG_OUTBOUND_MALWARE
- URL_DANNOSO

Configurazione Cloud Gateway Gold

Avviso: qualsiasi modifica apportata alle configurazioni in base alle best practice fornite in questo documento deve essere esaminata e compresa prima di eseguire il commit delle modifiche alla configurazione nell'ambiente di produzione. Consultare il tecnico Cisco CX, il DSM (Designated Service Manager) o l'Account Team prima di apportare modifiche alla configurazione.

Operazioni preliminari

La configurazione Gold per i clienti Cisco Secure Email cloud è la best practice e la configurazione a giorno zero sia per Cloud Gateway che per Cisco Secure Email e Web Manager. Le implementazioni Cisco Secure Email Cloud usano sia Cloud Gateway che almeno una (1) Email e Web Manager. Alcune parti della configurazione e delle procedure consigliate consentono agli amministratori di utilizzare la quarantena o le quarantene disponibili in Email and Web Manager per la gestione centralizzata.

Configurazione di base

Policy di posta > Tabella di accesso destinatari (RAT)

La tabella Accesso destinatario definisce i destinatari accettati da un listener pubblico. Nella tabella viene specificato almeno l'indirizzo e se accettarlo o rifiutarlo. Rivedi la RAT per aggiungere e gestire i tuoi domini secondo necessità.

Rete > Route SMTP

Se la destinazione della route SMTP è Microsoft 365, vedere Office365 Throttling CES New Instance con "4.7.500 Server occupato. Riprova più tardi".

Servizi di sicurezza

I servizi elencati sono configurati per tutti i clienti Cisco Secure Email Cloud con i valori forniti:

IPAS (IronPort Anti-Spam)

- Attivata e configurata Scansione costante da 1 MB e mai scansione da 2 MB
- Timeout per l'analisi di un singolo messaggio: 60 secondi

Filtro URL

- Abilitazione della categorizzazione URL e dei filtri per la reputazione
- (Facoltativo) Creare e configurare un elenco di URL consentiti denominato "bypass_urls".
- Abilita rilevamento interazione Web
- Impostazioni avanzate:
  - Timeout ricerca URL: 15 secondi
  - Numero massimo di URL analizzati nel corpo e nell'allegato: 400
  - Riscrivi testo URL e HREF nel messaggio: No
  - Registrazione URL: abilitata
- (Facoltativo) A partire dalla versione AsyncOS 14.2 for Cloud Gateway, sono disponibili il verdetto retrospettivo degli URL e la correzione degli URL. Vedere le note sulla versione fornite e configurare il filtro URL per Secure Email Gateway e Cloud Gateway

Rilevamento posta grigia

- Abilita e configura Scansione costante 1 MB e Nessuna scansione su 2 MB
- Timeout per l'analisi di un singolo messaggio: 60 secondi

Filtri epidemie

- Abilita regole adattive
- Dimensione massima messaggio da analizzare: 2 M
- Abilita rilevamento interazione Web

Protezione avanzata dal malware > Reputazione e analisi dei file

- Abilita reputazione file
- Abilita analisi file
  - Vedere Impostazioni globali per esaminare i tipi di file per l'analisi dei file

Verifica messaggi

- Abilita registrazione connessioni rifiutate (se richiesto)

Amministrazione del sistema

Utenti (Amministrazione sistema > Utenti)

- Ricorda di rivedere e impostare i criteri passphrase associati alle impostazioni account utente locale e passphrase
- Se possibile, configurare e abilitare il protocollo LDAP (Lightweight Directory Access Protocol) per l'autenticazione (Amministrazione sistema > LDAP)

Registra sottoscrizioni (Amministrazione sistema > Registra sottoscrizioni)

- Se non è configurato, creare e abilitare:
  - Log della cronologia della configurazione
  - Registri client reputazione URL
- In Impostazioni globali di registrazione sottoscrizioni modificare le impostazioni e aggiungere le intestazioni A, Da, Rispondi a, Mittente.

Configurazione aggiuntiva (opzionale)

Servizi aggiuntivi da esaminare e valutare:

Amministrazione sistema > LDAP

- Se si configura LDAP, Cisco consiglia LDAP con SSL abilitato

Difesa URL

- Per le best practice di configurazione più aggiornate per la difesa degli URL, vedere Configurazione del filtro URL per Secure Email Gateway e Cloud Gateway.
- Cisco analizza inoltre approfonditamente gli aspetti relativi alla difesa degli URL; consultare la Guida alla difesa degli URL.
- Nel presente documento sono inclusi anche alcuni esempi contenuti nella Guida alla difesa degli URL.

SPF

- I record DNS di Sender Policy Framework (SPF) vengono creati esternamente in Cloud Gateway. Pertanto, Cisco consiglia vivamente a tutti i clienti di integrare le best practice SPF, DKIM e DMARC nella propria postura di sicurezza. Per ulteriori informazioni sulla convalida di SPF, vedere Configurazione di SPF e procedure ottimali.
- Per i clienti Cisco Secure Email Cloud, viene pubblicata una macro per tutti i Cloud Gateway in base al nome host di allocazione per semplificare l'aggiunta di tutti gli host.
- Posizionare questo valore prima di ~all o -all all all'interno del record DNS TXT (SPF) corrente, se esistente:

```
exists:%{i}.spf.<allocation>.iphmx.com
```

Nota: assicurarsi che il record SPF termini con ~all o -all. Convalidare i record SPF dei domini prima e dopo qualsiasi modifica.

- Informazioni e strumenti consigliati per ulteriori informazioni su SPF:
  - Controllo record SPF - Ricerca SPF gratuita (dmarcian.com)
  - Tabella della sintassi dei record SPF - Everything SPF - dmarcian.com

Esempi aggiuntivi di SPF

- Un ottimo esempio di SPF è se si ricevono e-mail dal gateway del cloud e si inviano e-mail in uscita da altri server di posta. È possibile utilizzare il meccanismo "a:" per specificare gli host di posta:

<#root>

```
v=spf1 mx a:mail01.yourdomain.com a:mail99.yourdomain.com ~
all
```

- Se si inviano e-mail in uscita solo attraverso il Cloud Gateway, è possibile utilizzare:

<#root>

```
v=spf1 mx exists:%{i}.spf.<allocation>.iphmx.com ~
all
```

- Nell'esempio, il meccanismo "ip4:" o "ip6:" specifica un indirizzo IP o un intervallo di indirizzi IP:

<#root>

```
v=spf1 exists:%{i}.spf.<allocation>.iphmx.com ip4:192.168.0.1/16
~all
```

Modifiche a livello di CLI

- Come indicato in Prerequisiti, i clienti Cisco Secure Email Cloud possono richiedere l'accesso alla CLI; vedere Accesso all'interfaccia della riga di comando (CLI).

Filtro anti-spoof

- Consultare la Guida alle best practice per l'anti-spoofing
- Questa guida fornisce esempi approfonditi e best practice di configurazione per la prevenzione dello spoof dei messaggi di posta elettronica

Aggiungi filtro intestazione

- Solo CLI, scrivere e abilitare il filtro messaggi addHeaders:

```
addHeaders:  if (sendergroup != "RELAYLIST")
{
     insert-header("X-IronPort-RemoteIP", "$RemoteIP");
     insert-header("X-IronPort-MID", "$MID");
     insert-header("X-IronPort-Reputation", "$Reputation");
     insert-header("X-IronPort-Listener", "$RecvListener");
     insert-header("X-IronPort-SenderGroup", "$Group");
     insert-header("X-IronPort-MailFlowPolicy", "$Policy");
}
```

Tabella Accesso host (Policy di posta > Tabella Accesso host (HAT))

Panoramica HAT > Gruppi di mittenti aggiuntivi

- Guida utente ESA: creazione di un gruppo di mittenti per la gestione dei messaggi
  - BYPASS_SBRS - Posizionare più in alto per le origini che ignorano la reputazione
  - MY_TRUSTED_SPOOF_HOSTS - Parte del filtro di spoofing
  - TLS_REQUIRED - Per connessioni forzate TLS

Nel gruppo mittente SUSPECTLIST predefinito

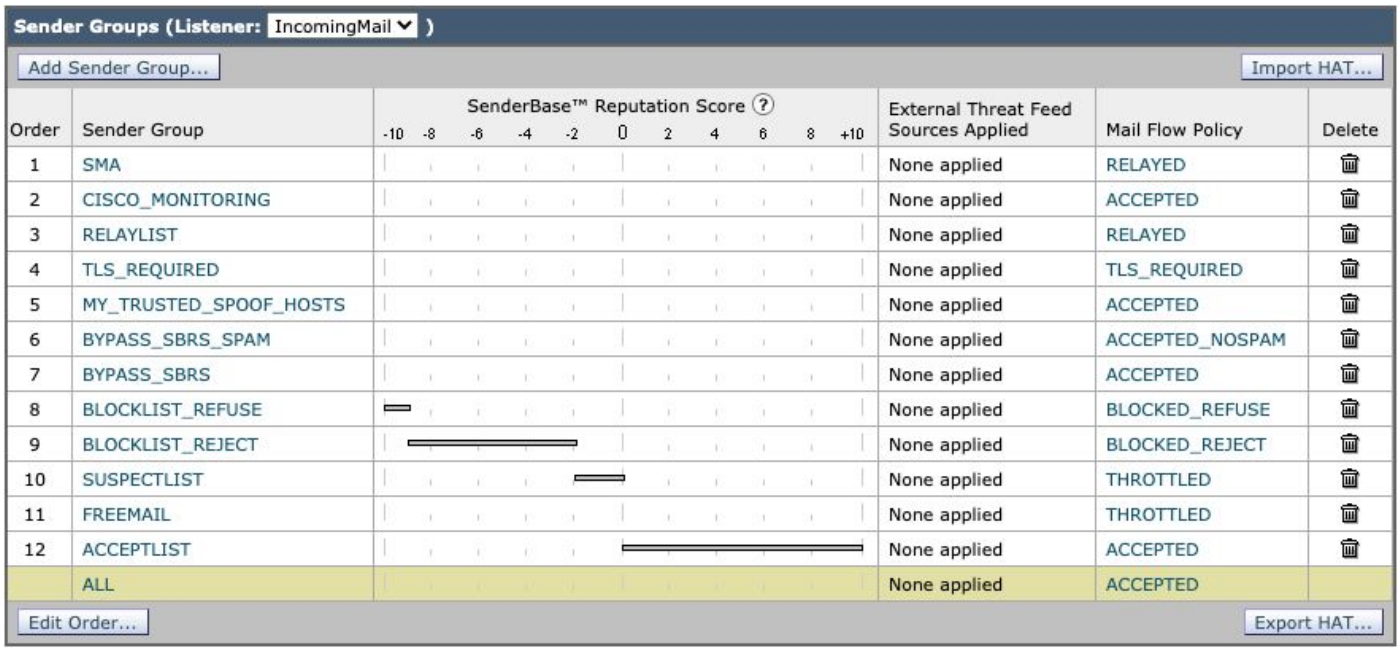
- Guida per l'utente ESA: Verifica del mittente: host
  - abilitare "Punteggi SBRS su nessuno".
  - (Facoltativo) abilitare "Connessione della ricerca dei record PTR dell'host non riuscita a causa di un errore DNS temporaneo."

Esempio di HAT aggressivo

- BLOCKLIST_REFUSE [-10.0 to -9.0] CRITERIO: BLOCKED_REFUSE
- CRITERIO BLOCKLIST_REJECT [-9.0 to -2.0]: BLOCKED_REJECT
- SUSPECTLIST [-2.0 a 0.0 e punteggi SBRS di "Nessuno"] POLICY: THROTTLED
- CRITERIO ACCEPTLIST [0.0-10.0]: ACCETTATO

Nota: gli esempi di HAT mostrano inoltre i criteri di flusso della posta (MFP) configurati. Per informazioni complete su MFP, fare riferimento a "Understanding the Email Pipeline > Incoming/Receiving" nel Manuale dell'utente per la versione appropriata di AsyncOS per Cisco Secure Email Gateway implementato.

Esempio:



Criterio flusso di posta (parametri dei criteri predefiniti)

Parametri criteri predefiniti

Impostazioni protezione

- Impostare Transport Layer Security (TLS) su Preferito
- Abilita struttura criteri mittente (SPF)
- Abilita DKIM (DomainKeys Identified Mail)
- Abilita autenticazione dei messaggi basata su dominio, creazione di report e verifica della conformità (DMARC) e invia report di feedback aggregati

Nota: DMARC richiede ulteriore ottimizzazione per la configurazione. Per ulteriori informazioni su DMARC, fare riferimento a "Email Authentication > DMARC Verification" (Autenticazione e-mail > Verifica DMARC) nel Manuale dell'utente per la versione appropriata di AsyncOS per Cisco Secure Email Gateway distribuito.

Criteri posta in arrivo

Il criterio predefinito è configurato in modo simile a:

Protezione da posta indesiderata

- Abilitato, con le soglie lasciate su quelle predefinite. (La modifica del punteggio potrebbe aumentare i falsi positivi.)

Antivirus

- Scansione messaggi: ricerca solo virus
  - Assicurarsi che la casella di controllo "Includi un'intestazione X" sia abilitata
- Per messaggi non analizzabili e messaggi infetti da virus, impostare Archivia messaggio originale su No

AMP

- Per Azioni non scansionabili sugli errori dei messaggi, utilizzare Advanced e Add Custom Header to Message, X-TG-MSGERROR, valore: True.
- Per Azioni non scansionabili sul limite di velocità, utilizzare Advanced e Add Custom Header to Message, X-TG-RATELIMIT, valore: True.
- Per i messaggi con analisi dei file in sospeso, utilizzare Azione applicata al messaggio: "Quarantena".

Graymail

- La scansione è abilitata per ogni verdetto (Marketing, Social, Bulk), con Anteprima per Aggiungi testo all'oggetto e azione è Consegna.
- Per Azione sulla posta inviata in blocco, utilizzare Avanzate e Aggiungi intestazione personalizzata (facoltativo): X-Bulk, valore: True.

Filtri dei contenuti

- Abilitato e URL_QUARANTINE_MALICIOUS, URL_REWRITE_SUSPICIOUS, URL_INAPPROPRIATE, DKIM_FAILURE, SPF_HARDFAIL, EXECUTIVE_SPOOF, DOMAIN_SPOOF, SDR, TG_RATE_LIMIT sono selezionati
- Questi filtri contenuti sono forniti più avanti in questa guida

Filtri epidemie

- Il livello di rischio predefinito è 3. Adattarsi ai requisiti di sicurezza.
  - Se il livello di minaccia di un messaggio è uguale o superiore a questa soglia, il messaggio viene spostato nella quarantena dell'epidemia. (1 = minaccia più bassa, 5 = minaccia più alta)
- Abilita modifica messaggi
- Riscrittura URL impostata su "Abilita per tutti i messaggi".
- Modifica Oggetto prima di: [Possibile $threat_category Frode]

Policies

Add Policy...

Order	Policy Name	Anti-Spam	Anti-Virus	Advanced Malware Protection	Graymail	Content Filters	Outbreak Filters	Advanced Phishing Protection	Delete
1	BLOCKLIST	Disabled	Disabled	(use default)	Disabled	BLOCKLIST_QUARANTINE	Disabled	(use default)	
2	ALLOWLIST	Disabled	(use default)	(use default)	Disabled	(use default)	Disabled	(use default)	
3	ALLOW_SPOOF	(use default)	(use default)	(use default)	(use default)	URL_QUARANTINE_MALICIOUS URL_REWRITE_SUSPICIOUS URL_INAPPROPRIATE SDR	(use default)	(use default)	
	Default Policy	IronPort Anti-Spam Positive: Drop Suspected: Quarantine	Sophos McAfee 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: Disabled Marketing: Deliver Social: Deliver Bulk: Deliver ...	URL_QUARANTINE_MALICIOUS URL_REWRITE_SUSPICIOUS URL_INAPPROPRIATE DKIM_FAILURE SPF_HARDFAIL EXECUTIVE_SPOOF ...	Retention Time: Virus: 1 day Other: 4 hours	Not Available	

Nomi criteri (visualizzati)

- Criterio di posta BLOCKLIST

  I criteri di posta BLOCKLIST sono configurati con tutti i servizi disabilitati, ad eccezione di Protezione avanzata da malware e sono collegati a un filtro contenuti con l'azione QUARANTENA.

- Criterio di posta ALLOWLIST

  Il criterio di posta ALLOWLIST dispone di Antispam, Graymail disabilitato e filtri contenuti abilitati per URL_QUARANTINE_MALICIOUS, URL_REWRITE_SUSPICIOUS, URL_INAPPROPRIATE, DKIM_FAILURE, SPF_HARDFAIL, EXECUTIVE SPOOF, DOMAIN_SPOOF, SDR, TG_RATE_LIMIT o filtri contenuti a scelta e configurazione.

- Criterio ALLOW_SPOOF Mail

  Per il criterio di posta ALLOW_SPOOF sono abilitati tutti i servizi predefiniti, con i filtri contenuti abilitati per URL_QUARANTINE_MALICIOUS, URL_REWRITE_SUSPICIOUS, URL_INAPPROPRIATE, SDR o i filtri contenuti a scelta e configurazione.

Criteri posta in uscita

Il criterio predefinito è configurato in modo simile a:

Protezione da posta indesiderata

- Disabled

Antivirus

- Scansione messaggi: ricerca solo virus
  - deselezionare la casella di controllo "Includi un'intestazione X".
- (Facoltativo) Per tutti i messaggi: Avanzate > Altre notifiche, abilitare "Altri" e includere l'indirizzo e-mail del contatto amministratore/SOC

Protezione avanzata da malware

- Abilita solo reputazione file
- Azioni non analizzabili sul limite di velocità: utilizzare Avanzate e aggiungere un'intestazione personalizzata al messaggio: X-TG-RATELIMIT, valore: "True".
- Messaggi con allegati malware: utilizzare Avanzate e aggiungere un'intestazione personalizzata al messaggio: X-TG-OUTBOUND, valore: "MALWARE DETECTED".

Graymail

- Disabled

Filtri dei contenuti

- Abilitato e sono selezionati i filtri TG_OUTBOUND_MALICIOUS, Strip_Secret_Header, EXTERNAL_SENDER_REMOVE, ACCOUNT_TAKEOVER o content.

Filtri epidemie

- Disabled

DLP

- Abilitare, in base alle licenze DLP e alla configurazione DLP.

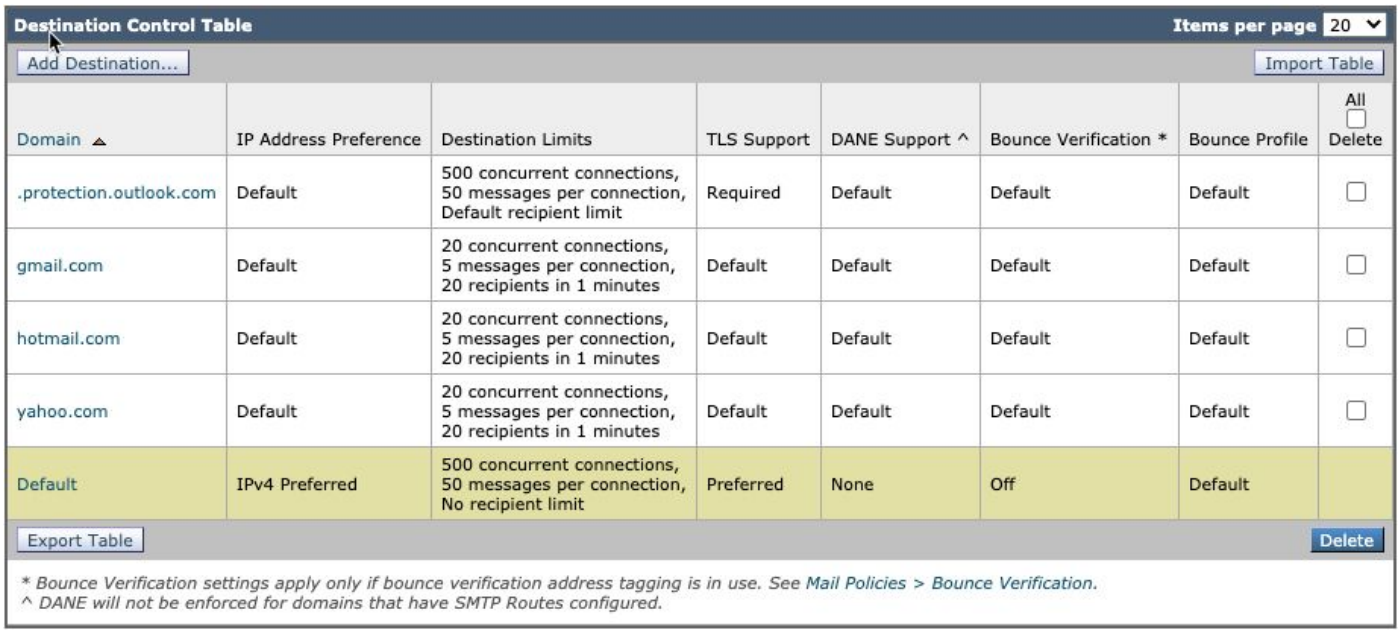
Altre impostazioni

Dizionari (Policy di posta > Dizionari)

- Abilita e rivedi dizionario Profanità e Contenuto_sessuale
- Creare il dizionario Executive_FED per il rilevamento di e-mail contraffatte con tutti i nomi dei dirigenti
- Creazione di dizionari aggiuntivi per parole chiave con restrizioni o di altro tipo in base alle esigenze di criteri, ambiente e controllo della protezione

Controlli destinazione (Mail Policies > Controlli destinazione)

- Per il dominio predefinito, configurare il supporto TLS come preferito
- È possibile aggiungere destinazioni per i domini di posta Web e impostare soglie inferiori
- Per ulteriori informazioni, vedere la guida Limita di velocità della posta in uscita con impostazioni di controllo di destinazione.



Destination Control Table — Items per page 20

Add Destination... | Import Table

Domain	IP Address Preference	Destination Limits	TLS Support	DANE Support ^	Bounce Verification *	Bounce Profile	All Delete
.protection.outlook.com	Default	500 concurrent connections, 50 messages per connection, Default recipient limit	Required	Default	Default	Default	
gmail.com	Default	20 concurrent connections, 5 messages per connection, 20 recipients in 1 minutes	Default	Default	Default	Default	
hotmail.com	Default	20 concurrent connections, 5 messages per connection, 20 recipients in 1 minutes	Default	Default	Default	Default	
yahoo.com	Default	20 concurrent connections, 5 messages per connection, 20 recipients in 1 minutes	Default	Default	Default	Default	
Default	IPv4 Preferred	500 concurrent connections, 50 messages per connection, No recipient limit	Preferred	None	Off	Default	

Export Table | Delete

* Bounce Verification settings apply only if bounce verification address tagging is in use. See Mail Policies > Bounce Verification.
^ DANE will not be enforced for domains that have SMTP Routes configured.

Filtri dei contenuti

Nota: per ulteriori informazioni sui filtri contenuti, consultare "Filtri contenuti" nel Manuale dell'utente per la versione appropriata di AsyncOS per Cisco Secure Email Gateway distribuito.

Filtri contenuti in arrivo

URL_QUARANTINE_MALICIOUS

Condizione: reputazione dell'URL; reputazione dell'URL(-10.00, -6.00 , "bypass_urls", 1, 1)

Azione: quarantena: quarantena("URL_MALICIOUS")

URL_REWRITE_SUSPICIOUS

Condizione: reputazione dell'URL; reputazione dell'URL (-5,90, -5,60 , "bypass_urls", 0, 1)

Azione: reputazione dell'URL; URL-reputation-proxy-redirect(-5,90, -5,60,"",0)

URL_NON APPROPRIATO

Condizione: Categoria dell'URL; categoria dell'URL (['Adult', 'Child Abuse Content', 'Extreme', 'Hate Speech', 'Illegal Activities', 'Illegal Downloads', 'Illegal Drugs', 'Pornography', 'Filter Avoidance'], "bypass_urls", 1, 1)

Azione: quarantena; duplicato-quarantena("INAPPROPRIATE_CONTENT")

ERRORE_DKIM

Condizione: autenticazione DKIM; autenticazione dkim == hardfail

Azione: quarantena; quarantena-duplicati("DKIM_FAIL")

SPF_HARDFAIL

Condizione: verifica SPF; spf-status = non riuscita

Azione: quarantena; duplicato-quarantena("SPF_HARDFAIL")

ESECUTIVO

Condizione: Forged Email Detection; forged-email-detection("Executive_FED", 90, "")

Condizione: Altra intestazione; header("X-IronPort-SenderGroup") != "(?i)allowspoof"

* set Apply rule: Solo se tutte le condizioni corrispondono

Azione: Aggiungi/Modifica intestazione; modifica-intestazione-testo("Subject", "(.*)", "[EXTERNAL]\\1")

Azione: quarantena; quarantena-duplicati("FORGED_EMAIL")

SPOOF_DOMINIO

Condizione: Altra intestazione; header("X-Spoof")

Azione: quarantena; duplicazione-quarantena("ANTI_SPOOF")

DSP

Condizione: reputazione del dominio; reputazione sdr (['awful'], "")

Condizione: Reputazione dominio; sdr-age ("giorni", <, 5, "")

* set Apply rule: Se una o più condizioni corrispondono

Azione: quarantena; duplicato-quarantena("SDR_DATA")

TG_RATE_LIMIT

Condizione: Altra intestazione; header("X-TG-RATELIMIT")

Azione: Aggiungi voce log; log-entry("X-TG-RATELIMIT: $filenames")

ELENCO_BLOCCHI_QUARANTENA

Condizione: (Nessuna)

Azione: quarantena; quarantena("BLOCKLIST")

Filters

Add Filter...

Order	Filter Name	Description | Rules | Policies	Duplicate	Delete
1	URL_QUARANTINE_MALICIOUS	URL_QUARANTINE_MALICIOUS: if (url-reputation(-10.00, -6.00 , "bypass_urls", 1, 1)) { quarantine("URL_MALICIOUS"); }		
2	URL_REWRITE_SUSPICIOUS	URL_REWRITE_SUSPICIOUS: if (url-reputation(-5.90, -5.60 , "bypass_urls", 0, 1)) { url-reputation-proxy-redirect(-5.90, -5.60,"",0); }		
3	URL_INAPPROPRIATE	URL_INAPPROPRIATE: if (url-category (['Adult', 'Child Abuse Content', 'Extreme', 'Hate Speech', 'Illegal Activities', 'Illegal Downloads', 'Illegal Drugs', 'Pornography', 'Filter Avoidance'], "bypass_urls", 1, 1)) { duplicate-quarantine("INAPPROPRIATE_CONTENT"); }		
4	DKIM_FAILURE	DKIM_FAILURE: if (dkim-authentication == "hardfail") { duplicate-quarantine("DKIM_FAIL"); }		
5	SPF_HARDFAIL	SPF_HARDFAIL: if (spf-status == "fail") { duplicate-quarantine("SPF_HARDFAIL"); }		
6	EXECUTIVE_SPOOF	EXECUTIVE_SPOOF: if (forged-email-detection("Executive_FED", 90, "")) AND (header("X-IronPort-SenderGroup") != "(?i)allowspoof") { edit-header-text("Subject", "(.*)", "[EXTERNAL]\\1"); duplicate-quarantine("FORGED_EMAIL"); }		
7	DOMAIN_SPOOF	DOMAIN_SPOOF: if (header("X-Spoof")) { duplicate-quarantine("ANTI_SPOOF"); }		
8	SDR	SDR: if (sdr-reputation (['awful'], "")) OR (sdr-age ("days", <, 5, "")) { duplicate-quarantine("SDR_DATA"); }		
9	TG_RATE_LIMIT	TG_RATE_LIMIT: if (header("X-TG-RATELIMIT")) { log-entry("X-TG-RATELIMIT: $filenames"); }		
10	BLOCKLIST_QUARANTINE	BLOCKLIST_QUARANTINE: if (true) { quarantine("BLOCKLIST"); }		
11	SAMPLE_ATTACHMENT_BLOCK	SAMPLE_ATTACHMENT_BLOCK: if (attachment-filetype == "Executable") OR (attachment-filename == "\\.(386|ad|ade|adp|asp|bas|bat|chm|cmd|com|cpl|crt|exe|hlp|hta|inf|ins|isp|js|jse|lnk|mdb|mde|msc|msi|msp|mst|pcd|pif|reg|scr|sct|shb|shs|url|vb|vbe|vbs|vss|vst|vsw|ws|wsc|wsf|wsh)$") { duplicate-quarantine("BLOCK_ATTACHMENTS"); drop(); }		
12	SAMPLE_SPF_SOFTFAIL	SAMPLE_SPF_SOFTFAIL: if (spf-status == "softfail") { duplicate-quarantine("SPF_SOFTFAIL"); }		
13	SAMPLE_MACRO	SAMPLE_MACRO: if (macro-detection-rule (['Adobe Portable Document Format', 'Microsoft Office Files', 'OLE File types'])) { quarantine("MACRO"); }		
14	SAMPLE_ATTACHMENT_PROTECTED	SAMPLE_ATTACHMENT_PROTECTED: if (attachment-protected) { log-entry("Encrypted: $MID"); }		
15	SAMPLE_LANGUAGE_UNKNOWN	SAMPLE_LANGUAGE_UNKNOWN: if (message-language == "unknown") { edit-header-text("Subject", "(.*)", "[SUSPICIOUS]\\1"); }		
16	SAMPLE_INAPPROPRIATE_CONTENT	SAMPLE_INAPPROPRIATE_CONTENT: if (dictionary-match("Profanity", 1)) OR (dictionary-match("Sexual_Content", 1)) { quarantine("INAPPROPRIATE_CONTENT"); }		
17	SAMPLE_REPLY-TO_MISMATCH	SAMPLE_REPLY-TO_MISMATCH: if (header("reply-to")) AND (header("reply-to") != "^$envelopefrom$") { add-heading("SAMPLE_REPLY-TO_WARN"); log-entry("REPLY-TO MISMATCH"); }		
18	SAMPLE_EXTERNAL_SENDER	SAMPLE_EXTERNAL_SENDER: if (subject != "[EXTERNAL]") { edit-header-text("Subject", "(.*)", "[EXTERNAL]\\1"); }		
19	SAMPLE_COUNTRY_FILTER	SAMPLE_COUNTRY_FILTER: if (geolocation-rule (['Canada'])) { log-entry("From Canada"); }		

Edit Filter Order...

Filtri contenuti in uscita

TG_OUTBOUND_MALICIOUS

Condizione: Altra intestazione; header("X-TG-OUTBOUND") == MALWARE

Azione: quarantena; quarantena("TG_OUTBOUND_MALWARE")

Strip_Secret_Header

Condizione: Altra intestazione; header("PLACEHOLDER") == PLACEHOLDER

Azione: Strip Header; strip-header("X-IronPort-Tenant")

ESTERNO_MITTENTE_RIMUOVI

Condizione: (Nessuna)

Azione: Aggiungi/Modifica intestazione; modifica-intestazione-testo("Subject", "\\[EXTERNAL\\]\\s?", "")

ACQUISIZIONE_ACCOUNT

Condizione: Altra intestazione; header("X-AMP-Result") == (?i)malicious

Condizione: reputazione dell'URL; reputazione-URL(-10.00, -6.00 , "", 1, 1)

*Impostare la regola di applicazione: se una o più condizioni corrispondono

Azione: Notify;notice ("<Indirizzo e-mail amministratore o destinatario>", "POSSIBILE ACQUISIZIONE ACCOUNT", "", "ACCOUNT_TAKEOVER_WARNING")

Azione: duplicate-quarantine("ACCOUNT_TAKEOVER")

Per i clienti Cisco Secure Email Cloud, abbiamo dei filtri di contenuto di esempio inclusi nella configurazione gold e nelle best practice consigliate. Consultare inoltre i filtri "SAMPLE_" per ulteriori informazioni sulle condizioni e le azioni associate che possono essere utili nella configurazione.

Cisco Live

Cisco Live ospita molte sessioni in tutto il mondo e offre sessioni di persona e interruzioni tecniche che coprono le best practice di Cisco Secure Email. Per le sessioni precedenti e l'accesso, visita Cisco Live (è necessario l'accesso CCO):

- Cisco Email Security: best practice e ottimizzazione - BRKSEC-2131

- DMARCate Your Email Perimeter - BRKSEC-2131
- Correzione dell'e-mail - Cisco Email Security - Risoluzione avanzata dei problemi - BRKSEC-3265
- Integrazioni delle API per Cisco Email Security - DEVNET-2326
- Protezione dei servizi delle caselle di posta SaaS con Cloud Email Security di Cisco - BRKSEC-1025
- Sicurezza e-mail: best practice e ottimizzazione - TECSEC-2345
- 250 non va bene - Sulla difensiva con Cisco Email Security - TECSEC-2345
- Cisco Domain Protection e Cisco Advanced Phishing Protection: come trarre il massimo vantaggio dal livello successivo di sicurezza della posta elettronica - BRKSEC-1243
- SPF non è l'acronimo di "Spoof"! Utilizziamo al meglio il livello successivo in Email Security! - DGTL-BRKSEC-2327

Se una sessione non è disponibile, Cisco Live si riserva il diritto di rimuoverla a causa dell'età della presentazione.

Ulteriori informazioni

Documentazione di Cisco Secure Email Gateway

- Note sulla release
- Guida dell'utente
- Guida di riferimento CLI
- Guide alla programmazione API per Cisco Secure Email Gateway
- Open Source utilizzato in Cisco Secure Email Gateway
- Guida all'installazione di Cisco Content Security Virtual Appliance (include vESA)

Documentazione su Secure Email Cloud Gateway

- Note sulla release
- Guida dell'utente

Documentazione di Cisco Secure Email e Web Manager

- Note sulla versione e matrice di compatibilità
- Guida dell'utente
- Guide alla programmazione API per Cisco Secure Email e Web Manager
- Guida all'installazione di Cisco Content Security Virtual Appliance (include vSMA)

Documentazione del prodotto Cisco Secure

- Architettura di denominazione del portafoglio Cisco Secure

Informazioni correlate

- Conformità a Cisco Secure Email Security
- Descrizione dell'offerta: email sicura
- Termini di Cisco Universal Cloud
- Supporto e download Cisco
- [EXTERNAL] OpenSPF: nozioni di base su SPF e informazioni avanzate

Informazioni su questa traduzione

Cisco ha tradotto questo documento utilizzando una combinazione di tecnologie automatiche e umane per offrire ai nostri utenti in tutto il mondo contenuti di supporto nella propria lingua. Si noti che anche la migliore traduzione automatica non sarà mai accurata come quella fornita da un traduttore professionista. Cisco Systems, Inc. non si assume alcuna responsabilità per l’accuratezza di queste traduzioni e consiglia di consultare sempre il documento originale in inglese (disponibile al link fornito).