Informazioni sui parametri correlati ai criteri di flusso della posta e ai controlli di destinazione

Sommario

Introduzione

Questo documento descrive un paio di aspetti della configurazione di Email Security Appliance (ESA) per come limitare/limitare i mittenti e recapitare i messaggi. Le funzionalità che verranno descritte nell'articolo sono Mail Flow Policies e Destination Controls.

Prerequisiti

Requisiti

Cisco raccomanda la conoscenza dei seguenti argomenti:

- Informazioni di base sui criteri di flusso della posta e sui controlli di destinazione
- Familiarità con l'uso di queste funzioni nella configurazione dell'ESA

Componenti usati

Il documento può essere consultato per tutte le versioni software o hardware.

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.

Vantaggi dei criteri di flusso della posta e dei controlli di destinazione

C'è una funzione molto importante che entrambe queste funzioni hanno, e che è Limitazione di Velocità / Limitazione di Velocità. Questo aspetto aiuta l'amministratore a controllare quale traffico deve scorrere liberamente e quale deve essere autorizzato con restrizioni.

Criteri flusso di posta

Queste sono le policy che si applicano ai Gruppi di Mittenti dell'ESA, sulla base dei quali viene fatta la modulazione del traffico di posta elettronica.

I criteri del flusso di posta si applicano sempre al traffico in entrata nell'ESA, a prescindere dal fatto che l'e-mail sia in entrata o in uscita.

I criteri di flusso della posta funzionano nel back-end in relazione al comportamento di connessione selezionato per il criterio. Le diverse modalità di connessione disponibili nelle ESA sono:

1. Accetta
2. Rifiuta
3. Relè
4. Rifiuto TCP
5. Continua

Accetta: La connessione viene accettata e l'accettazione della posta elettronica viene ulteriormente limitata dalle impostazioni del listener, inclusa la tabella Accesso destinatario (per i listener pubblici). Questo comportamento di connessione considera un messaggio di posta elettronica come in ingresso

Rifiuta: Il client che tenta di connettersi ottiene un codice di stato SMTP 4XX o 5XX. Nessun messaggio di posta elettronica accettato. Utilizzato principalmente per i mittenti delle liste nere

Inoltro: Connessione accettata. La ricezione per qualsiasi destinatario è consentita e non è vincolata dalla tabella Accesso destinatario. Tratta un messaggio di posta elettronica come in uscita

Rifiuto TCP: Connessione rifiutata a livello TCP.

Continua: La mappatura nell'HAT viene ignorata e l'elaborazione dell'HAT continua. Se la connessione in ingresso corrisponde a una voce successiva che non è CONTINUA, verrà utilizzata tale voce. La regola CONTINUE (CONTINUA) viene utilizzata per facilitare la modifica dell'HAT nella GUI.

Componenti di un criterio flusso di posta

Max Messaggi per connessione: Il numero massimo di messaggi che possono essere inviati tramite questo listener per connessione da un host remoto. Ogni ICID rappresenta una connessione

Max Destinatari per messaggio: Numero massimo di destinatari per messaggio che verranno accettati da questo host ed elaborati utilizzando i criteri di flusso della posta

Max Dimensione messaggio: La dimensione massima di un messaggio che verrà accettato da questo listener con tag nei criteri del flusso di posta. La dimensione massima più piccola possibile per i messaggi è 1 kilobyte.

Max Connessioni simultanee da un singolo IP: Il numero massimo di connessioni simultanee consentite per connettersi a questo listener da un singolo indirizzo IP.

Codice banner SMTP personalizzato: Il codice SMTP restituito quando viene stabilita una connessione con questo listener.

Testo banner SMTP personalizzato: Il testo del banner SMTP restituito quando viene stabilita una connessione con questo listener. In questo campo è possibile utilizzare alcune variabili.

Ignora nome host banner SMTP: per impostazione predefinita, l'accessorio includerà il nome host associato all'interfaccia del listener durante la visualizzazione del banner SMTP sugli host remoti (ad esempio, 220-hostname ESMTP). Puoi scegliere di ignorare questo banner immettendo un nome host diverso qui. Inoltre, è possibile lasciare vuoto il campo hostname (nome host) per scegliere di *non* visualizzare un nome host nell'intestazione.

Limiti flusso di posta

Max Destinatari all'ora: Il numero massimo di destinatari all'ora che questo listener riceverà da un host remoto. Il numero di destinatari per indirizzo IP mittente viene rilevato globalmente. Ogni listener tiene traccia della propria soglia di limitazione della velocità, tuttavia, poiché tutti i listener convalidano su un singolo contatore, è più probabile che il limite di velocità venga superato se lo stesso indirizzo IP (mittente) si connette a più listener. In questo campo è possibile utilizzare alcune variabili.

Max Codice destinatario all'ora: Il codice SMTP restituito quando un host supera il numero massimo di destinatari all'ora definito per questo listener.

Max Testo Destinatari all'ora: Il testo del banner SMTP restituito quando un host supera il numero massimo di destinatari all'ora definito per questo listener.

Limite di velocità per i mittenti della busta

Max Destinatari per intervallo di tempo: Il numero massimo di destinatari durante un periodo di tempo specificato che questo listener riceverà da un mittente di busta univoco, in base all'indirizzo di provenienza della posta. Il numero di destinatari viene registrato globalmente. Ogni listener tiene traccia della propria soglia di limitazione della velocità; tuttavia, poiché tutti i listener eseguono la convalida su un singolo contatore, è più probabile che il limite di velocità venga superato se i messaggi provenienti dallo stesso indirizzo di posta elettronica vengono ricevuti da più listener.

Codice errore limite velocità mittente: Il codice SMTP restituito quando una busta supera il numero massimo di destinatari per l'intervallo di tempo definito per questo listener.

Testo errore limite velocità mittente: Il testo del banner SMTP restituito quando un mittente della busta supera il numero massimo di destinatari per l'intervallo di tempo definito per questo listener.

Eccezioni: Se si desidera esentare alcuni mittenti di buste dal limite di velocità definito, selezionare un elenco indirizzi contenente i mittenti delle buste.

L'elenco di indirizzi viene definito da Criteri di posta elettronica a Elenco indirizzi (indirizzi di posta elettronica completi, Domini, Indirizzi IP possono essere utilizzati per le esenzioni)

Usa SenderBase per controllo del flusso: Abilitare le "ricerche" nel servizio SenderBase Reputation per questo listener.

Raggruppa per somiglianza di indirizzi IP: Utilizzato per tenere traccia della posta in arrivo e limitarne la velocità in base all'indirizzo IP, gestendo le voci nella tabella HAT (Host Access Table) di un listener in blocchi CIDR di grandi dimensioni. È possibile definire un intervallo di bit significativi (da 0 a 32) in base al quale raggruppare indirizzi IP simili per limitare la velocità, mantenendo comunque un contatore individuale per ogni indirizzo IP compreso in tale intervallo.

NOTA: Richiede la disabilitazione di "Use SenderBase".

Prevenzione degli attacchi Directory Harvest (DHAP)

Max Destinatari non validi all'ora: Numero massimo di destinatari non validi all'ora che il listener riceverà da un host remoto. Questa soglia rappresenta il numero totale di rifiuti RAT e di rifiuti del server di call-ahead SMTP combinati con il numero totale di messaggi inviati a destinatari LDAP non validi eliminati nella conversazione SMTP o rimbalzati nella coda di lavoro (come configurato nelle impostazioni di accettazione LDAP sul listener associato).

Elimina connessione se la soglia DHCP viene raggiunta in una conversazione SMTP:

Se viene raggiunta la soglia dei destinatari non validi, l'accessorio interromperà la connessione a un host.

Max Codice destinatario non valido all'ora: Specificare il codice da utilizzare quando si eliminano le connessioni. Il codice predefinito è 550.

Max Testo destinatari non validi all'ora: Specificare il testo da utilizzare per le connessioni interrotte. Il testo predefinito è "Troppi destinatari non validi.

Funzionalità di sicurezza

Verifica della reputazione del dominio di invio/verifica dei filtri epidemie/protezione avanzata dal phishing/Graymail/filtri contenuti e messaggi di posta indesiderata: Da qui è possibile abilitare o disabilitare la scansione dei motori di sicurezza/filtri e la relativa scansione

Crittografia e autenticazione: È possibile modificare le impostazioni come Disattivato, Preferito o Richiedi TLS (Transport Layer Security) nelle conversazioni SMTP per questo listener.

L'opzione Verifica certificato client indica all'appliance Email Security di stabilire una connessione TLS all'applicazione di posta elettronica dell'utente se il certificato client è valido.

Per il livello preferito TLS, l'accessorio consente comunque una connessione non TLS se l'utente non dispone di un certificato, ma rifiuta una connessione se l'utente dispone di un certificato non valido.

Se si seleziona questa opzione per l'impostazione TLS obbligatorio, l'utente dovrà disporre di un certificato valido affinché l'accessorio consenta la connessione.

Autenticazione SMTP: Consente, non consente o richiede l'autenticazione SMTP dagli host remoti che si connettono al listener

Se sono abilitate sia l'autenticazione TLS che l'autenticazione SMTP: Richiedi TLS per offrire autenticazione SMTP

Chiave di dominio/firma DKIM: Abilita chiavi di dominio o firma DKIM su questo listener

Verifica DKIM: Abilita verifica DKIM.

Verifica/decrittografia S/MIME: Abilita la decrittografia o la verifica S/MIME.

Firma dopo l'elaborazione: Scegliere se conservare o rimuovere la firma digitale dai messaggi dopo la verifica S/MIME.

Recupero chiavi pubbliche S/MIME: Abilita la raccolta della chiave pubblica S/MIME.

Certificati di raccolta in caso di errore di verifica: Scegliere se raccogliere le chiavi pubbliche se la verifica dei messaggi firmati in ingresso non riesce.

Archivia certificato aggiornato: Scegliere se raccogliere le chiavi pubbliche aggiornate

Verifica SPF/SIDF: Abilitare la firma SPF/SIDF su questo listener.

Livello di conformità : Impostare il livello di conformità SPF/SIDF. È possibile scegliere tra SPF, SIDF o compatibile con SIDF

Declassa risultato verifica PRA se sono stati utilizzati 'Resent-Sender:' o 'Resent-From:': Se si sceglie un livello di conformità compatibile con SIDF, specificare se si desidera declassare il risultato della verifica dell'identità PRA a Nessuno se è presente Resent-Sender: o inviato da: intestazioni presenti nel messaggio

Test HELO: Configurare se si desidera eseguire un test in base all'identità HELO (da utilizzare per i livelli di conformità compatibili con SPF e SIDF)

Verifica DMARC: Abilita verifica DMARC su questo listener

Usa profilo di verifica DMARC: Selezionare il profilo di verifica DMARC da utilizzare sul listener. Lo stesso viene creato da Mail Policies —> DMARC —> Add Profile

Report di feedback DMARC: Abilita l'invio di report di feedback aggregati DMARC.

Verifica Rimbalzo

Considera validi i limiti senza tag: Si applica solo se è abilitata l'etichettatura di verifica dei rimbalzi. Per impostazione predefinita, l'accessorio considera non validi i rimbalzi senza tag e rifiuta il rimbalzo oppure aggiunge un'intestazione personalizzata, a seconda delle impostazioni di Verifica rimbalzo. Se si sceglie di considerare validi i rimbalzi senza tag, l'accessorio accetta il messaggio di rimbalzo.

Verifica mittente

Verifica DNS mittente busta:

Èpossibile che i mittenti non vengano verificati per motivi diversi. I mittenti non verificati sono classificati nelle seguenti categorie:

- Il record PTR dell'host connesso non esiste nel DNS.
- La connessione della ricerca dei record PTR dell'host non è riuscita a causa di un errore DNS temporaneo.
- La connessione della ricerca DNS inversa dell'host (PTR) non corrisponde alla ricerca DNS diretta (A).

Possiamo abilitare o disabilitare la funzione di verifica del mittente.

Usa tabella eccezioni verifica mittente: È possibile utilizzare la tabella delle eccezioni del dominio di verifica mittente per consentire le esenzioni. È possibile avere una sola tabella eccezioni, ma è possibile abilitarla per ogni criterio del flusso di posta.

La tabella Eccezioni può essere creata da Criteri di posta elettronica —> Tabella Eccezioni verifica mittente —> Aggiungi eccezione verifica mittente

Controlli di destinazione

Questa funzionalità controlla le consegne dei messaggi e-mail. Tutte le e-mail che terminano l'elaborazione attraverso le ESA e stanno per uscire dalle ESA per ulteriori consegne possono essere controllate attraverso la funzione Controlli di destinazione.

Il profilo Controlli destinazione **predefiniti** si applica a tutte le consegne. Nel caso in cui sia necessario effettuare controlli di consegna specifici del dominio, è necessario creare un profilo personalizzato per i controlli di destinazione.

Componenti di un profilo Controlli destinazione

Limiti

Connessioni simultanee: Numero di connessioni simultanee (DCID) agli host remoti che l'accessorio tenterà di aprire per completare la consegna.

Numero di messaggi massimo per connessione: Numero di messaggi che l'ESA invierà a un dominio di destinazione tramite una connessione (DCID) prima che l'accessorio avvii una nuova

connessione.

Destinatari: Numero di destinatari che l'accessorio invierà a un determinato host remoto in un determinato periodo di tempo.

Applica limiti: Questi aspetti aiutano a decidere come applicare i limiti che abbiamo specificato per ogni destinazione e per nome host MGA.

Supporto TLS

In questo modo è possibile decidere se le connessioni TLS agli host remoti verranno impostate su Nessuno / Preferito / Richiesto

Supporto DANE: Se DANE viene configurato come 'Opportunistico' e l'host remoto non supporta DANE, per la crittografia delle conversazioni SMTP è preferibile utilizzare TLS opportunistico.

Se si configura DANE come 'Obbligatorio' e l'host remoto non supporta DANE, non verrà stabilita alcuna connessione all'host di destinazione.

Se si configura DANE come 'Obbligatorio' o 'Opportunistico' e l'host remoto supporta DANE, è preferibile crittografare le conversazioni SMTP.

NOTA: DANE non verrà applicato per i domini in cui sono configurate route SMTP.

Verifica Rimbalzo

Questo aiuta a decidere se eseguire o meno l'etichettatura dell'indirizzo del mittente della busta (prvs-xxxxxx-xxxx) tramite la verifica del rimbalzo.

La verifica dei rimbalzi può essere configurata da Mail Policies —> Verifica rimbalzi —> Aggiungi nuova chiave

Profilo rimbalzo

Il profilo di rimbalzo può essere utilizzato dall'accessorio per un determinato host remoto. Decide per quanto tempo un'e-mail sarà conservata nella Coda di Consegna dell'ESA in caso di problemi di consegna, prima che un'e-mail venga spedita via cavo

Il profilo di rimbalzo viene impostato tramite Rete —> Profili rimbalzo

Impostazioni globali

Certificato: In questo aspetto vengono definiti i certificati da utilizzare per stabilire le connessioni SSL/TLS durante l'avvio delle consegne e-mail all'hop successivo. Si consiglia sempre di utilizzare un certificato firmato da un'Autorità di certificazione (CA) in questo aspetto.

Invia un avviso quando una connessione TLS richiesta non riesce: è possibile specificare se l'accessorio deve inviare un avviso se la negoziazione TLS non riesce durante il recapito dei messaggi a un dominio che richiede una connessione TLS. Il messaggio di avviso contiene il

nome del dominio di destinazione per la negoziazione TLS non riuscita. L'accessorio invia il messaggio di avviso a tutti i destinatari impostati per ricevere gli avvisi sul livello di gravità **Avviso** per i tipi di **avviso Sistema**.

Èpossibile gestire i destinatari degli avvisi tramite Amministrazione sistema —> Avvisi