Kennenlernen von Parametern für Mail Flow-Richtlinien und Zielsteuerelemente

Inhalt

Einführung

Dieses Dokument beschreibt eine Reihe von Konfigurationsaspekten der E-Mail Security Appliance (ESA) zur Vorgehensweise beim Überschreiten/Durchsatzbegrenzung von Sendern und bei der Zustellung. Die im Artikel beschriebenen Features sind Mail Flow Policies (Mail-Fluss-Richtlinien) und Destination Controls (Zielsteuerelemente).

Voraussetzungen

Anforderungen

Cisco empfiehlt, dass Sie über Kenntnisse in folgenden Bereichen verfügen:

- Grundlegendes Verständnis von Mail Flow-Richtlinien und Zielsteuerelementen
- Vertrautheit mit der Verwendung dieser Funktionen in der ESA-Konfiguration

Verwendete Komponenten

Dieses Dokument ist nicht auf bestimmte Software- und Hardware-Versionen beschränkt.

Die Informationen in diesem Dokument beziehen sich auf Geräte in einer speziell eingerichteten Testumgebung. Alle Geräte, die in diesem Dokument benutzt wurden, begannen mit einer gelöschten (Nichterfüllungs) Konfiguration. Wenn Ihr Netzwerk in Betrieb ist, stellen Sie sicher, dass Sie die potenziellen Auswirkungen eines Befehls verstehen.

Vorteile von Mail Flow-Richtlinien und Zielsteuerelementen

Beide Funktionen bieten eine sehr wichtige Funktion: Durchsatzbegrenzung/Drosselung. Auf diese Weise kann der Administrator kontrollieren, welcher Datenverkehr frei fließen soll und welcher mit Einschränkungen zugelassen werden soll.

Mail Flow-Richtlinien

Dies sind die Richtlinien, die für die Absendergruppen der ESA gelten, auf deren Grundlage die Modulation des E-Mail-Datenverkehrs erfolgt.

Mail Flow-Richtlinien gelten immer für Datenverkehr, der an die ESA eingeht, unabhängig davon, ob es sich bei der E-Mail um eine eingehende oder ausgehende E-Mail handelt.

Die Mail Flow Policies (Mail-Flow-Richtlinien) funktionieren im Backend hinsichtlich des ausgewählten Verbindungsverhaltens für diese Richtlinie. Die verschiedenen Verbindungsverhalten, die in ESAs verfügbar sind, sind:

1. Akzeptieren
2. Ablehnen
3. Relay
4. TCP verweigern
5. Weiter

Akzeptieren: Die Verbindung wird akzeptiert, und die E-Mail-Annahme wird dann durch die Listener-Einstellungen weiter eingeschränkt, einschließlich der Recipient Access Table (für öffentliche Listener). Dieses Verbindungsverhalten behandelt eine E-Mail als eingehend.

Ablehnen: Der Client, der versucht, eine Verbindung herzustellen, erhält einen SMTP-Statuscode 4XX oder 5XX. Es wird keine E-Mail akzeptiert. Dies wird hauptsächlich für Blacklisting-Absender verwendet.

Relay: Verbindung wird akzeptiert. Die Annahme für einen beliebigen Empfänger ist zulässig und nicht durch die Recipient Access Table beschränkt. Dadurch wird eine E-Mail als ausgehende E-Mail behandelt.

TCP verweigern: Die Verbindung wird auf TCP-Ebene verweigert.

Weiter: Die Zuordnung in der HAT wird ignoriert, und die Verarbeitung der HAT wird fortgesetzt. Wenn die eingehende Verbindung mit einem späteren Eintrag übereinstimmt, der nicht CONTINUE ist, wird stattdessen dieser Eintrag verwendet. Die CONTINUE-Regel wird verwendet, um die Bearbeitung der HAT in der GUI zu vereinfachen.

Komponenten einer Mail Flow Policy

Max. Nachrichten pro Verbindung: Die maximale Anzahl von Nachrichten, die über diesen Listener pro Verbindung von einem Remotehost gesendet werden können. Jede ICID stellt eine Verbindung dar.

Max. Empfänger pro Nachricht: Die maximale Anzahl von Empfängern pro Nachricht, die von diesem Host akzeptiert wird und mit dieser Mail Flow Policy verarbeitet wird

Max. Nachrichtengröße: Die maximale Größe einer Nachricht, die von diesem Listener akzeptiert wird, der in die Mail Flow Policy getaggt ist. Die kleinstmögliche maximale Nachrichtengröße beträgt 1 Kilobyte.

Max. Gleichzeitige Verbindungen von einer einzigen IP: Die maximale Anzahl gleichzeitiger Verbindungen, die von einer einzigen IP-Adresse aus mit diesem Listener verbunden werden können.

Benutzerdefinierter SMTP-Bannercode: Der SMTP-Code, der zurückgegeben wird, wenn eine Verbindung mit diesem Listener hergestellt wird.

Benutzerdefinierter SMTP Banner-Text: Der SMTP-Bannertext wird zurückgegeben, wenn eine Verbindung mit diesem Listener hergestellt wird. In diesem Feld können Sie einige Variablen verwenden.

Überschreiben des SMTP-Banner-Hostnamens: Standardmäßig enthält die Appliance den Hostnamen, der der Schnittstelle des Listeners zugeordnet ist, wenn das SMTP-Banner auf Remotehosts angezeigt wird (z. B. ESMTP mit dem 220-Hostnamen). Sie können dieses Banner überschreiben, indem Sie hier einen anderen Hostnamen eingeben. Zusätzlich können Sie das Feld Hostname leer lassen, um *nicht* einen Hostnamen im Banner anzuzeigen.

E-Mail-Flow-Limits

Max. Empfänger pro Stunde: Die maximale Anzahl von Empfängern pro Stunde, die dieser Listener von einem Remotehost erhält. Die Anzahl der Empfänger pro Absender-IP-Adresse wird global verfolgt. Jeder Listener verfolgt seinen eigenen Grenzwert für die Durchsatzbegrenzung. Da jedoch alle Listener einen einzigen Zähler validieren, ist es wahrscheinlicher, dass der Durchsatzbegrenzer überschritten wird, wenn dieselbe IP-Adresse (Sender) eine Verbindung zu mehreren Listenern herstellt. In diesem Feld können Sie einige Variablen verwenden.

Max. Empfänger pro Stunde Code: Der SMTP-Code, der zurückgegeben wird, wenn ein Host die für diesen Listener definierte maximale Anzahl von Empfängern pro Stunde überschreitet.

Max. Empfänger pro Stunde Text: Der SMTP-Bannertext, der zurückgegeben wird, wenn ein Host die für diesen Listener festgelegte maximale Anzahl von Empfängern pro Stunde überschreitet.

Übertragungsratenlimit für Umschlagabsender

Max. Intervall für Empfänger pro Zeit: Die maximale Anzahl von Empfängern während eines bestimmten Zeitraums, die dieser Listener von einem eindeutigen Umschlagabsender erhält, basierend auf der E-Mail-von-Adresse. Die Anzahl der Empfänger wird global verfolgt. Jeder Listener verfolgt seinen eigenen Grenzwert für die Ratenbegrenzung. Da jedoch alle Listener für einen einzigen Zähler validieren, ist es wahrscheinlicher, dass die Durchsatzbegrenzung überschritten wird, wenn Nachrichten derselben E-Mail-Absenderadresse von mehreren Listenern

empfangen werden.

Fehlercode zur Beschränkung der Absenderrate: Der SMTP-Code, der zurückgegeben wird, wenn ein Umschlag die maximale Anzahl von Empfängern für das für diesen Listener definierte Zeitintervall überschreitet.

Absenderratenlimitierungstext: Der SMTP-Bannertext, der zurückgegeben wird, wenn ein Umschlagabsender die maximale Anzahl von Empfängern für das für diesen Listener definierte Zeitintervall überschreitet.

Ausnahmen: Wenn Sie möchten, dass bestimmte Umschlagabsender von der festgelegten Ratenbeschränkung ausgenommen werden, wählen Sie eine Adressliste aus, die die Umschlagabsender enthält.

Die Adressliste ist aus Mail-Policys in Adresslisten definiert (vollständige E-Mail-Adressen, Domänen, IP-Adressen können für Ausnahmen verwendet werden).

SenderBase für Flusssteuerung verwenden: Aktivieren Sie "Lookups" zum SenderBase-Reputationsdienst für diesen Listener.

Nach ähnlichen IP-Adressen gruppieren: Wird verwendet, um eingehende E-Mails auf Basis von IP-Adressen nachzuverfolgen und zu begrenzen und gleichzeitig Einträge in der Host Access Table (HAT) eines Listeners in großen CIDR-Blöcken zu verwalten. Sie definieren einen Bereich signifikanter Bits (von 0 bis 32), um ähnliche IP-Adressen für die Zwecke der Ratenbegrenzung zu gruppieren, wobei jedoch ein einzelner Zähler für jede IP-Adresse innerhalb dieses Bereichs beizubehalten ist.

HINWEIS: Erfordert die Deaktivierung von "SenderBase verwenden".

Directory Harvest Attack Prevention (DHAP)

Max. Ungültige Empfänger pro Stunde: Die maximale Anzahl ungültiger Empfänger pro Stunde, die dieser Listener von einem Remotehost erhält. Dieser Grenzwert stellt die Gesamtzahl der RAT-Ablehnungen und der Absagen des SMTP-Anrufvorgangs-Servers zusammen mit der Gesamtzahl der Nachrichten an ungültige LDAP-Empfänger dar, die in der SMTP-Konversation verworfen oder in der Arbeitswarteschlange abgesetzt wurden (wie im LDAP konfiguriert, werden die Einstellungen des zugeordneten Listeners akzeptiert).

Verbindung verwerfen, wenn der DHAP-Grenzwert innerhalb eines SMTP-Gesprächs erreicht wird:

Die Appliance verwirft eine Verbindung zu einem Host, wenn der Grenzwert für ungültige Empfänger erreicht ist.

Max. Ungültiger Empfänger pro Stunde-Code: Geben Sie den Code an, der beim Verwerfen von Verbindungen verwendet werden soll. Der Standardwert ist 550.

Max. Ungültiger Text für Empfänger pro Stunde: Geben Sie den Text für getrennte Verbindungen an. Der Standardtext lautet "Zu viele ungültige Empfänger.

Sicherheitsfunktionen

Spam/AMP/Virus/Absender-Domänenreputations-Verifizierung/Outbreak-Filter/Advanced Phishing Protection/Graymail/Content- und Nachrichtenfilter: Die Sicherheits-Engines/Scanning und die zugehörigen Scans von Filtern können hier aktiviert oder deaktiviert werden.

Verschlüsselung und Authentifizierung: In SMTP-Konversationen für diesen Listener können die Einstellungen als Off, Prefer (Bevorzugen) oder Require Transport Layer Security (TLS) geändert werden.

Die Option "Verify Client Certificate" (Client-Zertifikat verifizieren) weist die E-Mail-Security-Appliance an, eine TLS-Verbindung zur E-Mail-Anwendung des Benutzers herzustellen, wenn das Client-Zertifikat gültig ist.

Für TLS Preferred lässt die Appliance auch dann eine Nicht-TLS-Verbindung zu, wenn der Benutzer über kein Zertifikat verfügt. Wenn der Benutzer jedoch über ein ungültiges Zertifikat verfügt, lehnt sie jedoch eine Verbindung ab.

Für die Einstellung "TLS Required" (TLS erforderlich) ist für diese Option ein gültiges Zertifikat erforderlich, damit die Appliance die Verbindung zulassen kann.

SMTP-Authentifizierung: Ermöglicht, deaktiviert oder erfordert die SMTP-Authentifizierung von Remotehosts, die mit dem Listener verbunden sind

Wenn sowohl TLS- als auch SMTP-Authentifizierung aktiviert ist: TLS erforderlich, um SMTP-Authentifizierung anzubieten

Domänenschlüssel/DKIM-Signierung: Aktivieren von Domänenschlüsseln oder DKIM-Signierung auf diesem Listener

DKIM-Verifizierung: Aktivieren Sie die DKIM-Überprüfung.

S/MIME-Entschlüsselung/Überprüfung: Aktivieren Sie die S/MIME-Entschlüsselung oder -Überprüfung.

Unterschrift nach Verarbeitung: Legen Sie fest, ob die digitale Signatur nach der S/MIME-Überprüfung aus den Nachrichten beibehalten oder entfernt werden soll.

Harvesting für öffentlichen S/MIME-Schlüssel: Aktivieren Sie das Sammeln von öffentlichen S/MIME-Schlüsseln.

Erntezertifikate bei Prüffehler: Wählen Sie aus, ob öffentliche Schlüssel gesammelt werden sollen, wenn die Überprüfung der eingehenden signierten Nachrichten fehlschlägt.

Aktualisiertes Zertifikat speichern: Wählen Sie, ob aktualisierte öffentliche Schlüssel gesammelt werden sollen.

SPF/SIDF-Verifizierung: Aktivieren Sie die SPF/SIDF-Signierung auf diesem Listener.

Konformitätsstufe: Legen Sie die SPF/SIDF-Konformitätsstufe fest. Sie können zwischen SPF-, SIDF- oder SIDF-kompatiblen

PRA-Verifizierungsergebnis herabstufen, wenn "Resent-Sender:" oder "Resent-From:" verwendet wurden: Wenn Sie eine Kompatibilitätsstufe mit SIDF-Kompatibilität auswählen, legen Sie fest, ob

Sie das Ergebnis der PRA-Identitätsüberprüfung auf Keine herabstufen möchten, wenn ein Resent-Sender vorhanden ist: oder Resent-From: Header in der Nachricht vorhanden

HELO-Test: Konfigurieren Sie, ob Sie einen Test mit der HELO-Identität durchführen möchten (verwenden Sie dies für SPF- und SIDF-kompatible Konformitätsstufen).

DMARC-Verifizierung: Aktivieren der DMARC-Überprüfung auf diesem Listener

DMARC-Verifizierungsprofil verwenden: Wählen Sie das DMARC-Verifizierungsprofil aus, das Sie für diesen Listener verwenden möchten. Dasselbe wird aus Mail-Policys erstellt —> DMARC —> Profile hinzufügen

DMARC-Feedback-Berichte: Senden von DMARC-Aggregat-Feedback-Berichten aktivieren

Bounce-Verifizierung

Bounces ohne Tagging als gültig ansehen: Gilt nur, wenn die Bounce-Verifizierung aktiviert ist. Standardmäßig betrachtet die Appliance nicht markierte Bounces als ungültig und lehnt den Bounce ab oder fügt einen benutzerdefinierten Header hinzu, je nach den Einstellungen für die Bounce-Verifizierung. Wenn Sie festlegen, dass nicht markierte Bounces gültig sind, akzeptiert die Appliance die Bounce-Nachricht.

Absenderverifizierung

Umschlagabsender-DNS-Verifizierung:

Absender können aus unterschiedlichen Gründen nicht geprüft werden. Nicht verifizierte Absender werden in die folgenden Kategorien eingeteilt:

- Der PTR-Datensatz des verbindenden Hosts ist im DNS nicht vorhanden.
- Die PTR-Datensatzsuche des angeschlossenen Hosts schlägt aufgrund eines temporären DNS-Ausfalls fehl.
- Die umgekehrte DNS-Suche (PTR) des verbindenden Hosts stimmt nicht mit der vorwärts gerichteten DNS-Suche (A) überein.

Wir können die Funktion "Absenderverifizierung" aktivieren oder deaktivieren.

Ausnahmetabelle für die Absenderverifizierung verwenden: Sie können die Ausnahmetabelle für die Absenderverifizierungs-Domäne verwenden, um Ausnahmen zuzulassen. Es kann nur eine Ausnahmetabelle vorhanden sein, aber die Policy für den E-Mail-Fluss kann aktiviert werden.

Die Ausnahmetabelle kann aus Mail-Policys erstellt werden —> Ausnahmetabelle für die Absenderverifizierung —> Ausnahme für die Absenderverifizierung hinzufügen

Zielsteuerelemente

Diese Funktion steuert die E-Mail-Zustellungen. Alle E-Mails, die die Verarbeitung über die ESAs abschließen und die ESAs für weitere Sendungen verlassen werden, können über die Funktion Zielsteuerelemente gesteuert werden.

Das Standard-Zielsteuerelementprofil gilt für alle Lieferungen. Nur für den Fall, dass domänenspezifische Zustelloptionen erforderlich sind, müssen wir ein benutzerdefiniertes Zielsteuerelementprofil erstellen.

Komponenten eines Zielsteuerelementprofils

Einschränkungen

Gleichzeitige Verbindungen: Anzahl der gleichzeitigen Verbindungen (DCIDs) zu Remote-Hosts, die die Appliance zum Abschluss der Bereitstellung öffnen möchte.

Maximale Anzahl Nachrichten pro Verbindung: Die Anzahl der Nachrichten, die die ESA über eine Verbindung (DCID) an eine Zieldomäne sendet, bevor die Appliance eine neue Verbindung initiiert.

Empfänger: Die Anzahl der Empfänger, die die Appliance innerhalb eines bestimmten Zeitraums an einen bestimmten Remote-Host sendet.

Grenzwerte anwenden: Diese Aspekte helfen bei der Entscheidung, wie die angegebenen Grenzwerte auf Basis von Zielen und MGA-Hostnamen angewendet werden.

TLS-Unterstützung

Dies hilft bei der Entscheidung, ob TLS-Verbindungen zu Remote-Hosts auf Keine/Bevorzugt/Erforderlich eingestellt werden.

DANE-Unterstützung: Wenn Sie DANE als 'Opportunistisch' konfigurieren und der Remote-Host DANE nicht unterstützt, wird opportunistisches TLS für die Verschlüsselung von SMTP-Konversationen bevorzugt.

Wenn Sie DANE als 'Obligatorisch' konfigurieren und der Remote-Host DANE nicht unterstützt, wird keine Verbindung zum Ziel-Host hergestellt.

Wenn Sie DANE als 'Obligatorisch' oder 'Opportunistisch' konfigurieren und der Remote-Host DANE unterstützt, wird es für die Verschlüsselung von SMTP-Konversationen empfohlen.

HINWEIS: DANE wird für Domänen, für die SMTP-Routen konfiguriert sind, nicht erzwungen.

Bounce-Verifizierung

So können Sie festlegen, ob Umschlagabsender-Adressmarkierungen (prvs-xxxx-xxxx) über die Bounce-Verifizierung durchgeführt werden sollen oder nicht.

Bounce-Verifizierung kann über Mail-Richtlinien konfiguriert werden —> Bounce-Verifizierung —> Neuen Schlüssel hinzufügen

Bounce-Profil

Das Bounce-Profil kann von der Appliance für einen bestimmten Remote-Host verwendet werden.

Er entscheidet, wie lange eine E-Mail in der Zustellwarteschlange der ESA gespeichert wird, wenn Zustellprobleme auftreten, bevor eine E-Mail-Nachricht Hard Bounce gesendet wird.

Das Bounce-Profil wird über das Netzwerk —> Bounce-Profile festgelegt.

Globale Einstellungen

Zertifikat: In diesem Punkt definieren wir die Zertifikate, die beim Herstellen von SSL/TLS-Verbindungen beim Initiieren von E-Mail-Lieferungen an den nächsten Hop verwendet werden. Es wird immer empfohlen, in diesem Zusammenhang ein Zertifikat der Zertifizierungsstelle (Certificate Authority, CA) zu verwenden.

Eine Warnmeldung senden, wenn eine erforderliche TLS-Verbindung fehlschlägt: Bei der Übermittlung von Nachrichten an eine Domäne, die eine TLS-Verbindung erfordert, können wir angeben, ob die Appliance eine Warnmeldung sendet, wenn die TLS-Aushandlung fehlschlägt. Die Warnmeldung enthält den Namen der Zieldomäne für die fehlgeschlagene TLS-Aushandlung. Die Appliance sendet die Warnmeldung an alle Empfänger, die **Warning** Severity Level Alerts (Schweregradwarnungen bei **Systemwarnungen)** empfangen sollen.

Wir können Alert-Empfänger über die Systemverwaltung verwalten —> Alerts.