Konfiguration von Cloud Gateway Gold

Inhalt

Einleitung

Dieses Dokument beschreibt eine detaillierte Analyse der Gold-Konfiguration für Cisco Secure Email Cloud Gateway. Die Gold-Konfiguration für Cisco Secure Email Cloud-Kunden ist die Best Practice und Zero-Day-Konfiguration für das Cloud Gateway und Cisco Secure Email und Web Manager. Cisco Secure Email Für Cloud-Bereitstellungen werden sowohl Cloud Gateway(s) als auch mindestens ein (1) E-Mail- und Web-Manager verwendet. Im Rahmen der Konfiguration und der Best Practices können Administratoren Quarantänen auf dem E-Mail- und Web-Manager für ein zentrales Management verwenden.

Voraussetzungen

Anforderungen

Cisco empfiehlt, dass Sie folgende Themen kennen:

- Cisco Secure Email Gateway oder Cloud Gateway für UI- und CLI-Verwaltung
- Cisco Secure Email und Web Manager, Verwaltung auf Benutzeroberflächsebene
- Cisco Secure Email Cloud-Kunden können CLI-Zugriff anfordern; siehe: Zugriff über die Kommandozeile (CLI)

Verwendete Komponenten

Die Informationen in diesem Dokument stammen aus der Gold-Konfiguration und Empfehlungen zu Best Practices für Cisco Secure Email Cloud-Kunden und -Administratoren.

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 möglichen Auswirkungen aller Befehle verstehen.

Verwandte Produkte

Dieses Dokument gilt auch für:

- Cisco Secure Email Gateway - Hardware vor Ort oder virtuelle Appliance
- Cisco Secure Email und Web Manager Hardware und virtuelle Appliance vor Ort

Richtlinien-Quarantäne

Quarantänen werden auf dem Email und Web Manager für Cisco Secure Email Cloud-Kunden konfiguriert und verwaltet. Melden Sie sich bei Ihrem E-Mail- und Web-Manager an, um die Quarantänen anzuzeigen:

- ACCOUNT_ÜBERNAHME
- ANTI_SPOOF
- BLOCK_ANHÄNGE
- BLOCKLISTE
- DKIM_FAIL
- DMARC_QUARANTÄNE
- DMARC_ABLEHNEN
- GEFORMTE E-MAIL

- UNANGEMESSENER_INHALT
- MAKRO
- ÖFFNEN_RELAIS
- SDR_DATEN
- SPF_HARDFAIL
- SPF_SOFTFAIL
- TG_AUSGEHEND_MALWARE
- URL_SCHÄDLICH

Cloud Gateway - Gold-Konfiguration

> **Warnung**: Alle Änderungen an Konfigurationen, die auf den in diesem Dokument beschriebenen Best Practices basieren, müssen überprüft und verstanden werden, bevor Sie Ihre Konfigurationsänderungen in Ihrer Produktionsumgebung bestätigen. Wenden Sie sich vor Konfigurationsänderungen an Ihren Cisco CX-Techniker, Ihren Designated Service Manager (DSM) oder Ihr Kundenteam.

Basiskonfiguration

Mail-Policys > Recipient Access Table (RAT)

Die Recipient Access Table legt fest, welche Empfänger von einem öffentlichen Listener akzeptiert werden. Die Tabelle gibt mindestens die Adresse an und ob sie angenommen oder abgelehnt werden soll. Überprüfen Sie die RAT, um Ihre Domänen nach Bedarf hinzuzufügen und zu verwalten.

Netzwerk > SMTP-Routen

Wenn das SMTP-Routenziel Microsoft 365 ist, finden Sie Informationen unter Office365 Throttling CES New Instance with "4.7.500 Server busy. Versuchen Sie es später erneut."

Sicherheitsservices

Die aufgeführten Services sind für alle Cisco Secure Email Cloud-Kunden mit den angegebenen Werten konfiguriert:

IronPort Anti-Spam (IPAS)

- Aktiviert und konfiguriert Immer 1M scannen und nie 2M scannen
- Timeout für das Scannen einer einzelnen Nachricht: 60 Sekunden

URL-Filterung

- URL-Kategorisierung und Reputationsfilter aktivieren
- (Optional) Erstellen und konfigurieren Sie eine URL-Zulassungsliste mit dem Namen "bypass_urls".
- Web Interaction Tracking aktivieren
- Erweiterte Einstellungen: Timeout für URL-Suche: 15 SekundenMaximale Anzahl gescannter URLs in Text und Anhang: 400URL-Text und HREF in Nachricht umschreiben: NeinURL-Protokollierung: Aktiviert
- (Optional) Ab AsyncOS 14.2 für Cloud Gateway sind ein retrospektives URL-Verdict und eine URL-Bereinigung verfügbar. siehe die bereitgestellten Versionshinweise und Konfigurieren der URL-Filterung für Secure Email Gateway und Cloud Gateway

Graymail-Erkennung

- Aktivieren und konfigurieren Immer 1M scannen und nie 2M scannen
- Timeout für das Scannen einer einzelnen Nachricht: 60 Sekunden

Outbreak-Filter

- Adaptive Regeln aktivieren
- Maximale Nachrichtengröße: 2 Mio.
- Web Interaction Tracking aktivieren

Advanced Malware Protection > Dateireputation und -analyse

- Dateireputation aktivieren
- Dateianalyse aktivieren Unter Globale Einstellungen können Sie Dateitypen für die Dateianalyse überprüfen.

Nachrichtenverfolgung

- Protokollierung abgelehnter Verbindungen aktivieren (falls erforderlich)

Systemverwaltung

Benutzer (Systemverwaltung > Benutzer)

- Vergessen Sie nicht, die Passphrase-Richtlinien für das **lokale Benutzerkonto und die Passphrase-Einstellungen** zu überprüfen und festzulegen.
- Konfigurieren und aktivieren Sie nach Möglichkeit Lightweight Directory Access Protocol (LDAP) für die Authentifizierung (**Systemverwaltung > LDAP**)

Protokoll-Subscriptions (Systemverwaltung > Protokoll-Subscriptions)

- Falls nicht konfiguriert, erstellen und aktivieren Sie: KonfigurationsverlaufsprotokolleProtokolle des URL-Reputations-Clients
- Bearbeiten Sie in den globalen Einstellungen für Protokoll-Subscriptions die Einstellungen, und fügen Sie die Header **To**, **From**, **Reply-To**, **Sender hinzu**.

Zusätzliche Konfiguration (optional)

Zusätzliche Services, die geprüft und berücksichtigt werden sollten:

Systemverwaltung > LDAP

- Wenn Sie LDAP konfigurieren, empfiehlt Cisco LDAP mit aktivierter SSL-Funktion

URL-Schutz

- Unter Konfigurieren der URL-Filterung für sicheres E-Mail-Gateway und Cloud-Gateway finden Sie die aktuellsten Best Practices für die Konfiguration der URL-Abwehr.
- Darüber hinaus befasst sich Cisco intensiv mit URL-Schutz. finden Sie im URL-Verteidigungsleitfaden.
- Einige Beispiele aus dem URL-Verteidigungsleitfaden werden ebenfalls in dieses Dokument aufgenommen.

SPF

- Die DNS-Einträge des Sender Policy Framework (SPF) werden extern für das Cloud Gateway erstellt. Aus diesem Grund empfiehlt Cisco allen Kunden dringend, Best Practices für SPF, DKIM und DMARC in ihren Sicherheitsstatus einzubeziehen. Weitere Informationen zur SPF-Validierung finden Sie unter SPF-Konfiguration und Best Practices.
- Für Cisco Secure Email Cloud-Kunden wird ein Makro für alle Cloud-Gateways pro zugewiesenem Hostnamen veröffentlicht, um das Hinzufügen aller Hosts zu vereinfachen.
- Platzieren Sie diesen Eintrag vor ~all oder -all im aktuellen DNS TXT (SPF)-Datensatz, falls vorhanden:

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

> **Hinweis:** Stellen Sie sicher, dass der SPF-Datensatz entweder mit **~all** oder mit **-all** endet. Validieren Sie die SPF-Datensätze für Ihre Domänen vor und nach Änderungen!

- Empfohlene Informationen und Tools für mehr über SPF:
  SPF Record Checker - Kostenlose SPF-Suche (dmarcian.com)Syntaxtabelle für SPF-Datensätze - Alle SPFs - dmarcian.com

Weitere SPF-Beispiele

- Ein ausgezeichnetes Beispiel für SPF ist, wenn Sie E-Mails von Ihrem Cloud Gateway empfangen und ausgehende E-Mails von anderen Mail-Servern senden. Sie können den Mechanismus "a:" verwenden, um Mail-Hosts anzugeben:

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

- Wenn Sie ausgehende E-Mails nur über Ihr Cloud Gateway versenden, können Sie Folgendes verwenden:

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

- In diesem Beispiel gibt der Mechanismus "ip4:" oder "ip6:" eine IP-Adresse oder einen IP-Adressbereich an:

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

Änderungen auf CLI-Ebene

- Wie unter Voraussetzungen erwähnt, können Cisco Secure Email Cloud-Kunden den Zugriff auf die CLI anfordern. Weitere Informationen finden Sie unter CLI-Zugriff (Command Line Interface).

Anti-Spoof-Filter

- Lesen Sie unbedingt den Best Practices-Leitfaden für Anti-Spoofing durch.
- Dieser Leitfaden enthält ausführliche Beispiele und Best Practices für die Konfiguration zum Schutz vor E-Mail-Spoofing.

Header-Filter hinzufügen

- Nur CLI, bitte schreiben und aktivieren Sie den Nachrichtenfilter 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");
}
```

Host Access Table (Mail-Policys > Host Access Table (HAT))

HAT-Übersicht > Zusätzliche Absendergruppen

- ESA-Benutzerhandbuch: Erstellen einer Absendergruppe für die Nachrichtenverarbeitung BYPASS_SBRS - Höherer Wert für Quellen, die die Reputation überspringenMY_TRUSTED_SPOOF_HOSTS - Teil des Spoofing-FiltersTLS_REQUIRED - Für erzwungene TLS-Verbindungen

In der vordefinierten Absendergruppe SUSPECTLIST

- ESA-Benutzerhandbuch: Absenderverifizierung: Host Aktivieren Sie "SBRS Scores on None".(Optional) Aktivieren Sie "PTR-Eintrag-Suche des verbindenden Hosts schlägt aufgrund eines temporären DNS-Fehlers fehl."

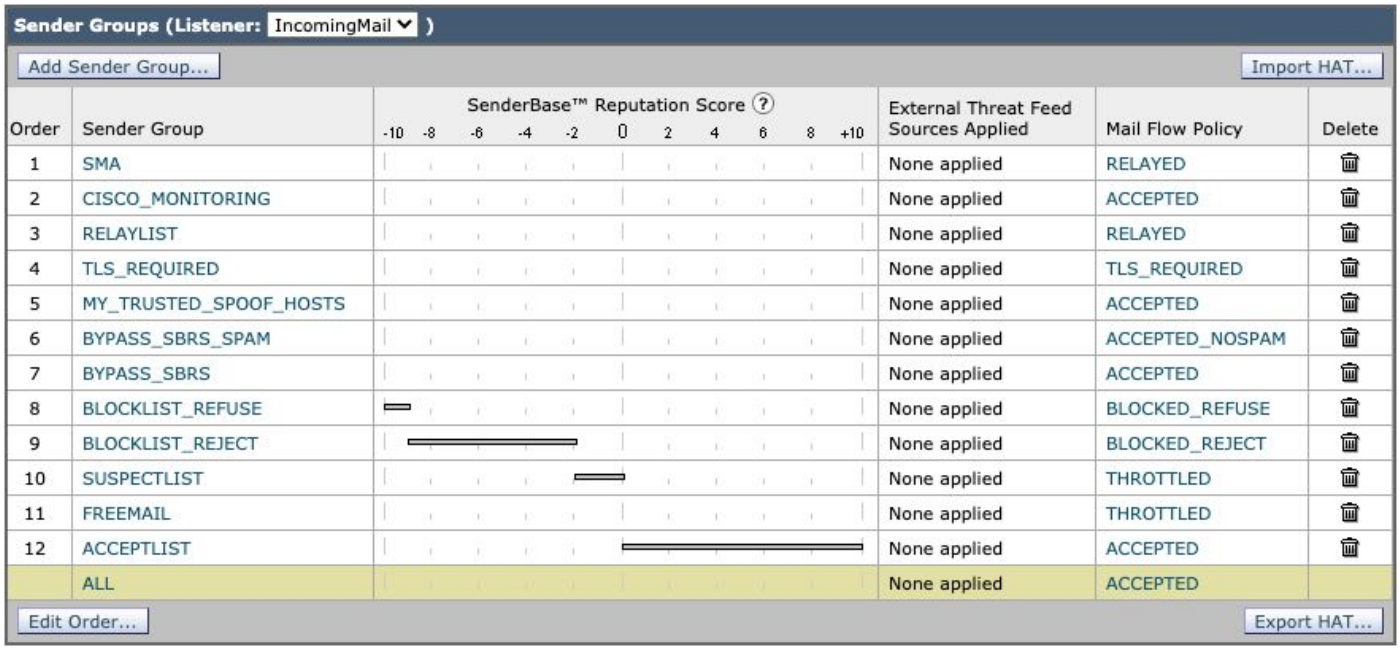
Aggressive HAT-Beispiel

- BLOCKLIST_REFUSE [-10.0 bis -9.0] RICHTLINIE: GESPERRT_ABLEHNEN

- BLOCKLIST_REJECT [-9.0 bis -2.0] RICHTLINIE: GESPERRT_ABLEHNEN
- SUSPECTLIST [-2.0 bis 0.0 und SBRS-Bewertungen von "Keine"] RICHTLINIE: GEDROSSELT
- ACCEPTLIST [0.0 bis 10.0] RICHTLINIE: AKZEPTIERT

Anmerkung: Die HAT-Beispiele zeigen zusätzlich konfigurierte Mail Flow Policies (MFP). Vollständige Informationen zu MFP finden Sie unter "Understanding the Email Pipeline > Incoming/Receiving" im Benutzerhandbuch für die entsprechende Version von AsyncOS für das von Ihnen bereitgestellte Cisco Secure Email Gateway.

HAT-Beispiel:



Mail Flow Policy (Standardrichtlinienparameter)

Standardrichtlinienparameter

Sicherheitseinstellungen

- Festlegen der Transport Layer Security (TLS) auf "Bevorzugt"
- Sender Policy Framework (SPF) aktivieren.
- DomainKeys Identified Mail (DKIM) aktivieren.
- Aktivieren der domänenbasierten Nachrichtenauthentifizierung, Berichterstellung und Konformitätsprüfung (DMARC) und Senden von aggregierten Feedback-Berichten

Anmerkung: DMARC erfordert zusätzliche Feineinstellung für die Konfiguration. Weitere Informationen zu DMARC finden Sie unter "E-Mail-Authentifizierung > DMARC-Verifizierung" im Benutzerhandbuch für die entsprechende Version von AsyncOS für das von Ihnen bereitgestellte Cisco Secure Email Gateway.

Richtlinien für eingehende Mails

Die Standardrichtlinie wird ähnlich konfiguriert wie:

Anti-Spam

- Aktiviert, Schwellenwerte verbleiben bei den Standardschwellenwerten. (Eine Änderung der Bewertung kann zu mehr Fehlalarmen führen.)

Antivirus

- Scannen von Nachrichten**: Nur nach Viren suchen** Stellen Sie sicher, dass das Kontrollkästchen "X-Header einschließen" aktiviert ist.
- Für **nicht scannbare Nachrichten** und **infizierte Nachrichten** legen Sie **Originalnachricht archivieren auf Nein fest**

AMP

- Für **nicht scanbare Aktionen bei Nachrichtenfehlern** verwenden Sie **Erweitert** und **Benutzerdefinierten Header zu Nachricht hinzufügen**, X-TG-MSGERROR, Wert: Richtig.
- Bei **nicht scanbaren Aktionen für Ratenlimit** verwenden Sie **Erweitert** und **Benutzerdefinierten Header zu Nachricht hinzufügen**, X-TG-RATELIMIT, Wert: Richtig.
- Bei **Nachrichten mit ausstehender Dateianalyse** verwenden Sie **Aktion auf Nachricht angewendet**: "Quarantäne".

Graymail

- Scannen ist für jedes Urteil (Marketing, Social, Bulk) aktiviert, mit **Prepend** for **Add Text to Subject** und Aktion ist **Deliver**.
- Verwenden Sie für **Massenmail-Aktionen** die Optionen **Erweitert** und **Benutzerdefinierten Header hinzufügen (optional)**: X-Bulk, Wert: Richtig.

Content-Filter

- Aktiviert und URL_QUARANTINE_MALICIOUS, URL_REWRITE_SUSPICIOUS, URL_INAPPROPRIATE, DKIM_FAILURE, SPF_HARDFAIL, EXECUTIVE_SPOOF, DOMAIN_SPOOF, SDR, TG_RATE_LIMIT sind ausgewählt.
- Diese Content-Filter werden später in diesem Leitfaden bereitgestellt.

Outbreak-Filter

- Die Standardbedrohungsstufe ist 3. passen Sie sich bitte Ihren Sicherheitsanforderungen an. Wenn die Bedrohungsstufe für eine Nachricht diesen Schwellenwert erreicht oder überschreitet, wird die Nachricht in die Outbreak-Quarantäne verschoben. (1 = geringste Bedrohung, 5 = höchste Bedrohung)
- Nachrichtenänderung aktivieren

- URL-Umschreibungssatz für "Für alle Nachrichten aktivieren".
- Betreff ändern vor: [Mögliche $Threat_category-Betrügereien]

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	

Richtliniennamen (abgebildet)

- **BLOCKLISTE - Mail-Richtlinie**
  Die BLOCKLIST-Mail-Richtlinie ist so konfiguriert, dass alle Dienste außer Advanced Malware Protection deaktiviert sind. Sie enthält Links zu Content-Filtern mit der Aktion QUARANTINE.

- **E-Mail-Richtlinie ZULASSEN**
  Für die E-Mail-Richtlinie ALLOWLIST wurde Antispam, Graymail deaktiviert und die Inhaltsfilter für URL_QUARANTINE_MALICIOUS, URL_REWRITE_SUSPICIOUS, URL_INAPPROPRIATE, DKIM_FAILURE, SPF_HARDFAIL, EXECUTIVE SPOOF, DOMAIN_SPOOF, SDR, TG_RATE_RATE aktiviert. LIMIT oder Content-Filter Ihrer Wahl und Konfiguration.

- **ALLOW_SPOOF-Mail-Richtlinie**
  Für die E-Mail-Richtlinie ALLOW_SPOOF sind alle Standarddienste aktiviert. Content-Filter sind für URL_QUARANTINE_MALICIOUS, URL_REWRITE_SUSPICIOUS, URL_INAPPROPRIATE, SDR oder Content-Filter Ihrer Wahl und Konfiguration aktiviert.

Richtlinien für ausgehende Mails

Die Standardrichtlinie wird ähnlich konfiguriert wie:

Anti-Spam

- Deaktiviert

Antivirus

- Scannen von Nachrichten: **Nur nach Viren suchen** Deaktivieren Sie das Kontrollkästchen für "X-Header einschließen".
- (Optional) Für alle Meldungen: **Erweitert > Benachrichtigung über andere**, aktivieren Sie "Andere" und geben Sie Ihre Admin-/SOC-Kontakt-E-Mail-Adresse an.

Advanced Malware Protection

- Nur Dateireputation aktivieren
- **Nicht scanbare Aktionen für Ratenlimit**: **Erweitert** verwenden und **benutzerdefinierten Header zu Nachricht hinzufügen**: X-TG-RATELIMIT, Wert: "Wahr."
- **Nachrichten mit Malware-Anhängen**: **Erweitert** verwenden und **benutzerdefinierten Header zu Nachricht hinzufügen**: X-TG-OUTBOUND, Wert: "MALWARE ERKANNT."

Graymail

- Deaktiviert

Content-Filter

- Aktiviert und TG_OUTBOUND_MALICIOUS, Strip_Secret_Header, EXTERNAL_SENDER_REMOVE, ACCOUNT_TAKEOVER oder Content-Filter Ihrer Wahl sind ausgewählt.

Outbreak-Filter

- Deaktiviert

SvD

- Aktivieren Sie diese Option je nach SvD-Lizenz und SvD-Konfiguration.

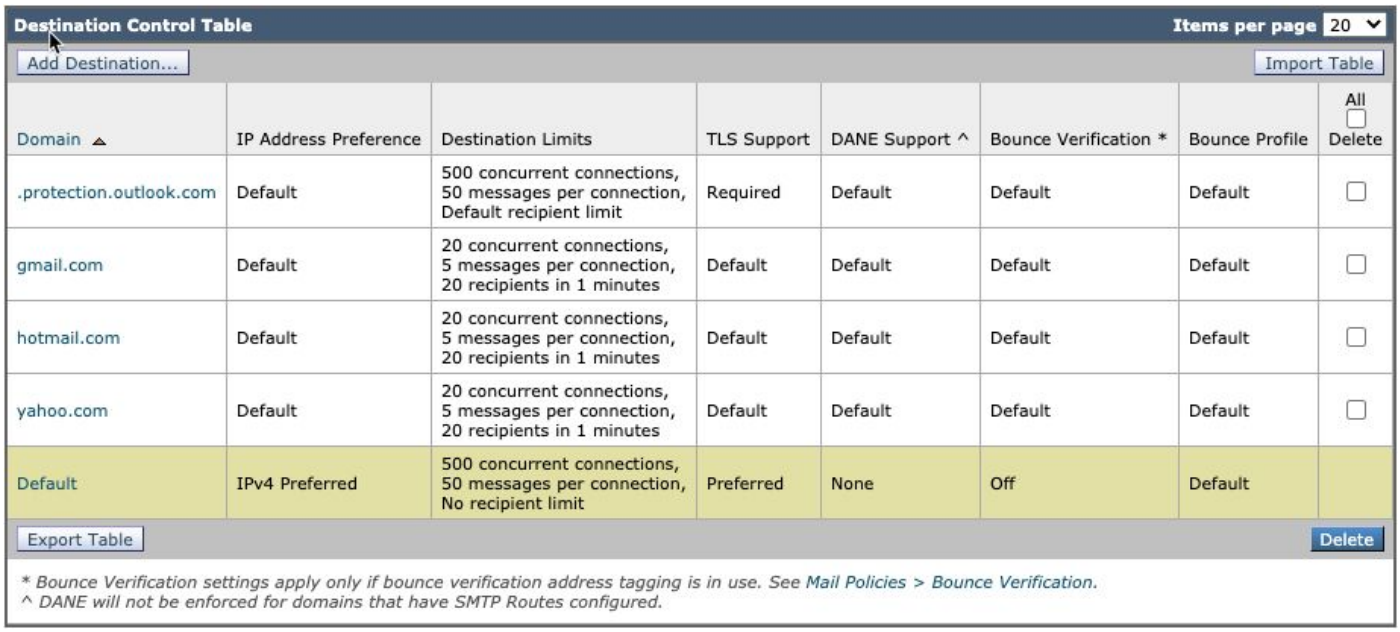
Weitere Einstellungen

Wörterbücher (Mail-Policys > Wörterbücher)

- Aktivieren und überprüfen Sie **Profanity** and **Sexual_Content** Dictionary
- Executive_**FED-**Wörterbuch für die Erkennung gefälschter E-Mails mit allen Führungskräften erstellen
- Erstellen Sie zusätzliche Wörterbücher für eingeschränkte oder andere Schlüsselwörter, die Sie für Ihre Richtlinien, Ihre Umgebung oder Ihre Sicherheitskontrolle benötigen.

Zielsteuerelemente (Mail-Policys > Zielsteuerelemente)

- Konfigurieren Sie für die Standarddomäne den **TLS-Support** als **Bevorzugt.**
- Sie können Ziele für Webmail-Domänen hinzufügen und niedrigere Grenzwerte festlegen.
- Weitere Informationen finden Sie in unserer Anleitung Rate Limit Your Outbound Mail with Destination Control Settings.



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.

Content-Filter

Anmerkung: Weitere Informationen zu Inhaltsfiltern finden Sie unter "Inhaltsfilter" im Benutzerhandbuch für die jeweilige Version von AsyncOS für das von Ihnen bereitgestellte Cisco Secure Email Gateway.

Filter für eingehende Inhalte

URL_QUARANTÄNE_SCHÄDLICH

Bedingung: URL-Reputation; url-reputation(-10,00, -6,00 , "bypass_urls", 1, 1)

Aktion: Quarantäne: quarantine("URL_MALICIOUS")

URL_UMSCHREIBEN_VERDÄCHTIG

Bedingung: URL-Reputation; url-reputation(-5.90, -5.60 , "bypass_urls", 0, 1)

Aktion: URL-Reputation; url-reputation-proxy-redirect(-5.90, -5.60,"",0)

URL_UNANGEMESSEN

Bedingung: URL-Kategorie; url-category (['Adult', 'Child Abuse Content', 'Extreme', 'Hate Speech', 'Illegal Activities', 'Illegal Downloads', 'Illegal Drugs', 'Pornografie', 'Filter Avoidance'], "bypass_urls", 1, 1)

Aktion: Quarantine; double-quarantine("INAPPROPRIATE_CONTENT")

DKIM_FEHLER

Bedingung: DKIM-Authentifizierung; dkim-Authentifizierung == hardfail

Aktion: Quarantine; double-quarantine("DKIM_FAIL")

SPF_HARDFAIL

Bedingung: SPF-Verifizierung; spf-status == fehlgeschlagen

Aktion: Quarantine; double-quarantine("SPF_HARDFAIL")

EXECUTIVE_SPOOF

Bedingung: Erkennung gefälschter E-Mails; Erkennung gefälschter E-Mails("Executive_FED", 90, "")

Bedingung: Anderer Header; Header("X-IronPort-SenderGroup") != "(?i)allowspoof"

* **Regel anwenden: Nur wenn alle Bedingungen übereinstimmen**

Aktion: Header hinzufügen/bearbeiten; edit-header-text("Subject", "(.*)", "[EXTERNAL]\\1")

Aktion: Quarantine; double-quarantine("FORGED_EMAIL")

DOMAIN_SPOOF

Bedingung: Anderer Header; header("X-Spoof")

Aktion: Quarantine; double-quarantine("ANTI_SPOOF")

SZR

Bedingung: Domänenreputation; SDR-Reputation (['furchtbar'], "")

Bedingung: Domänenreputation; SDR-Alter ("Tage", <, 5, "")

* Regel anwenden: Wenn eine oder mehrere Bedingungen zutreffen

Aktion: Quarantine; double-quarantine("SDR_DATA")

TG_RATE_LIMIT

Bedingung: Other Header; Header("X-TG-RATELIMIT")

Aktion: Protokolleintrag hinzufügen; Protokolleintrag("X-TG-RATELIMIT: $filenames")

BLOCKLISTE_QUARANTÄNE

Bedingung: (None)

Aktion: Quarantäne; Quarantäne("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...

Filter für ausgehenden Inhalt

TG_AUSGEHEND_SCHÄDLICH

Bedingung: Andere Header; Header("X-TG-OUTBOUND") == MALWARE

Aktion: Quarantine; quarantine("TG_OUTBOUND_MALWARE")

Strip_Secret_Header

Bedingung: Anderer Header; Header("PLACEHOLDER") == PLACEHOLDER

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

EXTERNER_ABSENDER_ENTFERNEN

Bedingung: (None)

Aktion: Header hinzufügen/bearbeiten; Header-Text bearbeiten("Betreff", "\\[EXTERNAL\\]\\s?", "")

ACCOUNT_ÜBERNAHME

Bedingung: Anderer Header; Header("X-AMP-Result") == (?i)bösartig

Bedingung: URL-Reputation; url-reputation(-10,00, -6,00 , "", 1, 1)

*Anwenden-Regel festlegen: Wenn eine oder mehrere Bedingungen zutreffen

Aktion: Benachrichtigen;benachrichtigen ("<Admin- oder Distribution-E-Mail-Adresse einfügen>", "MÖGLICHE ÜBERNAHME EINES KONTOS", "", "ACCOUNT_TAKEOVER_WARNING")

Aktion: double-quarantine("ACCOUNT_TAKEOVER")

Filters

Add Filter...

Order	Filter Name	Description | Rules | Policies	Duplicate	Delete
1	Stop_O365_OpenRelay	Stop_O365_OpenRelay: if (header("X-IronPort-Tenant") != "placeholder") { duplicate-quarantine("OPEN_RELAY"); }		
2	TG_OUTBOUND_MALICIOUS	TG_OUTBOUND_MALICIOUS: if (header("X-TG-OUTBOUND") == "MALWARE") { quarantine("TG_OUTBOUND_MALWARE"); }		
3	Strip_Secret_Header	Strip_Secret_Header: if (header("PLACEHOLDER") == "PLACEHOLDER") { strip-header("X-IronPort-Tenant"); }		
4	EXTERNAL_SENDER_REMOVE	EXTERNAL_SENDER_REMOVE: if (true) { edit-header-text("Subject", "\\[EXTERNAL\\]\\s?", ""); }		
5	ACCOUNT_TAKEOVER	ACCOUNT_TAKEOVER: if (header("X-AMP-Result") == "(?i)malicious") OR (url-reputation(-10.00, -6.00 , "", 1, 1)) { notify ("myit@mycompany.com", "POSSIBLE ACCOUNT TAKEOVER", "", "ACCOUNT_TAKEOVER_WARNING"); duplicate-quarantine("ACCOUNT_TAKEOVER"); }		
6	ENCRYPT_OUT	ENCRYPT_OUT: if (subject == "(?i)*encrypt*") { edit-header-text("Subject", "(?i)*encrypt*\\s?", ""); encrypt-deferred ("CRES_HIGH", "$Subject", 0); }		
7	TG_RATE_LIMIT	TG_RATE_LIMIT: if (header("X-TG-OUTBOUND-RATELIMIT")) { tag-message ("NOOP"); }		

Edit Filter Order...

Für Kunden der Cisco Secure E-Mail Cloud sind in der Gold-Konfiguration und den Best Practice-Empfehlungen Beispiele für Content-Filter enthalten. Lesen Sie darüber hinaus die Filter "SAMPLE_", um weitere Informationen zu den entsprechenden Bedingungen und Aktionen zu erhalten, die für Ihre Konfiguration von Vorteil sein können.

Cisco Live

Auf der Cisco Live werden weltweit viele Sessions abgehalten. Neben persönlichen Sessions

stehen technische Breakouts zur Verfügung, die sich mit den Best Practices von Cisco Secure Email befassen. Ältere Sitzungen und Zugriff finden Sie auf der Cisco Live (CCO-Anmeldung erforderlich):

- Cisco Email Security: Best Practices und Feinabstimmung - BRKSEC-2131
- DMARCate Your Email Perimeter - BRKSEC-2131
- E-Mail wird behoben! - Cisco Email Security - Erweiterte Fehlerbehebung - BRKSEC-3265
- API-Integrationen für Cisco Email Security - DEVNET-2326
- Sicherung von SaaS-Mailbox-Services mit Cloud Email Security von Cisco - BRKSEC-1025
- E-Mail-Sicherheit: Best Practices und Feinabstimmung - TECSEC-2345
- 250 not OK - Mit Cisco Email Security in die Defensive gehen - TECSEC-2345
- Cisco Domain Protection und Cisco Advanced Phishing Protection: Die nächste Stufe der E-Mail-Sicherheit - BRKSEC-1243
- SPF ist kein Akronym für "Spoof"! Nutzen wir das Beste aus der nächsten Ebene der E-Mail-Sicherheit! - DGTL-BRKSEC-2327

Zusätzliche Informationen

Cisco Secure Email Gateway-Dokumentation

- Versionshinweise
- Benutzerhandbuch
- CLI-Referenzhandbuch
- API-Programmierhandbücher für Cisco Secure Email Gateway
- Open Source für Cisco Secure Email Gateway
- Installationsanleitung für die Cisco Content Security Virtual Appliance (mit vESA)

Secure Email Cloud Gateway - Dokumentation

- Versionshinweise
- Benutzerhandbuch

Cisco Secure Email und Web Manager-Dokumentation

- Versionshinweise und Kompatibilitätsmatrix
- Benutzerhandbuch
- API-Programmierhandbücher für Cisco Secure Email und Web Manager
- Cisco Content Security Virtual Appliance Installationshandbuch (einschl. vSMA)

Cisco Secure-Produktdokumentation

- Cisco Secure Portfolio Naming Architecture

Zugehörige Informationen

- Cisco Secure Email Security - Compliance
- Angebotsbeschreibung: Sichere E-Mails
- Cisco Universal Cloud - Begriffe
- Cisco Support und Downloads
- [EXTERN] OpenSPF: SPF - Grundlegende und erweiterte Informationen

Informationen zu dieser Übersetzung

Cisco hat dieses Dokument maschinell übersetzen und von einem menschlichen Übersetzer editieren und korrigieren lassen, um unseren Benutzern auf der ganzen Welt Support-Inhalte in ihrer eigenen Sprache zu bieten. Bitte beachten Sie, dass selbst die beste maschinelle Übersetzung nicht so genau ist wie eine von einem professionellen Übersetzer angefertigte. Cisco Systems, Inc. übernimmt keine Haftung für die Richtigkeit dieser Übersetzungen und empfiehlt, immer das englische Originaldokument (siehe bereitgestellter Link) heranzuziehen.