Configuratie van Cloud Gateway Gold configureren

Inhoud

Inleiding

Dit document beschrijft een diepgaande analyse van de gouden configuratie voor Cisco Secure Email Cloud Gateway. De Gold Configuration voor klanten van Cisco Secure Email Cloud is de beste praktijk en configuratie op nul dagen voor zowel de Cloud Gateway als Cisco Secure Email en Web Manager. Cisco Secure Email Cloud-implementaties maken gebruik van zowel een of meer cloudgateway(s) als ten minste één (1) e-mail en webbeheer. Onderdelen van de configuratie en best practices geven beheerders de opdracht om quarantaine(s) op de e-mail en

Web Manager te gebruiken voor gecentraliseerde beheerdoeleinden.

Voorwaarden

Vereisten

Cisco raadt u aan deze onderwerpen te kennen:

- Cisco Secure Email Gateway voor cloudgateway, zowel UI- als CLI-beheer
- Cisco Secure Email and Web Manager, beheer op UI-niveau
- Cisco Secure Email Cloud-klanten kunnen CLI-toegang aanvragen; zie: CLI-toegang (Command Line Interface)

Gebruikte componenten

De informatie in dit document is afkomstig van de gouden configuratie en de aanbevelingen voor beste praktijken voor klanten en beheerders van Cisco Secure Email Cloud.

De informatie in dit document is gebaseerd op de apparaten in een specifieke laboratoriumomgeving. Alle apparaten die in dit document worden beschreven, hadden een opgeschoonde (standaard)configuratie. Als uw netwerk live is, moet u zorgen dat u de potentiële impact van elke opdracht begrijpt.

Verwante producten

Dit document is ook van toepassing met:

- Cisco Secure Email Gateway-hardware of virtuele applicatie op locatie
- Cisco Secure Email en Web Manager op locatie voor hardware en virtuele apparaten

Beleidskwartieren

Quarantines worden geconfigureerd en onderhouden op de Email en Web Manager voor Cisco Secure Email Cloud-klanten. Meld u aan bij uw Email and Web Manager om de quarantaine te bekijken:

- ACCOUNT_OVERNAME
- ANTI_SPOOF
- BLOK_BIJLAGEN
- BLOKLIJST
- DKIM_FAIL
- DMARC_QUARANTAINE

- DMARC_AFWIJZEN
- VERVALST_E-MAIL
- ONGEWENSTE_INHOUD
- MACRO
- OPEN_RELAY
- SDR_GEGEVENS
- SPF_HARDFAIL
- SPF_SOFTFAIL
- TG_UITGAANDE_MALWARE
- URL_KWAADAARDIG

Gold-configuratie voor cloudgateway

> **Waarschuwing**: alle wijzigingen in de configuratie(s) op basis van de best practices zoals in dit document verstrekt, moeten worden beoordeeld en begrepen voordat u uw configuratiewijzigingen in uw productieomgeving doorvoert. Raadpleeg uw Cisco CX Engineer, Aangewezen Service Manager (DSM) of Accountteam voordat u de configuratie wijzigt.

Basisconfiguratie

E-mailbeleid > Toegangstabel voor ontvangers (RAT)

De Begunstigde Toegangstabel bepaalt welke ontvangers door een openbare luisteraar worden goedgekeurd. Op zijn minst, de tabel specificeert het adres en of je het moet accepteren of weigeren. Beoordeel de RAT om je domeinen toe te voegen en te beheren zoals nodig.

Netwerk > SMTP-routers

Als de SMTP routebestemming Microsoft 365 is, raadpleeg dan Office365 Throttling CES New Instance met "4.7.500 Server bezig. Probeer het later opnieuw".

Beveiligingsservices

De vermelde services worden geconfigureerd voor alle klanten van Cisco Secure Email Cloud met de volgende waarden:

IronPort Anti-Spam (IPAS)

- Ingeschakeld en configureren Altijd scannen 1M en Nooit scannen 2M
- Time-out voor scannen van één bericht: 60 seconden

URL-filtering

- URL-categorisatie- en reputatiefilters inschakelen
- (Optioneel) Maak en configureer URL Allowlist genaamd "bypass_urls."
- Webinteractietracking inschakelen
- Geavanceerde instellingen: Time-out bij URL-zoeken: 15 secondenMaximum aantal gescande URL's in hoofdtekst en bijlage: 400Herschrijf URL tekst en HREF in bericht: NeeURL-vastlegging: Ingeschakeld
- (Optioneel) Vanaf AsyncOS 14.2 voor Cloud Gateway zijn URL Retrospective Verdict en URL Remediation beschikbaar. zie Releaseopmerkingen en URL-filtering voor beveiligde e-mailgateway en cloudgateway configureren

Graymail-detectie

- Altijd 1M scannen en nooit 2M scannen inschakelen en configureren
- Time-out voor scannen van één bericht: 60 seconden

Uitbraakfilters

- Adaptieve regels inschakelen
- Maximale berichtgrootte voor scannen: 2 M
- Webinteractietracking inschakelen

Advanced Malware Protection > Bestandsreputatie en -analyse

- Bestandsreputatie inschakelen
- Bestandsanalyse inschakelen Zie Algemene instellingen voor bestandstypen voor bestandanalyse

Berichttracering

- Vastlegging afgewezen verbinding inschakelen (indien nodig)

Systeembeheer

Gebruikers (systeembeheer > gebruikers)

- Vergeet niet het beleid te bekijken en in te stellen dat is gekoppeld aan de **instellingen voor lokale gebruikersaccount en wachtwoord**
- Indien mogelijk Lichtgewicht Directory Access Protocol (LDAP) voor verificatie configureren en inschakelen (**Systeembeheer > LDAP**)

Logabonnementen (systeembeheer > logabonnementen)

- Indien niet geconfigureerd, maken en inschakelen: Logbestanden met configuratiegeschiedenisClientlogboeken voor URL-reputatie
- In de Global Settings van de Abonnementen van het Logboek, geef instellingen uit en voeg de kopballen **aan**, **van**, **antwoord-aan**, **Afzender toe**.

Aanvullende configuratie (optioneel)

Aanvullende diensten om te beoordelen en te overwegen:

Systeembeheer > LDAP

- Als u LDAP configureert, raadt Cisco LDAP aan met SSL ingeschakeld

URL-defensie

- Zie URL-filtering voor beveiligde e-mailgateway en cloudgateway configureren voor de meest recente best practices voor configuratie van URL-defensie.
- Cisco is ook diep verwikkeld in URL Defense; raadpleeg de URL Defense Guide.
- Sommige voorbeelden in de URL Defense Guide zijn ook opgenomen in dit document.

SPF

- DNS-records (Sender Policy Framework) worden extern gemaakt op Cloud Gateway. Daarom raadt Cisco alle klanten ten zeerste aan de best practices voor SFP, DKIM en DMARC in hun beveiligingspositie te bouwen. Zie SPF Configuration en Best Practices voor meer informatie over SPF validatie.
- Voor klanten van Cisco Secure Email Cloud wordt er een macro gepubliceerd voor alle Cloud Gateway(s) per de toewijzing hostnaam om het toevoegen van alle hosts te vergemakkelijken.
- Plaats dit voor ~all of -all in de huidige DNS TXT (SPF)-record, indien aanwezig:

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

> **Opmerking**: zorg ervoor dat de SPF-record eindigt met **~all** of -**all**. Bevestig de SPF-records voor uw domeinen voor en na eventuele wijzigingen!

- Aanbevolen informatie en hulpmiddelen voor meer informatie over SFP:
  SPF Record Checker - Free SPF Lookup (dmarcian.com)SPF Record Syntax Tabel - Alles SPF - dmarcian.com

Aanvullende SPF-voorbeelden

- Een uitstekend voorbeeld van SPF is als u e-mails ontvangt van uw Cloud Gateway en uitgaande e-mails verstuurt van andere mailservers. U kunt het mechanisme "a:" gebruiken om mailhosts op te geven:

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

- Als u alleen uitgaande e-mails verstuurt via uw Cloud Gateway, kunt u gebruik maken van:

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

- In dit voorbeeld geeft het mechanisme "ip4:" of "ip6:" een IP-adres of IP-adresbereik aan:

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

Wijzigingen op CLI-niveau

- Zoals in vereisten is vermeld, kunnen klanten van Cisco Secure Email Cloud CLI-toegang aanvragen; raadpleeg Command Line Interface (CLI) Access.

Anti-Spoof Filter

- Lees de Best Practices Guide for Anti-Spoofing
- Deze gids biedt u uitgebreide voorbeelden en configuratie best practices voor e-mailspofpreventie

Kop filter toevoegen

- CLI alleen, schrijf en schakel de berichtfilter addHeaders in:

```
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 (mailbeleid > Host Access Table (HAT))

HAT - Overzicht > Aanvullende verzendgroepen

- ESA Gebruikershandleiding: Een afzendergroep maken voor berichtenverwerking BYPASS_SBRS - Plaats hoger voor bronnen die reputatie overslaanMY_TRUSTED_SPOOF_HOSTS - Onderdeel van spoofingfilterTLS_VERPLICHT - Voor gedwongen TLS-verbindingen

In de vooraf gedefinieerde groep SENDERS

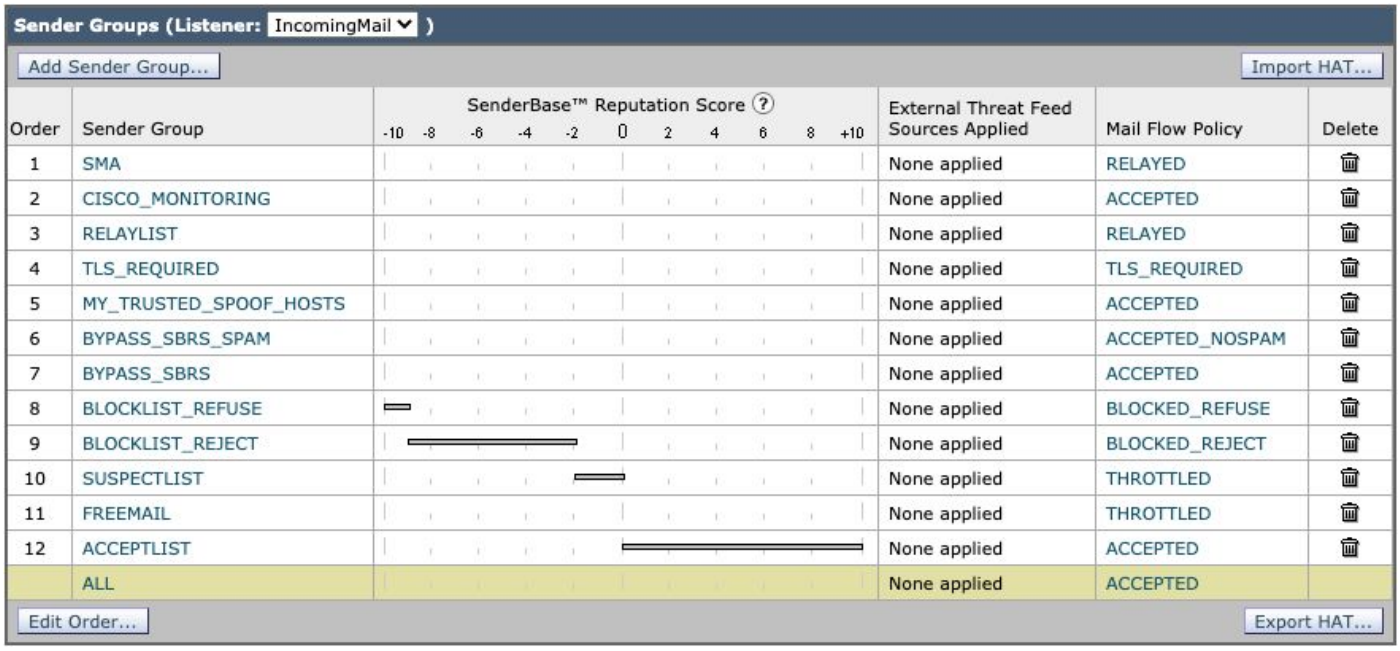
- ESA Gebruikershandleiding: Verificatie afzender: Host Schakel "SBRS Scores on none" in.(Optioneel) Schakel "Connecting host PTR record lookup mislukt vanwege tijdelijke DNS-storing" in.

Agressieve HAT-steekproef

- BLOCKLIST_REFUSE [-10.0 tot -9.0] BELEID: GEBLOKKEERD_AFVAL
- BLOCKLIST_REJECT [-9.0 tot -2.0] BELEID: GEBLOKKEERD_AFWIJZEN
- SUSPECTLIST [-2.0 tot 0.0 en SBRS scores van "Geen"] BELEID: GESTOORD
- ACCEPTLIST [0.0 tot 10.0] BELEID: AANVAARD

Opmerking: De HAT voorbeelden tonen bovendien geconfigureerd Mail Flow Policies (MFP). Raadpleeg voor volledige informatie over MFP "Understanding the Email Pipeline > Incoming/Receiving" in de Gebruikershandleiding voor de juiste versie van AsyncOS voor de Cisco Secure Email Gateway die u hebt geïmplementeerd.

Voorbeeld:



Sender Groups (Listener: IncomingMail)

Add Sender Group... | Import HAT...

Order	Sender Group	SenderBase™ Reputation Score -10 -8 -6 -4 -2 0 2 4 6 8 +10	External Threat Feed Sources Applied	Mail Flow Policy	Delete
1	SMA		None applied	RELAYED	
2	CISCO_MONITORING		None applied	ACCEPTED	
3	RELAYLIST		None applied	RELAYED	
4	TLS_REQUIRED		None applied	TLS_REQUIRED	
5	MY_TRUSTED_SPOOF_HOSTS		None applied	ACCEPTED	
6	BYPASS_SBRS_SPAM		None applied	ACCEPTED_NOSPAM	
7	BYPASS_SBRS		None applied	ACCEPTED	
8	BLOCKLIST_REFUSE		None applied	BLOCKED_REFUSE	
9	BLOCKLIST_REJECT		None applied	BLOCKED_REJECT	
10	SUSPECTLIST		None applied	THROTTLED	
11	FREEMAIL		None applied	THROTTLED	
12	ACCEPTLIST		None applied	ACCEPTED	
	ALL		None applied	ACCEPTED	

Edit Order... | Export HAT...

Mail Flow Policy (standaard beleidsparameters)

Standaard beleidsparameters

Beveiligingsinstellingen

- Set Transport Layer Security (TLS) op voorkeursniveau
- Sender Policy Framework (SPF) inschakelen
- DomainKeys Identified Mail (DKIM) inschakelen
- Domeingebaseerde Berichtverificatie, -rapportage en -verificatie (DMARC) inschakelen en geaggregeerde feedback-rapporten verzenden

Opmerking: DMARC vereist extra afstemming om te configureren. Raadpleeg voor meer informatie over DMARC "E-mailverificatie > DMARC-verificatie" in de gebruikershandleiding voor de juiste versie van AsyncOS voor de Cisco Secure Email Gateway die u hebt geïmplementeerd.

Beleid voor inkomende post

Default Policy is ingesteld op:

anti-spam

- Ingeschakeld, met drempelwaarden bij standaarddrempelwaarden. (Wijziging van de score zou vals positieven kunnen verhogen.)

antivirus

- Berichten scannen: **alleen op virussen scannen** verzekeren dat het selectievakje "Inclusief een X-header" is ingeschakeld
- Voor **unscannable Berichten** en **Virus Infected Berichten**, plaats het **Originele Bericht van het Archief aan Nr**

AMP

- Voor **Onscanbare acties op Berichtfouten**, gebruik **Geavanceerd** en **voeg Aangepaste Kop toe aan Bericht**, X-TG-MSGERROR, waarde: Waar.
- Voor **niet-scanbare acties op snelheidslimiet**, gebruik **geavanceerde** en **voeg aangepaste header toe aan bericht**, X-TG-RATELIMINIT, waarde: Waar.
- Voor **Berichten met Bestandsanalyse in behandeling**, gebruik **Actie toegepast op Bericht**: "Quarantaine."

Graymail

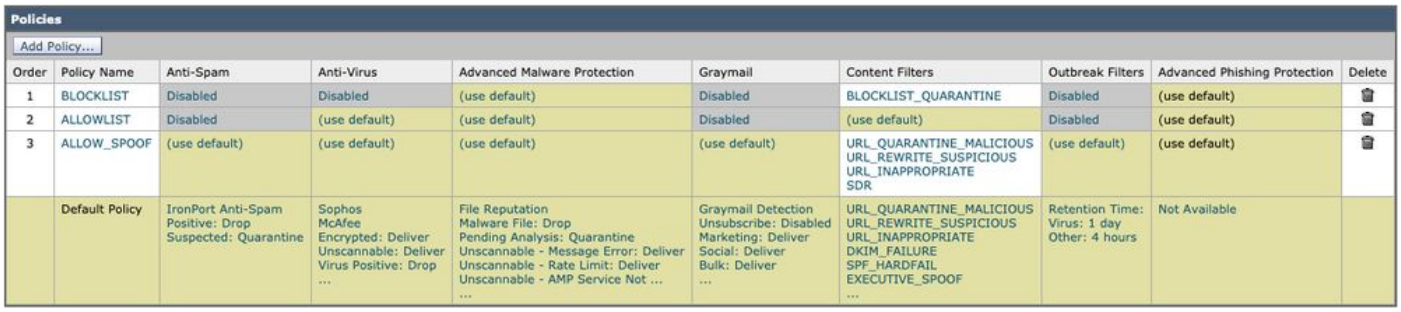
- Scannen is mogelijk voor elk vonnis (Marketing, Social, Bulk), met **Prepend** voor **Add Text to Onderwerp** en actie is **Deliver**.
- Voor **Actie op bulk Mail**, gebruik **Geavanceerd** en **voeg Aangepaste Kop toe (optioneel)**: X-bulk, waarde: Waar.

Contentfilters

- Ingeschakeld en URL_QUARANTAINE_MALICIOUS, URL_REWrite_suspICIOUS, URL_INFIT, DKIM_ERROR, SPF_HARDFAIL, Executive_SPOOF, DOMAIN_SPOOF, SDR, TG_RATE_limit zijn geselecteerd
- Deze inhoudsfilters worden later in deze gids verstrekt

Uitbraakfilters

- Het standaard bedreigingsniveau is 3; pas uw beveiligingsvereisten aan. Als het bedreigingsniveau voor een bericht gelijk is aan of deze drempel overschrijdt, beweegt het bericht naar de Quarantaine van de Uitbraak. (1=laagste dreiging, 5=hoogste dreiging)
- Berichtwijziging inschakelen
- URL-herschrijfset voor "Inschakelen voor alle berichten"
- Wijzig onderwerp voorafgaand aan: [Mogelijk $threat_category Fraud]



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	

Beleidsnamen (weergegeven)

- **E-mailbeleid voor BLOKLIJST**
  Het beleid van de post van BLOCKLIST wordt gevormd met alle diensten gehandicapt, behalve Geavanceerde Bescherming Malware, en verbindingen aan een inhoudsfilter met de actie van QUARANTAINE.

- **E-mailbeleid voor EMISSIELIJSTEN**
  Het beleid van de de postpost van allowLIST heeft Antispam, Graymail gehandicapt en de Filters van de Inhoud toegelaten voor URL_QUARANTAINE_MALICIOUS, URL_REWrite_suspICIOUS, URL_INFIT, DKIM_ERROR, SPF_HARDFAIL, Executive SPOOF, DOMAIN_SPOOF, SDR, TG_RATE_limit, of inhoudsfilters van uw keus en configuratie.

- **Mailbeleid van ENABLE_SPOOF**
  Het allow_SPOOF mailbeleid heeft alle standaard services ingeschakeld, met Content Filters ingeschakeld voor URL_QUARANTAINE_MALICIOUS, URL_REWrite_suspICIOUS, URL_INFIT, SDR of content filters van uw keuze en configuratie.

Beleid voor uitgaande post

Default Policy is ingesteld op:

anti-spam

- Uitgeschakeld

antivirus

- Berichten scannen: **Alleen op virussen scannen** Schakel het aankruisvakje "Een X-header opnemen" uit.
- (Optioneel) Voor alle berichten: **Geavanceerd > Overige meldingen**, "Overige" inschakelen en uw admin/SOC contact e-mailadres opnemen

Advanced Malware Protection

- Alleen bestandsnaam inschakelen
- **Niet-scannerbare acties op snelheidsbeperking**: Gebruik **Geavanceerd** en **voeg Aangepaste Kop toe aan Bericht**: X-TG-RATELIMINIT, waarde: "Waar".

- **Berichten met Malware Attachments**: Gebruik **Geavanceerd** en **voeg Aangepaste Kop toe aan Bericht**: X-TG-UITGAANDE, waarde: "MALWARE GEDETECTEERD."

Graymail

- Uitgeschakeld

Contentfilters

- Ingeschakeld en TG_OUTBOUND_MALICIOUS, Strip_Secret_Header, EXTERN_SENDER_DELETE, ACCOUNT_TAKEOVER, of inhoudsfilters van uw keuze worden geselecteerd.

Uitbraakfilters

- Uitgeschakeld

DLP

- inschakelen op basis van uw DLP-licentie en DLP-configuratie.

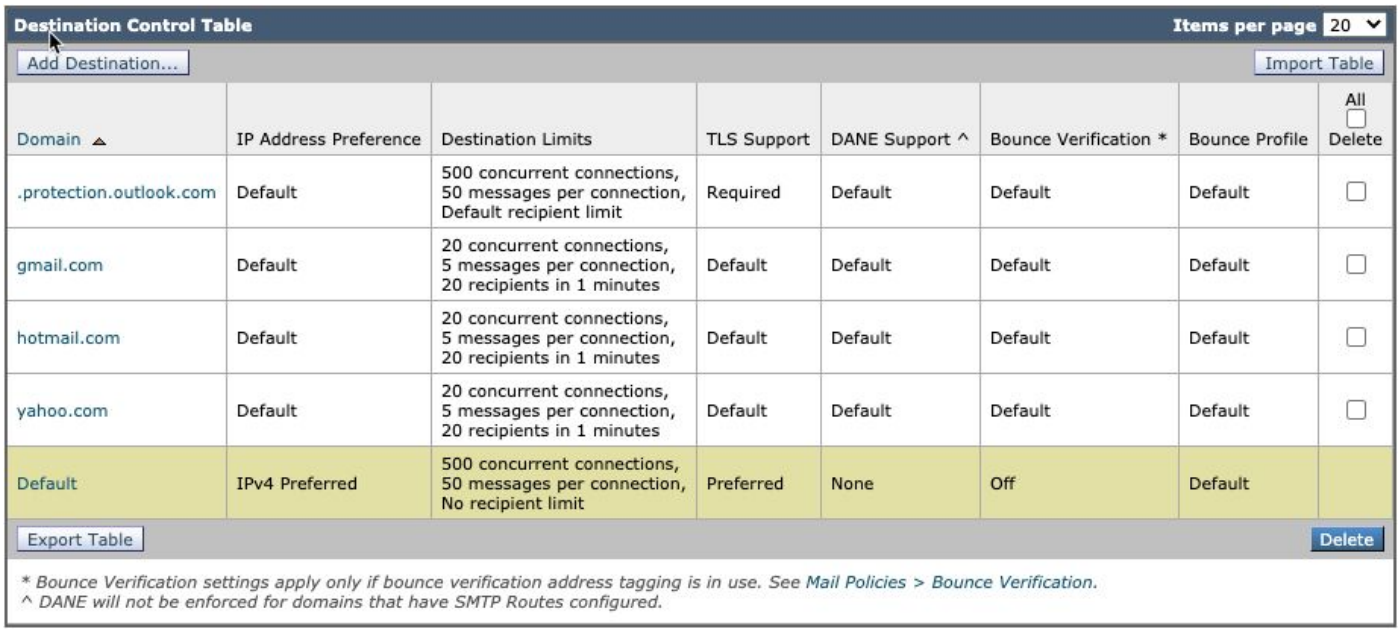
Overige instellingen

Woordenboeken (mailbeleid > Woordenboeken)

- **Profanity** en **Sexual_Content** Dictionary inschakelen en bekijken
- Maak **Executive_FED** woordenboek voor vervalste e-mail detectie met alle uitvoerende namen
- Maak extra woordenboeken voor beperkte of andere trefwoorden zoals u nodig ziet voor uw beleid, omgeving, beveiligingscontrole

Bestemmingscontroles (postbeleid > Bestemmingscontroles)

- Voor het standaarddomein moet u **TLS-ondersteuning** configureren als **voorkeursdomein**
- U kunt bestemmingen toevoegen voor webmaildomeinen en lagere drempelwaarden instellen
- Raadpleeg onze gids Snelheidsbeperking uw uitgaande mail met doelcontrole voor meer informatie.



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.

Contentfilters

> **Opmerking:** Raadpleeg voor extra informatie over contentfilters "contentfilters" in de gebruikershandleiding voor de juiste versie van AsyncOS voor de Cisco Secure Email Gateway die u hebt geïmplementeerd.

Inkomende contentfilters

URL_QUARANTAINE_KWAADAARDIG

Voorwaarde: URL reputatie; url-reputatie(-10.00, -6.00, "bypass_urls", 1, 1)

Actie: Quarantaine: quarantaine("URL_MALICIOUS")

URL_HERSCHRIJVEN_ACHTERDOCHTIG

Voorwaarde: URL reputatie; url-reputatie(-5.90, -5.60, "bypass_urls", 0, 1)

Actie: URL reputatie; url-reputatie-proxy-redirect(-5.90, -5.60,"",0)

URL_ONJUIST

Voorwaarde: URL-categorie; url-categorie (['Adult', 'Child Abuse Content', 'Extreme', 'Hate Speech', 'Illegal Activities', 'Illegal Downloads', 'Illegal Drugs', 'Pornography', 'Filter Avoidance'], "bypass_urls", 1, 1)

Actie: Quarantaine; duplicaat-quarantaine("INPASSEND_CONTENT")

DKIM_FALEN

Voorwaarde: DKIM-verificatie; dkim-verificatie == defect

Actie: Quarantaine; duplicaat-quarantaine("DKIM_FAIL")

SPF_HARDFAIL

Voorwaarde: SPF-verificatie; spf-status == mislukt

Actie: Quarantaine; duplicaat-quarantaine("SPF_HARDFAIL")

Executive_SPOOF

Voorwaarde: Vervalste e-maildetectie; vervalste e-mail detectie("Executive_FED", 90, "")

Voorwaarde: Andere kop; header ("X-IronPort-SenderGroup") != "(?i)allowspoof"

* instellen **Regel toepassen: Alleen als alle voorwaarden overeenkomen**

Actie: Kop toevoegen/bewerken; header-tekst bewerken ("Onderwerp", "(.*)", "[EXTERN]\\1")

Actie: Quarantaine; duplicaat-quarantaine("FORGED_EMAIL")

DOMEIN_LEPEL

Voorwaarde: Andere kop; header("X-Spoof")

Actie: Quarantaine; duplicaat-quarantaine("ANTI_SPOOF")

SDR

Voorwaarde: Domeinnaam; sdr-reputatie (['vreselijk'], "")

Voorwaarde: Domain Reputation; sdr-age ("days", <, 5, "")

* instellen **Regel toepassen: Als een of meer voorwaarden overeenkomen**

Actie: Quarantaine; duplicaat-quarantaine("SDR_DATA")

TG_TARIEF_LIMIET

Voorwaarde: Andere kop; header("X-TG-RATELIMINIT")

Actie: Loginvoer toevoegen; loginvoer("X-TG-RATELIMINIT: $bestandsnamen")

BLOKLIJST_QUARANTAINE

Voorwaarde: (None)

Actie: Quarantaine; quarantaine ("BLOKLIJST")

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...

Uitgaande contentfilters

TG_UITGAAND_KWAADAARDIG

Voorwaarde: Andere header; header ("X-TG-OUTBOUND") == MALWARE

Actie: Quarantaine; quarantaine("TG_OUTBOUND_MALWARE")

Strip_Secret_Header

Voorwaarde: Andere kop; kop ("PLAATSAANDUIDING") == PLAATSAANDUIDING

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

EXTERN_AFZENDER_VERWIJDEREN

Voorwaarde: (None)

Actie: Kop toevoegen/bewerken; kop-kop-tekst bewerken ("Onderwerp", "\\[EXTERN\]\\s?", "")

ACCOUNT_OVERNAME

Voorwaarde: Andere header; header("X-AMP-Resultaat") == (?i)kwaadaardig

Voorwaarde: URL reputatie; url-reputatie(-10.00, -6.00, "", 1, 1)

*Instellen **Regel toepassen: Als een of meer voorwaarden overeenkomen**

Actie: Waarschuwen;verwittigen ("<Insert admin or distro email address>", "MAY ACCOUNT TAKEOVER", "", "ACCOUNT_TAKEOVER_WARNING")

Actie: duplicate-quarantaine("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...

Voor klanten van Cisco Secure Email Cloud hebben we voorbeelden van inhoudsfilters die zijn opgenomen in de gouden configuratie en aanbevelingen voor best practices. Bekijk daarnaast de "VOORBEELD_" filters voor meer informatie over de bijbehorende voorwaarden en acties die gunstig kunnen zijn voor uw configuratie.

Cisco live

Cisco Live presenteert wereldwijd vele sessies en biedt persoonlijke sessies en technische doorbraken die de best practices van Cisco Secure Email dekken. Voor eerdere sessies en toegang gaat u naar Cisco Live (hiervoor is CCO-aanmelding vereist):

- Cisco e-mail security: Best practices en fijnafstemming - BRKSEC-2131
- DMARCate Uw e-mailperimeter - BRKSEC-2131
- E-mail repareren! - Cisco e-mail security geavanceerde probleemoplossing - BRKSEC-3265
- API-integraties voor Cisco e-mail security - DEVNET-2326
- SaaS-mailboxservices beveiligen met Cloud Email Security van Cisco - BRKSEC-1025
- E-mail security: Best practices en fijnafstemming - TECSEC-2345
- 250 not OK - Op weg naar het defensief met Cisco Email Security - TECSEC-2345
- Cisco Domain Protection en Cisco geavanceerde phishing-bescherming: Haal het meeste uit de Next Layer in Email Security! - BRKSEC-1243
- SPF is geen acroniem voor "Spoof"! Laten we de meeste uit de volgende laag in e-mail security gebruiken! - DGTL-BRKSEC-2327

Aanvullende informatie

Cisco Secure E-mail gateway-documentatie

- Release-opmerkingen
- Gebruikershandleiding
- CLI-referentiegids
- API-programmeerhandleidingen voor Cisco Secure Email Gateway
- Open bron die in Cisco Secure Email Gateway wordt gebruikt
- Installatiehandleiding voor Cisco Content Security virtuele applicatie (inclusief vESA)

Documentatie voor beveiligde e-mail met Cloud Gateway

- Release-opmerkingen
- Gebruikershandleiding

Cisco Secure Email en Web Manager-documentatie

- Releaseopmerkingen en compatibiliteitsmatrix
- Gebruikershandleiding
- API-programmeerhandleidingen voor Cisco Secure Email and Web Manager
- Installatiehandleiding voor Cisco Content Security virtuele applicatie (inclusief vSMA)

Cisco beveiligde productdocumentatie

- Cisco Secure-portfolio-naamgevingsarchitectuur

Gerelateerde informatie

- Naleving van Cisco Secure Email Security

- Beschrijving van aanbieding: Secure-e-mail
- Termen voor Cisco Universal Cloud
- Cisco-ondersteuning en -downloads
- [EXTERN] OpenSPF: SPF-basisgegevens en geavanceerde informatie

Over deze vertaling

Cisco heeft dit document vertaald via een combinatie van machine- en menselijke technologie om onze gebruikers wereldwijd ondersteuningscontent te bieden in hun eigen taal. Houd er rekening mee dat zelfs de beste machinevertaling niet net zo nauwkeurig is als die van een professionele vertaler. Cisco Systems, Inc. is niet aansprakelijk voor de nauwkeurigheid van deze vertalingen en raadt aan altijd het oorspronkelijke Engelstalige document (link) te raadplegen.