Secure Email Gateway および Cloud Gateway の URL フィルタリングの設定

内容

はじめに

このドキュメントでは、Cisco Secure Email GatewayおよびクラウドゲートウェイでURLフィルタリングを設定する方法と、URLフィルタリングの使用に関するベストプラクティスについて説明します。

背景説明

URLフィルタリングは、AsyncOS 11.1 for Email Securityで最初に導入されました。このリリースでは、Cisco Secure Emailの設定で、メッセージ添付ファイル内のURLをスキャンし、そのようなメッセージに対して設定されたアクションを実行できるようになりました。メッセージフィルタとコンテンツフィルタは、URLレピュテーションとURLカテゴリを使用して、メッセージと添付ファイルのURLを確認します。詳細については、ユーザガイドまたはオンラインヘルプの「メッセージフィルタを使用した電子メールポリシーの適用」、「コンテンツフィルタ」、および「信頼できない、または望ましくないURLからの保護」の各章を参照してください。

信頼できないリンクや望ましくないリンクに対する制御と保護は、アンチスパム、アウトブレイク、コンテンツ、およびメッセージフィルタリングプロセスの作業キューに組み込まれます。次のコントロールがあります。

- メッセージや添付ファイルの信頼できないURLからの保護の効果を高めます。
- また、URLフィルタリングはアウトブレイクフィルタに組み込まれています。この強化された保護は、Cisco Webセキュリティアプライアンス(WSA)を導入済みの組織であっても、またはWebベースの脅威からの同様の保護を導入済みの組織であっても適用できます。これは、侵入時点で脅威をブロックするためです。
- コンテンツまたはメッセージフィルタを使用して、メッセージ内のURLのWebベースのレピュテーションスコア(WBRS)に基づいてアクションを実行することもできます。たとえば、ニュートラルまたは未知のレピュテーションを含むURLを書き換えてCisco Webセキュリティプロキシにリダイレクトし、安全性のクリック時の評価を行うことができます。
- スパムの特定の改善
- このアプライアンスは、メッセージ内のリンクのレピュテーションとカテゴリ、およびその他のスパム識別アルゴリズムを使用して、スパムを識別します。たとえば、メッセージ内のリンクがマーケティングWebサイトに属している場合、そのメッセージはマーケティングメッセージである可能性が高くなります。
- 企業のアクセプタブルユースポリシーの適用をサポート
- URLのカテゴリ（アダルトコンテンツや違法行為など）は、コンテンツおよびメッセージフィルタと共に使用して、許容される企業使用ポリシーを適用できます。
- 保護用に書き換えられたメッセージ内のURLを最も頻繁にクリックした組織内のユーザー、および最も一般的にクリックされたリンクを特定できます。

注:AsyncOS 11.1 for Email Securityリリースでは、URLフィルタリングによって短縮されたURLのサポートが導入されました。CLIコマンド「websecurityadvancedconfig」を使用すると、短縮形サービスを表示して設定できます。この設定オプションは、AsyncOS 13.5 for Email Securityで更新されました。このリリースにアップグレードすると、短縮されたすべてのURLが展開されます。短縮されたURLの拡張を無効にするオプションはありません。このため、URL防御に最新の保護を提供するには、Eメールセキュリティ用のAsyncOS 13.5以降を推奨します。ユーザガイドまたはオンラインヘルプの「悪意のあるURLまたは望ましくないURLからの保護」の章と、AsyncOS for Cisco Eメールセキュリティアプライアンスの CLIリファレンスガイドを参照してください。

注：このドキュメントでは、AsyncOS 14.2 for Email Securityを例とスクリーンショットに使用しています。

注:Cisco Secure Emailでは、docs.ces.cisco.comで詳細なURL防御ガイドも提供しています。

前提条件

Cisco Secure Email GatewayまたはクラウドゲートウェイでURLフィルタリングを設定する場合は、必要な機能に応じて他の機能も設定する必要があります。URLフィルタリングとともに有効

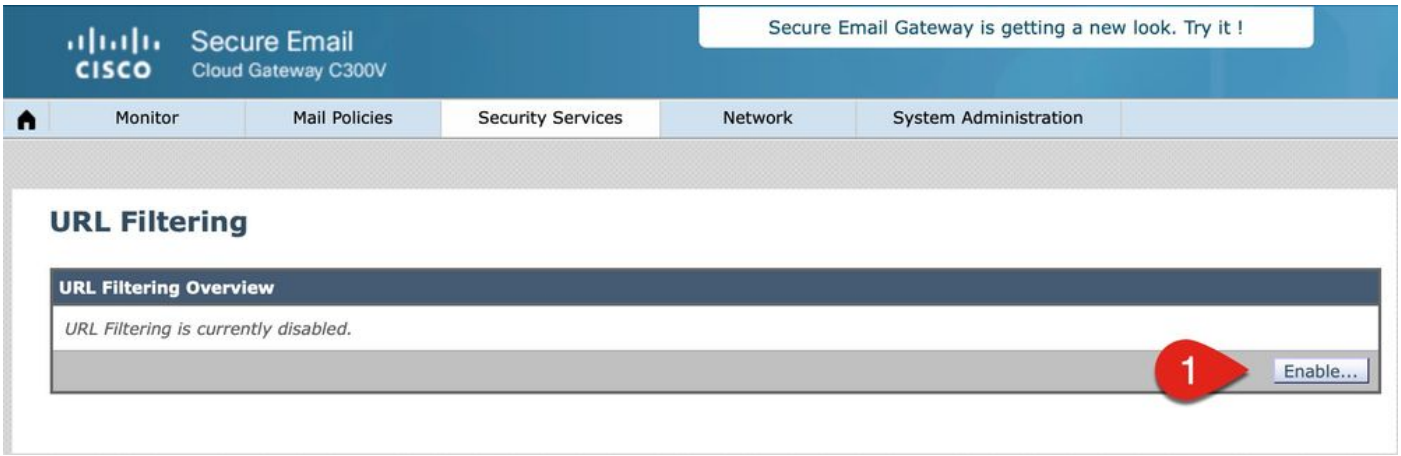
になる一般的な機能を次に示します。

- スパムに対する保護を強化するには、該当するメールポリシーに従ってアンチスパムスキャン機能をグローバルに有効にする必要があります。アンチスパムは、Cisco IronPort Anti-Spam(IPAS)またはCisco Intelligent Multi-Scan(IMS)機能のいずれかとみなされます。
- マルウェアに対する保護を強化するには、アウトブレイクフィルタまたはVirus Outbreak Filters(VOF)機能を該当するメールポリシーごとにグローバルに有効にする必要があります。
- URLレピュテーションに基づくアクションの場合、またはメッセージフィルタとコンテンツフィルタを使用してアクセプタブルユースポリシー(AUP)を適用する場合は、VOFをグローバルに有効にする必要があります。

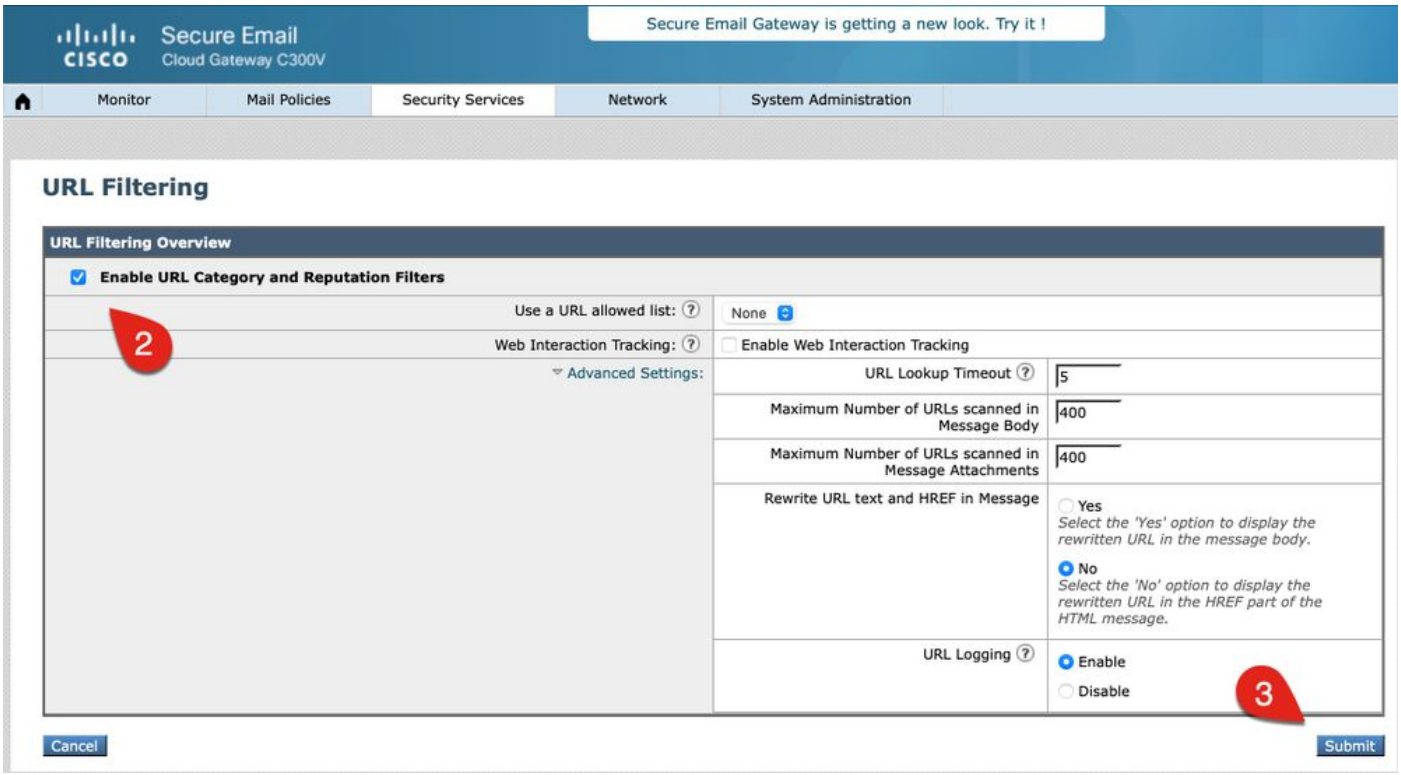
URL フィルタリングの有効化

まず、Cisco Secure Email GatewayまたはクラウドゲートウェイでURLフィルタリングを実装する機能を有効にする必要があります。URLフィルタリングは、管理者がGUIまたはCLIから有効にできます。

URLフィルタリングを有効にするには、GUIからSecurity Services > URL Filteringに移動し、Enableをクリックします。



次に、Enable URL Category and Reputation Filtersをクリックします。この例には、URL検索タイムアウト、スキャンされるURLの最大数に関するベストプラクティス値が含まれており、URLをログに記録するオプションを有効にします。



注：この時点で、設定に対する変更をコミットしていることを確認してください。

URLフィルタリングアクションの作成

URLフィルタリングだけを有効にすると、メッセージ内のURLや添付ファイルを含むメッセージに対してアクションは実行されません。

受信および送信メールポリシーのメッセージと添付ファイルに含まれるURLが評価されます。URLに対して有効な文字列はすべて、次のコンポーネントを含む文字列を含むように評価されます。

- HTTP、HTTPS、またはWWW
- ドメインまたはIPアドレス
- ポート番号の前にコロン(:)を付ける
- 大文字または小文字

注:URLログエントリは、ほとんどのURLのmail_logsから確認できます。URLがmail_logsに記録されていない場合は、メッセージID(MID)のメッセージトラッキングを確認してください。メッセージトラッキングには、「URLの詳細」のタブが含まれています。

システムがURLを評価してメッセージがスパムであるかどうかを判断する際、負荷管理に必要な場合は、発信メッセージよりも着信メッセージを優先してスクリーニングします。

メッセージに対するアクションは、メッセージ本文のURLレピュテーションまたはURLカテゴリ、または添付ファイルを含むメッセージに基づいて実行できます。

たとえば、Adultカテゴリの URLを含むすべてのメッセージに対してDrop (Final Action)アクションを適用する場合は、Adultカテゴリを選択した状態でURL Categoryタイプの条件を追加します。

カテゴリを指定しない場合、選択したアクションはすべてのメッセージに適用されます。

Trusted、Proferred、Neutral、Suspected、およびUntrustedのURLレピュテーションスコア範囲は事前に定義されており、編集できません。カスタム範囲を指定できます。レピュテーションスコアがまだ決定されていないURLには「Unknown」を使用します。

URLをすばやくスキャンしてアクションを実行するには、コンテンツフィルタを作成して、メッセージに有効なURLが含まれている場合にそのアクションが適用されるようにします。GUIから、Mail Policies > Incoming Content Filters > Add Filterの順に移動します。

URLに関連するアクションは次のとおりです。

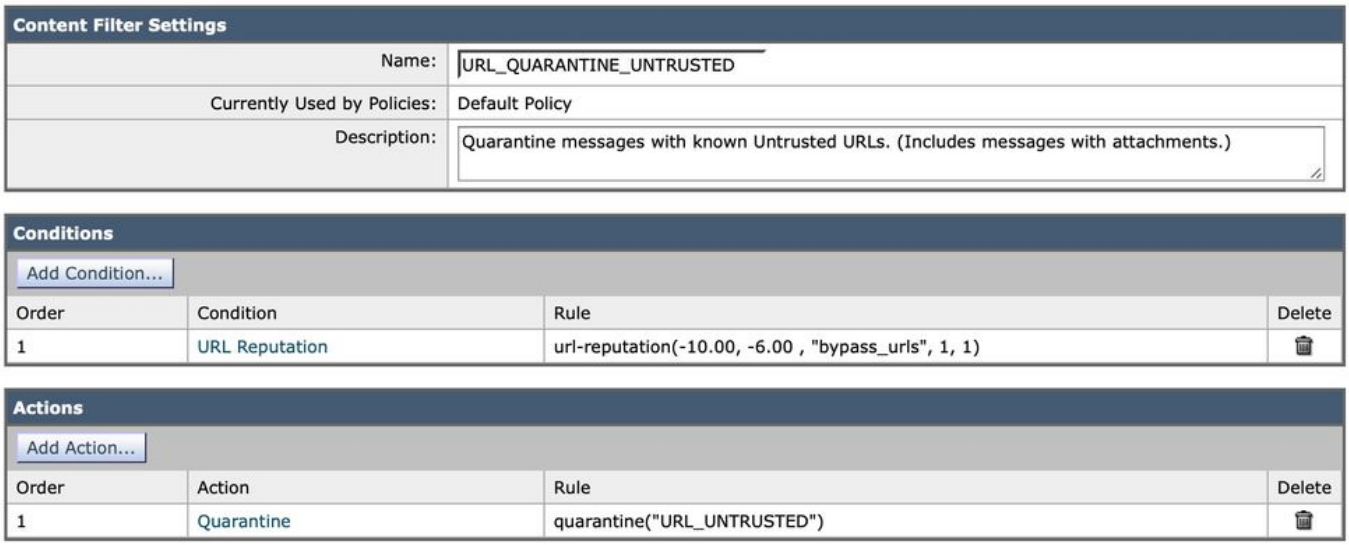
- URLの定義
  - URLはクリックできないように変更されますが、メッセージの受信者は目的のURLを読み取ることができます（元のURLに余分な文字が挿入されます）。
- Ciscoセキュリティプロキシにリダイレクトする
  - クリックすると、追加の検証のためにCisco Security Proxyを通過するURLが書き換えられます。Cisco Security Proxyの判定に基づいて、ユーザがサイトにアクセスできない可能性があります。
- URLをテキストメッセージで置き換える
  - このオプションを使用すると、管理者はメッセージ内のURLを書き換えて、リモートブラウザの隔離のために外部に送信できます。

信頼できないURL

Untrusted（信頼できない）：非常に悪い、悪意がある、または望ましくないURLの動作。これは最も安全な推奨ブロックリストのしきい値ですが、URLの脅威レベルが低いためにブロックされないメッセージが存在する可能性があります。セキュリティよりも配信を優先

推奨処置：ブロックします。（管理者はメッセージ全体を隔離または削除できます）。

次の例は、信頼できないURLを検出するためのURLフィルタリングのコンテンツフィルタのコンテキストを示しています。



Content Filter Settings

Name:	URL_QUARANTINE_UNTRUSTED
Currently Used by Policies:	Default Policy
Description:	Quarantine messages with known Untrusted URLs. (Includes messages with attachments.)

Conditions

Add Condition...

Order	Condition	Rule	Delete
1	URL Reputation	url-reputation(-10.00, -6.00 , "bypass_urls", 1, 1)	

Actions

Add Action...

Order	Action	Rule	Delete
1	Quarantine	quarantine("URL_UNTRUSTED")	

このコンテンツフィルタを設定すると、Cisco Secure Emailは信頼できないレピュテーション(-10.00 ~ -6.00)を持つURLをスキャンし、そのメッセージを検疫URL_UNTRUSTEDに入れます。mail_logsの例を次に示します。

<#root>

```
Tue Jul 5 15:01:25 2022 Info: ICID 5 ACCEPT SG MY_TRUSTED_HOSTS match 127.0.0.1 SBRS None country Unite
Tue Jul 5 15:01:25 2022 Info: ICID 5 TLS success protocol TLSv1.2 cipher ECDHE-RSA-AES256-GCM-SHA384
Tue Jul 5 15:01:25 2022 Info: Start MID 3 ICID 5
Tue Jul 5 15:01:25 2022 Info: MID 3 ICID 5 From: <test@test.com>
Tue Jul 5 15:01:25 2022 Info: MID 3 SDR: Domains for which SDR is requested: reverse DNS host: example.
Tue Jul 5 15:01:25 2022 Info: MID 3 SDR: Consolidated Sender Threat Level: Neutral, Threat Category: N/
Tue Jul 5 15:01:25 2022 Info: MID 3 ICID 5 RID 0 To: <end_user>
Tue Jul 5 15:01:25 2022 Info: MID 3 Message-ID '<20220705145935.1835303@ip-127-0-0-1.internal>'
Tue Jul 5 15:01:25 2022 Info: MID 3 Subject "test is sent you a URL => 15504c0618"
Tue Jul 5 15:01:25 2022 Info: MID 3 SDR: Domains for which SDR is requested: reverse DNS host:ip-127-0-
Tue Jul 5 15:01:25 2022 Info: MID 3 SDR: Consolidated Sender Threat Level: Neutral, Threat Category: N/
Tue Jul 5 15:01:25 2022 Info: MID 3 SDR: Tracker Header : 62c45245_jTikQ2lV2NYfmrGzMwQMBd68fxqFFueNmElw
Tue Jul 5 15:01:25 2022 Info: MID 3 ready 3123 bytes from <test@test.com>
Tue Jul 5 15:01:25 2022 Info: MID 3 matched all recipients for per-recipient policy DEFAULT in the inbo
Tue Jul 5 15:01:25 2022 Info: ICID 5 close

Tue Jul 5 15:01:25 2022 Info: MID 3 URL https://www.ihaveabadreputation.com/ has reputation -9.5 matched


Tue Jul 5 15:01:25 2022 Info: MID 3 quarantined to "Policy" (content filter:URL_QUARANTINE_UNTRUSTED)


Tue Jul 5 15:01:25 2022 Info: Message finished MID 3 done
```

URL ihaveabadreputation.comはUNTRUSTEDと見なされ、-9.5で採点されます。URLフィルタリングによって信頼できないURLが検出され、URL_UNTRUSTEDに対して検疫されました。

前述のmail_logsの例では、URLフィルタリングのコンテンツフィルタのみが着信メールポリシーに対して有効になっている場合の例を示しています。同じメールポリシーでスパム対策などの追加サービスが有効になっている場合、他のサービスは、それらのサービスとそのルールからURLが検出されたかどうかを示します。同じURLの例では、着信メールポリシーに対してCisco Anti-Spam Engine(CASE)が有効になっており、メッセージ本文がスキャンされてスパム陽性と判定されます。アンチスパムはメール処理パイプラインの最初のサービスであるため、これはmail_logsで最初に示されます。コンテンツフィルタは、メール処理パイプラインの後半に追加されます。

<#root>

```
Tue Jul 5 15:19:48 2022 Info: ICID 6 ACCEPT SG MY_TRUSTED_HOSTS match 127.0.0.1 SBRS None country Unite
Tue Jul 5 15:19:48 2022 Info: ICID 6 TLS success protocol TLSv1.2 cipher ECDHE-RSA-AES256-GCM-SHA384
Tue Jul 5 15:19:48 2022 Info: Start MID 4 ICID 6
Tue Jul 5 15:19:48 2022 Info: MID 4 ICID 6 From: <test@test.com>
Tue Jul 5 15:19:48 2022 Info: MID 4 SDR: Domains for which SDR is requested: reverse DNS host:ip-127-0-
Tue Jul 5 15:19:49 2022 Info: MID 4 SDR: Consolidated Sender Threat Level: Neutral, Threat Category: N/
Tue Jul 5 15:19:49 2022 Info: MID 4 ICID 6 RID 0 To: <end_user>
Tue Jul 5 15:19:49 2022 Info: MID 4 Message-ID '<20220705151759.1841272@ip-127-0-0-1.internal>'
Tue Jul 5 15:19:49 2022 Info: MID 4 Subject "test is sent you a URL => 646aca13b8"
Tue Jul 5 15:19:49 2022 Info: MID 4 SDR: Domains for which SDR is requested: reverse DNS host:ip-127-0-
Tue Jul 5 15:19:49 2022 Info: MID 4 SDR: Consolidated Sender Threat Level: Neutral, Threat Category: N/
Tue Jul 5 15:19:49 2022 Info: MID 4 SDR: Tracker Header : 62c45695_mqwplhpxGDqtgUp/XTLGFKD60hwNKKsghUKA
Tue Jul 5 15:19:49 2022 Info: MID 4 ready 3157 bytes from <test@test.com>
Tue Jul 5 15:19:49 2022 Info: MID 4 matched all recipients for per-recipient policy DEFAULT in the inbo
Tue Jul 5 15:19:49 2022 Info: ICID 6 close
```

Tue Jul 5 15:19:49 2022 Info: MID 4 interim verdict using engine: CASE spam positive

Tue Jul 5 15:19:49 2022 Info: MID 4 using engine: CASE spam positive

```
Tue Jul 5 15:19:49 2022 Info: ISQ: Tagging MID 4 for quarantine
Tue Jul 5 15:19:49 2022 Info: MID 4 URL https://www.ihaveabadreputation.com/ has reputation -9.5 matche
Tue Jul 5 15:19:49 2022 Info: MID 4 quarantined to "URL_UNTRUSTED" (content filter:URL_QUARANTINE_UNTRU
Tue Jul 5 15:19:49 2022 Info: Message finished MID 4 done
```

CASEルールとIPASルールに、特定の送信者、ドメイン、またはメッセージの内容と照合してURLの脅威だけを検出するルール、レピュテーション、またはスコアが含まれている場合があります。この例では、スパム検疫(ISQ)用にタグ付けされたihaveabadreputation.comと、URL_QUARANTINE_UNTRUSTEDコンテンツフィルタによるURL_UNTRUSTED検疫が確認されています。メッセージは、最初にURL_UNTRUSTED隔離に入ります。管理者によってメッセージがその隔離から解放されるか、URL_UNTRUSTED隔離の時間制限/設定基準が満たされると、メッセージは次にISQに移動されます。

管理者の設定に基づいて、コンテンツフィルタに追加の条件とアクションを設定できます。

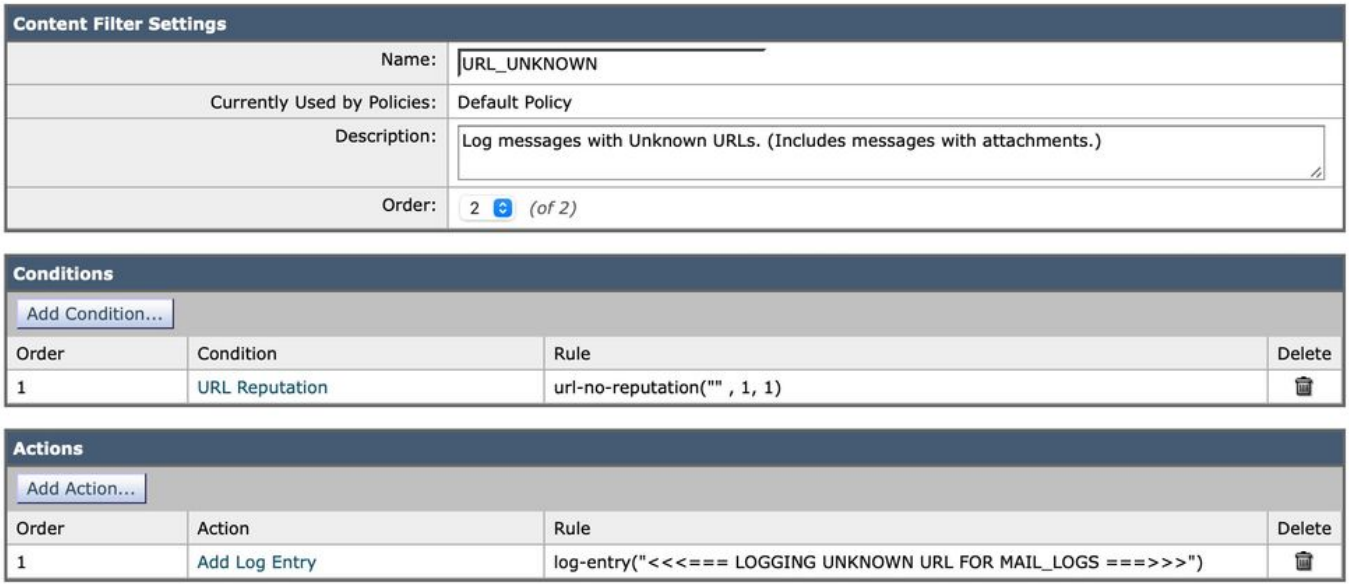
不明なURL

Unknown:以前に評価されていないか、または脅威レベルの判定をアサートする機能が表示されていません。URLレピュテーションサービスにレピュテーションを確立するための十分なデータがありません。この判定は、URLレピュテーションポリシーでの直接のアクションには適していません。

推奨処置：後続のエンジンをスキャンして、他の悪意のある可能性のあるコンテンツを確認します。

未知のURLまたは「レピュテーションなし」は、新しいドメインを含むURLや、トラフィックがほとんどまたはまったく検出されず、評価されたレピュテーションや脅威レベルの判定を受けることができないURLである可能性があります。これらのドメインと発信元に関する詳細な情報が取得されると、これらはUntrustedに変わる可能性があります。このようなURLについては、ログに記録するコンテンツフィルタ、または不明なURLの検出を含むコンテンツフィルタを使用することをお勧めします。AsyncOS 14.2では、不明なURLがTalos Intelligence Cloud Serviceに送信され、さまざまな脅威インジケータでトリガーされる詳細なURL分析が行われます。また、不明なURLのメールログエントリは、MIDに含まれているURLの表示と、URL保護による修復の可能性を管理者に提供します。(詳細については、『Microsoft Azure (Microsoft 365) API - CiscoのCisco Secure Email Account Settingsの設定方法』を参照してください)。

次の例は、不明なURLを検出するためのURLフィルタリングのコンテンツフィルタのコンテキストを示しています。



このコンテンツフィルタを設定すると、Cisco Secure EmailはレピュテーションがUnknownのURLをスキャンし、ログ行をmail_logsに書き込みます。mail_logsの例を次に示します。

<#root>

```
Tue Jul 5 16:51:53 2022 Info: ICID 20 ACCEPT SG MY_TRUSTED_HOSTS match 127.0.0.1 SBRS None country Unit
```

```
Tue Jul 5 16:51:53 2022 Info: ICID 20 TLS success protocol TLSv1.2 cipher ECDHE-RSA-AES256-GCM-SHA384
Tue Jul 5 16:51:53 2022 Info: Start MID 16 ICID 20
Tue Jul 5 16:51:53 2022 Info: MID 16 ICID 20 From: <test@test.com>
Tue Jul 5 16:51:53 2022 Info: MID 16 SDR: Domains for which SDR is requested: reverse DNS host:ip-127-0
Tue Jul 5 16:51:53 2022 Info: MID 16 SDR: Consolidated Sender Threat Level: Neutral, Threat Category: N
Tue Jul 5 16:51:53 2022 Info: MID 16 ICID 20 RID 0 To: <end_user>
Tue Jul 5 16:51:53 2022 Info: MID 16 Message-ID '<20220705165003.1870404@ip-127-0-0-1.internal>'
Tue Jul 5 16:51:53 2022 Info: MID 16 Subject "test is sent you a URL => e835eadd28"
Tue Jul 5 16:51:53 2022 Info: MID 16 SDR: Domains for which SDR is requested: reverse DNS host:ip-127-0
Tue Jul 5 16:51:53 2022 Info: MID 16 SDR: Consolidated Sender Threat Level: Neutral, Threat Category: N
Tue Jul 5 16:51:53 2022 Info: MID 16 SDR: Tracker Header : 62c46c29_vrAqZZys2Hqk+BFINVrzdNLLn81kuIf/K6o
Tue Jul 5 16:51:53 2022 Info: MID 16 ready 3208 bytes from <test@test.com>
Tue Jul 5 16:51:53 2022 Info: MID 16 matched all recipients for per-recipient policy DEFAULT in the inb
Tue Jul 5 16:51:53 2022 Info: ICID 20 close
Tue Jul 5 16:51:54 2022 Info: MID 16 interim verdict using engine: CASE spam negative
Tue Jul 5 16:51:54 2022 Info: MID 16 using engine: CASE spam negative

Tue Jul 5 16:51:54 2022 Info: MID 16 URL http://mytest.example.com/test_url_2022070503 has reputation no


Tue Jul 5 16:51:54 2022 Info: MID 16 Custom Log Entry: <<<=== LOGGING UNKNOWN URL FOR MAIL_LOGS ===>>>


Tue Jul 5 16:51:54 2022 Info: MID 16 queued for delivery
Tue Jul 5 16:51:54 2022 Info: Delivery start DCID 13 MID 16 to RID [0]
Tue Jul 5 16:51:56 2022 Info: Message done DCID 13 MID 16 to RID [0]
Tue Jul 5 16:51:56 2022 Info: MID 16 RID [0] Response '2.6.0 <20220705165003.1870404@ip-127-0-0-1.inter
Tue Jul 5 16:51:56 2022 Info: Message finished MID 16 done
Tue Jul 5 16:52:01 2022 Info: DCID 13 close
```

URL mytest.example.com/test_url_2022070503はレピュテーションがなく、「noscore」で表示されます。 URL_UNKNOWNコンテンツフィルタは、設定されたとおりにloglineをmail_logsに書き込みます。

Cisco Secure Email GatewayからTalos Intelligence Cloud Serviceへのポーリングサイクルの後、URLがスキャンされ、信頼できないと判断されます。これは、ECSログの「Trace」レベルで確認できます。

```
Tue Jul  5 16:54:42 2022 Debug: ECS: Finish polling
Tue Jul  5 16:55:42 2022 Debug: ECS: Remediation service notified.
Tue Jul  5 16:55:42 2022 Debug: ECS: Initiating remediation
Tue Jul  5 16:55:42 2022 Info: ECS: Initiating message remediation:
{'from': ['test@test.com'], 'URL': 'http://mytest.example.com/test_url_2022070503', 'message ID':
'<20220705165003.1870404@ip-172-31-43-120.us-east-2.compute.internal>', 'MID': 16, 'verdict':
'MALICIOUS', 'message UUID': 'e90dec74-f50b-4a63-9ab2-6adda4fcf422'}
Tue Jul  5 16:55:42 2022 Debug: ECS: Unprocessed Remediation Data : [{'url_hash':
'8c6915e2ebbc9225ff8958db06db33beb4e932ae9e0d8c5b35805a2fxxyyxxyy', 'message_details': '{"mid": 16,
"birth_time": "1657039913", "from_addrs": ["test@test.com"], "recipients": ["[redacted]"],
"delivery_status": 1, "remediation_req_status": 3}', 'created_at': '2022-07-05 16:52:42.04515',
'verdict': '{"url": "http://mytest.example.com/test_url_2022070503", "verdict": "MALICIOUS"}',
'message_uuid': 'e90dec74-f50b-4a63-9ab2-6adda4fcf422', 'message_id':
'<20220705165003.1870404@ip-127-0-0-1.internal>'}]
Tue Jul  5 16:55:42 2022 Debug: ECS: Remediation records: [
    [
        16,
        "<20220705165003.1870404@ip-127-0-0-1.internal>",
        1657039913,
        "delete",
        3,
        "[{\"url\": \"http://mytest.example.com/test_url_2022070503\", \"conviction_timestamp\":
\"2022-07-05 16:52:42.04515\", \"url_hash\":
\"8c6915e2ebbc9225ff8958db06db33beb4e932ae9e0d8c5b35805a2fxxyyxxyy\"}]",
        [
            "[redacted]"
        ],
        [
            "test@test.com"
        ]
    ]
]
Tue Jul  5 16:55:42 2022 Debug: ECS: Remediation initiated.
Tue Jul  5 16:55:42 2022 Debug: ECS: Successfully recorded remediation initiation status into datastore.
```

その後、mail_logsで修復自体が呼び出されて完了すると、次のようになります。

```
Tue Jul 5 16:55:42 2022 Info: Message 16 containing URL 'http://mytest.example.com/test_url_2022070503'
Tue Jul 5 16:55:55 2022 Info: Message 16 was processed due to URL retrospection by Mailbox Remediation
```

管理者は、自分の裁量で不明なURLに対するアクションを検討する必要があります。フィッシング関連の電子メールおよび添付ファイルが増加している場合は、mail_logsおよびコンテンツフィルタレポートを確認してください。さらに、管理者は、クリック時の評価のためにUnknown URL(s)をCisco Security proxyサービスにリダイレクトするように設定できます。この例では、URL_UNKNOWNコンテンツフィルタ内でAdd Action > URL Reputationに移動します。

URL Reputation

Help

What is the reputation of the URL in the message body, subject or the message attachments? This rule evaluates the URL using either the Web Based Reputation Score (WBRS) or using information from the External Threat Feed engine.

Matching Condition

- (•) URL Reputation
  - ( ) Untrusted (-10.0 to -6.0)
  - ( ) Questionable (-5.9 to -3.1)
  - ( ) Neutral (-3.0 to 0.0)
  - ( ) Favorable (0.1 to 5.9)
  - ( ) Trusted (6.0 to 10.0)
  - ( ) Custom Range (min to max)
  - (•) Unknown
- ( ) External Threat Feeds

This option is currently unavailable because no threat feed sources have been configured. To create one, go to Mail Policies > External Threat Feeds Manager.

Use a URL allowed list: None

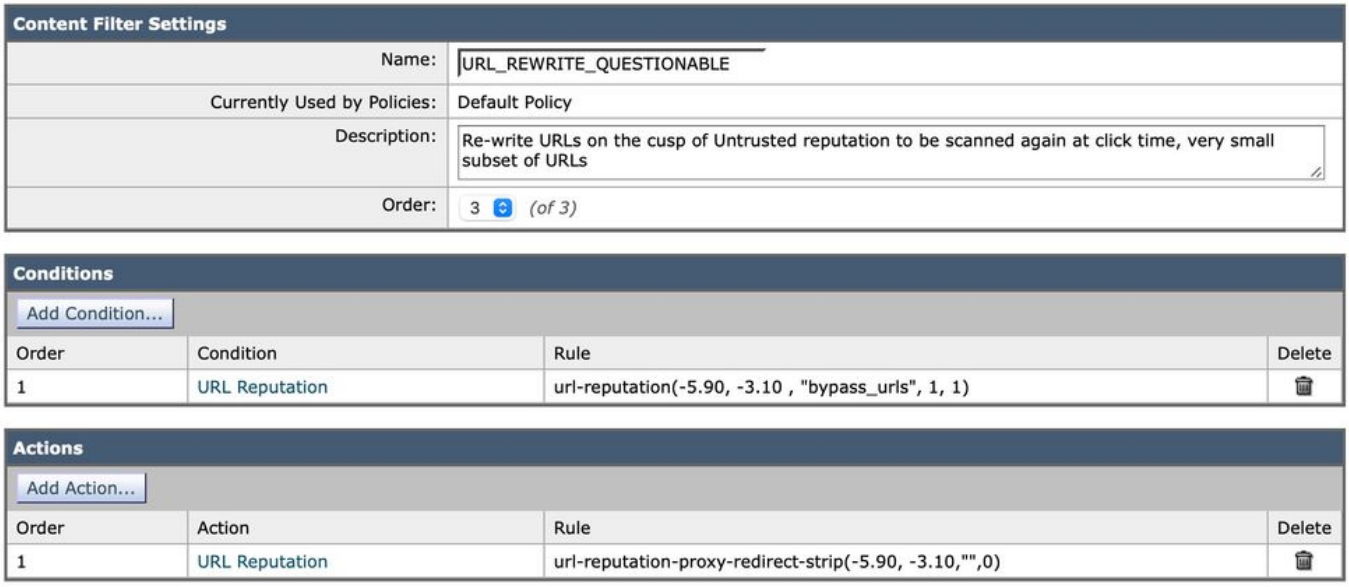
Check URLs within

- ( ) Message Body and Subject
- ( ) Attachments
- (•) All (Message Body, Subject and Attachments)

Action on URL within the message body and subject:

推奨処置：後続のエンジンでスキャンし、確認後にブロックします。

「不明なURL」で設定したとおり、管理者はCisco Security Proxyに「問題のあるURL」を送信するか、URLを完全に定義するアクションを利用することが有益であると判断できます。



Content Filter Settings

Name:	URL_REWRITE_QUESTIONABLE
Currently Used by Policies:	Default Policy
Description:	Re-write URLs on the cusp of Untrusted reputation to be scanned again at click time, very small subset of URLs
Order:	3 (of 3)

Conditions

Add Condition...

Order	Condition	Rule	Delete
1	URL Reputation	url-reputation(-5.90, -3.10 , "bypass_urls", 1, 1)	

Actions

Add Action...

Order	Action	Rule	Delete
1	URL Reputation	url-reputation-proxy-redirect-strip(-5.90, -3.10,"",0)	

ニュートラルURL

ニュートラル：正または負の動作を持たないURL。ただし、評価は完了しています。つまり、URLには現時点で既知のリスクはありません。したがって、これがレピュテーション判定の大部分です。
推奨処置：後続のエンジンをスキャンして、他の悪意のある可能性のあるコンテンツを確認します。

管理者は、負のスコアが付いたニュートラルURLを脅威として見ることができます。メッセージの数とニュートラルURLの発生回数は、お客様の裁量で評価してください。シスコのセキュリティプロキシにURLを送信するアクションを利用するために不明なURLや疑わしいURLを更新した方法と同様に、ニュートラルURL、またはニュートラルのマイナス側のサブセットを含むカスタム範囲を検討できます。次の例は、この着信コンテンツフィルタの実装によるニュートラルURLのスキャンを示しています。

Content Filter Settings

Name:	URL_NEUTRAL
Currently Used by Policies:	*No policies currently use this rule.*
Description:	Send questionable Neutral URLs to be scanned again at click time. (Includes messages with attachments.)
Order:	4 *(of 4)*

Conditions

Add Condition...

Order	Condition	Rule	Delete
1	URL Reputation	url-reputation(-3.00, -0.50 , "", 1, 1)	

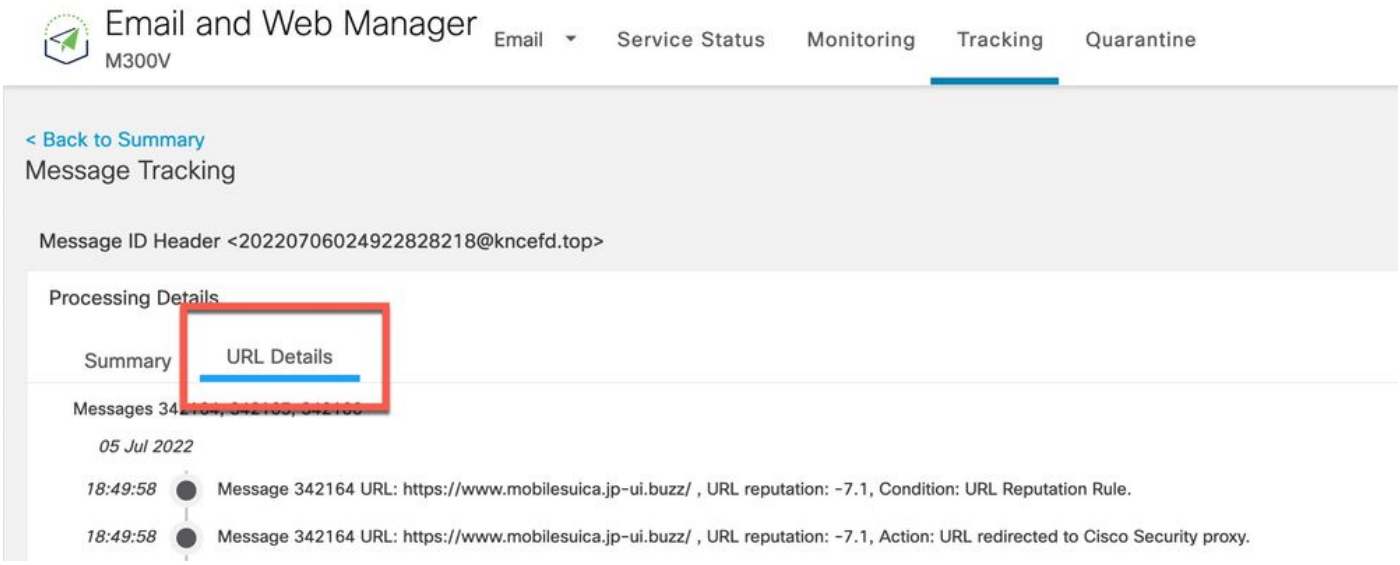
Actions

Add Action...

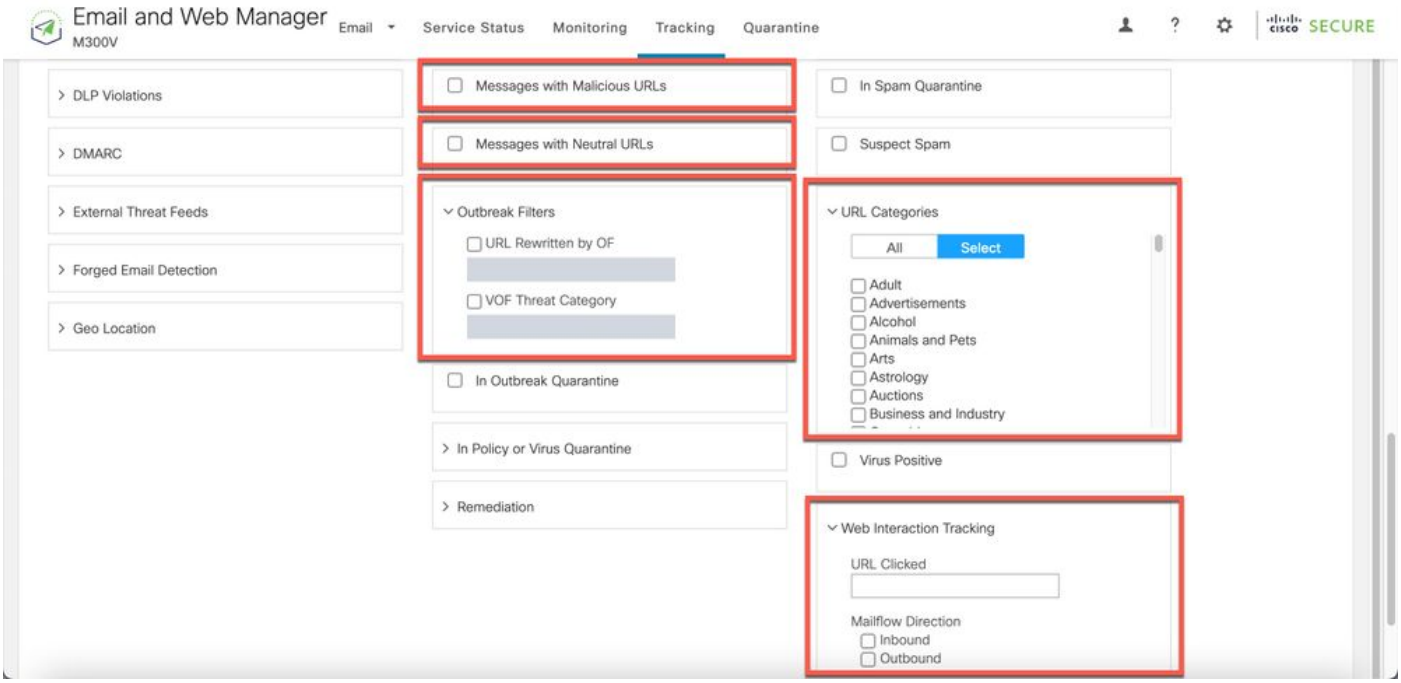
Order	Action	Rule	Delete
1	URL Reputation	url-reputation-proxy-redirect-strip(-3.00, -0.50,"",0)	

メッセージ トラッキング

MIDに関連付けられたURLのメッセージトラッキングオプションを確認します。 URLがmail_logsに記録されない場合があり、メッセージ追跡の詳細で見つけることができます。例：



また、メッセージトラッキングには、URL防御とインタラクションを備えたメッセージの高度な検索オプションもあります。



未分類および誤って分類されたURLのレポート

URLは、レピュテーションまたは分類なしでレポートされることがあります。誤って分類されたURLもあります。これらのURL目撃情報を報告するには、Talos'Reputation Center Supportページにあるcisco Talos'のWeb Categorization Requestsにアクセスしてください。

URLをレポートした後は、URLのステータスを マイチケット ページを使用します。

悪意のあるURLとマーケティングメッセージがスパム対策フィルタまたはアウトブレイクフィルタで検出されない

これは、サイトのレピュテーションとカテゴリが、スパム対策フィルタやアウトブレイクフィルタが判定を行う際に使用する多くの基準の中で2つしかないために発生する可能性があります。これらのフィルタの感度を高めるには、書き換えやURLのテキストへの置き換え、検疫、またはメッセージのドロップなど、アクションを実行するために必要な閾値を低くします。

または、URLレピュテーションスコアに基づいてコンテンツフィルタまたはメッセージフィルタを作成できます。

付録

短縮されたURLに対するURLフィルタリングサポートの有効化

注：このセクションは、AsyncOS 11.1 ~ 13.0 for Email Securityにのみ適用されます。

短縮されたURLに対するURLフィルタリングサポートは、CLIでのみwebsecurityadvancedconfigコマンドを使用して実行できます。

```
<#root>

myesa.local>

websecurityadvancedconfig


...

Do you want to enable URL filtering for shortened URLs? [N]>

Y


For shortened URL support to work, please ensure that ESA is able to connect to following domains:
bit.ly, tinyurl.com, ow.ly, tumblr.com, ff.im, youtu.be, tl.gd, plurk.com, url4.eu, j.mp, goo.gl, yfrog
```

シスコでは、URLフィルタリング設定のベストプラクティスに従って、これを有効にすることを推奨しています。有効にすると、短縮されたURLがメッセージ内で使用されるたびにメールログに反映されます。

```
Mon Aug 27 14:56:49 2018 Info: MID 1810 having URL: http://bit.ly/2tztQUi has been expanded to https://
```

この記事で説明するようにURLフィルタリングを有効にすると、mail_logsの例から、bit.lyリンクが記録され、展開先の元のリンクも記録されていることがわかります。

- ## 追加情報

  ### Cisco Secure Email Gatewayに関するドキュメント

  - リリース ノート
  - ユーザガイド
  - CLIリファレンスガイド
  - Cisco Secure Email GatewayのAPIプログラミングガイド

- Cisco Secure Email Gatewayで使用されるオープンソース
- Ciscoコンテンツセキュリティ仮想アプライアンスインストールガイド（vESAを含む）

セキュアなEメールクラウドゲートウェイに関する文書

- リリース ノート
- ユーザガイド

Cisco Secure Email and Web Managerに関するドキュメント

- リリースノートと互換性マトリクス
- ユーザガイド
- Cisco Secure Email and Web ManagerのAPIプログラミングガイド
- Ciscoコンテンツセキュリティ仮想アプライアンスインストールガイド（vSMAを含む）

Cisco Secure製品ドキュメント

- Cisco Secureポートフォリオの命名アーキテクチャ

翻訳について
シスコは世界中のユーザにそれぞれの言語でサポート コンテンツを提供するために、機械と人による翻訳を組み合わせて、本ドキュメントを翻訳しています。ただし、最高度の機械翻訳であっても、専門家による翻訳のような正確性は確保されません。シスコは、これら翻訳の正確性について法的責任を負いません。原典である英語版（リンクからアクセス可能）もあわせて参照することを推奨します。