Cisco Umbrella

Cisco Umbrella で定義されている FQDN ポリシーをユーザ接続に適用できるようにするため、DNS 要求を Cisco Umbrella へリダイレクトするようにデバイスを設定できます。次のトピックでは、デバイスを Cisco Umbrella と統合するように Umbrella Connector を設定する方法について説明します。

Cisco Umbrella Connector について

Cisco Umbrella を使用する場合、Cisco Umbrella Connector を設定して DNS クエリーを Cisco Umbrella へリダイレクトできます。これにより、Cisco Umbrella でブラックリストまたはグレーリストのドメイン名に対する要求を特定し、DNS ベースのセキュリティ ポリシーを適用することができます。

Umbrella Connector は、システムの DNS インスペクションの一部です。既存の DNS インスペクション ポリシー マップにより、DNS インスペクションの設定に基づく要求をブロックまたはドロップするように決められている場合、その要求は Cisco Umbrella へ転送されません。したがって、ローカルの DNS インスペクション ポリシーと Cisco Umbrella のクラウドベースのポリシーの 2 つが保護されます。

DNS ルックアップ要求を Cisco Umbrella へリダイレクトすると、Umbrella Connector は EDNS（DNS の拡張メカニズム）レコードを追加します。EDNS レコードには、デバイス識別子情報、組織 ID、およびクライアント IP アドレスが含まれています。クラウドベースのポリシーでこれらの条件を使用することで、FQDN のレピュテーションだけでなくアクセスを制御することができます。また、DNSCrypt を使用して DNS 要求を暗号化し、ユーザ名と内部の IP アドレスのプライバシーを確保することもできます。

Cisco Umbrella エンタープライズ セキュリティ ポリシー

クラウドベースの Cisco Umbrella エンタープライズ セキュリティ ポリシーでは、DNS ルックアップ要求で完全修飾ドメイン名（FQDN）のレピュテーションに基づいてアクセスを制御することができます。エンタープライズ セキュリティ ポリシーによって、次のいずれかのアクションを強制できます。

- ホワイトリスト：FQDN に対するブロック ルールがなく、Cisco Umbrella で悪意のないサイトに属していると判断した場合は、サイトの実際の IP アドレスが返されます。これは、DNS ルックアップの通常の動作です。
- グレーリスト：FQDN に対するブロック ルールがないが、Cisco Umbrella で疑わしいサイトに属していると判断した場合は、DNS 応答で Umbrella インテリジェント プロキシの IP アドレスが返されます。次に、プロキシで HTTP 接続を検査し、URL フィルタリングを適用します。インテリジェント プロキシが Cisco Umbrella ダッシュ ボード（**[Security Setting]** > **[Enable Intelligent Proxy]**）でイネーブルになっていることを確認する必要があります。
- ブラックリスト：FQDN が明示的にブロックされているか、Cisco Umbrella で悪意のあるサイトに属していると判断した場合は、DNS 応答でブロックされた接続の Umbrella クラウド ランディング ページの IP アドレスが返されます。

Cisco Umbrella の登録

Umbrella Connector をデバイスに設定するときに、クラウドで Cisco Umbrella に登録します。登録プロセスでは、次のいずれかを特定する単一のデバイス ID が割り当てられます。

- シングル コンテキスト モードのスタンドアロン デバイス。
- シングル コンテキスト モードのハイ アベイラビリティ ペア。
- シングル コンテキスト モードのクラスタ。
- マルチコンテキスト スタンドアロン デバイスのセキュリティ コンテキスト。
- ハイ アベイラビリティ ペアのセキュリティ コンテキスト。
- クラスタのセキュリティ コンテキスト。

登録が完了すると、Cisco Umbrella ダッシュボードにデバイスの詳細が表示されます。次に、デバイスに関連付けられているポリシーを変更できます。登録中は、設定で指定するポリシーが使用されるか、デフォルト ポリシーが割り当てられます。複数のデバイスに同じ Umbrella ポリシーを割り当てることができます。ポリシーを指定する場合、受信するデバイス ID はポリシーを指定しなかった場合に取得する ID とは異なります。

Cisco Umbrella Connector のライセンス要件

Cisco Umbrella Connector を使用するには、3DES ライセンスが必要です。スマート ライセンスを使用している場合は、アカウントで輸出規制による機能限定をイネーブルにする必要があります。

Cisco Umbrella ポータルには、別のライセンス要件があります。

Cisco Umbrella のガイドラインと制限事項

コンテキスト モード

- マルチコンテキスト モードでは、コンテキストごとに Umbrella Connector を設定します。各コンテキストが異なるデバイス ID を持ち、Cisco Umbrella Connector ダッシュボードに別のデバイスとして表示されます。デバイス名は、コンテキストで設定されたホスト名にハードウェア モデルおよびコンテキスト名を追加した形式で作成されます。たとえば、CiscoASA-ASA5515-Context1 となります。

フェールオーバー

- ハイ アベイラビリティ ペアのアクティブ ユニットでは、ペアを単一ユニットとして Cisco Umbrella に登録します。両方のピアで、それぞれのシリアル番号から形成された同じデバイス ID が使用されます（*primary-serial-number_secondary-serial-number*）。マルチ コンテキスト モードでは、セキュリティ コンテキストの各ペアが単一ユニットと見なされます。ハイ アベイラビリティを設定する必要があります。ユニットでは、スタンバイ デバイスが現在障害発生状態であったとしても、Cisco Umbrella をイネーブルにする前にハイ アベイラビリティ グループを正常に作成する必要があります。これを作成しないと、登録に失敗します。

クラスタ

- クラスタ マスターでは、クラスタを単一ユニットとして Cisco Umbrella に登録します。すべてのピアで同じデバイス ID を使用します。マルチ コンテキスト モードでは、クラスタ内のセキュリティ コンテキストがすべてのピアで単一ユニットと見なされます。

その他のガイドライン

- Cisco Umbrella へのリダイレクションは、通過トラフィックの DNS 要求に対してのみ実行されます。システム自体で開始する DNS 要求が Cisco Umbrella にリダイレクトされることはありません。たとえば、FQDN ベースのアクセス制御ルールが Umbrella のポリシーをベースに解決されたり、他のコマンドまたは構成設定で使用される任意の FQDN となったりすることはありません。

- Cisco Umbrella Connector は、通過トラフィックの任意の DNS 要求で動作します。ただし、ブラックリストおよびグレーリストのアクションは DNS レスポンスが HTTP/HTTPS 接続で使用される場合にのみ有効です（返される IP アドレスが Web サイト用であるため）。ブラックリストまたはグレーリストにある非 HTTP/HTTPS 接続のアドレスは、失敗するか誤った方法で完了します。たとえば、ブラックリストにある FQDN の ping を実行すると、Cisco Umbrella クラウドのブロック ページをホストするサーバに対して ping を実行します。

  

  （注） Cisco Umbrella を試行して、非 HTTP/HTTPS になる可能性がある FQDN をインテリジェントに特定します。グレーリストにあるドメイン名の FQDN では、インテリジェント プロキシに IP アドレスを返しません。

- システムでは、Cisco Umbrella へのみ DNS/UDP トラフィックを送信します。DNS/TCP インスペクションをイネーブルにすると、システムは、Cisco Umbrella に DNS/TCP 要求を送信しません。ただし、DNS/TCP 要求によって Umbrella バイパス カウンタが増えることはありません。

- Umbrella インスペクションで DNScrypt をイネーブルにすると、システムは暗号化されたセッションに UDP/443 を使用します。DNScrypt が正常に機能するために Cisco Umbrella の DNS インスペクションを適用するクラス マップでは、UDP/443 を UDP/53 とともに含める必要があります。UDP/443 と UDP/53 はいずれも DNS のデフォルトのインスペクション クラスに含まれていますが、カスタム クラスを作成する場合は、一致するクラスに両方のポートが含まれる ACL を定義する必要があります。

- DNScrypt は、証明書の更新ハンドシェイクに対してのみ、IPv4 を使用します。ただし、DNSscrypt では、IPv4 と IPv6 の両方のトラフィックを暗号化します。

- Cisco Umbrella と ASA FirePOWER の処理は、特定の接続に対して互換性がありません。両方のサービスを利用する場合は、ASA FirePOWER の処理から UDP/53 と UDP/443 を除外する必要があります。たとえば、現在すべてのトラフィックを ASA FirePOWER モジュールにリダイレクトしている場合、クラスを更新してアクセス リストを照合する必要があります。アクセス リストは宛先ポート UDP/53 および UDP/443 の Umbrella サーバに対するすべての接続を拒否し、次にすべての宛先に対する送信元を許可してから開始する必要があります。ACL と match ステートメントは、次のように類似しています。

```
access-list sfr extended deny udp any host 208.67.220.220 eq domain
access-list sfr extended deny udp any host 208.67.220.220 eq 443
access-list sfr extended permit ip any any

class-map sfr
 match access-list sfr
policy-map global_policy
 class sfr
  sfr fail-open
```

- api.opendns.com（登録では IPv4 のみを使用）にアクセスできるインターネットへの Ipv4 ルートが必要です。また、次の DNS リゾルバへのルートも必要となるほか、アクセス ルー

ルでこれらのホストにDNSトラフィックを許可する必要があります。これらのルートは、データインターフェイスまたは管理インターフェイスのいずれかを通過できます。有効なルートが登録と DNS 解決の両方で機能します。

- 208.67.220.220
- 2620:119:53::53

- デバイスの登録を解除するには、Umbrella の設定を削除した後で Cisco Umbrella ダッシュボードからデバイスを削除します。
- FQDN ではなく IP アドレスを使用するすべての Web 要求では、Cisco Umbrella がバイパスされます。また、ローミング クライアントは、Umbrella がイネーブルになっているデバイスを通過せずに別の WAN 接続から DNS 解決を取得した場合、この DNS 解決を使用する接続で Cisco Umbrella をバイパスします。
- ユーザに HTTP プロキシがある場合は、プロキシで DNS 解決を実行し Cisco Umbrella を通過しない可能性があります。
- NAT DNS46 および DNS64 はサポートされていません。IPv4 アドレスと IPv6 アドレスの間で DNS 要求を変換することはできません。
- EDNS レコードには、IPv4 と IPv6 の両方のホスト アドレスが含まれます。
- クライアントが HTTPS 経由で DNS を使用している場合、クラウド セキュリティ サービスでは DNS および HTTP/HTTPS トラフィックが検査されません。

Cisco Umbrella Connector の設定

クラウドでCisco Umbrellaを操作できるようにデバイスを設定できます。システムはDNSルックアップ要求をCisco Umbrellaにリダイレクトします。次に、クラウドベースのエンタープライズセキュリティの完全修飾ドメイン名（FQDN）ポリシーを適用します。悪意のある、疑わしいトラフィックでは、ユーザがサイトからブロックされるか、またはクラウドベースのポリシーに基づいて URL フィルタリングが実行できるインテリジェント プロキシにリダイレクトすることができます。

次の手順では、Cisco Umbrella Connector の設定におけるエンドツーエンドのプロセスについて説明します。

始める前に

マルチコンテキスト モードでは、Cisco Umbrella を使用する必要のある各セキュリティ コンテキストでこの手順を実行します。

手順

ステップ 1 Cisco Umbrella のアカウント（https://umbrella.cisco.com）を確立します

ステップ 2 Cisco Umbrella 登録サーバからの CA 証明書のインストール （6 ページ）。

デバイスの登録では HTTPS を使用します。これによりルート証明書をインストールするように要求されます。

ステップ 3 イネーブルになっていない場合は、DNS サーバを設定してインターフェイス上で DNS ルックアップをイネーブルにします。

[Configuration] > **[Device Management]** > **[DNS]** > **[DNS Client]** ページで構成を設定します。

自分のサーバを使用することも、Cisco Umbrella サーバを設定することもできます。別のサーバを設定する場合でも、DNS インスペクションによって Cisco Umbrella リゾルバへ自動的にリダイレクトされます。

- 208.67.220.220
- 2620:119:53::53

ステップ 4 Umbrella Connector のグローバル設定 （7 ページ）。

ステップ 5 DNS インスペクション ポリシー マップでの Umbrella のイネーブル化 （8 ページ）.

ステップ 6 Umbrella の登録確認 （9 ページ）.

Cisco Umbrella 登録サーバからの CA 証明書のインストール

Cisco Umbrella 登録サーバとの間で HTTPS 接続を確立するには、ルート証明書のインポートが必要です。システムは、デバイスの登録時に HTTPS 接続を使用します。

インポートする必要のある PEM 証明書を次に示します。

```
-----BEGIN CERTIFICATE-----
MIIElDCCA3ygAwIBAgIQAf2j627KdciIQ4tyS8+8kTANBgkqhkiG9w0BAQsFADBh
MQswCQYDVQQGEwJVUzEVMBMGA1UEChMMRGlnaUNlcnQgSW5jMRkwFwYDVQQLExB3
d3cuZGlnaWNlcnQuY29tMSAwHgYDVQQDExdEaWdpQ2VydCBHbG9iYWwgUm9vdCBD
QTAeFw0xMzAzMDgxMjAwMDBaFw0yMzAzMDgxMjAwMDBaME0xCzAJBgNVBAYTAlVT
MRUwEwYDVQQKEwxEaWdpQ2VydCBJbmMxJzAlBgNVBAMTHkRpZ2lDZXJ0IFNIQTIg
U2VjdXJlIFNlcnZlciBDQTCCASIwDQYJKoZIhvcNAQEBBQADggEPADCCAQoCggEB
ANyuWJBNwcQwFZA1W248ghX1LFy949v/cUP6ZCWA1O4Yok3wZtAKc24RmDYXZK83
nf36QYSvx6+M/hpzTc8zl5CilodTgyu5pnVILR1WN3vaMTIa16yrBvSqXUu3R0bd
KpPDkC55gIDvEwRqFDu1m5K+wgdlTvza/P96rtxcflUxDOg5B6TXvi/TC2rSsd9f
/ld0Uzs1gN2ujkSYs58O09rg1/RrKatEp0tYhG2SS4HD2nOLEpdIkARFdRrdNzGX
kujNVA075ME/OV4uuPNcfhCOhkEAjUVmR7ChZc6gqikJTvOX6+guqw9ypzAO+sf0
/RR3w6RbKFfCs/mC/bdFWJsCAwEAAaOCAVowggFWMBIGA1UdEwEB/wQIMAYBAf8C
AQAwDgYDVR0PAQH/BAQDAgGGMDQGCCsGAQUFBwEBBCgwJjAkBggrBgEFBQcwAYYY
aHR0cDovL29jc3AuZGlnaWNlcnQuY29tMHsGA1UdHwR0MHIwN6A1oDOGMWh0dHA6
Ly9jcmwzLmRpZ2ljZXJ0LmNvbS9EaWdpQ2VydEdsb2JhbFJvb3RDQS5jcmwwN6A1
oDOGMWh0dHA6Ly9jcmw0LmRpZ2ljZXJ0LmNvbS9EaWdpQ2VydEdsb2JhbFJvb3RD
QS5jcmwwPQYDVR0gBDYwNDAyBgRVHSAAMCowKAYIKwYBBQUHAgEWHGh0dHBzOi8v
d3d3LmRpZ2ljZXJ0LmNvbS9DUFMwHQYDVR0OBBYEFA+AYRyCMWHVLyjnjUY4tCzh
xtniMB8GA1UdIwQYMBaAFAPeUDVW0Uy7ZvCj4hsbw5eyPdFVMA0GCSqGSIb3DQEB
CwUAA4IBAQAjPt9L0jFCpbZ+QlwaRMxp0Wi0XUvgBCFsS+JtzLHgl4+mUwnNqipl
5TlPHoOlblyYoiQm5vuh7ZPHLgLGTUq/sELfeNqzqPlt/yGFUzZgTHbO7Djc1lGA
8MXW5dRNJ2Srm8c+cftIl7gzbckTB+6WohsYFfZcTEDts8Ls/3HB40f/1LkAtDdC
2iDJ6m6K7hQGrn2iWZiIqBtvLfTyyRRfJs8sjX7tN8Cp1Tm5gr8ZDOo0rwAhaPit
c+LJMto4JQtV05od8GiG7S5BNO98pVAdvzr508EIDObtHopYJeS4d60tbvVS3bR0
```

```
j6tJLp07kzQoH3jOlOrHvdPJbRzeXDLz
-----END CERTIFICATE-----
```

手順

ステップ 1 **[Configuration]** > **[Firewall]** > **[Advanced]** > **[Certificate Management]** > **[CA Certificates]** を選択します。

ステップ 2 [Add] をクリックします。

ステップ 3 **トラストポイント名**（ctx1 または umbrella_server など）を入力します。

ステップ 4 [Paste Certificate in PEM Format] を選択し、証明書をボックスに貼り付けます。

BEGIN CERTIFICATE 行および END CERTIFICATE 行は、含めても含めなくても構いません。

ステップ 5 [Install Certificate] をクリックします。

証明書はデバイスで作成されます。ビューを更新してリストされたトラストポイントを表示する必要があります。

Umbrella Connector のグローバル設定

Umbrella のグローバル設定では、主に、Cisco Umbrella へのデバイスの登録に必要な API トークンを定義します。グローバル設定だけでは Umbrella のイネーブル化には不十分です。DNS インスペクション ポリシー マップでの Umbrella のイネーブル化 （8 ページ）の説明に従って、DNS インスペクション ポリシー マップでも Umbrella をイネーブルにする必要があります。

始める前に

- Cisco Umbrella ネットワーク デバイス ダッシュボード（https://login.umbrella.com/）にログインし、組織のネットワーク デバイス API トークンを取得します。トークンは、16 進数の文字列（例：AABBA59A0BDE1485C912AFE）になります。Umbrella では、**[Deployments]** > **[Core Identities]** > **[Network Devices]** を選択してこれを確認できます。ページに API トークンが表示されていない場合は、ページ右上の [API Token] ボタンをクリックします。
- Cisco Umbrella 登録サーバの証明書をインストールします。

手順

ステップ 1 **[Configuration]** > **[Firewall]** > **[Objects]** > **[Umbrella]** を選択します。

ステップ 2 [Enable Umbrella] を選択します。

ステップ 3 [Token] フィールドに API トークンを入力します。

ステップ 4 （任意）DNS インスペクション ポリシー マップで DNScrypt をイネーブルにする場合は、必要に応じて証明書の検証に DNScrypt プロバイダーの**公開キー**を設定できます。キーを設定しない場合は、現在配布されているデフォルトの公開キーが検証に使用されます。

キーは 32 バイトの 16 進数値です。2 バイトごとにコロンで区切った ASCII の 16 進数値を入力します。キー長は 79 バイトです。このキーは Cisco Umbrella から取得します。

デフォルト キーは B735:1140:206F:225D:3E2B:D822:D7FD:691E:A1C3:3CC8:D666:8D0C:BE04:BFAB:CA43:FB79 です。

デフォルトの公開キーの使用に戻すには、キーを [Public Key] フィールドから削除します。

ステップ 5 （任意）[EDNS Timeout] を選択してアイドル タイムアウトを変更します。その時間が経過するまでサーバからの応答がない場合、クライアントから Umbrella サーバへの接続は削除されます。

タイムアウトは hours:minutes:seconds の形式で、0:0:0 ～ 1193:0:0 の範囲で指定できます。デフォルトは 0:02:00（2 分）です。

DNS インスペクション ポリシー マップでの Umbrella のイネーブル化

Umbrella のグローバル設定だけではデバイスの登録には不十分なため、DNS ルックアップ リダイレクションをイネーブルにします。アクティブな DNS インスペクションの一部として Umbrella を追加する必要があります。

Umbrella を preset_dns_map DNS インスペクション ポリシーマップに追加して、グローバルにイネーブルにできます。

ただし、カスタマイズされた DNS インスペクションを使用して、異なるインスペクション ポリシー マップを異なるトラフィック クラスに適用する場合は、Umbrella をサービスを必要とするクラスごとにイネーブルにする必要があります。

次の手順では、Umbrella をグローバルに実装する方法について説明します。カスタマイズされた DNS ポリシー マップがある場合は、DNS インスペクション ポリシー マップの設定を参照してください。

手順

ステップ 1 **[Configuration]** > **[Firewall]** > **[Objects]** > **[Inspect Maps]** > **[DNS]** を選択します。

ステップ 2 **preset_dns_map** インスペクション マップをダブルクリックして編集します。

ステップ 3 [Umbrella Connections] タブをクリックして、クラウドでの Cisco Umbrella への接続をイネーブルにします。

- [Umbrella]：Cisco Umbrella を有効にします。必要に応じて、デバイスに適用する Cisco Umbrella ポリシーの名前を [Umbrella タグ（Umbrella Tag）] フィールドに指定します。ポ

リシーを指定しない場合は、デフォルトの ACL が適用されます。登録が完了すると、Umbrella のデバイス ID がタグの横に表示されます。

- [Dnscrypt の有効化（Enable Dnscrypt）]：DNScrypt を有効にしてデバイスと Cisco Umbrella 間の接続を暗号化します。DNScrypt を有効にすると、Umbrella リゾルバとのキー交換スレッドが開始されます。キー交換スレッドは、1 時間ごとにリゾルバとのハンドシェイクを実行し、新しい秘密鍵でデバイスを更新します。DNScrypt では UDP/443 を使用するため、そのポートが DNS インスペクションに使用するクラス マップに含まれていることを確認する必要があります。デフォルトのインスペクション クラスには DNS インスペクションに UDP/443 がすでに含まれています。

ステップ 4 [OK] をクリックします。

Umbrella の登録確認

Umbrella のグローバル設定を実行し、DNS インスペクションで Umbrella をイネーブルにしたら、デバイスから Cisco Umbrella に接続して登録を行う必要があります。Cisco Umbrella にデバイス ID が指定されているかどうかを確認することで、登録が正常に完了したかどうかをチェックできます。

コマンドを入力するには、**[Tools]** > **[Command Line Interface]** または SSH セッションを使用します。

最初にサービス ポリシーの統計情報を確認し、Umbrella の登録回線を検出します。ここには、Cisco Umbrella で適用されるポリシー（タグ）、接続の HTTP ステータス（401 は API トークンが正しくないことを示し、409 はデバイスがすでに Cisco Umbrella に存在することを示します）、およびデバイス ID が示されている必要があります。

```
asa(config)# show service-policy inspect dns
Interface inside:
  Service-policy: global_policy
    Class-map: inspection_default
      Inspect: dns preset_dns_map, packet 0, lock fail 0, drop 0, reset-drop 0,
5-min-pkt-rate 0 pkts/sec, v6-fail-close 0 sctp-drop-override 0
        message-length maximum client auto, drop 0
        message-length maximum 512, drop 0
        dns-guard, count 0
        protocol-enforcement, drop 0
        nat-rewrite, count 0
        umbrella registration: tag: default, status: 200 success, device-id:
010a13b8fbdfc9aa
        Umbrella: bypass 0, req inject 0 - sent 0, res recv 0 - inject 0
        DNScrypt egress: rcvd 402, encrypt 402, bypass 0, inject 402
        DNScrypt ingress: rcvd 804, decrypt 402, bypass 402, inject 402
        DNScrypt: Certificate Update: completion 10, failure 1
```

また、実行コンフィギュレーション（ポリシーマップでのフィルタリング）も確認できます。ポリシー マップの umbrella コマンドを更新して、デバイス ID を表示します。このコマンドをイネーブルにしても、デバイス ID を直接設定することはできません。次の例では、出力を編集して関連する情報を表示します。Umbrella に使用される DNS インスペクション マップを編

集して ASDM のデバイス ID を表示することもできます。ID は、[Umbrella Connections] タブに表示されます。

```
ciscoasa(config)# show running-config policy-map
!
policy-map type inspect dns preset_dns_map
parameters
  message-length maximum client auto
  message-length maximum 512
  dnscrypt
  umbrella device-id 010a3e5760fdd6d3
  no tcp-inspection
policy-map global_policy
class inspection_default
  inspect dns preset_dns_map
```

Umbrella Connector のモニタリング

ここでは、Umbrella Connector をモニタする方法について説明します。

Umbrella サービス ポリシーの統計情報のモニタリング

Umbrella をイネーブルにすると、DNS インスペクションの統計情報の概要と詳細を両方表示できます。

コマンドを入力するには、**[Tools]** > **[Command Line Interface]** または SSH セッションを使用します。

show service-policy inspect dns ［**detail**］

detail キーワードを使用しないと、すべての基本的な DNS インスペクション カウンタと Umbrella の設定情報が表示されます。ステータス フィールドに、システムで Cisco Umbrella への登録を試行するための HTTP ステータス コードを指定します。

```
asa(config)# show service-policy inspect dns
Interface inside:
  Service-policy: global_policy
    Class-map: inspection_default
      Inspect: dns preset_dns_map, packet 0, lock fail 0, drop 0, reset-drop 0,
5-min-pkt-rate 0 pkts/sec, v6-fail-close 0 sctp-drop-override 0
        message-length maximum client auto, drop 0
        message-length maximum 512, drop 0
        dns-guard, count 0
        protocol-enforcement, drop 0
        nat-rewrite, count 0
        umbrella registration: tag: default, status: 200 success, device-id:
010a13b8fbdfc9aa
        Umbrella: bypass 0, req inject 0 - sent 0, res recv 0 - inject 0
        DNScrypt egress: rcvd 402, encrypt 402, bypass 0, inject 402
        DNScrypt ingress: rcvd 804, decrypt 402, bypass 402, inject 402
        DNScrypt: Certificate Update: completion 10, failure 1
```

詳細な出力では、DNScrypt の統計情報と使用されるキーが表示されます。

```
asa(config)# show service-policy inspect dns detail
Global policy:
  Service-policy: global_policy
    Class-map: inspection_default
    Class-map: dnscrypt30000
      Inspect: dns dns_umbrella, packet 12, lock fail 0, drop 0, reset-drop 0,
               5-min-pkt-rate 0 pkts/sec, v6-fail-close 0 sctp-drop-override 0
        message-length maximum client auto, drop 0
        message-length maximum 1500, drop 0
        dns-guard, count 3
        protocol-enforcement, drop 0
        nat-rewrite, count 0
        Umbrella registration: tag: default, status: 200 SUCCESS, device-id:
010af97abf89abc3, retry 0
        Umbrella: bypass 0, req inject 6 - sent 6, res recv 6 - inject 6
          Umbrella app-id fail, count 0
          Umbrella flow alloc fail, count 0
          Umbrella block alloc fail, count 0
          Umbrella client flow expired, count 0
          Umbrella server flow expired, count 0
          Umbrella request drop, count 0
          Umbrella response drop, count 0
        DNScrypt egress: rcvd 6, encrypt 6, bypass 0, inject 6
        DNScrypt ingress: rcvd 18, decrypt 6, bypass 12, inject 6
          DNScrypt length error, count 0
          DNScrypt add padding error, count 0
          DNScrypt encryption error, count 0
          DNScrypt magic_mismatch error, count 0
          DNScrypt disabled, count 0
          DNScrypt flow error, count 0
          DNScrypt nonce error, count 0
        DNScrypt: Certificate Update: completion 1, failure 1
          DNScrypt Receive internal drop count 0
          DNScrypt Receive on wrong channel drop count 0
          DNScrypt Receive cannot queue drop count 0
          DNScrypt No memory to create channel count 0
          DNScrypt Send no output interface count 1
          DNScrypt Send open channel failed count 0
          DNScrypt Send no handle count 0
          DNScrypt Send dupb failure count 0
          DNScrypt Create cert update no memory count 0
          DNScrypt Store cert no memory count 0
          DNScrypt Certificate invalid length count 0
          DNScrypt Certificate invalid magic count 0
          DNScrypt Certificate invalid major version count 0
          DNScrypt Certificate invalid minor version count 0
          DNScrypt Certificate invalid signature count 0
          Last Successful: 01:42:29 UTC May 2 2018, Last Failed: None
          Magic DNSC, Major Version 0x0001, Minor Version 0x0000,
          Query Magic 0x714e7a696d657555, Serial Number 1517943461,
          Start Time 1517943461 (18:57:41 UTC Feb 6 2018)
          End Time 1549479461 (18:57:41 UTC Feb 6 2019)
          Server Public Key
240B:11B7:AD02:FAC0:6285:1E88:6EAA:44E7:AE5B:AD2F:921F:9577:514D:E226:D552:6836
          Client Secret Key Hash
48DD:E6D3:C058:D063:1098:C6B4:BA6F:D8A7:F0F8:0754:40B0:AFB3:CB31:2B22:A7A4:9CEE
          Client Public key
6CB9:FA4B:4273:E10A:8A67:BA66:76A3:BFF5:2FB9:5004:CD3B:B3F2:86C1:A7EC:A0B6:1A58
          NM key Hash
9182:9F42:6C01:003C:9939:7741:1734:D199:22DF:511E:E8C9:206B:D0A3:8181:CE57:8020
```

Umbrella の syslog メッセージのモニタリング

次の Umbrella 関連の syslog メッセージをモニタできます。

- %ASA-3-339001: DNSCRYPT certificate update failed for *number* tries.

  Umbrellaサーバへのルートが存在すること、および出力インターフェイスが表示され正常に機能していることを確認してください。また、DNScrypt 用に設定された公開キーが正しいことも確認してください。Cisco Umbrella から新しいキーを取得する必要が生じる場合があります。

- %ASA-3-339002: Umbrella device registration failed with error code *error_code*.

  各エラー コードの内容は、次のとおりです。

  - 400：要求の形式またはコンテンツに問題があります。トークンが短すぎるか、破損している可能性があります。トークンがUmbrellaダッシュボードのトークンと一致していることを確認してください。
  - 401：API トークンが承認されていません。トークンを再設定してください。Umbrella ダッシュボードでトークンを更新していた場合は、必ず新しいトークンを使用してください。
  - 409：デバイス ID が別の組織と競合しています。問題の内容について Umbrella 管理者に確認してください。
  - 500：内部サーバエラーが発生しました。問題の内容についてUmbrella管理者に確認してください。

- %ASA-6-339003: Umbrella device registration was successful.

- %ASA-3-339004: Umbrella device registration failed due to missing token.

  Cisco Umbrella から API トークンを取得し、Umbrella のグローバル設定で指定する必要があります。

- %ASA-3-339005: Umbrella device registration failed after *number* retries.

  syslog 339002 メッセージを確認し、修正する必要のあるエラーを特定します。

Cisco Umbrella Connector の履歴

機能名	プラットフォーム リリース	説明
Cisco Umbrella サポート。	9.10(1)	Cisco Umbrella で定義されている エンタープライズ セキュリティ ポリシーをユーザ接続に適用できるように DNS 要求を Cisco Umbrella へリダイレクトするようにデバイスを設定できます。FQDN に基づいて接続を許可またはブロックできます。または、疑わしい FQDN の場合は Cisco Umbrella インテリジェント プロキシにユーザをリダイレクトして URL フィルタリングを実行できます。Umbrella の設定は、DNS インスペクション ポリシーに含まれています。 次の画面を追加または変更しました。 **[Configuration]** > **[Firewall]** > **[Objects]** > **[Umbrella]**、**[Configuration]** > **[Firewall]** > **[Objects]** > **[Inspect Maps]** > **DNS**。