包括DNSを適用し、ファイアウォールルールでバイパスを防止

内容

はじめに

このドキュメントでは、ファイアウォールルールとネットワークポリシーを使用して、DNSバイパスを防止し、包括DNS保護を適用する方法について説明します。

前提条件

- ネットワークファイアウォール
- ファイアウォールアクセス権限
- ファイアウォール設定に関する知識

包括DNSの適用：最も一般的な方法

ほとんどのルータおよびファイアウォールでは、ポート53経由のすべてのDNSトラフィックを強制できます。そのため、すべてのネットワークデバイスは、ルータで定義されている、包括DNSサーバを指すDNS設定を使用する必要があります。

推奨されるアプローチは、非包括IPアドレスからのすべてのDNS要求を、次に示す包括DNS IPに転送することです。この方式では、DNS要求が透過的に転送され、手動DNS設定が失敗することがなくなります。

または、Umbrella DNSサーバに対してのみDNS(TCP/UDP)を許可し、他の任意のIPアドレスへの他のすべてのDNSトラフィックをブロックするファイアウォール規則を作成します。

ファイアウォール規則の例

1. エッジファイアウォールに次のルールを追加します。
    - 208.67.222.222または208.67.220.220に対し、ポート53でTCP/UDPの着信および発信を許可します。
    - ポート53でのすべてのIPアドレスに対するTCP/UDPの着信および発信をブロックします。

Umbrella DNSの許可ルールは、ブロックルールよりも優先されます。UmbrellaへのDNS要求は許可されますが、他のすべてのDNS要求はブロックされます。

ファイアウォール設定インターフェイスに応じて、プロトコルごとに個別のルールを設定するか、TCPとUDPの両方を対象とする単一のルールを設定します。ネットワークエッジデバイスにルールを適用します。WindowsやmacOSの組み込みファイアウォールなど、ワークステーションのソフトウェアファイアウォールにも同様のルールを適用できます。

ローミングクライアントとActive Directoryグループポリシーを使用している場合は、「グループポリシーを使用したEnterprise Roaming Clientのロックダウン」に関するドキュメントを参照してください。

DNS over HTTPS(DoH)に対する適用

推奨設定

1. Umbrellaで、Proxy / AnonymizerandDoH / DoTcontentカテゴリを有効にします。
2. 既知のDoHプロバイダーのIPアドレスをファイアウォールでブロックします。

詳細と背景

Umbrellaでは、use-application-dns.netドメイン(Mozillaの定義)をサポートしており、Firefoxがデフォルトで DoHを有効にすることを防いでいます。FirefoxおよびDoHの詳細については、関連ドキュメントを参照してください。

代替DNSプロバイダーをブロックした後でも、DNSはDoHでバイパスできます。ローカルDNSリゾルバは、DNS要求をHTTPSに変換し、JSONまたはPOST/GETを使用してエンドポイントに送信します。このトラフィックは通常、DNSインスペクションを回避します。

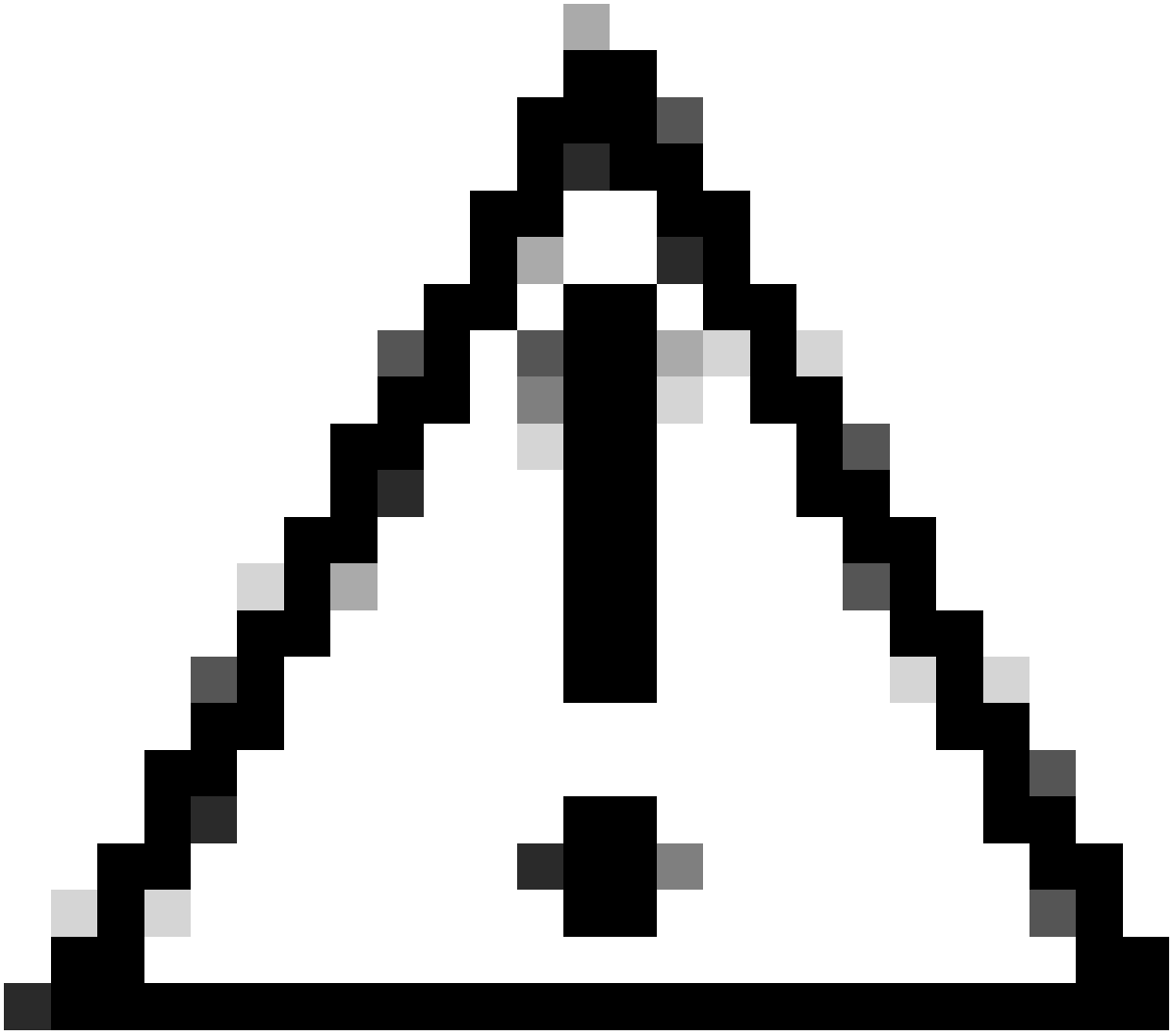
DoHはUmbrellaをバイパスするために使用できるため、Umbrellaでは既知のDoHサーバをプロキシ/アノニマイザコンテンツカテゴリに含めます。このメカニズムには、いくつかの制限がありま

す。

- 未知の新しいDoHプロバイダーをブロックすることはできません。
- IPアドレスを使用して直接使用されるDoHをブロックすることはできません。

新しいDoHプロバイダーに対応するには、アップデートをモニタし、新しく検出されたドメインをブロックしてカバレッジを改善します。

IPアドレスを使用したDoHの場合、シナリオは制限されます。CloudFlareがインストールされたFirefoxがその顕著な例です。



注意：ブロックリストにMozilla Kill Switchドメインを追加しないでください。これらのドメインをブロックすると、ブロックページのAレコードが生成され、Firefoxはこれを有効なものとして処理し、DoHの使用状況を自動的にアップグレードします。

TLS経由のDNSに対する適用(DoT)

代替のDNSプロバイダーとDoHをブロックした後でも、TLS経由でDNSをバイパスできます。TLSではポート853経由でRFC7858が使用されます。たとえば、CloudFlareはDoTプロバイダーです。

適用例

- ポート853(CloudFlare)でIPアドレス1.1.1.1および1.0.0.1をブロックします。

ファイアウォールサポートの免責事項

このドキュメントは、Umbrella DNSを適用する際にネットワーク管理者を支援します。Cisco Umbrellaサポートでは、各デバイスに固有の設定インターフェイスがあるため、個々のファイアウォールまたはルータの設定に対するサポートは提供されません。これらの設定が可能かどうかを確認するには、ルータまたはファイアウォールのマニュアルを参照するか、デバイスの製造元に問い合わせてください。

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。