Web セキュリティ アプライアンスがオープン プロキシになるのを防ぐ方法

目次

概要

この資料に開いたプロキシであるために Web セキュリティ アプライアンス（WSA）を防ぐ方法を記述されています。

環境

Cisco WSA、AsyncOS のすべてのバージョン

WSA が開いたプロキシの考慮することができる 2 つのエリアがあります:

1. ネットワークに住まない HTTP クライアントはプロキシにできます。
2. 非 HTTP トラフィックをトンネル伝送する HTTP 接続要求を使用するクライアント。

これらのシナリオのそれぞれに全く異なる影響があり、次の セクションでより詳しく説明されています。

ネットワークに住まない HTTP クライアントはプロキシにできます

WSA は、デフォルトで、プロキシそれに送信 されるあらゆる HTTP 要求。 これは要求が WSA が受信するポートにあると仮定します（デフォルトは 80 3128）であり。 これは WSA を使用あらゆるネットワークからのクライアントをできてほしくないかもしれませんので問題であるために提起するかもしれません。 これは WSA がパブリックIPアドレスを使用すればですインターネットからアクセス可能あります巨大な問題である場合もあり。

これが直すことができること 2 つの方法があります:

1. HTTP アクセスからの許可されていないソースをブロックするために WSA にファイアウォールをアップストリームに利用して下さい。
2. 望ましいサブネットのクライアントしか許可しないためにポリシー グループを作成して下さい。 このポリシーの簡単なデモは次のとおりです:
   ポリシー グループ 1: これがクライアント ネットワークであることを）適用対象サブネット 10.0.0.0/8（仮定します。 望ましい アクションを追加して下さい。
   Default policy: ブロックして下さいすべてのプロトコル- HTTP、HTTPS、HTTP 上の FTP

より詳しいポリシーはポリシー グループ 1.の上で下部ので他のルールが適切なクライアントのサ

ブネットにだけ適用される限り、他のすべてのトラフィックつかまえます「拒否をすべての」ルール作成することができます。

非 HTTP トラフィックをトンネル伝送する HTTP 接続要求を使用するクライアント

HTTP 接続要求が HTTP プロキシによって非 HTTP データをトンネル伝送するのに使用されています。 HTTP 接続要求のもっとも一般的な使用状況は HTTPS トラフィックをトンネル伝送することです。 HTTPS サイトにアクセスする明示的に設定 された クライアントのためにそれは WSA に最初に HTTP 接続要求を送信 する必要があります。

接続要求の例は自体あります: 接続応答 http://www.website.com:443/ HTTP/1.1

これはクライアントがポート 443 の http://www.website.com/ に WSA によってトンネル伝送することを望むことを WSA に告げます。

HTTP 接続要求がポートをトンネル伝送するのに使用することができます。 潜在的なセキュリティ上の問題が原因で、WSA はこれらのポートにだけ接続要求をデフォルトで可能にします:

20、21、443、563、8443、8080

追加接続応答トンネル ポートを、セキュリティの理由から追加するためになら、必要この追加アクセスを必要とするクライアントIP サブネットにだけ適用する追加ポリシー グループでそれらを追加することが推奨されます。 許可された接続応答ポートはアプリケーション > プロトコル 制御の下の各ポリシー グループで、検出することができます。

開いたプロキシによって送信 される SMTP 要求の例はここに示されています:

```
myhost$ telnet proxy.mydomain.com 80
Trying xxx.xxx.xxx.xxx...
Connected to proxy.mydomain.com.
Escape character is '^]'.
CONNECT smtp.foreigndomain.com:25 HTTP/1.1
Host: smtp.foreigndomain.com HTTP/1.0 200 Connection established
220 smtp.foreigndomain.com ESMTP
HELO test
250 smtp.foreigndomain.com
```