How to Prevent the Web Security Appliance to Be an Open Proxy

Contents

Introduction

This document describes how to prevent the Web Security Appliance (WSA) to be an open proxy.

Environment

Cisco WSA, all versions of AsyncOS

There are two areas where the WSA can be considered to be an open proxy:

1. HTTP clients that do not reside on your network are able to proxy through.
2. Clients that use HTTP CONNECT requests to tunnel non-HTTP traffic through.

Each of these scenarios has completely different implications and will be discussed in more detail in the next sections.

HTTP Clients That Do Not Reside on Your Network Are Able to Proxy Through

The WSA will, by default, proxy any HTTP request sent to it. This assumes that the request is on the port the WSA listens on (defaults are 80 and 3128). This might pose to be a problem, as you might not want any client from any network to be able to use the WSA. This is can be a huge issue if the WSA uses a public IP address and is accessible from the Internet.

There are two ways that this can be remedied:

1. Utilize a firewall upstream to the WSA in order to block unauthorized sources from HTTP access.
2. Create policy groups to only allow the clients on your desired subnets. A simple demonstration of this policy is:
   Policy Group 1: Applies to subnet 10.0.0.0/8 (assumes this is your client network). Add your desired actions.
   Default Policy: Block all protocols - HTTP, HTTPS, FTP over HTTP

More detailed policies can be created above Policy Group 1. As long as other rules only apply to the appropriate client subnets, all other traffic will catch the "deny all" rule at the bottom.

Clients That Use HTTP CONNECT Requests to Tunnel Non-HTTP Traffic Through

HTTP CONNECT requests are used to tunnel non-HTTP data via an HTTP proxy. The most common usage of an HTTP CONNECT request is to tunnel HTTPS traffic. In order for an explicitly configured client to access an HTTPS site, it MUST first send an HTTP CONNECT request to the WSA.

An example of a CONNECT request is as such: CONNECT http://www.website.com:443/ HTTP/1.1

This tells the WSA that the client desires to tunnel through the WSA to http://www.website.com/ on port 443.

HTTP CONNECT requests can be used to tunnel any port. Due to potential security issues, the WSA only allows CONNECT requests to these ports by default:

20, 21, 443, 563, 8443, 8080

If it is needed to add additional CONNECT tunnel ports, for security reasons, it is recommended that you add them in an additional policy group that applies only to the client IP subnets that need this additional access. The allowed CONNECT ports can be found in each policy group, under Applications > Protocol Controls.

An example of an SMTP request sent through an open proxy is shown here:

```
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
```