So verhindern Sie, dass die Websicherheits-Appliance ein offener Proxy ist

Inhalt

Einführung

In diesem Dokument wird beschrieben, wie verhindert wird, dass die Web Security Appliance (WSA) ein offener Proxy ist.

Umgebung

Cisco WSA, alle Versionen von AsyncOS

Es gibt zwei Bereiche, in denen die WSA als offener Proxy angesehen werden kann:

1. HTTP-Clients, die sich nicht in Ihrem Netzwerk befinden, können die Proxydienste verwenden.
2. Clients, die HTTP CONNECT-Anfragen verwenden, um Nicht-HTTP-Datenverkehr durch Tunnel zu leiten.

Jedes dieser Szenarien hat völlig andere Auswirkungen und wird in den nächsten Abschnitten ausführlicher behandelt.

HTTP-Clients, die sich nicht im Netzwerk befinden, können über

Die WSA leitet standardmäßig alle an sie gesendeten HTTP-Anfragen weiter. Dabei wird davon ausgegangen, dass sich die Anforderung auf dem Port befindet, auf dem die WSA überwacht (die Standardwerte sind 80 und 3128). Dies kann ein Problem darstellen, da Sie möglicherweise nicht möchten, dass ein Client aus einem Netzwerk die WSA verwenden kann. Dies kann ein großes Problem darstellen, wenn die WSA eine öffentliche IP-Adresse verwendet und vom Internet aus darauf zugreifen kann.

Es gibt zwei Möglichkeiten, dies zu beheben:

1. Verwenden Sie eine Firewall vor der WSA, um nicht autorisierte Quellen vom HTTP-Zugriff zu blockieren.
2. Erstellen Sie Richtliniengruppen, um nur Clients in den gewünschten Subnetzen zuzulassen. Eine einfache Demonstration dieser Richtlinie ist:
   Richtliniengruppe 1: Gilt für Subnetz 10.0.0.0/8 (es wird davon ausgegangen, dass es sich um Ihr Client-Netzwerk handelt). Fügen Sie die gewünschten Aktionen hinzu.

Standardrichtlinie: Alle Protokolle sperren - HTTP, HTTPS, FTP über HTTP

Über "Policy Group 1" können detailliertere Richtlinien erstellt werden. Solange andere Regeln nur für die entsprechenden Client-Subnetze gelten, wird für den gesamten anderen Datenverkehr die Regel "Alle verweigern" am unteren Ende des Fensters angezeigt.

Clients, die HTTP CONNECT-Anforderungen verwenden, um Nicht-HTTP-Datenverkehr über

HTTP CONNECT-Anforderungen werden verwendet, um Nicht-HTTP-Daten über einen HTTP-Proxy zu tunneln. Die häufigste Verwendung einer HTTP CONNECT-Anforderung ist die Tunnelung von HTTPS-Datenverkehr. Damit ein explizit konfigurierter Client auf eine HTTPS-Site zugreifen kann, MUSS er zunächst eine HTTP CONNECT-Anforderung an die WSA senden.

Ein Beispiel für eine CONNECT-Anforderung ist: CONNECT http://www.website.com:443/ HTTP/1.1

Dies teilt der WSA mit, dass der Client eine Tunnelverbindung durch die WSA zu http://www.website.com/ an Port 443 herstellen möchte.

HTTP CONNECT-Anfragen können zum Tunnel aller Ports verwendet werden. Aufgrund potenzieller Sicherheitsprobleme erlaubt die WSA standardmäßig nur CONNECT-Anfragen an diese Ports:

20, 21, 443, 563, 8443, 8080

Wenn aus Sicherheitsgründen zusätzliche CONNECT-Tunnel-Ports hinzugefügt werden müssen, wird empfohlen, diese in eine zusätzliche Richtliniengruppe aufzunehmen, die nur für die Client-IP-Subnetze gilt, die diesen zusätzlichen Zugriff benötigen. Die zulässigen CONNECT-Ports finden Sie in jeder Richtliniengruppe unter Anwendungen > Protokollsteuerelemente.

Ein Beispiel für eine SMTP-Anfrage, die über einen offenen Proxy gesendet wurde, ist hier dargestellt:

```
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
```