Come impedire che Web Security Appliance sia un proxy aperto

Sommario

[Introduzione](#)
[Ambiente](#)
[I client HTTP che non risiedono nella rete possono eseguire il proxy tramite](#)
[Client che utilizzano richieste CONNECT HTTP per il tunneling del traffico non HTTP tramite](#)

Introduzione

In questo documento viene descritto come impedire che Web Security Appliance (WSA) sia un proxy aperto.

Ambiente

Cisco WSA, tutte le versioni di AsyncOS

Esistono due aree in cui il WSA può essere considerato un proxy aperto:

1. I client HTTP che non risiedono nella rete possono eseguire il proxy.
2. Client che utilizzano richieste CONNECT HTTP per eseguire il tunnel del traffico non HTTP attraverso.

Ognuno di questi scenari ha implicazioni completamente diverse e verrà analizzato più in dettaglio nelle sezioni successive.

I client HTTP che non risiedono nella rete possono eseguire il proxy tramite

Per impostazione predefinita, WSA invia tramite proxy qualsiasi richiesta HTTP. Si presume che la richiesta si trovi sulla porta su cui WSA è in ascolto (i valori predefiniti sono 80 e 3128). Ciò potrebbe rappresentare un problema, in quanto si potrebbe desiderare che nessun client di qualsiasi rete sia in grado di utilizzare WSA. Questo può essere un problema enorme se il WSA utilizza un indirizzo IP pubblico ed è accessibile da Internet.

Èpossibile risolvere questo problema in due modi:

1. Utilizzare un firewall a monte del WSA per bloccare l'accesso HTTP alle origini non autorizzate.
2. Creare gruppi di criteri per consentire solo i client nelle subnet desiderate. Una semplice dimostrazione di questa politica è:
   Gruppo di criteri 1: Si applica alla subnet 10.0.0.0/8 (presuppone che si tratti della rete client). Aggiungere le azioni desiderate.
   Criterio predefinito: Blocca tutti i protocolli - HTTP, HTTPS, FTP su HTTP

Èpossibile creare criteri più dettagliati sopra il gruppo di criteri 1. Finché le altre regole si applicano solo alle subnet client appropriate, tutto il resto del traffico intercetterà la regola "nega tutto" nella parte inferiore.

Client che utilizzano richieste CONNECT HTTP per il tunneling del traffico non HTTP tramite

Le richieste HTTP CONNECT vengono utilizzate per eseguire il tunnel dei dati non HTTP tramite un proxy HTTP. L'utilizzo più comune di una richiesta HTTP CONNECT è quello di eseguire il tunnel del traffico HTTPS. Affinché un client configurato in modo esplicito possa accedere a un sito HTTPS, DEVE prima inviare una richiesta HTTP CONNECT al server WSA.

Di seguito è riportato un esempio di richiesta CONNECT: CONNETTI http://www.website.com:443/ HTTP/1.1

In questo modo il WSA viene informato che il client desidera eseguire il tunnel attraverso il WSA per raggiungere il sito http://www.website.com/ sulla porta 443.

Le richieste HTTP CONNECT possono essere utilizzate per eseguire il tunnel di qualsiasi porta. A causa di potenziali problemi di sicurezza, per impostazione predefinita WSA consente solo le richieste CONNECT a queste porte:

20, 21, 443, 563, 8443, 8080

Per motivi di sicurezza, se è necessario aggiungere ulteriori porte del tunnel CONNECT, è consigliabile aggiungerle in un gruppo di criteri aggiuntivo che si applichi solo alle subnet IP client che richiedono questo accesso aggiuntivo. Le porte CONNECT consentite si trovano in ciascun gruppo di criteri, in Applicazioni > Controlli protocollo.

Di seguito è riportato un esempio di richiesta SMTP inviata tramite un proxy aperto:

```
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
```