Comment empêcher l'appliance de sécurité Web pour être un proxy ouvert

Contenu

Introduction

Ce document décrit comment empêcher l'appliance de sécurité Web (WSA) pour être un proxy ouvert.

Environnement

Cisco WSA, toutes les versions d'AsyncOS

Il y a deux zones où le WSA peut être considéré un proxy ouvert :

1. Les clients de HTTP qui ne résident pas sur votre réseau peuvent au proxy.
2. Clients qui utilisent des requêtes de connexion de HTTP de percer un tunnel le trafic de non-HTTP.

Chacun de ces scénarios a des implications complètement différentes et sera discuté plus en détail dans les sections suivantes.

Les clients de HTTP qui ne résident pas sur votre réseau peuvent au proxy

Le WSA, par défaut, proxy n'importe quelle requête envoyée de HTTP à lui. Ceci suppose que la demande est sur le port que le WSA écoute en fonction (les par défaut sont 80 et 3128). Ceci pourrait poser pour être un problème, car vous ne pourriez vouloir qu'aucun client d'aucun réseau puisse utiliser le WSA. C'est peut être une question énorme si le WSA utilise une adresse IP publique et est accessible de l'Internet.

Il y a deux manières que ceci peut être remédié à :

1. Utilisez un en amont de Pare-feu au WSA afin de bloquer des sources non autorisées d'accès HTTP.
2. Créez les policy group pour permettre seulement les clients sur vos sous-réseaux désirés. Une démonstration simple de cette stratégie est :
   Policy group 1 : S'applique au sous-réseau 10.0.0.0/8 (suppose que c'est votre réseau de client). Ajoutez vos actions désirées.

Stratégie par défaut : Bloquez tous les protocoles - HTTP, HTTPS, FTP au-dessus de HTTP
Des stratégies plus détaillées peuvent être créées au-dessus du policy group 1. tant que d'autres règles s'appliquent seulement aux sous-réseaux de client appropriés, tout autre trafic attraperont « refusent toute la » règle au bas.

Clients qui utilisent des requêtes de connexion de HTTP de percer un tunnel le trafic de Non-HTTP

Des requêtes de connexion de HTTP sont utilisées de percer un tunnel des données de non-HTTP par l'intermédiaire d'un proxy HTTP. L'utilisation la plus commune d'une requête de connexion de HTTP est de percer un tunnel le trafic HTTPS. Pour qu'un client explicitement configuré accède à un site HTTPS, il DOIT d'abord envoyer une requête de connexion de HTTP au WSA.

Un exemple d'une requête de connexion est en tant que tels : CONNECTEZ http://www.website.com:443/ HTTP/1.1

Ceci indique au WSA que le client désire percer un tunnel par le WSA à http://www.website.com/ sur le port 443.

Des requêtes de connexion de HTTP peuvent être utilisées pour percer un tunnel n'importe quel port. En raison des questions de sécurité potentielle, le WSA permet seulement des requêtes de connexion à ces ports par défaut :

20, 21, 443, 563, 8443, 8080

S'il est nécessaire pour ajouter supplémentaire CONNECTEZ les ports de tunnel, pour des raisons de sécurité, il est recommandé que que vous les ajoutez à un policy group supplémentaire qui s'applique seulement aux sous-réseaux IP de client qui ont besoin de cet accès supplémentaire. Permis CONNECTENT des ports peuvent être trouvés à chaque policy group, sous des applications > des contrôles de Protocol.

Un exemple d'une requête envoyée de SMTP par un proxy ouvert est affiché ici :

```
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
```