Contenu

Question :

Environnement : Appliance de sécurité Web de 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. Les clients utilisent des requêtes de connexion de HTTP de percer un tunnel non le trafic http

Chacun de ces scénarios a des implications complètement différentes et sera discuté plus en détail ci-dessous.

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, assumer la demande est allumé en fonction port que le WSA écoute en fonction (les par défaut sont 80 et 3128). Ceci peut poser pour être un problème pour vous, car vous ne pouvez vouloir qu'aucun client d'aucun réseau puisse utiliser le WSA. C'est peut être une question énorme si le WSA utilise l'adresse IP publique et est accessible de l'Internet.

Il y a 2 manières que ceci peut être remédié à :

1. Utilisez un en amont de Pare-feu à 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 ci-dessous :

Policy group 1 : S'applique au sous-réseau 10.0.0.0/8 (assumer ceci 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.

Les clients utilisent des requêtes de connexion de HTTP de percer un tunnel non le trafic http

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

le 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 aux ports suivants 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 » - > « Protocol contrôle ».

Un exemple d'envoyer une demande de SMTP par un proxy ouvert est ci-dessous :
telnet proxy.mydomain.com 80 myhost$
Essayant xxx.xxx.xxx.xxx…
Connecté à proxy.mydomain.com.
Le caractère d'échappement est « ^] ».
CONNECTEZ smtp.foreigndomain.com:25 HTTP/1.1
Hôte : smtp.foreigndomain.com

Connexion HTTP/1.0 200 établie

220 smtp.foreigndomain.com ESMTP
Test d'HÉLICOPTÈRE
250 smtp.foreigndomain.com