

Contenido

Pregunta:

Entorno: Dispositivo de seguridad de la red de Cisco (WSA), todas las versiones de AsyncOS

Hay dos áreas donde el WSA se puede considerar para ser un proxy abierto:

1. Los clientes HTTP que no residen en su red pueden al proxy a través
2. Los clientes están utilizando los pedidos de conexión HTTP de hacer un túnel no el tráfico HTTP a través

Cada uno de estos escenarios tiene implicaciones totalmente diversas y será discutido más detalladamente abajo.

Los clientes HTTP que no residen en su red pueden al proxy a través

El WSA, por abandono, proxy cualquier pedido de HTTP enviado a él, si se asume que la petición encendido está prendido puerto que está escuchando el WSA encendido (los valores por defecto son 80 y 3128). Esto puede presentar para ser un problema para usted, pues usted no puede quisiera que cualquier cliente de ninguna red pudiera utilizar el WSA. Esto es puede ser un problema enorme si el WSA está utilizando al IP Address público y es accesible de Internet.

Hay 2 maneras que esto puede ser remediada:

1. Utilice una conexión en sentido ascendente del Firewall a WSA para bloquear las fuentes no autorizadas del acceso HTTP.
2. Cree a los grupos de políticas para permitir solamente a los clientes en sus subredes deseadas. Una demostración simple de esta directiva está abajo:

Grupo de políticas 1: Se aplica a la subred 10.0.0.0/8 (si se asume que esto es su Client Network). Agregue sus acciones deseadas.

Política predeterminada: Bloquee todos los protocolos - HTTP, HTTPS, FTP sobre el HTTP

Directivas más detalladas se pueden crear sobre el grupo de políticas 1. mientras otras reglas se apliquen solamente a las subredes cliente apropiadas, el resto del tráfico cogerán "niegan toda la" regla en la parte inferior.

Los clientes están utilizando los pedidos de conexión HTTP de hacer un túnel no el tráfico HTTP a través

Se utilizan los pedidos de conexión HTTP de hacer un túnel no los datos HTTP vía un proxy de HTTP. El uso más común de un pedido de conexión HTTP está para hacer un túnel el tráfico

HTTPS. Para que explícitamente un cliente configurado acceda un sitio HTTPS, DEBE primero enviar un pedido de conexión HTTP al WSA.

Un ejemplo de un pedido de conexión está como tal: CONECTE http://www.website.com:443/ HTTP/1.1

Esto dice al WSA que el cliente desea hacer un túnel con el WSA a http://www.website.com/ en el puerto 443.

Los pedidos de conexión HTTP se pueden utilizar para hacer un túnel cualquier puerto. Debido a los problemas de seguridad potencial, el WSA permite solamente los pedidos de conexión a los puertos siguientes por abandono:

20, 21, 443, 563, 8443, 8080

Si es necesario agregar adicional CONECTE los puertos del túnel, por razones de seguridad, él se recomienda que usted los agrega en un grupo de políticas adicional que se aplique solamente IP del cliente a las subredes que necesitan este acceso adicional. Permitidos CONECTAN los puertos se pueden encontrar en cada grupo de políticas, bajo "aplicaciones" -> los "controles del protocolo".

Un ejemplo de enviar una petición SMTP con un proxy abierto está abajo:

```
telnet proxy.mydomain.com 80 myhost$
```

```
Xxx.xxx.xxx.xxx que intenta...
```

```
Conectado con proxy.mydomain.com.
```

```
El carácter de escape es "^".
```

```
CONECTE smtp.foreigndomain.com:25 HTTP/1.1
```

```
Host: smtp.foreigndomain.com
```

```
Conexión HTTP/1.0 200 establecida
```

```
220 smtp.foreigndomain.com ESMTP
```

```
Prueba HELO
```

```
250 smtp.foreigndomain.com
```