Como impedir a ferramenta de segurança da Web para ser um proxy aberto

Índice

Introdução

Este original descreve como impedir a ferramenta de segurança da Web (WSA) para ser um proxy aberto.

Ambiente

Cisco WSA, todas as versões de AsyncOS

Há duas áreas onde o WSA pode ser considerado para ser um proxy aberto:

1. Os clientes HTTP que não residem em sua rede podem ao proxy completamente.
2. Clientes que usam requisições de conexão HTTP escavar um túnel completamente o tráfego NON-HTTP.

Cada um destas encenações tem implicações completamente diferentes e será discutida com maiores detalhes nas próximas seções.

Os clientes HTTP que não residem em sua rede podem ao proxy completamente

O WSA, à revelia, proxy todo o pedido do HTTP enviado a ele. Isto supõe que o pedido está na porta que o WSA escuta sobre (os padrões são 80 e 3128). Isto pôde levantar para ser um problema, porque você não pôde querer nenhum cliente de nenhuma rede poder usar o WSA. Isto é pode ser uma edição enorme se o WSA usa um endereço IP público e é acessível do Internet.

Há duas maneiras que este pode ser remediado:

1. Utilize um Firewall rio acima ao WSA a fim obstruir origens não autorizada do acesso HTTP.
2. Crie grupos de política para permitir somente os clientes em suas sub-redes desejadas.
   Uma demonstração simples desta política é:
   Grupo de política 1: Aplica-se à sub-rede 10.0.0.0/8 (supõe que esta é sua rede cliente).
   Adicionar suas ações desejadas.
   Política padrão: Obstrua todos os protocolos - HTTP, HTTPS, FTP sobre o HTTP

Umas políticas mais detalhadas podem ser criadas acima do grupo de política 1. enquanto outras regras se aplicam somente às sub-redes apropriadas do cliente, todo tráfego restante travarão “negam toda a” regra na parte inferior.

Clientes que usam requisições de conexão HTTP escavar um túnel completamente o tráfego NON-HTTP

As requisições de conexão HTTP são usadas escavar um túnel os dados NON-HTTP através de um proxy HTTP. O uso o mais comum de uma requisição de conexão HTTP é escavar um túnel o tráfego HTTPS. Para que explicitamente um cliente configurado alcance um local HTTPS, DEVE primeiramente enviar uma requisição de conexão HTTP ao WSA.

Um exemplo de uma requisição de conexão é como esta'n: CONECTE http://www.website.com:443/ HTTP/1.1

Isto diz ao WSA que o cliente deseja escavar um túnel com o WSA a http://www.website.com/ na porta 443.

As requisições de conexão HTTP podem ser usadas para escavar um túnel toda a porta. Devido às questões de segurança potenciais, o WSA permite somente requisições de conexão a estas portas à revelia:

20, 21, 443, 563, 8443, 8080

Se é precisado de adicionar adicional CONECTE portas do túnel, por razões de segurança, ele está recomendado que você as adiciona em um grupo de política adicional que se aplique somente às sub-redes do IP de cliente que precisam este acesso adicional. Permitidos CONECTAM portas podem ser encontrados em cada grupo de política, sob aplicativos > controles de protocolo.

Um exemplo de um pedido S TP enviado com um proxy aberto é mostrado aqui:

```
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
```