Hoe te voorkomen dat web security applicatie een open proxy wordt

Inhoud

Inleiding

Dit document beschrijft hoe u voorkomt dat Web Security Appliance (WSA) als een open proxy wordt gebruikt.

Omgeving

Cisco WSA, alle versies van AsyncOS

Er zijn twee gebieden waarop de WSA als een open volmacht kan worden beschouwd:

1. HTTP-clients die niet op uw netwerk aanwezig zijn, kunnen proxy-through gebruiken.
2. Clients die HTTP CONNECT-verzoeken gebruiken om niet-HTTP-verkeer doorheen te tunnen.

Elk van deze scenario's heeft totaal andere implicaties en zal in de volgende paragrafen nader worden besproken.

HTTP-clients die niet op uw netwerk aanwezig zijn, kunnen doorlopen

De WSA zal, standaard, elke HTTP aanvraag die naar de WSA wordt gestuurd proxy uitvoeren. Dit veronderstelt dat het verzoek op de poort is waarop de WSA luistert (standaardwaarden zijn 80 en 3128). Dit kan een probleem zijn, omdat u geen client van een netwerk wilt hebben om de WSA te gebruiken. Dit kan een groot probleem zijn als de WSA een openbaar IP-adres gebruikt en vanaf het internet toegankelijk is.

Dit kan op twee manieren worden verholpen:

1. Gebruik een firewall stroomopwaarts naar het WSA om onbevoegden bronnen tegen HTTP toegang te blokkeren.
2. Maak beleidsgroepen om alleen de klanten op uw gewenste subnetten toe te staan. Een simpele demonstratie van dit beleid is:
   Beleidsgroep 1: Is van toepassing op Subnet 10.0.0.0/8 (veronderstelt dit uw clientnetwerk is). Voeg je gewenste acties toe.

Standaardbeleid: Alle protocollen blokkeren - HTTP, HTTPS, FTP en HTTP

Meer gedetailleerd beleid kan worden gecreëerd boven Policy Group 1. Zolang andere regels alleen van toepassing zijn op de juiste clientsubnetten, zal al het andere verkeer de "alle" regel onderaan ontkennen.

Clients die HTTP-CONNECT-aanvragen gebruiken om niet-HTTP-verkeer via tunnelkanalen te verzenden

HTTP CONNECT-verzoeken worden gebruikt om niet-HTTP-gegevens te tunnelen via een HTTP-proxy. Het meest gebruikelijke gebruik van een HTTP CONNECT-verzoek is tunnelverkeer voor HTTPS. Als een client die expliciet is geconfigureerd toegang tot een HTTPS-site wil hebben, MOET deze eerst een HTTP CONNECT-aanvraag naar de WSA verzenden.

Een voorbeeld van een CONNECT-verzoek is als zodanig: CONNECT http://www.website.com:443/ HTTP/1.1

Dit vertelt de WSA dat de cliënt door de WSA aan http://www.website.com/ wil tunnels op haven 443.

HTTP CONNECT-verzoeken kunnen worden gebruikt om elke poort te tunnelen. Vanwege mogelijke beveiligingsproblemen staat WSA alleen CONNECT-verzoeken naar deze poorten standaard toe:

20, 21, 443, 563, 8443, 8080

Als het nodig is om extra CONNECT tunnelpoorten toe te voegen, om veiligheidsredenen, wordt aanbevolen om ze toe te voegen aan een extra beleidsgroep die alleen van toepassing is op de client-IP subnetten die deze extra toegang nodig hebben. De toegestane CONNECT-poorten kunnen in elke beleidsgroep worden gevonden onder Toepassingen > Protocol-controllers.

Een voorbeeld van een verzoek dat via een open volmacht wordt verzonden wordt hier getoond:

```
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
```