Contents

Introduction

This configuration example is meant to be interpreted with the aid of the official documentation from the configuration guide located here:

http://www.cisco.com/en/US/docs/security/asa/asa82/configuration/guide/conns_botnet.htm

Overview

Malware is malicious software that is installed on an unknowing host. Malware that attempts network activity such as sending private data (passwords, credit card numbers, key strokes, or proprietary data) can be detected by the Botnet Traffic Filter when the malware starts a connection to a known bad IP address. The Botnet Traffic Filter checks incoming and outgoing connections against a dynamic database of known bad domain names and IP addresses (the blacklist), and then logs or blocks any suspicious activity.

Prerequisite

The ASA must be running minimum 8.2 code to be able to configure botnet feature.

```
ASA-5505# sh ver

Cisco Adaptive Security Appliance Software Version 8.2(1)
Manager Version 6.2(5)
.......
```

Botnet license must be installed on the ASA

```
ASA-5505# sh ver

Cisco Adaptive Security Appliance Software Version 8.2(1)
Device Manager Version 6.2(5)
.......

Botnet Traffic Filter        : Enabled
```

Limitations

Botnet Traffic Filter does not share any information between Failover pairs. Failovers or Reboots require a re-download of the Dynamic Database.

Currently there is no support for IPV6.

Configuration

Enable DNS client on ASA

This steps is required to allow it to resolve the address of CSIO's updater service, so the dynamic filter update client to fetch updates.

```
ASA(config)#dns domain-lookup outside
ASA(config)#dns server-group DefaultDNS
ASA(config-dns-server-group)#name-server 4.2.2.2
```

Enable dynamic traffic filtering (Botnet Traffic Filter)

```
ASA(config)#dynamic-filter updater-client enable
```

Enable the Botnet Traffic Filter database update

```
ASA(config)#dynamic-filter use-database
```

Classify the traffic that will be exempted and subjected.

```
ASA(config)#access-list botnet-exclude extended deny ip any 192.168.0.0 255.255.0.0  ---> exempted
ASA(config)#access-list botnet-exclude extended permit ip any any  ---> subjected traffic
```

Enable dynamic-filter classification on outside interface

```
ASA(config)#dynamic-filter enable interface outside classify-list botnet-exclude
```

Configure a class map and only match dns traffic

```
ASA(config)#class-map botnet-DNS
ASA(config-cmap)#match port udp eq domain
```

Enable DNS snooping on the external interface

```
ASA(config)#policy-map botnet-policy
ASA(config-pmap)#class botnet-DNS
ASA(config-pmap-c)#inspect dns dynamic-filter-snoop

ASA(config)# service-policy botnet-policy interface outside
```

Alternatively, you can also choose to apply this to the existing global policy that is already configured on the ASA.

```
class-map inspection_default
match default-inspection-traffic
!
policy-map global_policy
class inspection_default
 inspect dns dynamic-filter-snoop
 ...
service-policy global_policy global
```

Define local whitelists and/or blacklists if needed.

Never block addresses:

This is traffic to or from an IP address that is considered to be good. It is part of administrator configured lists.

```
ASA(config)# dynamic-filter whitelist
ASA(config-llist)#name www.google.com
ASA(config-llist)#name www.cisco.com
```

Manual Black List:

This is traffic to or from an IP address that is considered to be malicious. This IP address can be either an IP address/network entry in the dynamic blacklist or administrator configured blacklist, or it can be a snooped IP address that was found in a DNS reply for a blacklisted domain.

```
ASA(config)# dynamic-filter blacklist
ASA(config-llist)#name www.crackhell.com
ASA(config-llist)#name www.megaport.hu
ASA(config-llist)#address 164.109.48.46 255.255.255.255
```

Related show Commands

```
show dynamic-filter data
show dynamic-filter database find <string>
show dynamic-filter reports top botnet-sites
show dynamic-filter reports top infected-hosts
show dynamic-filter reports top botnet-ports
```

Show running-config

```
dns domain-lookup outside
dns server-group DefaultDNS
name-server 64.102.6.247
```

```
!
dynamic-filter updater-client enable
dynamic-filter use-database
!
access-list botnet-exclude extended deny ip any 192.168.0.0 255.255.0.0
access-list botnet-exclude extended permit ip any any
!
dynamic-filter enable interface outside classify-list botnet-exclude
!
class-map botnet-DNS
match port udp eq domain
!
policy-map botnet-policy
class botnet-DNS
 inspect dns dynamic-filter-snoop
!
service-policy botnet-policy interface outside
```

Related Information

Logging

```
338001 - 338004
338101 - 338104
338201 - 338204
338301 - 338310
```

http://www.cisco.com/en/US/docs/security/asa/asa82/system/message/logmsgs.html#wp5787165