自适应安全设备的BotNet流量过滤器问题

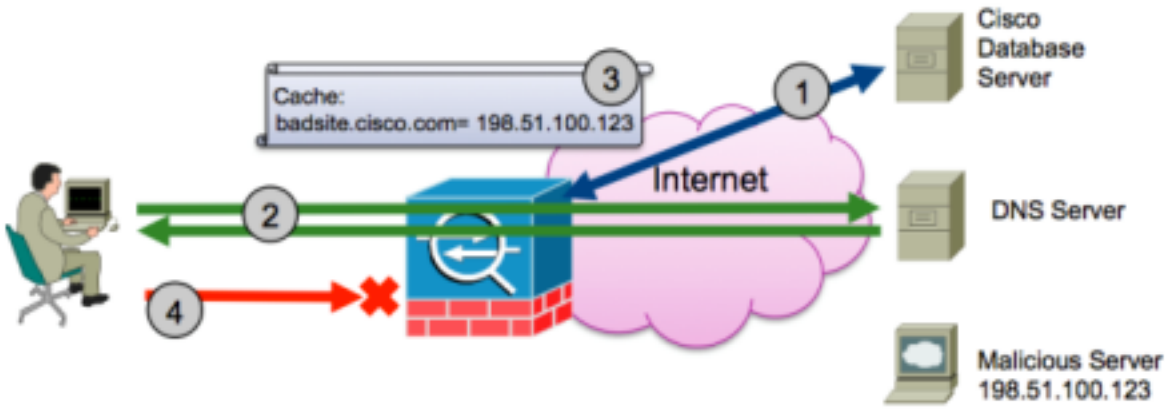
目录

简介

本文档介绍在自适应安全设备(ASA)上排除BotNet流量过滤器功能故障的步骤。 有关BotNet流量过滤器配置的帮助，请参阅本配置指南：配置BotNet流量过滤器。

背景信息

BotNet流量过滤器监控内部DNS客户端和外部DNS服务器之间的域名服务器(DNS)请求和响应。处理DNS响应时，会根据已知恶意域的数据库检查与响应关联的域。如果存在匹配项，则阻止任何进一步到DNS响应中IP地址的流量。请参阅此图。



1. **检查动态过滤器数据库。**ASA定期下载已知恶意域和IP地址的当前数据库。思科的安全智能运营中心(SIO)确定此数据库中的域和IP地址为恶意软件或其他恶意内容提供服务。
2. **确保DNS流量通过ASA。**内部网络上的用户或内部网络上受感染的计算机尝试访问恶意服务器，以下载恶意软件或参与BotNet。要连接到恶意服务器，主机必须执行DNS查找。在本例中，计算机尝试访问badsite.cisco.com。主机向本地DNS服务器或直接向外部DNS服务器发送DNS请求。在这两种情况下，DNS请求必须遍历ASA，而DNS响应也必须遍历同一ASA。
3. **检查DNS-snoop缓存。**DNS检测的DNS监听功能（如果启用）可监控DNS流量并确定DNS服务器已返回DNS A记录响应。DNS-snoop功能获取A-Record响应中存在的域和IP地址，并将

其添加到DNS-snoop缓存。根据步骤1中下载的数据库检查域，并找到匹配项。DNS响应不会丢弃，并允许通过。

4. **测试带流量的BotNet流量过滤器。**由于步骤3中存在匹配项，ASA会添加一条内部规则，指示与badsite.cisco.com关联的IP的所有流量都将被丢弃。然后，受感染的计算机尝试访问URL badsite.cisco.com服务器，流量被丢弃。

排除工作流程故障

使用这些步骤排除故障并检验功能是否正常工作。

步骤 1：检查动态过滤器数据库

检查数据库是否已下载，然后输入命令**show dynamic-filter data**。看此输出示例：：

```
# show dynamic-filter data
Dynamic Filter is using downloaded database version '1404865586'
Fetched at 21:32:02 EDT Jul 8 2014, size: 2097145
Sample contents from downloaded database:
dfgdsfgsdfg.com bulldogftp.com bnch.ru 52croftonparkroad.info
paketoptom.ru lzvideo.altervista.org avtovirag.ru cnner.mobi
Sample meta data from downloaded database:
threat-level: very-high, category: Malware,
description: "These are sources that use various exploits to deliver adware,
spyware and other malware to victim computers. Some of these are associated
with rogue online vendors and distributors of dialers which deceptively
call premium-rate phone numbers." threat-level: high, category: Bot
and Threat Networks, description: "These are rogue systems that
control infected computers. They are either systems hosted on
threat networks or systems that are part of the botnet itself
threat-level: moderate, category: Malware,
description: "These are sources that deliver deceptive or malicious anti-spyware,
anti-malware, registry cleaning, and system cleaning software."
threat-level: low, category: Ads,
description: "These are advertising networks that deliver banner ads,
interstitials, rich media ads, pop-ups, and pop-unders for websites,
spyware and adware. Some of these networks send ad-oriented HTML emails
and email verification services."
Total entries in Dynamic Filter database:
Dynamic data&colon; 80677 domain names , 4168 IPv4 addresses
Local data&colon; 0 domain names , 0 IPv4 addresses
Active rules in Dynamic Filter asp table:
Dynamic data&colon; 0 domain names , 4168 IPv4 addresses
Local data&colon; 0 domain names , 0 IPv4 addresses
```

在此输出中，ASA指示上次成功获取数据库的时间以及此数据库中内容的示例。如果运行命令**show dynamic-filter data**，并且该命令显示没有下载任何数据库，请首先排除此步骤的故障。阻止ASA获取动态过滤器数据库的常见问题包括：

- **ASA上缺少或不正确的DNS配置。**动态过滤器更新程序客户端必须解析更新服务器的主机名。DNS必须在ASA上配置并运行。从命令行对已知域执行ping操作，并确定ASA是否可以解析主机名。
- **无法从ASA访问Internet。**如果ASA位于无权访问Internet的网络中，或者上游设备阻止ASA的外部IP地址访问Internet，则更新失败。
- **更新程序客户端未启用。**必须配**置命令dynamic-filter updater-client enable**，以便ASA可以下载

数据库。

输入命令debug dynamic-filter updater-client以调试数据库。请参阅以下命令输出示例：

```
Dynamic Filter: Updater client fetching dataDynamic Filter: update
startingDBG:01:2902417716:7fff2c33ec28:0000: Creating fiber
0x7fff2c4dce90 [ipe_request_fiber], stack(16384) =
0x7fff2c505c60..0x7fff2c509c58 (fc=2),
sys 0x7fff20906038 (FIBERS/fibers.c:fiber_create:544)
DBG:02:2902417779:7fff2c4dce90:0000: Jumpstarting ipe_request_fiber 0x7fff2c4dce90,
sys 0x7fff2c33eba0 (FIBERS/fibers-jumpstart.c:_fiber_jumpstart:36)
Dynamic Filter: Created lua machine, launching lua script
DBG:03:2902422654:7fff2c4dce90:0000: Connecting to 00000000:1591947792
(SAL/netsal.c:netsal_client_sock_connect:323)
DBG:04:2902422667:7fff2c4dce90:0000: otherPifNum 3, nexthop4 17c12ac
(SAL/netsal.c:netsal_client_sock_connect:374)
DBG:05:2902422691:7fff2c4dce90:0000: about to call netsal__safe_encapsulate for
(sal-np/ssl/CONNECT/3/208.90.58.5/443/M/0/NOTUNGW)
(SAL/netsal.c:netsal_client_sock_connect:446)
DBG:06:2902422920:7fff2c4dce90:0000: connection timeout set for 10 seconds
(SAL/netsal.c:netsal_client_sock_connect:473)
DBG:07:2902750615:7fff2c4dce90:0000: SALNPCLOSENOTIFY: p=0x0 0/0 more buffered
(SAL/channel-np.c:_sal_np_ioctl:1312)
Dynamic Filter: Processing updater server response
Dynamic Filter: update file url1 =
http://updates.ironport.com/threatcast/1.0/blacklist/2mb-1file/1404865586
Dynamic Filter: update file url2 =
http://updates.ironport.com/threatcast/1.0/blacklist/2mb-1file/1404865586
Channel NP p=0x0000000000000000 0/0 more bufferedchannel-np.cDBG:08:2902784011:
7fff2c4dce90:0000: Connecting to 00000000:538976288
(SAL/netsal.c:netsal_client_sock_connect:323)
DBG:09:2902784026:7fff2c4dce90:0000: otherPifNum 3, nexthop4 17c12ac
(SAL/netsal.c:netsal_client_sock_connect:374)
DBG:10:2902784051:7fff2c4dce90:0000: about to call netsal__safe_encapsulate for
(sal-np/tcp/CONNECT/3/208.90.58.25/80/M/0/NOTUNGW)
(SAL/netsal.c:netsal_client_sock_connect:446)
DBG:11:2902784241:7fff2c4dce90:0000: connection timeout set for 10 seconds
(SAL/netsal.c:netsal_client_sock_connect:473)
DBG:12:2902914651:7fff2c4dce90:0000: SALNPCLOSENOTIFY: p=0x0 0/0 more buffered
(SAL/channel-np.c:_sal_np_ioctl:1312)
DBG:13:2902914858:7fff2c4dce90:0000: Connecting to 00000000:25465757
(SAL/netsal.c:netsal_client_sock_connect:323)
DBG:14:2902914888:7fff2c4dce90:0000: otherPifNum 3, nexthop4 17c12ac
(SAL/netsal.c:netsal_client_sock_connect:374)
DBG:15:2902914912:7fff2c4dce90:0000: about to call netsal__safe_encapsulate for
(sal-np/tcp/CONNECT/3/208.90.58.25/80/M/0/NOTUNGW)
(SAL/netsal.c:netsal_client_sock_connect:446)
DBG:16:2902915113:7fff2c4dce90:0000: connection timeout set for 10 seconds
(SAL/netsal.c:netsal_client_sock_connect:473)
Channel NP p=0x0000000000000000 0/0 more bufferedchannel-np.cDBG:17:2907804137:
7fff2c4dce90:0000: SALNPCLOSENOTIFY: p=0x0 0/0 more buffered
(SAL/channel-np.c:_sal_np_ioctl:1312)
Dynamic Filter: Successfully downloaded the update file from url1
Dynamic Filter: Successfully finished lua script
DBG:18:2907804722:7fff2c4dce90:0000: Fiber 0x7fff2c4dce90 finished leaving 3 more
(FIBERS/fibers-jumpstart.c:_fiber_jumpstart:64)
DBG:19:2907804746:7fff2c4dce90:0000: Exiting fiber 0x7fff2c4dce90
(FIBERS/fibers.c:fiber__kill:1287)
DBG:20:2907804752:7fff2c4dce90:0000: Fiber 0x7fff2c4dce90 terminated, 2 more
(FIBERS/fibers.c:fiber__kill:1358)
Dynamic Filter: Downloaded file successfully
Channel NP p=0x0000000000000000 0/0 more bufferedchannel-np.cDynamic Filter: read
ramfs bytes 2097152
```

```
Dynamic Filter: file MD5 verification check succeeded
Dynamic Filter: decrypt key succeeded
Dynamic Filter: decrypt file succeeded byte = 2097145
Dynamic Filter: updating engine bytes = 2097145
Dynamic Filter: meta data length = 2987
INFO: Dynamic Filter: update succeeded
```

在此输出中，您可以看到更新程序在获取新数据库时执行的以下步骤：

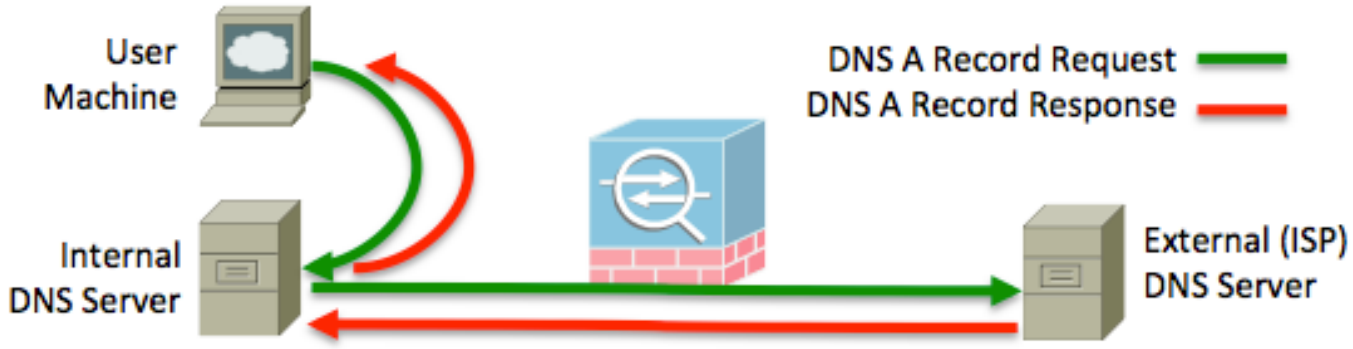
- 更新程序访问URL http://update-manifests.ironport.com，以确定其下载的数据库。
- 清单服务器返回两个可能的URL进行下载。
- 更新程序客户端下载数据库。
- 数据库被解密并存储在存储器中以供动态过滤器进程使用。

不同更新服务器的连接问题在此输出中表现为错误，并有助于进一步排除故障。使用dynamic-filter database fetch命令强制更新程序客**户端手动运行**。

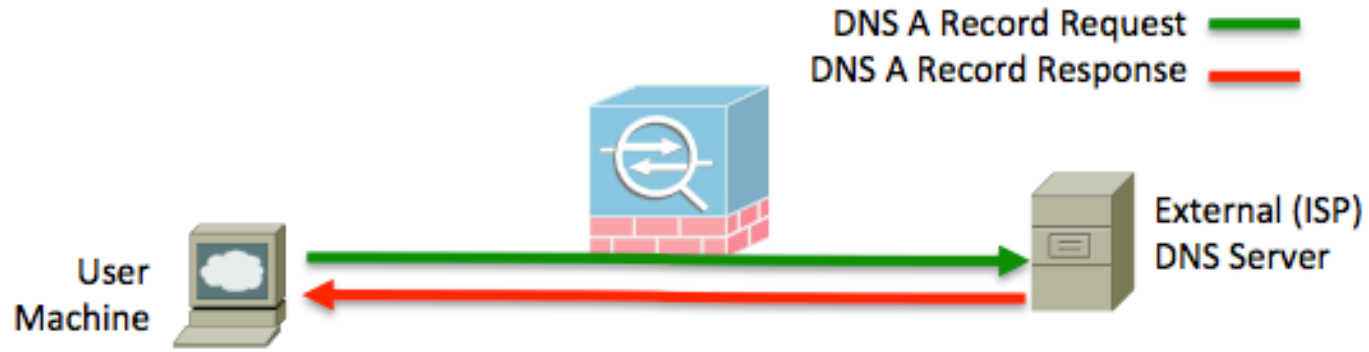
步骤 2：确保DNS流量通过此ASA

ASA的BotNet流量过滤功能由匹配域的IP地址构建，因此ASA必须与流经网络的DNS请求和响应保持一致。某些拓扑可能导致DNS流量采用不包含问题ASA的路径。大多数网络都有内部DNS服务器，充当内部用户的DNS转发器和缓存。只要这些服务器转发其不拥有或无法应答的域的DNS请求，就会将该请求转发到需要通过ASA的服务器，不会出现任何问题。请参阅这些带内部DNS服务器和不带内部DNS服务器的拓扑：

此示例拓扑显示指向内部DNS服务器的用户，该服务器将转发到外部DNS服务器。



此示例拓扑显示直接指向外部DNS服务器的用户。



在这两个拓扑示例中，功能BotNet流量过滤器部署的关键是，对外部域的DNS A记录请求必须通过运行DNS监听功能的ASA。在内部服务器示例中，如果内部DNS服务器采用与用户计算机不同的网络路径来访问互联网，并且在该过程中不遍历ASA，则DNS监听表将不包含由用户机DNS请求引起的IP到域映射，并且用户计算机可能不会按预期过滤。

使用以下技术检查DNS流量是否通过ASA:

- 检查服务策略。查看**show service-policy**的输出，以确定是否应用了DNS检测(使用dynamic-filter-snoop关键字**进行配置)并查**看流量。在您发出DNS请求时，与DNS检测关联的数据包计数应增加。
- 使用捕获。DNS监听功能会查看通过ASA的DNS数据包，因此检查数据包是否到达ASA非常重要。使用ASA的内置捕获功能确保DNS流量正确进入并离开此ASA。

步骤 3：检查DNS监听缓存

DNS监听现金应填充IP到域映射。单个IP地址可能具有与其关联的无限个域。托管网站的公司可以通过这种方式为数千个域提供服务，而只需几个IP地址。输入命令**show dynamic-filter dns-snoop detail**，并查看DNS-snoop缓存中当前数据的转储。这是ASA使用DNS检测的DNS监听功能获取的所有IP到域映射的记录。看此输出示例：：

```
DNS Reverse Cache Summary Information: 3 addresses, 3 names
Next housekeeping scheduled at 22:28:01 EDT Jul 8 2014,
DNS reverse Cache Information:
[198.151.100.77] flags=0x1, type=0, unit=0 b:u:w=0:1:0, cookie=0x0
[cisco.com] type=0, ttl=31240
[198.151.100.91] flags=0x23, type=0, unit=0 b:u:w=1:1:0, cookie=0x0
[magnus.cisco.com] type=1, ttl=0
[raleigh.cisco.com] type=0, ttl=0
[198.151.100.1] flags=0x2, type=0, unit=0 b:u:w=1:0:0, cookie=0x0
[badsite.cisco.com] type=1, ttl=0
```

在本示例中，ASA获取有关三个IP地址（四个域）的信息。**magnus.cisco.com和raleigh.cisco.com**都解析为198.151.100.91。在本例中，两个域**magnus.cisco.com和**badsite.cisco.com列表为类型1。这意味着该域在数据库中被发现为黑名单域。其他域列为类型0，这表示域未列入黑名单或列入白名单，只是正常域。

1. 检查来自用户机器的DNS请求是否会经过防火墙，并由DNS监听处理并发出DNS请求。检查缓存中是否有匹配的条目。测试并使用解析但模糊到最近未查询且已在表中的域。例如，选择域asa.cisco.com。命令行工具nslookup用于查询该主机名。请参阅以下示例：

   ```
   $ nslookup asa.cisco.com

   Name: asa.cisco.com
   Address: 198.151.100.64
   ```

2. 检查DNS-snoop缓存。请参阅以下示例：

   ```
   DNS Reverse Cache Summary Information: 5 addresses, 7 names
   Next housekeeping scheduled at 22:48:01 EDT Jul 8 2014,
   DNS reverse Cache Information:
   [198.151.100.64] flags=0x11, type=0, unit=0 b:u:w=0:1:0, cookie=0x0
   [asa.cisco.com] type=0, ttl=86359
   ```

该条目存在于DNS-snoop缓存中。如果在nslookup测试之前该条目不存在，则表示DNS监听功能正常工作，并且ASA能够正确处理DNS请求和响应。

如果条目未显示，请确保DNS流量通过ASA。您可能需要刷新主机或内部DNS服务器上的DNS缓存（如果适用），以确保不从缓存处理请求。

DNS监听功能不支持EDNS0。如果DNS客户端或服务器使用EDNS0，则如果响应存在其他资源记录，ASA可能不会用IP到域映射填充DNS监听缓存。此限制由Cisco Bug ID CSCta36873跟踪。

步骤 4：使用流量测试BotNet流量过滤器

在步骤3中，DNS-snoop缓存显示域badsite.cisco.com位于黑名单中。Ping相关域以测试僵尸网络功能。当您ping域时，比尝试在Web浏览器中加载域更安全。请勿使用Web浏览器测试动态过滤器功能，因为如果浏览器加载恶意内容，您的计算机可能会受到危害。使用互联网控制消息协议(ICMP)，因为它是一种更安全的方法，而且是BotNet流量过滤器的有效测试，因为它基于IP阻止流量，而不特定于端口或协议。

如果您不知道列入黑名单的站点，您可以轻松找到一个。输入命令**dynamic-filter database find <search_term>**以查找列入黑名单并与提供的搜索术语匹配的域。请参阅以下示例：

```
ASA# dynamic-filter database find cisco verybadsite.cisco.com
m=44098 acmevirus.cisco.com m=44098Found more than 2 matches,
enter a more specific string to find an exact match
```

Ping返回的域之一。当您对此域执行ping操作时，将导致发生以下操作：

1. 主机为相关域生成DNS请求。
2. DNS请求会直接从主机或由内部服务器转发到ASA。
3. DNS响应会遍历ASA，返回主机或内部服务器。
4. DNS-snoop功能将填充DNS-snoop缓存中的此IP到域映射。
5. ASA将域与动态过滤器数据库进行比较并确定匹配项。ASA会阻止来自与恶意域关联的IP的进一步入站和出站流量。
6. 主机发送ICMP回应请求，ASA会丢弃该请求，因为该请求的目的地是与恶意域关联的IP。

当ASA丢弃ICMP测试流量时，它会记录系统日志（系统日志），类似于以下示例：

```
Jul 08 2014 23:14:17: %ASA-4-338006: Dynamic Filter dropped blacklisted
ICMP traffic from inside:192.168.1.100/23599 (203.0.113.99/23599) to
outside:198.151.100.72/0 (198.151.100.72/0), destination 198.151.100.72
resolved from dynamic list: acmevirus.cisco.com, threat-level: very-high,
category: Malware
```

命令show dynamic-filter statistics的输**出指示已分类**并可能丢弃的连接。请参阅以下示例：

```
ASA(config)# show dynamic-filter statistics
Enabled on interface inside
Total conns classified 163, ingress 163, egress 0
Total whitelist classified 0, ingress 0, egress 0
Total greylist classified 8, dropped 0, ingress 8, egress 0
Total blacklist classified 155, dropped 154, ingress 155, egress 0
Enabled on interface outside
Total conns classified 0, ingress 0, egress 0
Total whitelist classified 0, ingress 0, egress 0
Total greylist classified 0, dropped 0, ingress 0, egress 0
Total blacklist classified 0, dropped 0, ingress 0, egress 0
Enabled on interface management
Total conns classified 0, ingress 0, egress 0
Total whitelist classified 0, ingress 0, egress 0
Total greylist classified 0, dropped 0, ingress 0, egress 0
```

```
Total blacklist classified 0, dropped 0, ingress 0, egress 0
```

仅当对列入黑名单、列入白名单或灰名单的IP地址进行连接尝试时，分类计数器才会增加。所有其他流量不会导致分类计数器增加。分类列表的数字低并不意味着ASA没有根据BotNet流量过滤器评估新连接尝试。相反，此低数字表示很少有源或目标IP地址被列入黑名单、白名单或灰名单。使用本文档中的说明以正确确认功能。

如果测试流量未丢弃，请检查配置以确保其配置为丢弃具有适当威胁级别的流量。请参阅此示例配置，该配置在ASA上全局启用BotNet流量过滤器：

```
dynamic-filter updater-client enable
dynamic-filter use-database
dynamic-filter enable
dynamic-filter drop blacklist
```