僵尸网络数据流过滤器问题用可适应安全工具

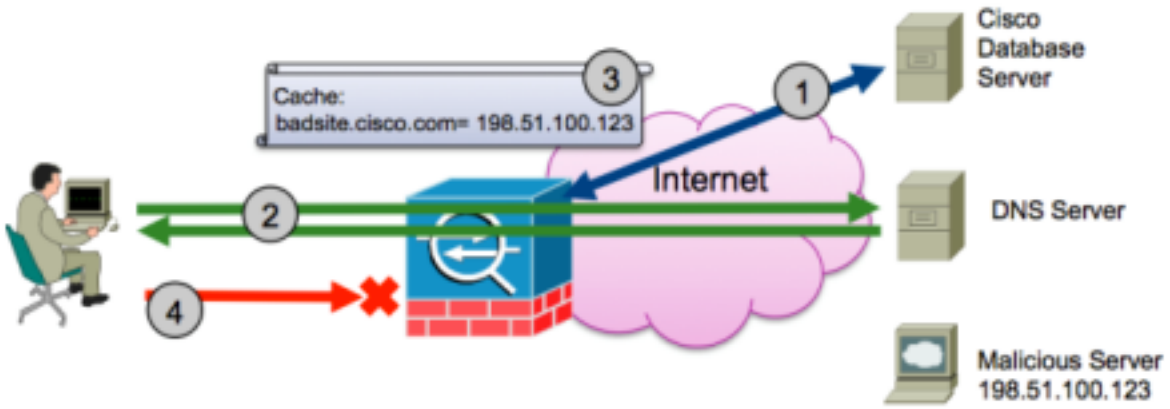
目录

简介

本文描述步骤排除故障僵尸网络在可适应安全工具(ASA)的数据流过滤器功能。关于与僵尸网络数据流过滤器配置的协助，请参阅此此配置指南： [配置僵尸网络数据流过滤器](#)。

背景信息

僵尸网络数据流过滤器监视器域名服务器(DNS)请求和答复在内部DNS客户端和外部DNS服务器之间。当DNS答复处理时，域关联与答复根据已知有恶意的域数据库核对。如果有匹配，对IP地址的任何另外流量现在DNS答复阻塞。请参阅此图表。



1. **检查动态过滤器数据库。**ASA周期地下载已知有恶意的域和IP地址一个当前数据库。思科的安全智能操作(SIO)确定域和IP地址在此数据库为恶意软件或其他有恶意的内容服务。
2. **保证DNS流量交叉ASA。**内部网络或一个受感染的机器的一个用户在内部网络设法访问一个有恶意的服务器为了下载恶意软件或参加僵尸网络。为了连接到有恶意的服务器，主机必须执行DNS查找。在本例中，对badsite.cisco.com的计算机尝试访问。主机发送DNS请求到本地DNS服务器或直接地到一个外部DNS服务器。在这两种情况下， DNS请求必须横断ASA，并且DNS答复必须也横断同样ASA。
3. **检查Dns监听缓存。**DNS检查的Dns监听功能，如果启用，监控DNS流量并且确定DNS A类记

录答复从DNS服务器返回。Dns监听功能采取域，并且IP地址在A类记录答复提交并且添加它到Dns监听缓存。域根据从step1的下载的数据库核对，并且找到匹配。DNS答复没有丢弃和允许通过通过。

4. **测试有流量的僵尸网络数据流过滤器。**由于有在步骤3的一匹配， ASA增加指示的一个内部规则到/从IP的所有流量关联与badsite.cisco.com丢弃。感染的计算机然后设法访问URL badsite.cisco.com服务器，并且流量丢弃。

排除故障工作流

请使用这些步骤为了排除故障和验证功能运作。

步骤 1：检查动态过滤器数据库

检查数据库是否下载并且输入show命令动态**过滤器数据**。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指示最后成功的数据库取指令的时期和内容的示例在此数据库的。如果运作show命令动态**过滤器数据**，并且命令显示数据库未下载，首先排除故障此步骤。防止ASA获取动态过滤器数据库的常见问题包括：

- **在ASA的缺失或不正确的DNS配置。**动态过滤器更新客户端必须解析更新服务器的主机名。DNS一定是配置和工作在ASA。ping从命令行的著名的域并且确定ASA是否能解决主机名。
- **从ASA的没有互联网访问。** 如果ASA在不访问的网络互联网，或者一个上行设备阻塞从访问的ASA的外部IP地址到互联网，更新发生故障。
- **更新客户端没有启用。**必须配置命令动态**过滤器更新客户端enable (event)，**以便ASA能下载数据库。

输入debug命令动态**过滤器更新客户端**为了调试数据库。请参阅从命令的此输出示例：：

```
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，您能看到更新采取的这些步骤，当得到一个新的数据库时：

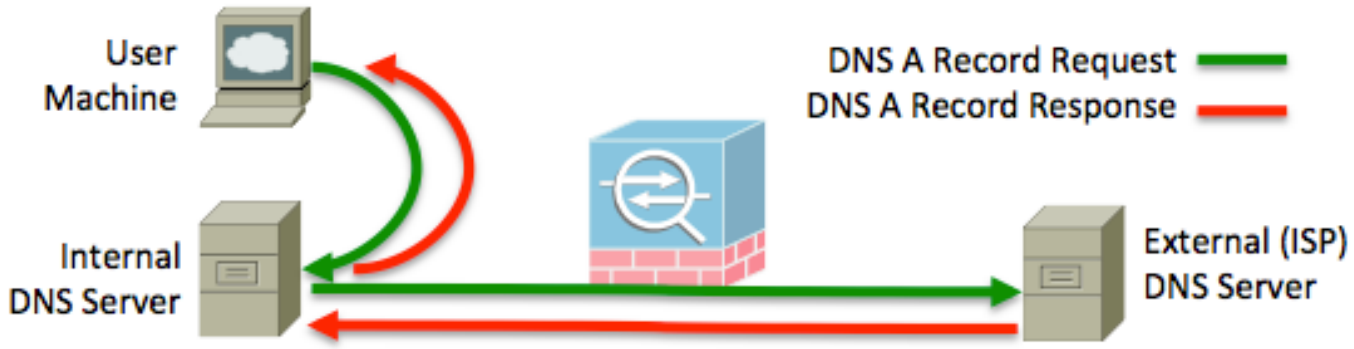
- 更新提供援助对URL http://update-manifests.ironport.com为了确定哪个数据库下载。
- 明显服务器返回下载的两个可能的URL。
- 更新客户端下载数据库。
- 数据库在内存解密并且存储供动态过滤过程使用。

不同的更新服务器的连通性问题在此输出中表明作为错误并且帮助进一步排除故障。迫使更新客户端以命令**动态过滤器数据库取指令**手工运行。

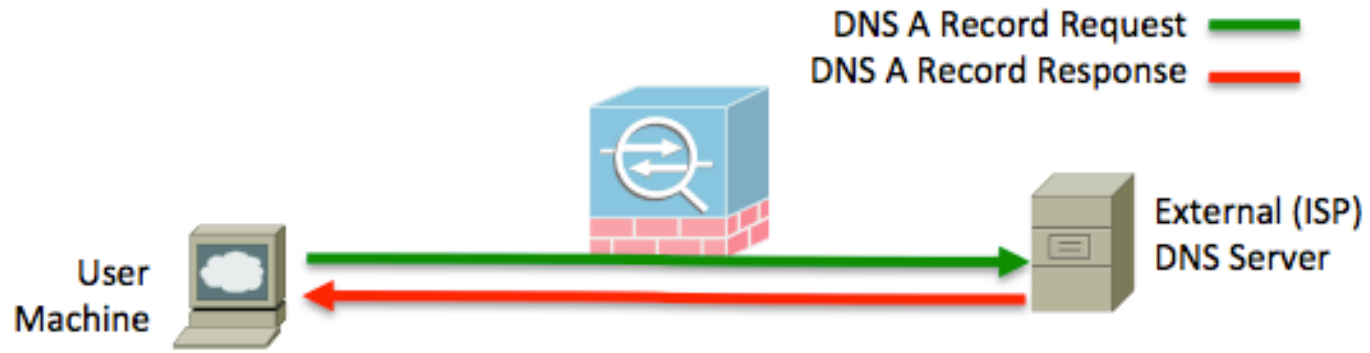
步骤 2：保证DNS流量交叉此ASA

僵尸网络ASA的数据流过滤器功能被建立匹配域的IP地址，因此ASA必须是根据穿程网络的DNS请求和答复。一些拓扑也许造成DNS流量采取不包括有问题的ASA的路径。多数网络有作为DNS转发器和缓存内部usrs的内部DNS服务器。只要这些服务器，当他们转发一个DNS要求域他们时没拥有也不能应答为，寄请求给要求横断ASA的服务器，问题不应该发生。请参阅这些拓扑有和没有内部DNS服务器：

此拓扑示例显示指向内部DNS服务器的用户哪些转发到一个外部DNS服务器。



此拓扑示例显示指向直接地一个外部DNS服务器的用户。



在两个结构示例中，对运行Dns监听功能的一功能僵尸网络数据流过滤器部署的密钥是DNS A类记录要求外部域必须穿过ASA。在内部服务器示例中，如果内部DNS服务器比用户计算机采取一个不同的网络路径为了到达互联网和在进程不横断ASA， Dns监听表不会包含用户计算机DNS请求和用户计算机威力造成的IP对域地图不被过滤正如所料。

请使用这些技术为了检查DNS流量穿过ASA ：

- 检查服务策略。查看**show service策略**输出为了确定DNS检查是否应用，配置与动态过滤器**监听**关键字，并且看到流量。当您做DNS请求，数据包计数关联与DNS检查应该增加。
- 请使用捕获。Dns监听功能查看横断ASA的DNS数据包，因此重要的是您检查数据包到达ASA。请使用ASA的内置的捕获功能为了确保， DNS流量适当地输入并且离开此ASA。

步骤 3：检查DNS监听缓存

Dns监听现金应该用IP对域地图填充。单个IP地址也许有域一个不可限量的编号assocated用它。这是主机网站的公司如何能服务千位域用一些个IP地址。在Dns监听缓存输入show命令动态**过滤器dns监听详细信息**并且当前请参阅数据的转储。这是ASA得到与使用DNS检查的Dns监听功能所有IP对域地图的记录。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
```

在本例中， ASA学习关于三个IP地址，但是四个域的信息。**magnus.cisco.com**和**raleigh.cisco.com**两个解决对198.151.100.91。在本例中，两域， **magnus.cisco.com**和**badsite.cisco.com**列出作为类型1。这意味着域在数据库被找到作为一个列入黑名单的域。其他域列出作为类型0，表明域没有列入黑名单或whitelisted并且是一个正常域。

1. 检查从用户计算机的DNS请求eventially横断防火墙和由Dns监听处理并且做DNS请求。检查缓存配比的条目。测试并且请使用解决的一个域，但是足够无名的最近未被查询并且已经在表里。例如，域asa.cisco.com选择。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监听缓存。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
   ```

条目是存在Dns监听缓存。如果条目不存在，在nslookup测验，它将含义Dns监听功能工作，并且前ASA正确地与DNS请求和答复一起使用。

如果条目不显示，请保证DNS流量穿过ASA。您也许需要淹没主机或内部DNS服务器的DNS缓存，如果适用，为了保证请求没有从缓存服务。

Dns监听功能不支持EDNS0。如果DNS客户端或服务器使用EDNS0， ASA也许不填充Dns监听缓存用IP对域地图，如果答复有现在其他资源的记录。此限制由Cisco Bug ID CSCta36873跟踪。

步骤 4：测试有流量的僵尸网络数据流过滤器

在步骤3， Dns监听缓存显示域badsite.cisco.com在黑名单。ping有问题的域为了测试僵尸网络功能。当您ping域时，比，如果设法装载在Web浏览器的域安全。请勿测试动态过滤器功能通过使用您的Web浏览器，因为您的计算机也许折衷，如果浏览器装载有恶意的内容。请使用互联网控制消息协议(ICMP)，因为它是一个更加安全的方法并且是僵尸网络数据流过滤器的一有效测验，因为阻塞基于IP和没什么特定对端口或协议。

如果不知道一个列入黑名单的站点，您能容易地找到一。输入命令动态**过滤器数据库查找<search_term>**查找列入黑名单的域和匹配提供的搜索术语。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返回的其中一个域。当您ping此域，将导致这些操作发生：

1. 主机生成一个DNS要求有问题的域。
2. DNS请求横断ASA，直接地从主机或转发由内部服务器。
3. DNS答复横断ASA，回到主机或到内部服务器。
4. Dns监听功能在Dns监听缓存填充此IP对域地图。
5. ASA对dyanmic过滤器数据库比较域并且确定匹配。ASA阻塞从IP的进一步入站和出站通流量关联与有恶意的域。
6. 因为被注定对IP关联与一个有恶意的域，主机发送该的ICMP echo请求ASA丢包。

当ASA降低ICMP测试流量时，记录系统日志(Syslog)类似于此示例：

```
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
```

show命令动态**过滤器统计信息的**输出指示分类和潜在已丢失的连接。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
```

分级计数器只增加，如果连接尝试被做对列入黑名单， whitelisted或者greylisted的IP地址。与增加相反，其他流量不导致分级。分级列表的低数值不意味着ASA没有评估新连接尝试僵尸网络数据流过滤器。此低数值表明少量来源或目的地IP地址列入黑名单， whitelisted或者greylisted。请使用说明在本文为了适当地确认功能功能。

如果测试流量没有降低，请检查配置为了保证配置降低与一个适当的威胁级别的流量。请参阅此配置示例，启用僵尸网络数据流过滤器全局在ASA此处：

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

```
dynamic-filter enable
dynamic-filter drop blacklist
```