配置静态文件名誉主机或一个更替文件名誉Cloud服务器池在ESA

Contents

Introduction

本文描述如何配置Cisco电子邮件安全工具(ESA)传达和使用静态主机或一个代替名誉网云服务器池文件名誉与使用先进的Malware保护(AMP)。

背景信息

文件名誉查询是第一AMP的两层在ESA。 当横断ESA并且发送它到名誉判决的，安培的基于网云的智力网络文件名誉捕获每个文件指纹。产生这些结果， ESA管理员能自动地阻拦有恶意的文件和运用管理员定义的策略。 文件名誉网云服务在亚马逊网站服务(AW)主机。当您执行DNS查询在本文描述的主机名，您看到“.amazonaws.com”列出了。

AMP第二个层在ESA的是文件分析。 那在本文没有被覆盖。

文件名誉数据流的默认情况下SSL通信使用端口32137。在服务的配置时，端口443也许使用作为选择。参见ESA用户指南， “文件名誉过滤和文件分析”部分关于完全详细资料。ESA和网络管理员也许希望验证连接到IP地址、IP位置并且端口通信的(32137池与443)，在他们继续进行配置前。

默认AMERICAS(Legacy)名誉网云服务器池(网云sa.amp.sourcefire.com)

一旦文件名誉在ESA准许，被启用，并且被配置，默认情况下为此名誉网云服务器池将设置：

- AMERICAS(Legacy) (网云sa.amp.sourcefire.com)

主机名- “网云sa.amp.sourcefire.com”是DNS标准名记录(CNAME)。 CNAME是资源记录的类型在用于的DNS的指定域名是另一个域的一个别名，是“规范”域。相关的hostnamesin池附加对此CNAME也许类似于：

- ec2-107-22-180-78.compute-1.amazonaws.com (107.22.180.78)
- ec2-54-225-142-100.compute-1.amazonaws.com (54.225.142.100)
- ec2-23-21-208-4.compute-1.amazonaws.com (23.21.208.4)
- ec2-54-83-195-228.compute-1.amazonaws.com (54.83.195.228)

有可能选择的两个其它文献名誉服务器选择：

- 美洲(网云Sa.amp.cisco.com)
- 欧洲(cloud-sa.eu.am p.cisco.com)

这两个服务器在本文的“静态文件名誉服务器主机名(.cisco.com)”部分被覆盖。

您也许验证在任何时间被关联对从您的网络的美洲cloud-sa-amp.sourcefire.com CNAME的主机，当您运行此**开掘**或**nslookup**查询时：

```
$ dig cloud-sa.amp.sourcefire.com +short
cloud-sa-589592150.us-east-1.elb.amazonaws.com.
107.22.180.78
54.225.208.214
23.21.208.4
54.83.195.228

$ nslookup cloud-sa.amp.sourcefire.com
Server: 208.67.222.222
Address: 208.67.222.222#53

Non-authoritative answer:
cloud-sa.amp.sourcefire.com canonical name = cloud-sa-589592150.us-east-1.elb.amazonaws.com.
Name: cloud-sa-589592150.us-east-1.elb.amazonaws.com
Address: 54.225.208.214
Name: cloud-sa-589592150.us-east-1.elb.amazonaws.com
Address: 54.83.195.228
Name: cloud-sa-589592150.us-east-1.elb.amazonaws.com
Address: 107.22.180.78
Name: cloud-sa-589592150.us-east-1.elb.amazonaws.com
Address: 23.21.208.4
```

> **Note**:这些主机不是静态的，并且推荐不限制ESA文件名誉数据流根据对仅这些主机。您的查询的结果也许变化，作为在池的主机不预先通知将更改。

您能验证从此第三方工具的IP地理位置：

- http://geoiplookup.net/ip/107.22.180.78
- http://geoiplookup.net/ip/54.225.208.214
- http://geoiplookup.net/ip/23.21.208.4
- http://geoiplookup.net/ip/54.83.195.228

静态文件名誉服务器主机名(.cisco.com)

Cisco在2016年开始提供“.cisco.com”基于主机名为AMP的文件名誉服务。 有静态主机名和IP地址可用为从此的文件名誉：

- cloud-sa.amp.cisco.com (北美- USA)
- cloud-sa.eu.amp.cisco.com (欧洲–爱尔兰共和国)
- cloud-sa.apjc.amp.cisco.com (亚太–日本)

您也许验证主机和相关的IP地址从您的网络和运行**开掘**或**nslookup**查询：

北美(美国) ：

```
$ dig cloud-sa.amp.cisco.com +short
52.21.117.50
```

欧洲(爱尔兰共和国) ：

```
$ nslookup cloud-sa.eu.amp.cisco.com
Server: 208.67.222.222
Address: 208.67.222.222#53

Non-authoritative answer:
Name: cloud-sa.eu.amp.cisco.com
Address: 52.30.124.82
```

亚太(日本) ：

```
 $ dig cloud-sa.apjc.amp.cisco.com +short
52.69.39.127
```

您能验证从此第三方工具的IP地理位置：

- http://geoiplookup.net/ip/52.21.117.50
- http://geoiplookup.net/ip/52.30.124.82
- http://geoiplookup.net/ip/52.69.39.127

此时，没有退役“.sourcefire.com”主机名的计划。

代替欧洲名誉网云服务器池(cloud-sa.eu.am p.sourcefire.com)

对于欧盟(EU)要求发送特定的流量的基于用户EU根据服务器和仅数据中心，管理员能配置ESA指向EU静态主机或EU名誉网云服务器池：

- 网云SAeu.amp.cisco.com
- cloud-sa.eu.am p.sourcefire.com

类似默认主机名- “网云sa.amp.sourcefire.com”，主机名- “cloud-sa.eu.am p.sourcefire.com”也是CNAME。在池的相关的主机名附加对此CNAME也许类似于：

- ec2-54-217-245-97.eu-west-1.compute.amazonaws.com (54.217.245.97)
- ec2-54-247-186-153.eu-west-1.compute.amazonaws.com (54.247.186.153)
- ec2-176-34-122-245.eu-west-1.compute.amazonaws.com (176.34.122.245)

您也许验证被关联对从您的网络的欧洲cloud-sa.eu.amp.sourcefire.com CNAME并且运行**开掘或nslookup**查询：的主机：

```
$ dig cloud-sa.eu.amp.sourcefire.com +short
cloud-sa-162723281.eu-west-1.elb.amazonaws.com.
54.217.245.97
54.247.186.153
```

```
176.34.122.245

$ nslookup cloud-sa.eu.amp.sourcefire.com
Server: 208.67.222.222
Address: 208.67.222.222#53

Non-authoritative answer:
cloud-sa.eu.amp.sourcefire.com canonical name = cloud-sa-162723281.eu-west-1.elb.amazonaws.com.
Name: cloud-sa-162723281.eu-west-1.elb.amazonaws.com
Address: 54.247.182.97
Name: cloud-sa-162723281.eu-west-1.elb.amazonaws.com
Address: 176.34.122.245
Name: cloud-sa-162723281.eu-west-1.elb.amazonaws.com
Address: 54.247.186.153
```

> **Note**:这些主机不是静态的，并且推荐不限制ESA文件名誉数据流根据对仅这些主机。您的查询的结果也许变化，作为在池的主机不预先通知将更改。

您能验证从此第三方工具的IP地理位置：

- http://geoiplookup.net/ip/176.34.122.245
- http://geoiplookup.net/ip/54.247.186.153
- http://geoiplookup.net/ip/54.217.245.97

配置静态文件名誉主机或更替文件名誉Cloud服务器池在ESA

文件名誉可以从GUI或CLI被配置在ESA。在本文列出的配置步骤将展示CLI配置。然而，同样步骤和信息可以适用通过GUI (**安全服务>文件名誉和分析> Edit整体设置...文件名誉的>Advanced设置**)。

AsyncOS 10.x和更新

允许ESA配置AsyncOS 10.x新功能使用专用的名誉网云(在前提文件名誉服务器)或基于网云的文件名誉服务器。使用此更改， AMP配置不再提示输入主机名-与“请输入名誉网云服务器池”步骤。您必须选择设置其它文献名誉服务器作为专用的名誉网云和为该主机名提供公共密钥-。

对于10.0.x和更新，当您配置一个代替AMP名誉服务器时，也许要求您输入一个公共密钥被关联对该主机名-。

所有AMP名誉服务器使用同一个公共密钥：

```
-----BEGIN PUBLIC KEY-----
MFkwEwYHKoZIzj0CAQYIKoZIzj0DAQcDQgAEchIap1VqPuGibM2n3wjfhqQZdzC9
WI1Z7QZ2Q7VesLe+A53TxYujeo7fCDKJEQKrPjU6kI36PSZusObr9Cur/g==
-----END PUBLIC KEY-----
```

此示例将帮助您设置代替文件名誉服务器到cloud-sa.eu.amp.sourcefirce.com ：

```
my11esa.local > ampconfig

NOTICE: This configuration command has not yet been configured for the current cluster mode
(Machine 122.local).

What would you like to do?
```

```
1. Switch modes to edit at mode "Cluster Test_cluster".
2. Start a new, empty configuration at the current mode (Machine 122.local).
3. Copy settings from another cluster mode to the current mode (Machine 122.local).
[1]>

File Reputation: Enabled
File Analysis: Enabled
File types selected for File Analysis:
Adobe Portable Document Format (PDF)
Microsoft Office 2007+ (Open XML)
Microsoft Office 97-2004 (OLE)
Microsoft Windows / DOS Executable
Other potentially malicious file types
Appliance Group ID/Name: Not part of any group yet


Choose the operation you want to perform:
- SETUP - Configure Advanced-Malware protection service.
- ADVANCED - Set values for AMP parameters (Advanced configuration).
- SETGROUP - Add this appliance to the group of appliances that can share File Analysis
reporting details.
- CLEARCACHE - Clears the local File Reputation cache.
- CLUSTERSET - Set how advanced malware protection is configured in a cluster.
- CLUSTERSHOW - Display how advanced malware protection is configured in a cluster.
[]> advanced

Enter cloud query timeout?
[15]>

Choose a file reputation server:
1. AMERICAS (cloud-sa.amp.sourcefire.com)
2. Private reputation cloud
[2]>

Enter AMP reputation server hostname or IP address?
[]> cloud-sa.eu.amp.sourcefire.com

Do you want to input new public key? [N]> y

Paste the public key followed by a . on a new line
-----BEGIN PUBLIC KEY-----
MFkwEwYHKoZIzj0CAQYIKoZIzj0DAQcDQgAEchIap1VqPuGibM2n3wjfhqQZdzC9
WI1Z7QZ2Q7VesLe+A53TxYujeo7fCDKJEQKrPjU6kI36PSZusObr9Cur/g==
-----END PUBLIC KEY-----
.
Enter cloud domain?
[a.immunet.com]>

Do you want use the recommended reputation threshold from cloud service? [Y]>

Enter heartbeat interval?
[15]>

Do you want to enable SSL communication (port 443) for file reputation? [Y]>

Please make sure you have added the Amp onprem reputation server CA certificate in certconfig-
>CERTAUTHOROTIES->CUSTOM
Proxy server detail:
Server :
Port :
User :

Do you want to change proxy detail [N]>
```

```
Choose a file analysis server:
1. AMERICAS (https://panacea.threatgrid.com)
2. Private analysis cloud
[1]>
```

确认所有配置更改。

AsyncOS 9.7.x和前

在AsyncOS 9.7.2-065的此示例电子邮件安全的将帮助您代替名誉网云服务器池对cloud-sa.eu.amp.sourcefirce.com ：

```
my97esa.local> ampconfig

File Reputation: Enabled
File Analysis: Enabled
File types selected for File Analysis:
Adobe Portable Document Format (PDF)
Microsoft Office 2007+ (Open XML)
Microsoft Office 97-2004 (OLE)
Microsoft Windows / DOS Executable
Other potentially malicious file types
Appliance Group ID/Name: Not part of any group yet


Choose the operation you want to perform:
- SETUP - Configure Advanced-Malware protection service.
- ADVANCED - Set values for AMP parameters (Advanced configuration).
- SETGROUP - Add this appliance to the group of appliances that can share File Analysis
reporting details.
- CLEARCACHE - Clears the local File Reputation cache.
[]> advanced

Enter cloud query timeout?
[15]>

Enter cloud domain?
[a.immunet.com]>

Enter reputation cloud server pool?
[cloud-sa.amp.sourcefire.com]> cloud-sa.eu.amp.sourcefire.com

Do you want use the recommended reputation threshold from cloud service? [Y]>

Choose a file analysis server:
1. AMERICAS (https://panacea.threatgrid.com)
2. Private Cloud
[1]>

Enter heartbeat interval?
[15]>

Do you want to enable SSL communication (port 443) for file reputation? [Y]>

Proxy server detail:
Server :
Port :
User :

Do you want to change proxy detail [N]>
```

确认所有配置更改。

在前提文件名誉服务器(FireAMP专用的Cloud)

的使用在前提文件名誉服务器，亦称FireAMP专用的Cloud从电子邮件安全的AsyncOS 10.x开始，引入。

如果配置了在您的网络的Cisco AMP虚拟专用的Cloud工具，您能当前查询消息附件的文件名誉，无需发送他们到公共名誉网云。要配置您的工具使用在前提文件名誉服务器，请参阅“文件名誉过滤和文件分析”章节在ESA用户指南或在线帮助。

Verify

使用本部分可确认配置能否正常运行。

为了看到文件名誉数据流通过到被配置的静态主机或名誉网云服务器池，请执行从ESA的信息包获取以指定的过滤器捕获端口32137或端口443数据流。

对于此示例，请使用cloud-sa.eu.amp.sourcefire.com网云服务器池和SSL通信与使用端口443…

这被记录对在AMP日志的ESA ：

```
my97esa.local> ampconfig

File Reputation: Enabled
File Analysis: Enabled
File types selected for File Analysis:
Adobe Portable Document Format (PDF)
Microsoft Office 2007+ (Open XML)
Microsoft Office 97-2004 (OLE)
Microsoft Windows / DOS Executable
Other potentially malicious file types
Appliance Group ID/Name: Not part of any group yet


Choose the operation you want to perform:
- SETUP - Configure Advanced-Malware protection service.
- ADVANCED - Set values for AMP parameters (Advanced configuration).
- SETGROUP - Add this appliance to the group of appliances that can share File Analysis
reporting details.
- CLEARCACHE - Clears the local File Reputation cache.
[]> advanced

Enter cloud query timeout?
[15]>

Enter cloud domain?
[a.immunet.com]>

Enter reputation cloud server pool?
[cloud-sa.amp.sourcefire.com]> cloud-sa.eu.amp.sourcefire.com

Do you want use the recommended reputation threshold from cloud service? [Y]>

Choose a file analysis server:
1. AMERICAS (https://panacea.threatgrid.com)
```

```
2. Private Cloud
[1]>

Enter heartbeat interval?
[15]>

Do you want to enable SSL communication (port 443) for file reputation? [Y]>

Proxy server detail:
Server :
Port :
User :

Do you want to change proxy detail [N]>
```

ESA信息包踪影运行捕获此会话：

```
my97esa.local> ampconfig

File Reputation: Enabled
File Analysis: Enabled
File types selected for File Analysis:
Adobe Portable Document Format (PDF)
Microsoft Office 2007+ (Open XML)
Microsoft Office 97-2004 (OLE)
Microsoft Windows / DOS Executable
Other potentially malicious file types
Appliance Group ID/Name: Not part of any group yet


Choose the operation you want to perform:
- SETUP - Configure Advanced-Malware protection service.
- ADVANCED - Set values for AMP parameters (Advanced configuration).
- SETGROUP - Add this appliance to the group of appliances that can share File Analysis
reporting details.
- CLEARCACHE - Clears the local File Reputation cache.
[]> advanced

Enter cloud query timeout?
[15]>

Enter cloud domain?
[a.immunet.com]>

Enter reputation cloud server pool?
[cloud-sa.amp.sourcefire.com]> cloud-sa.eu.amp.sourcefire.com

Do you want use the recommended reputation threshold from cloud service? [Y]>

Choose a file analysis server:
1. AMERICAS (https://panacea.threatgrid.com)
2. Private Cloud
[1]>

Enter heartbeat interval?
[15]>

Do you want to enable SSL communication (port 443) for file reputation? [Y]>

Proxy server detail:
Server :
Port :
User :
```

```
Do you want to change proxy detail [N]>
```

您看到数据流在端口443沟通。从我们的ESA (my11esa.local)，它沟通对主机名- ec2-176-34-122-245.eu-west-1.compute.amazonaws.com。此主机名-附加对IP地址176.34.122.245 ：

```
my97esa.local> ampconfig

File Reputation: Enabled
File Analysis: Enabled
File types selected for File Analysis:
Adobe Portable Document Format (PDF)
Microsoft Office 2007+ (Open XML)
Microsoft Office 97-2004 (OLE)
Microsoft Windows / DOS Executable
Other potentially malicious file types
Appliance Group ID/Name: Not part of any group yet


Choose the operation you want to perform:
- SETUP - Configure Advanced-Malware protection service.
- ADVANCED - Set values for AMP parameters (Advanced configuration).
- SETGROUP - Add this appliance to the group of appliances that can share File Analysis
reporting details.
- CLEARCACHE - Clears the local File Reputation cache.
[]> advanced

Enter cloud query timeout?
[15]>

Enter cloud domain?
[a.immunet.com]>

Enter reputation cloud server pool?
[cloud-sa.amp.sourcefire.com]> cloud-sa.eu.amp.sourcefire.com

Do you want use the recommended reputation threshold from cloud service? [Y]>

Choose a file analysis server:
1. AMERICAS (https://panacea.threatgrid.com)
2. Private Cloud
[1]>

Enter heartbeat interval?
[15]>

Do you want to enable SSL communication (port 443) for file reputation? [Y]>

Proxy server detail:
Server :
Port :
User :

Do you want to change proxy detail [N]>
```

176.34.122.245的IP地址是CNAME的池成员cloud-sa.eu.amp.sourcefire.com的：

```
my97esa.local> ampconfig

File Reputation: Enabled
File Analysis: Enabled
File types selected for File Analysis:
```

```
Adobe Portable Document Format (PDF)
Microsoft Office 2007+ (Open XML)
Microsoft Office 97-2004 (OLE)
Microsoft Windows / DOS Executable
Other potentially malicious file types
Appliance Group ID/Name: Not part of any group yet


Choose the operation you want to perform:
- SETUP - Configure Advanced-Malware protection service.
- ADVANCED - Set values for AMP parameters (Advanced configuration).
- SETGROUP - Add this appliance to the group of appliances that can share File Analysis
reporting details.
- CLEARCACHE - Clears the local File Reputation cache.
[]> advanced

Enter cloud query timeout?
[15]>

Enter cloud domain?
[a.immunet.com]>

Enter reputation cloud server pool?
[cloud-sa.amp.sourcefire.com]> cloud-sa.eu.amp.sourcefire.com

Do you want use the recommended reputation threshold from cloud service? [Y]>

Choose a file analysis server:
1. AMERICAS (https://panacea.threatgrid.com)
2. Private Cloud
[1]>

Enter heartbeat interval?
[15]>

Do you want to enable SSL communication (port 443) for file reputation? [Y]>

Proxy server detail:
Server :
Port :
User :

Do you want to change proxy detail [N]>
```

对于此示例，通信是由被配置的名誉网云服务器池处理的并且接受， cloud-sa.eu.amp.sourcefire.com。

Troubleshoot

本部分提供了可用于对配置进行故障排除的信息。

请使用Telnet测试连接

为了验证端口级别连接到文件名誉网云，请使用主机名-被配置的名誉网云服务器池的，并且测试与telnet对端口32137或者端口443，如被配置。

```
my97esa.local> telnet cloud-sa.amp.sourcefire.com 443

Trying 23.21.208.4...
```

```
Connected to ec2-23-21-208-4.compute-1.amazonaws.com.
Escape character is '^]'.
^]
telnet> quit
Connection closed.
```
对EU的Verfiy连接，成功在端口443 ：

```
my97esa.local> telnet cloud-sa.eu.amp.sourcefire.com 443

Trying 176.34.113.72...
Connected to ec2-176-34-113-72.eu-west-1.compute.amazonaws.com.
Escape character is '^]'.
^]
telnet> quit
Connection closed.
```
对EU的Verfiy连接，不能在端口32137连接：

```
my97esa.local> telnet cloud-sa.eu.amp.sourcefire.com 32137

Trying 176.34.113.72...
telnet: connect to address 176.34.113.72: Operation timed out
telnet: Unable to connect to remote host
```
您能测试telnet到直接IP或主机名在CNAME后为名誉网云服务器池与同一个telnet测试方法，与使用端口32137或端口443。如果不能顺利地远程登录到主机名-和端口，您也许需要检查网络连通性和防火墙设置外部对ESA。

telnet成功的验证对一个前提文件名誉服务器的将由进程完成和显示一样。

公共密钥的输入

当您输入在运行AsyncOS 10.x的ESA的公共密钥和更新时，请保证您是成功的在粘贴或装载公共密钥。在公共密钥的所有错误将显示给配置输出：

```
my97esa.local> telnet cloud-sa.eu.amp.sourcefire.com 32137

Trying 176.34.113.72...
telnet: connect to address 176.34.113.72: Operation timed out
telnet: Unable to connect to remote host
```
如果收到一个错误，请再试配置。对于持续错误，请与Cisco支持联系。

检查AMP日志

当您查看AMP登录ESA时，请保证您看到“文件在文件名誉查询时从Cloud的名誉查询”指定的：

```
my97esa.local> telnet cloud-sa.eu.amp.sourcefire.com 32137

Trying 176.34.113.72...
telnet: connect to address 176.34.113.72: Operation timed out
telnet: Unable to connect to remote host
```
如果看到此，查询拉了回应自本地ESA高速缓冲存储器和不自被配置的名誉网云服务器池：

```
my97esa.local> telnet cloud-sa.eu.amp.sourcefire.com 32137

Trying 176.34.113.72...
telnet: connect to address 176.34.113.72: Operation timed out
telnet: Unable to connect to remote host
```

另外的错误和戒备

ESA管理员也许收到此公告。如果这被接受，再STEP通过配置和验证进程。

```
my97esa.local> telnet cloud-sa.eu.amp.sourcefire.com 32137

Trying 176.34.113.72...
telnet: connect to address 176.34.113.72: Operation timed out
telnet: Unable to connect to remote host
```

Related Information

- 适当的AMP操作的所需的服务器地址
- Technical Support & Documentation - Cisco Systems