目录

简介

本文描述警报归因于思科电子邮件安全工具(ESA)有对此(安培)启用的先进的恶意软件保护的服务不在安全套接字协议层(SSL)的地方端口443通信。

更正在网云的“文件名誉服务是为安培接收的不可得到的”错误

安培发布为在ESA的使用在AsyncOS版本8.5.5和以上。 使用在ESA准许和启用的安培，管理员收到此消息：

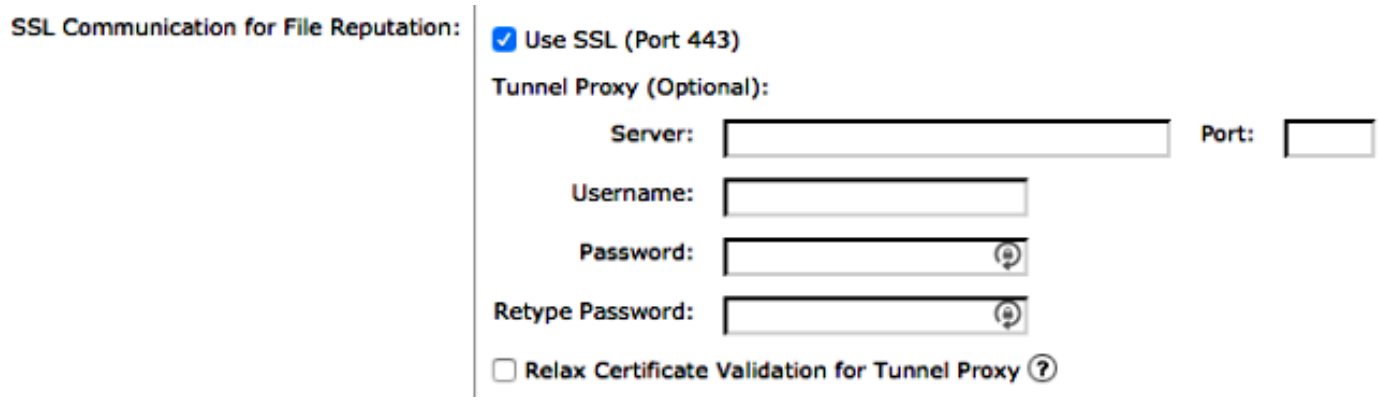
安培服务也许启用，但是不在端口443很可能通信。

为了保证安培通信443，从CLI运行**ampconfig >提前**并且请务必Y选择为**您要启用SSL通信(端口443)文件名誉的？[Y] >** ：

```
> 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


Choose the operation you want to perform:
- SETUP - Configure Advanced-Malware protection service.
- ADVANCED - Set values for AMP parameters (Advanced configuration).
- 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]>

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

Enter file analysis server URL?
```

```
[https://intel.api.sourcefire.com]>

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]>
```

如果使用GUI，请点击**安全服务>文件名誉和分析> Edit全局设置>Advanced (下拉式)**并且保证**使用SSL**复选框启用如显示此处：



确认您的配置的任意更改。

最后，请检查当前安培日志发现服务和连接成功或者失败。 您能从与**尾标amp.的**CLI完成此。

在做的变动之前对**ampconfig >**在安培日志**提前**，您将看到此：

```
> 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


Choose the operation you want to perform:
- SETUP - Configure Advanced-Malware protection service.
- ADVANCED - Set values for AMP parameters (Advanced configuration).
- 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]>

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

```
Enter file analysis server URL?
[https://intel.api.sourcefire.com]>

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]>
```

在变动做对**ampconfig >先进后**，您在安培日志看到此：

```
> 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


Choose the operation you want to perform:
- SETUP - Configure Advanced-Malware protection service.
- ADVANCED - Set values for AMP parameters (Advanced configuration).
- 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]>

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

Enter file analysis server URL?
[https://intel.api.sourcefire.com]>

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]>
```

amp_watchdog.txt文件显示在日志的每10分钟。此文件是一部分的keep-alive AMP.的。

在安培日志，一正常查询类似于此：

```
> 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


Choose the operation you want to perform:
- SETUP - Configure Advanced-Malware protection service.
- ADVANCED - Set values for AMP parameters (Advanced configuration).
- 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]>

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

Enter file analysis server URL?
[https://intel.api.sourcefire.com]>

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]>
```

有此信息，您应该能关联消息ID (MID)在邮件日志。

故障排除

查看防火墙和网络设置为了保证SSL通信为这些打开：

波尔特	协议	In/out	主机名	说明
443	TCP		如安全服务>文件名誉和分析所配置的一样，Advanced部分。	覆盖文件分析的服务的访问。
32137	TCP		如安全服务>文件名誉和分析所配置的一样，Advanced部分，Advanced部分，Cloud服务器池参数。	覆盖获取的文件名誉服务的访

您能测试从您的ESA的基本连通性到网云服务443通过Telnet为了保证您的设备能成功地到达安培服务。

注意：文件名誉和文件分析的地址在CLI配置与**ampconfig >先进**，或者从与**安全服务>文件名**

誉和分析> Edit全局设置>Advanced的GUI (下拉式)。

文件名誉示例：

```
ironport:service 36] telnet cloud-sa.amp.sourcefire.com 443
Trying 184.73.186.190...
Connected to cloud-sa.amp.sourcefire.com.
Escape character is '^]'.
^]
telnet> quit
Connection closed.
```

文件分析示例：

```
ironport:service 37] telnet intel.api.sourcefire.com 443
Trying 198.148.79.52...
Connected to intel.api.sourcefire.com.
Escape character is '^]'.
^]
telnet> quit
Connection closed.
```

相关信息

- ESA提前的恶意软件保护(安培)测验
- ESA用户指南
- ESA FAQ ：什么是消息ID (MID)，射入连接ID (ICID)，或者交付连接ID (DCID) ？
- 如何搜索，并且查看邮件注册ESA ？