目录

问题

如何提供Cisco TAC远程访问或支持通道给思科电子邮件或Web安全工具？

环境

思科电子邮件安全工具(ESA)，思科Web安全Appliance(WSA)

思科电子邮件/Web安全工具能使用一个安全SSH通道为了允许Cisco TAC获得访问到操作系统的设备的。默认情况下，设备不允许此种连接默认情况下(含义远程访问禁用)。

您能通过CLI或GUI启用此。请参阅如下说明：

从CLI

```
ESA.example.com> techsupport

Service Access currently disabled.
Serial Number: <S/N of the appliance>

Choose the operation you want to perform:
```

- SSHACCESS -允许客户服务代表远程访问您的系统，
  没有设立通道。
- 通道-允许客户服务代表远程访问您的系统，
  并且请设立通信的一个安全隧道。
- 状态-显示当前techsupport状态。
  []>通道

输入用户支持的一个临时密码能使用。此密码不能使用直接地访问您的系统。

- 密码必须在长6个和128个的字符之间。
- 它不能是空白或仅包括空间。
- 它一定是与管理员密码不同。
  []> *<supportpassword>*

```
Enter the port number for tunnel connection:
[25]> <Specify port or press Enter>
```

```
Are you sure you want to enable service access? [N]> Y

Service access has been ENABLED. Please provide your temporary password to your
Cisco Customer Support representative.

Waiting for ssh tunnel to connect, Ctrl-C to cancel...
```

从GUI

去**'帮助和支持'** *(右上角)*--> **'**在'技术支持下的'**远程访问的。**

1. 点击**'编辑远程访问设置的**按钮。
2. 在**'用户支持密码'**字段输入一个密码。
3. 检查'安全隧道(建议使用) ：'选项和回车端口编号。默认是25。
4. 点击'**提交**'按钮。
5. 提供选定的密码给Cisco TAC。

在您提供他们您的序列号和临时密码后， Cisco TAC能控制设备。所有数据安全地转接(使用加密)并且不可能由任何当事人读其他然后Cisco TAC人员。如果思科电子邮件/Web安全工具不能在SMTP (TCP端口25)连接，则其他可用端口是22， 80， 443和4766。

注意：在最新的AsyncOS版本中，我们做了在"远程访问"部分的下面的变动附加安全性目的：

- 密码当前指***"种子字符串"***。
- 有选项生成一个随机的种子字符串：这将创建将使用作为密码远程访问连接的随机的更高的位密钥。
- 密码/种子字符串的长度：密码必须在长12个和128个的字符之间。