

# 目录

[简介](#)

[先决条件](#)

[要求](#)

[使用的组件](#)

[如何执行思科内容安全工具的一数据包捕获？](#)

## 简介

本文描述如何执行思科内容安全工具的数据包捕获。

## 先决条件

### 要求

Cisco 建议您了解以下主题：

- 思科电子邮件安全工具(ESA)
- 思科Web安全工具(WSA)
- Cisco安全管理设备(SMA)
- AsyncOS

### 使用的组件

本文档中的信息是基本的在AsyncOS所有版本。

本文档中的信息都是基于特定实验室环境中的设备编写的。本文档中使用的所有设备最初均采用原始（默认）配置。如果您使用的是真实网络，请确保您已经了解所有命令的潜在影响。

## 如何执行思科内容安全工具的数据包捕获？

完成这些步骤为了执行数据包捕获(tcpdump命令)与GUI：

1. 导航帮助和GUI的支持>数据包捕获。
2. 编辑数据包捕获设置如所需求，例如的网络接口数据包捕获运作。您能使用其中一个预定义的

过滤器，或者您能创建有unix tcpdump命令支持的使用的一个自定义过滤器所有语法。

3. 点击**启动捕获**为了开始捕获。

4. 点击**终止捕获**为了结束捕获。

5. 下载数据包捕获。

完成这些步骤为了执行数据包捕获(tcpdump命令)与CLI：

1. 输入此命令到CLI：

```
wsa.run> packetcapture
```

```
Status: No capture running
```

```
Current Settings:
```

```
Max file size:      200 MB
```

```
Capture Limit:     None (Run Indefinitely)
```

```
Capture Interfaces: Management
```

```
Capture Filter:    (tcp port 80 or tcp port 3128)
```

2. 选择您要执行的操作：

```
- START - Start packet capture.
```

```
- SETUP - Change packet capture settings.
```

```
[> setup
```

3. 输入捕获文件的最大容许的大小(在MB)：

```
[200]> 200
```

```
Do you want to stop the capture when the file size is reached? (If not, a new file will be started and the older capture data will be discarded.)
```

```
[N]> n
```

```
The following interfaces are configured:
```

```
1. Management
```

```
2. T1
```

```
3. T2
```

4. 进入获取数据包，分离由逗号一个或更多接口的名称或数量：

```
[1]> 1
```

5. 输入您要使用捕获的过滤器。输入词**结算**为了清除过滤器和获取所有在所选接口的数据包。

```
[(tcp port 80 or tcp port 3128)]> host 10.10.10.10 && port 80
```

```
Status: No capture running
```

Current Settings:

Max file size: 200 MB

Capture Limit: None (Run Indefinitely)

Capture Interfaces: Management

Capture Filter: host 10.10.10.10 && port 80

## 6. 选择启动操作为了开始捕获：

- START - Start packet capture.
- SETUP - Change packet capture settings.

[> **start**

Status: Capture in progress (Duration: 0s)

File Name: S650-00137262569A-8RVFDB1-20080919-174302.cap (Size: 0K)

Current Settings:

Max file size: 200 MB

Capture Limit: None (Run Indefinitely)

Capture Interfaces: Management

Capture Filter: host 10.10.10.10 && port 80

## 7. 选择终止操作为了结束捕获：

- STOP - Stop packet capture.
- STATUS - Display current capture status.
- SETUP - Change packet capture settings.

[> **stop**

Status: No capture running (Capture stopped by user)

Current Settings:

Max file size: 200 MB

Capture Limit: None (Run Indefinitely)

Capture Interfaces: Management

Capture Filter: host 10.10.10.10 && port 80