

# 内容安全工具FAQ：如何执行在Cisco内容安全工具上的信息包获取？

## Contents

[Introduction](#)

[Prerequisites](#)

[Requirements](#)

[Components Used](#)

[如何执行在Cisco内容安全工具上的信息包获取？](#)

## Introduction

本文描述如何执行在Cisco内容安全工具上的信息包获取。

## Prerequisites

## Requirements

Cisco 建议您了解以下主题：

- Cisco电子邮件安全工具(ESA)
- Cisco Web安全工具(WSA)
- Cisco安全管理工具(SMA)
- AsyncOS

## Components Used

本文的信息是基本的在AsyncOS的所有版本。

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. If your network is live, make sure that you understand the potential impact of any command.

## 如何执行在Cisco内容安全工具上的信息包获取？

完成这些步骤为了执行信息包获取(tcpdump命令)与GUI :

1. 连接帮助和技术支持>在GUI的信息包获取。
2. 编辑信息包获取设置如所需求，例如信息包获取运行的网络接口。您能使用其中一台预定义的过滤器，或者您能用unix tcpdump命令支持的使用所有语法创建一台自定义过滤器。
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. 下载信息包获取。

完成这些步骤为了执行信息包获取(tcpdump命令)与CLI :

1. 输入此命令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. 输入获取信息包，分离由逗号一个或更多接口的名字或数量：

```
[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信息包。

```
[(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