

# Ferramentas de segurança satisfeitas FAQ: Como você executa uma captura de pacote de informação em uma ferramenta de segurança do índice de Cisco?

## Índice

[Introdução](#)

[Pré-requisitos](#)

[Requisitos](#)

[Componentes Utilizados](#)

[Como você executa uma captura de pacote de informação em uma ferramenta de segurança do índice de Cisco?](#)

## Introdução

Este documento descreve como executar capturas de pacote de informação nas ferramentas de segurança do índice de Cisco.

## Pré-requisitos

### Requisitos

A Cisco recomenda que você tenha conhecimento destes tópicos:

- Cisco envia por correio eletrônico a ferramenta de segurança (o ESA)
- Ferramenta de segurança da Web de Cisco (WSA)
- Dispositivo do Gerenciamento do Cisco Security (S A)
- AsyncOS

### [Componentes Utilizados](#)

A informação neste documento é baixa em todas as versões de AsyncOS.

As informações neste documento foram criadas a partir de dispositivos em um ambiente de laboratório específico. Todos os dispositivos utilizados neste documento foram iniciados com uma

configuração (padrão) inicial. Se a sua rede estiver ativa, certifique-se de que entende o impacto potencial de qualquer comando.

## Como você executa uma captura de pacote de informação em uma ferramenta de segurança do índice de Cisco?

Termine estas etapas a fim executar uma captura de pacote de informação (comando `tcpdump`) com o GUI:

1. Navegue para **ajudar e apoio > captura de pacote de informação** no GUI.
2. Edite os ajustes da captura de pacote de informação como necessário, como a interface de rede em que a captura de pacote de informação é executado. Você pode usar um dos filtros predefinidos, ou você pode criar um filtro feito sob encomenda com o uso de toda a sintaxe que for apoiada pelo comando `tcpdump` de Unix.
3. **Captação do começo** do clique a fim começar a captação.
4. **Captação da parada** do clique a fim terminar a captação.
5. Transfira a captura de pacote de informação.

Termine estas etapas a fim executar uma captura de pacote de informação (comando `tcpdump`) com o CLI:

1. Incorpore este comando no 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. Escolha a operação que você quer executar:

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

```
[ ]> setup
```

3. Incorpore o máximo - tamanho permissível para o arquivo de captura (no 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. Incorpore o nome ou o número de umas ou várias relações de que para capturar os pacotes, separados por vírgulas:

```
[1]> 1
```

5. Entre no filtro que você quer usar para a captação. Incorpore a palavra **ESPAÇO LIVRE** a fim cancelar o filtro e capturar todos os pacotes nas interfaces selecionada.

```
[(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. Escolha a operação do **começo** a fim começar a captação:

- 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. Escolha a operação da **parada** a fim terminar a captação:

- 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