

Usando o comando tcpdump no software de ACNS

Índice

[Introdução](#)

[Pré-requisitos](#)

[Requisitos](#)

[Componentes Utilizados](#)

[Convenções](#)

[Capturando pacotes](#)

[Opções](#)

[FTP](#)

[Etéreo](#)

[Informações Relacionadas](#)

[Introdução](#)

O Cisco Application and Content Networking Software (ACNS) 4.2.1 introduziu o **comando tcpdump**. Este comando permite-o de recolher um farejador de rastreamento no Content Engine, no roteador de conteúdo, ou no gerenciador de distribuição do índice com a finalidade do Troubleshooting, quando perguntado recolher os dados pelo [Suporte técnico de Cisco](#). Esta utilidade é muito similar ao **comando tcpdump** de Linux/Unix.

[Pré-requisitos](#)

[Requisitos](#)

Os leitores deste documento devem estar cientes destes tópicos:

- FTP
- ACNS
- Comando line interface(cli) do ACNS

[Componentes Utilizados](#)

As informações neste documento são baseadas nas versões de software e hardware:

- Software ACNS 4.2.1 e mais tarde
- Todas as Plataformas que executam ACNS 4.2.X e acima

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.

Convenções

Para obter mais informações sobre convenções de documento, consulte as [Convenções de dicas técnicas Cisco](#).

Capturando pacotes

O CLI no ACNS permite agora que o administrador (deve ser o usuário admin) capture pacotes dos Ethernet. No Content Engine 500 Series, os nomes da relação são eth0 e eth1. Em todas as plataformas ACNS, recomenda-se que você especifique um trajeto/nome de arquivo no diretório do local1.

Você pode fazer uma descarga reta do cabeçalho de pacote de informação à tela se você emite o comando `tcpdump` no CLI. Pressione o **Ctrl-c** a fim parar a descarga.

Opções

O comando `tcpdump` tem estas opções:

- - *nome de arquivo w* — Escreve a saída crua da captura de pacote de informação a um arquivo.
- - *contagem s* — Captura os primeiros bytes do <count> de cada pacote.
- - *relação i* — Permite que você especifique uma relação específica para usar-se para capturar os pacotes.
- - *limites de contagem c* a captação *para contar* pacotes.

Este é um exemplo de comando:

```
tcpdump -w /local1/dump.pcap -eth0 i -s 1500 -c 10000
```

Este comando captura os primeiros 1500 bytes dos 10,000 pacotes seguintes do interface ethernet 0, e põe a saída em um arquivo nomeado **dump.pcap** no diretório do local1 sobre o Content Engine.

Note: Assegure-se de que você especifique a opção `-s` para ajustar o comprimento snap de pacote. O valor padrão captura somente 64 bytes, e este salvar somente cabeçalhos de pacote de informação no arquivo de captura. Para pesquisar defeitos dos pacotes reorientados ou do tráfego de mais alto nível (HTTP, autenticação, e assim por diante), uma cópia de pacotes completos é precisada.

Você pode igualmente executar o `tcpdump` e o filtro em um endereço IP particular:

- Adicionar o **host 10.255.1.34** à extremidade da linha do `tcpdump`. **Note:** Substitua **10.255.1.34** com o endereço IP de Um ou Mais Servidores Cisco ICM NT que o cliente está usando.
- Também, use 1600 como o tamanho a fim travar os pacotes ruins que podem ser maiores de 1500 bytes.

Aqui está um exemplo:

```
tcpdump -w /local/mydump -s 1600 -c10000 host 10.255.2.34
```

FTP

Depois que a descarga TCP foi recolhida, você precisa de mover o arquivo do Content Engine para um PC de modo que possa ser visto por um decodificador de farejador.

```
ftp <ip address of the CE>  
!--- Log in with the admin username and password. cd local1 bin hash get <name of the file> !--  
- Using the previous example, it is dump.pcap.
```

bye

Etéreo

Etéreo é o aplicativo de software recomendado para ler a descarga TCP, devido à extensão de suas características e de seu uso com Rede de conteúdo, incluindo a capacidade para decodificar os pacotes que são encapsulados em um túnel GRE, usados pelo redirecionamento de WCCP. Refira o Web site de [Wireshark](#) para mais informação.

Note: Na maioria dos casos, os pacotes reorientados capturados pela **facilidade de dump de tcp** disponível com o ACNS CLI diferem dos dados recebidos na relação. Devido à aplicação e à manipulação internas de pacotes reorientados, do endereço IP de destino e do número de porta de TCP são alterados para refletir o endereço IP de Um ou Mais Servidores Cisco ICM NT do dispositivo e o número de porta 8999.

Informações Relacionadas

- [Suporte de software do Cisco Application and Content Networking Software \(ACNS\)](#)
- [Suporte Técnico e Documentação - Cisco Systems](#)