Procedimentos da captura de pacote de informação ESA

Índice

Introdução

Este documento descreve como executar capturas de pacote de informação na ferramenta de segurança do email de Cisco (ESA).

Pré-requisitos

Requisitos

Cisco recomenda que você tem o conhecimento de Cisco ESA.

Componentes Utilizados

A informação neste documento é baseada em Cisco ESA que executa toda a versão de AsyncOS.

Informações de Apoio

Quando você contacta o suporte de cliente de IronPort com uma edição, você pôde ser pedido para fornecer a introspecção na atividade de rede de partida e de entrada do ESA. O dispositivo

fornecem a capacidade para interceptar e indicar o TCP, o IP, e outros pacotes que são transmitidos ou recebidos sobre a rede a que o dispositivo é anexado. Você pôde querer executar uma captura de pacote de informação a fim debugar a instalação de rede e a fim verificar o tráfego de rede que alcança ou sae do dispositivo.

> **Note**: Este documento provê o software que não é mantido nem é apoiado por IronPort. A informação é fornecida como uma cortesia para sua conveniência. Para a assistência adicional, contacte por favor o fornecedor de software.

Éimportante notar que o comando CLI previamente usado do **tcpdump** está substituído com o comando novo do **packetcapture em** versões 7.0 e mais recente de AsyncOS. Este comando oferece a funcionalidade similar ao **comando tcpdump**, e está igualmente disponível para o uso no GUI.

Se você executa a versão 6.x ou anterior de AsyncOS, refira as instruções em como usar o **comando tcpdump nas capturas de pacote de informação na** seção das **versões 6.x e anterior de AsyncOS d**este documento. Também, as opções de filtro que são descritas nos **filtros da captura de pacote de informação** secionam são válidas para o comando novo do **packetcapture** também.

Capturas de pacote de informação em versões 7.x e mais recente de AsyncOS

Esta seção descreve o processo da captura de pacote de informação em versões 7.x e mais recente de AsyncOS.

Comece ou pare uma captura de pacote de informação

A fim começar uma captura de pacote de informação com o GUI, navegue ao apoio e ao menu de ajuda, **captura de pacote de informação** seleta, e clique então a **captação do começo**. A fim parar o processo da captura de pacote de informação, clique a **captação da parada**.

> **Note**: Uma captação que comece no GUI é preservada entre sessões.

A fim começar uma captura de pacote de informação com o CLI, inscreva o **packetcapture > o comando start**. A fim parar o processo da captura de pacote de informação, inscreva o **packetcapture > o comando stop**, e o ESA para a captura de pacote de informação quando a sessão termina.

Funcionalidade da captura de pacote de informação

Está aqui uma lista de informação útil que você possa usar a fim manipular as capturas de pacote de informação:

- O ESA salvar a atividade capturada do pacote a um arquivo e armazena o arquivo localmente. Você pode configurar o tamanho de arquivo de captura do pacote máximo, o

intervalo de tempo para que a captura de pacote de informação é executado, e em que interface de rede a captação executa. Você pode igualmente usar um filtro a fim limitar a captura de pacote de informação para traficar com uma porta ou um tráfego específico de um cliente ou de um endereço IP do servidor específico.

- Navegue **para apoiar e ajuda > captura de pacote de informação do** GUI a fim ver uma lista completa dos arquivos da captura de pacote de informação que são armazenados no disco rígido. Quando uma captura de pacote de informação é executado, a página da captura de pacote de informação indica o estado da captação em andamento com as estatísticas atual, tais como o tamanho do arquivo e o tempo decorreu.

- Clique o **botão File Button da transferência** a fim transferir um arquivo da captura de pacote de informação. Você pode encaminhar-lo em um email ao suporte de cliente de IronPort a fim debugar e pesquisar defeitos todas as edições.

- A fim suprimir de um arquivo da captura de pacote de informação, para selecionar uns ou vários arquivos e para clicar a **supressão selecionou arquivos**.

- A fim editar os ajustes da captura de pacote de informação com o GUI, a **captura de pacote de informação** seleta do apoio e o menu de ajuda e o clique **editam ajustes**.

- A fim editar os ajustes da captura de pacote de informação com o CLI, inscreva o **packetcapture > o comando setup**.

Note: O GUI indica somente as capturas de pacote de informação que começam no GUI, não aqueles que começam com o CLI. Similarmente, o CLI indica somente o estado de uma captação do pacote atual que comece no CLI. Somente uma captação pode ser executado em um momento.

Tip: Para obter informações adicionais sobre das opções da captura de pacote de informação e dos ajustes do filtro, refira a seção dos **filtros da captura de pacote de informação d**este documento. A fim alcançar a ajuda online de AsyncOS o do GUI, navegar **para ajudar e apoiar a ajuda do >Online > o deslocamento predeterminado > o P > a captura de pacote de informação**.

Capturas de pacote de informação em versões 6.x e anterior de AsyncOS

Esta seção descreve o processo da captura de pacote de informação em versões 6.x e anterior de AsyncOS.

Comece ou pare uma captura de pacote de informação

Você pode usar o **comando tcpdump** a fim capturar o TCP/IP e os outros pacotes que são transmitidos ou recebidos sobre uma rede a que o ESA é anexado.

Termine estas etapas a fim começar ou parar uma captura de pacote de informação:

1. Entre no **diagnóstico > rede > comando tcpdump no** CLI do ESA. Estão aqui umas saídas de exemplo:

```
example.com> diagnostic

Choose the operation you want to perform:
- RAID - Disk Verify Utility.
- DISK_USAGE - Check Disk Usage.
- NETWORK - Network Utilities.
- REPORTING - Reporting Utilities.
- TRACKING - Tracking Utilities.
[]> network

Choose the operation you want to perform:
- FLUSH - Flush all network related caches.
- ARPSHOW - Show system ARP cache.
- SMTPPING - Test a remote SMTP server.
- TCPDUMP - Dump ethernet packets.
[]> tcpdump

- START - Start packet capture
- STOP - Stop packet capture
- STATUS - Status capture
- FILTER - Set packet capture filter
- INTERFACE - Set packet capture interface
- CLEAR - Remove previous packet captures
[]>
```

2. Ajuste a relação (dados 1, dados 2, ou Gerenciamento) e o filtro.

   Note: O filtro usa o mesmo formato que o **comando tcpdump de** Unix.
3. Selecione o **COMEÇO** a fim começar a captação e **PARÁ-LA** a fim terminá-la.

   Note: Não retire o menu do tcpdump quando a captação for em andamento. Você deve usar um segundo indicador CLI a fim executar todos os outros comandos. Uma vez o processo da captação está completo, você deve usar o Secure Copy (SCP) ou o File Transfer Protocol (FTP) de seu desktop local a fim transferir os arquivos do diretório nomeado Diagnóstico (refira a seção dos **filtros da captura de pacote de informação** para detalhes). Os arquivos usam o formato da captura de pacote de informação (PCAP) e podem ser revistos com um programa tal como etéreo ou Wireshark.

Filtros da captura de pacote de informação

O diagnóstico > comando CLI da **REDE** usa a sintaxe padrão do filtro do tcpdump. Esta seção fornece a informação com respeito à captação do tcpdump filtra e fornece alguns exemplos.

Estes são os filtros padrão que são usados:

- **IP -** Filtros para todo o tráfego do protocolo IP
- **tcp -** Filtros para todo o tráfego do protocolo de TCP
- **filtros do host IP** para uma fonte ou um destino específico do endereço IP de Um ou Mais Servidores Cisco ICM NT

Estão aqui alguns exemplos dos filtros no uso:

- **host 10.1.1.1 IP** - Este filtro captura todo o tráfego que incluir 10.1.1.1 como uma fonte ou um destino.
- **host 10.1.1.1 IP ou host 10.1.1.2 IP** - este filtro captura o tráfego que contém 10.1.1.1 ou 10.1.1.2 como uma fonte ou o destino.

Para a recuperação do arquivo capturado, navegue a **var > log > diagnóstico** ou **dados > bar > diagnóstico** a fim alcançar o diretório diagnóstico.

> **Note**: Quando este comando é usado, pode fazer com que seu espaço de disco ESA encha-se acima, e pode igualmente causar a degradação do desempenho. Cisco recomenda que você usa somente este comando com a ajuda de um engenheiro de suporte ao cliente de Cisco IronPort.