O FirePOWER Management Center exibe alguns eventos de conexão TCP na direção errada

Contents

Introduction

Este documento descreve os motivos e as etapas de mitigação para o FirePOWER Management Center(FMC) exibindo eventos de conexão TCP na direção inversa, onde o IP do iniciador é o IP do servidor da conexão TCP e o IP do respondedor é o IP do cliente da conexão TCP.

> **Note**: Há várias razões para a ocorrência de tais eventos. Este documento explica a causa mais comum desse sintoma.

Prerequisites

Requirements

A Cisco recomenda que você tenha conhecimento destes tópicos:

- Tecnologia FirePOWER
- Conhecimento básico do Adaptive Security Appliance (ASA)
- Entendendo o mecanismo de temporização do Transmission Control Protocol (TCP)

Componentes Utilizados

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

- ASA Firepower Threat Defense (5506X/5506H-X/5506W-X, ASA 5508-X, ASA 5516-X) que executa a versão de software 6.0.1 e posterior
- ASA Firepower Threat Defense (5512-X,5515-X, ASA 5525-X, ASA 5545-X, ASA 555-X,FP9300,FP4100) que executa o Software Versão 6.0.1 e posterior

- ASA com módulos Firepower (5506X/5506H-X/5506W-X, ASA 5508-X, ASA 5516-X, 5515-X, ASA 5525-X, ASA 5545-X, ASA 555 5-X, ASA 5585-X) que executa as versões de software 6.0.0 e posteriores
- Firepower Management Center (FMC) versão 6.0.0 e posterior

The information in this document was created from the devices in a specific lab environment. Todos os dispositivos usados neste documento foram iniciados com uma configuração clara (padrão). If your network is live, make sure that you understand the potential impact of any command.

Background

Em uma conexão TCP, o **cliente** se refere ao IP que envia o pacote inicial. O FirePOWER Management Center gera um evento de conexão quando o dispositivo gerenciado (sensor ou FTD) vê o pacote TCP inicial de uma conexão.

Os dispositivos que rastreiam o estado de uma conexão TCP têm um **timeout de ociosidade** definido para garantir que as conexões que não estão fechadas erroneamente por endpoints não consumam a memória disponível por longos períodos de tempo. O tempo limite de ociosidade padrão para conexões TCP estabelecidas no FirePOWER é de **três minutos**. Uma conexão TCP que permanece ociosa por três minutos ou mais, não é rastreada pelo sensor FirePOWER IPS.

O pacote subsequente após o tempo limite é tratado como um novo fluxo TCP e a decisão de encaminhamento é tomada de acordo com a regra que corresponde a esse pacote.Quando o pacote é do servidor, o IP do servidor é registrado como o iniciador desse novo fluxo. Quando o registro é ativado para a regra, um evento de conexão é gerado no FirePOWER Management Center.

> **Note**: Conforme as políticas configuradas, a decisão de encaminhamento do pacote que vem após o tempo limite é diferente da decisão do pacote TCP inicial. Se a ação padrão configurada for "Bloquear", o pacote será descartado.

Um exemplo desse sintoma é conforme a captura de tela abaixo:

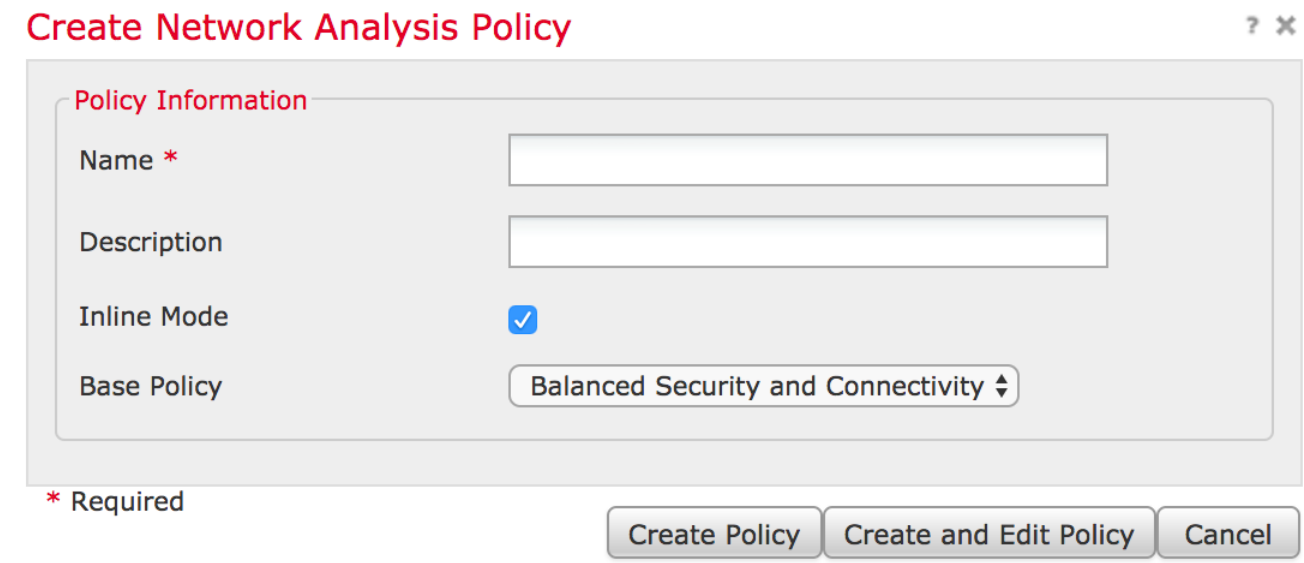
First Packet	Last Packet	Action	Reason	Initiator IP	Initiator Country	Responder IP	Responder Country	Ingress Security Zone	Egress Security Zone	Source Port / ICMP Type	Destination Port / ICMP Code
2017-05-12 17:48:05		Block		10.32.38.30		192.168.38.30				443 (https) / tcp	44705 / tcp
2017-05-12 17:39:13		Allow		192.168.38.30		10.32.38.30				44705 / tcp	443 (https) / tcp

Solução

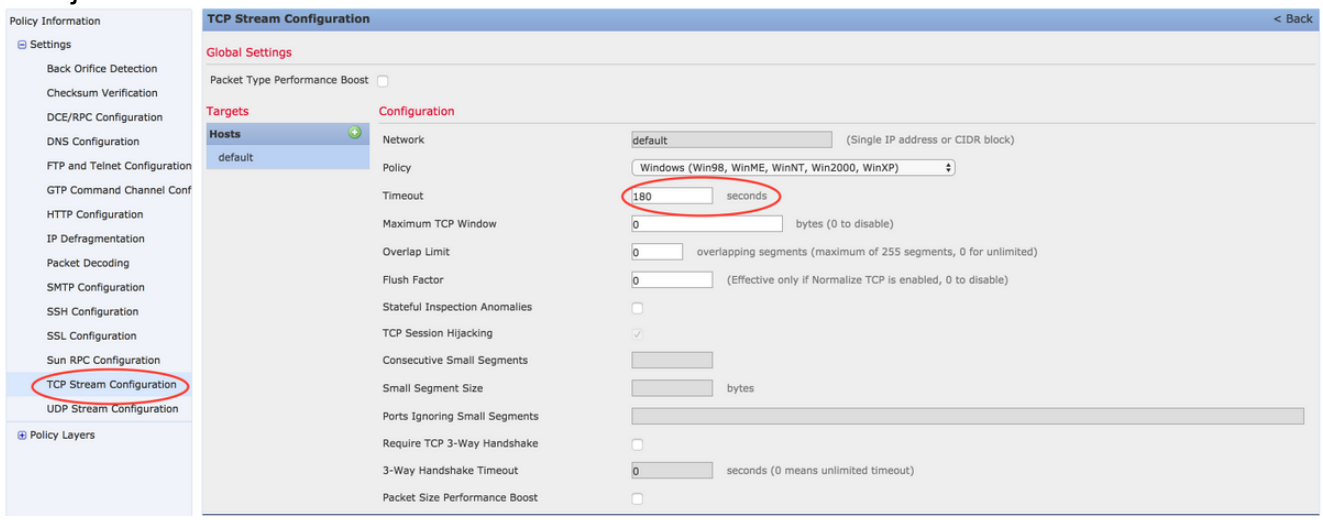
O problema mencionado acima é atenuado pelo aumento do **tempo limite** das conexões TCP. Para alterar o tempo limite,

1. Navegue até **Políticas > Controle de acesso > Invasão**.
2. Navegue até o canto superior direito e selecione **Network Access Policy**.

3. Selecione **Criar política** , escolha um nome e clique em **Criar e editar política**. Não modifique a **política básica.**

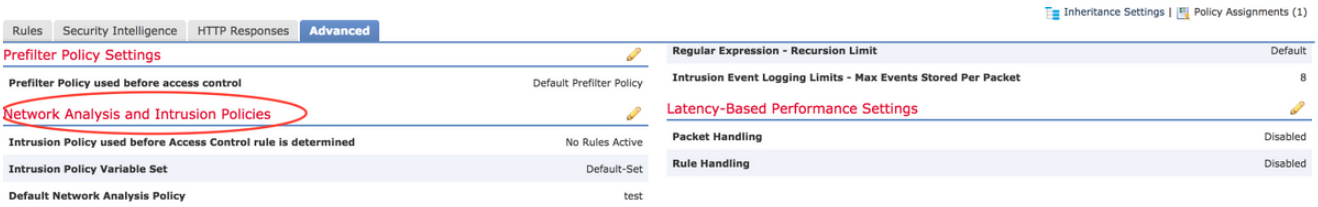


4. Expanda a opção **Settings** e escolha **TCP Stream Configuration**.
5. Navegue até a seção de configuração e altere o valor de **Timeout** conforme desejado.



6. Navegue até **Políticas > Controle de acesso > Controle de acesso**.
7. Selecione a opção **Editar** para editar a política aplicada ao dispositivo gerenciado relevante ou criar uma nova política.

8. Selecione a guia **Avançado** na política de acesso.
9. Localize a seção **Análise de rede e Políticas de intrusão** e clique no ícone **Editar**.



10. No menu suspenso da **Política de análise de rede padrão**, escolha a política criada na etapa 2.
11. Clique em **OK** e **Salvar** as alterações.
12. Clique na opção **Implantar** para implantar as políticas em dispositivos gerenciados relevantes.

Caution: Espera-se que o aumento do tempo limite cause maior utilização de memória, o FirePOWER precisa rastrear fluxos que não são fechados por endpoints por um período mais longo. O aumento real na utilização da memória é diferente para cada rede exclusiva, pois depende de quanto tempo os aplicativos de rede mantêm as conexões TCP ociosas.

Conclusão

O benchmark de cada rede para o timeout de ociosidade de conexões TCP é diferente. Depende completamente dos aplicativos que estão em uso. Um valor ótimo deve ser estabelecido observando quanto tempo os aplicativos de rede mantêm as conexões TCP ociosas. Para problemas relacionados ao módulo de serviço do FirePOWER em um Cisco ASA, quando um valor ótimo não pode ser deduzido, o tempo limite pode ser ajustado aumentando-o em etapas até o valor de tempo limite do ASA.

Informações Relacionadas

- Guia de início rápido do Cisco Firepower Threat Defense para o ASA
- Suporte Técnico e Documentação - Cisco Systems
- Guia de início rápido do ASA Firepower