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

# Contents

Introduction Prerequisites Requirements Componentes Utilizados Background Solução Conclusão Informações Relacionadas

#### 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	<u>Reason</u>	Initiator IP	<u>Initiator</u> <u>Country</u>	Responder IP	Responder Country	Ingress Security Zone	Egress Security Zone	Source Port / ICMP Type	Destination Port / ICMP Code
1	2017-05-12 17:48:05		Block		10.32.38.30		192.168.38.30				443 (https) / tcp	44705 / tcp
4	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.

Access Control + In	ntrusion Network [	iscovery	Application Detectors	Correlation	Actions •			
Access Control							Import/Export Intrusion Rules Access Contro Ne	work Analysis Policy
Malware & File							Compare Policies	Create Policy
DNS		Drop	when Inline	Sta	us		Last Modified	
Identity usio	on	Yes		<u>Use</u> Polis	i by 1 access con y not applied on	trol policy any devices	2017-05-12 09:17:51 Modified by "admin"	🕒 🕞 🥒 🕤
331								

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

? X

#### básica.

#### Create Network Analysis Policy

Policy Information	
Name *	
Description	
Inline Mode	
Base Policy	Balanced Security and Connectivity \$
* Required	Create Policy Create and Edit Policy Cancel

- 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.

Policy Information	TCP Stream Configuration	1		< Back				
<ul> <li>Settings</li> </ul>	Global Settings							
Back Orifice Detection	Packet Type Performance Boost							
Checksum Verification								
DCE/RPC Configuration	Targets							
DNS Configuration	Hosts 🙂	Network	default (Single IP address or CIDR block)					
FTP and Telnet Configuration	default	Policy	Windows (Win98, WinME, WinNT, Win2000, WinXP)					
GTP Command Channel Conf		Timeout	180 seconds					
HTTP Configuration		Maximum TCP Window	0 bytes (0 to disable)					
IP Defragmentation		Quedao Limit	ouerlanning segments (maximum of 255 segments 0 for unlimited)					
Packet Decoding		Overlap Linic	overlapping segments (maximum or 255 segments, o tor unininced)					
SMTP Configuration		Flush Factor	0 (Effective only if Normalize TCP is enabled, 0 to disable)					
SSH Configuration		Stateful Inspection Anomalies						
SSL Configuration		TCP Session Hijacking						
Sun RPC Configuration		Consecutive Small Segments						
TCP Stream Configuration		Small Segment Size	bytes					
UDP Stream Configuration		Ports Ignoring Small Segments						
Policy Layers		Require TCP 3-Way Handshake						
		3-Way Handshake Timeout	o seconds (0 means unlimited timeout)					
		Packet Size Performance Boost						

- 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.					
Access Control + Access Control	Network Discovery	Application Detectors	Correlation	Actions •	
Access Control					Object Management Intrusion Network Analysis Policy DNS Import/Export
Malware & File					New Policy

- 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**.

Rules	Security Intelligence	HTTP Responses	Advanced			
Prefilter	Policy Settings			Ø	Regular Expression - Recursion Limit	Default
Prefilter	Policy used before acce	ess control		Default Prefilter Policy	Intrusion Event Logging Limits - Max Events Stored Per Packet	8
Network Analysis and Intrusion Policies					Latency-Based Performance Settings	Ø
Intrusio	n Policy used before Ac	cess Control rule is o	letermined	No Rules Active	Packet Handling	Disabled
Intrusion Policy Variable Set Default-Set					Rule Handling	Disabled
Default	Notwork Analysis Deliny					

- 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
- <u>Suporte Técnico e Documentação Cisco Systems</u>
- Guia de início rápido do ASA Firepower