# Fase 4 de solução de problemas de caminho de dados do Firepower: Política de controle de acesso

# Contents

Introduction Troubleshooting da Fase de Política de Controle de Acesso (ACP) Verificar eventos de conexão Etapas de mitigação rápida Depurando o ACP Exemplo 1: O tráfego corresponde a uma regra de confiança Exemplo 2: O tráfego correspondente a uma regra de confiança está bloqueado Cenário 3: Tráfego bloqueado pela etiqueta do aplicativo Dados a fornecer ao TAC Próxima etapa: Solucionar problemas da camada de política SSL

# Introduction

Este artigo faz parte de uma série de artigos que explicam como solucionar problemas sistematicamente no caminho de dados em sistemas Firepower para determinar se os componentes do Firepower podem estar afetando o tráfego. Consulte o <u>artigo Visão geral</u> para obter informações sobre a arquitetura das plataformas Firepower e links para outros artigos de solução de problemas de caminho de dados.

Este artigo abrange o quarto estágio da solução de problemas de caminho de dados do Firepower, a Política de Controle de Acesso (ACP - Access Control Policy). Essas informações se aplicam a todas as plataformas e versões do Firepower suportadas atualmente.



# Troubleshooting da Fase de Política de Controle de Acesso (ACP)

Em termos gerais, determinar qual regra ACP um fluxo corresponde deve ser bastante direta. Os eventos de conexão podem ser revisados para ver qual regra/ação está sendo aplicada. Se isso não mostrar claramente o que o ACP está fazendo com o tráfego, a depuração pode ser executada na CLI (Command Line Interface, interface de linha de comando) do Firepower.

# Verificar eventos de conexão

Depois de obter uma ideia da interface de entrada e saída, o tráfego deve corresponder, bem

como as informações de fluxo, o primeiro passo para identificar se o Firepower está bloqueando o fluxo seria verificar os Eventos de Conexão para o tráfego em questão. Eles podem ser vistos no Firepower Management Center em **Analysis > Connections > Events.** 

**Note**: Antes de verificar Eventos de conexão, verifique se o registro está habilitado em suas regras ACP. O registro é configurado na guia "Registro" em cada regra da política de controle de acesso, bem como na guia Inteligência de segurança. Verifique se as regras suspeitas estão configuradas para enviar os registros para o "Visualizador de Eventos". Isso também se aplica à ação padrão.

0	verviev	v Analysis Polic	ies Devices Obj	ects A	MP Inte	lligence								Deploy	🤗 System Help <del>v</del>	Global \ admin +			
Co	intext E	xplorer Connectio	ons + Events Intr	usions 🔻	Files v	Hosts • User	s 🕶 Vuln	erabilities • Corr	elation •	Custorn • Loo	kup • Search								
Bookmark This Page Report Desideard View Bookmarks Search																			
0	Connection Events (week working)																		
	Connections with Application Details > Table View of Connection Foreits																		
N	Search	Constraints (Edit Search)														Expanding			
	Jump to																		
		<ul> <li>First Packet</li> </ul>	Last Packet	Action	Reason	Initiator IP	Initiator	Responder IP	Responder	Ingress Security Zone	Egress Security Zone	Source Port /	Destination Port /	Application	Client	Web Application			
- 5		2012.05.11.14.54.22	2012.05.11.14.55.02	Aller		all 102 168 1 200	<u>Contract</u>	all 22 122 102 226	Non Inc.	PROFILE KONE	PERSONAL ROUND	60084 / http	PO (http) / http		Ulab between	Web Brending			
	• U	2017-05-11 14:54:32	2017-03-11 14:55:02	ALLOW .		192.168.1.200		ME 73.173.197.235	102A			660/64 / tcp	80 (http) / tcp		web browser	web browsing			
		2017-05-11 14:54:02	2017-05-11 14:54:32	Allow		192.168.1.200		H 73.173.197.235	<b>USA</b>			600827 tcp	80 (http) / tcp	HIP	Web browser	Web browsing			
		2017-05-11 14:53:40	2017-05-11 14:53:55	Allow		M 192.168.1.200		10.83.181.139				60077 / tcp	135 (loc-srv) / tcp	DCE/RPC	L Epmap		£		
		2017-05-11 14:52:40	2017-05-11 14:52:55	Allow		192.168.1.200		10.83.181.139				60069 / tcp	Connection Events	8	(unnamed search)		C Private	Save Save As New	Search
		2017-05-11 14:51:40	2017-05-11 14:51:53	Allow		B 192.168.1.200		H 10.83.181.139				60064 / tcp	Sections		Networking				
4		2017-05-11 14:51:24	2017-05-11 14:51:24	Allow		192.168.1.200		172.217.26.206	USA			60058 / tcp	General Information		Initiator IPs	192.168.1.200	-	192.168.1.0/24, 1192.168.1.3, 2	001108-8
1		2017-05-11 14:50:40	2017-05-11 14:50:55	Allow		192.168.1.200		10.83.181.139				60056 / tcp	Networking		Responder IP*			192.168.1.0/24, (192.168.1.3, 2	001:db8:8
4		2017-05-11 14:50:24	2017-05-11 14:50:24	Allow		192.168.1.200		172.217.26.206	🔜 USA			60050 / tcp	Geolocation		Original Client IP* Initiator / Responder IP			192.168.1.0/24, 1192.168.1.3, 21 192.168.1.0/24, 1192.168.1.3, 21	001:658:8.
		2017-05-11 14:50:23	2017-05-11 14:50:53	Allow		192.168.1.200		<b>#</b> 73.173.197.235	USA USA			60051 / tcp	854		Initiator / Original Client IP			192.168.1.0/24, 1192.168.1.3, 2	001:088:8
4		2017-05-11 14:49:47	2017-05-11 14:49:47	Allow		192.168.1.200		172.217.26.206	JUSA			60043 / tcp	Application		Initiator / Responder / Original 0	Dient IP		192.168.1.0/24, 1192.168.1.3, 2	.001:08.8
		2017-05-11 14:49:40	2017-05-11 14:49:55	Allow		192.168.1.200		10.83.181.139				60046 / tcp	Netflow		Egress Security Zone Egress Security Zone			My Security Zone My Security Zone	
4		2017-05-11 14:48:46	2017-05-11 14:51:23	Allow		192.168.1.200		72.246.56.139	USA			60041 / tcp	QuS		Ingress / Egress Security Zone			My Security Zone	
- 7		2017-05-11 14:48:46	2017-05-11 14:49:16	Allow		192.168.1.200		73.173.197.235	USA			60040 / tcp		_	Source Port / ICMP Type Destination Bost / ICMR Code*			1-1024, 6000-6011, 180	
		2017-05-11 14:48:40	2017-05-11 14:48:55	Allow		192.168.1.200		10.83.181.139				60037 / tcp			Protocol*			lcp, udp	
		2017-05-11 14:48:32	2017-05-11 14:48:32	Allow		192.168.1.200		172,217,26,206	LUSA			60031 / tcp	Global		DNS Query			suspicious.com, evil*	
		2017-05-11 14:48:16	2017-05-11 14:48:46	Allow		192 168 1 200		73 173 107 235	IISA			60034 / hrp	SuperConnectionTest		DNS Response DNS Record Type			A. PTR	
		2012-05-11 14:42:46	2012-05-11 14:48-16	Allow		102 168 1 200						60030 / http	Predefined Searches		DNS TTL			43200	
		2017-03-11 14:47:40	2017-03-11 14:48:10	ALC: NO		192.108.1.200		13.173.197.235	1020			5000307 tup			DNS Sinkhole Name			My Sinkhole	
		2017-05-11 14:47:40	2017-05-11 14:47:55	Allow		<b>9192.168.1.200</b>		<b>B</b> <u>10.83.181.139</u>				60027 / tcp	Risky Applications with Lov	v business	VLAN ID			10	
		2017-05-11 14:47:15	2017-05-11 14:48:46	Allow		192.168.1.200		BE 72.246.56.169	USA			60022 / tcp			Geolocation				
-		2017-05-11 14:47:15	2017-05-11 14:47:45	Allow		192.168.1.200		73.173.197.235	SA USA			60021 / tcp	Standard Hail		Initiator Country			USA, United States, United*	
		2017-05-11 14:46:45	2017-05-11 14:47:15	Allow		192.168.1.200		73.173.197.235	usa usa			60017 / tcp			Responder Country			USA, United States, United*	
1.0	et locia o	Tuesday, 2017-04-25 at	12:42:21 PM from rtn-filo	my-88111.0	isco.com										Original Client Country Initiator / Bestender Country			USA, United States, United*	
-			and a second																

Ao clicar em "Editar pesquisa" e filtrado por um IP de origem (iniciador) exclusivo, você pode ver os fluxos que estavam sendo detectados pelo Firepower. A coluna Ação mostra "Permitir" para o tráfego deste host.

Se o Firepower estiver bloqueando intencionalmente o tráfego, a Ação conterá a palavra "Bloquear". Clicar em "Table View of Connection Events" fornece mais dados. Os seguintes campos nos Eventos de Conexão podem ser revisados se a ação for "Bloquear":

-Razão

- Regra de controle de acesso

# Etapas de mitigação rápida

A fim de atenuar rapidamente um problema que se acredita ser causado pelas regras ACP, podese realizar o seguinte:

- Crie uma regra com a ação de "Confiar" ou "Permitir" para o tráfego em questão e coloque-a no topo do ACP ou, acima de tudo, regras de bloqueio.
- Desative temporariamente quaisquer regras com uma ação que contenha a palavra "Bloquear"
- Se a ação padrão estiver definida como "Bloquear todo o tráfego", mude temporariamente para "Somente descoberta de rede"

**Note**: Essas atenuações rápidas exigem alterações de política que podem não ser possíveis em todos os ambientes. Recomenda-se primeiro tentar usar o rastreamento de suporte do sistema para determinar qual regra o tráfego corresponde antes de fazer alterações de política.

# Depurando o ACP

Mais solução de problemas pode ser executada em relação às operações ACP através do > utilitário CLI de suporte de firewall-engine-debug.

**Note**: Nas plataformas Firepower 9300 e 4100, o shell em questão pode ser acessado por meio dos seguintes comandos:

# conectar o módulo 1
Firepower-module1> connect ftd
>

Para várias instâncias, a CLI do dispositivo lógico pode ser acessada com os seguintes comandos.

# connect module 1 telnet
Firepower-module1> conectar ftd ftd1
Conectando ao console do contêiner ftd(ftd1)... digite "exit" para voltar à CLI de inicialização
>

O utilitário **firewall-engine-debug do sistema** tem uma entrada para cada pacote que está sendo avaliado pelo ACP. Mostra o processo de avaliação de regra que está ocorrendo, juntamente com o motivo pelo qual uma regra é correspondida ou não.

**Note**: Na versão 6.2 e superior, a ferramenta **de rastreamento de suporte do sistema** pode ser executada. Ele usa os mesmos parâmetros, mas inclui mais detalhes. Certifique-se de inserir 'y' quando solicitado com "**Enable firewall-engine-debug too?**".

#### Exemplo 1: O tráfego corresponde a uma regra de confiança

No exemplo abaixo, o estabelecimento de uma sessão SSH é avaliado usando o **suporte do** sistema firewall-engine-debug.

#	Name	Source Zones	Dest Zones	Source Networks	Dest Networks	VLAN	Users	Applic	Sourc	Dest P	URLs	ISE/S Attrib	Acti	•
-	Mandatory - JG AC	(all) (1-6)												
1	Trust ssh for host	Any	Any	灵 192.168.0.7	Any	Any	Any	Any	Any	🥟 SSH	Any	Any	⇒ Tru	ist 🛈 🗓
2	inspect	Any	Any	👳 10.0.0/8 🗜	Any	Any	Any	Any	Any	Any	Any	Any	🛹 Allo	owiji 順
3	trust server backup	Any	Any	2 192.168.62.3	2 10.123.175.22	Any	Any	Any	Any	Any	Any	Any	⇒ Tru	ist 🗍 🗓

Este é o ACP que está sendo executado no dispositivo Firepower.

O ACP tem três regras.

1. A primeira regra é confiar em qualquer tráfego de 192.168.0.7 com portas de destino usadas

pelo SSH.

- A segunda regra inspeciona todo o tráfego originado de 10.0.0.0/8 no qual os critérios de rede correspondem com base nos dados do cabeçalho XFF (conforme indicado pelo ícone ao lado do objeto de rede)
- 3. A terceira regra confia em todo o tráfego de 192.168.62.3 a 10.123.175.22

No cenário de solução de problemas, uma conexão SSH de 192.168.62.3 a 10.123.175.22 está sendo analisada.

A expectativa é que a sessão corresponda à regra 3 de AC "backup de servidor confiável". A questão é, quantos pacotes deve ser necessário para que esta sessão corresponda a esta regra. Todas as informações necessárias no primeiro pacote para determinar a regra CA ou vários pacotes são necessários e, se for esse o caso, quantas?

Na CLI do Firepower, é inserido o seguinte para ver qual processo de avaliação de regras ACP.

#### >system support firewall-engine-debug

```
Please specify an IP protocol: tcp
Please specify a client IP address: 192.168.62.3
Please specify a client port:
Please specify a server IP address: 10.123.175.22
Please specify a server port: 22
Monitoring firewall engine debug messages
```

**Tip**: É melhor preencher o máximo possível de parâmetros ao executar o **firewall-enginedebug**, para que somente as mensagens de depuração interessantes sejam impressas na tela.

Na saída de depuração abaixo, você vê os quatro primeiros pacotes da sessão sendo avaliados.

SYN

SYN,ACK

ACK

Primeiro pacote SSH (cliente para servidor)



Este é um gráfico que ilustra a lógica de depuração.

SYN 192.168.62.3 → 10.123.175.22
 SYN,ACK 10.123.175.22 → 192.168.62.3

3. ACK 192.168.62.3 → 10.123.175.22

4. SSH 192.168.62.3 → 10.123.175.22

Starts evaluation at 'inspect' rule

Service identified as SSH No match 'inspect' rule (non-http) Match 'trust server backup' rule and Trust flow

Para esse fluxo, são necessários 4 pacotes para que o dispositivo corresponda à regra.

Esta é uma explicação detalhada da saída de depuração.

- O processo de avaliação ACP inicia na regra "inspecionar" porque a regra "confiar no host" não foi correspondida, pois o endereço IP não correspondia ao requisito. Essa é uma correspondência rápida devido a todas as informações necessárias para determinar se essa regra deve corresponder está presente no primeiro pacote (IPs e portas)
- Não é possível determinar se o tráfego corresponde à regra "inspecionar" até que o aplicativo seja identificado, uma vez que as informações X-Forwarded-For (XFF) são encontradas no tráfego do aplicativo HTTP, o aplicativo ainda não é conhecido, portanto isso coloca a sessão em um estado pendente para a regra 2, dados pendentes do aplicativo.
- Quando o aplicativo é identificado no quarto pacote, a regra "inspecionar" resulta em uma não correspondência, já que o aplicativo é SSH, em vez de HTTP

• A regra de "backup de servidor confiável" é então combinada, com base nos endereços IP.

Em resumo, a conexão leva 4 pacotes para corresponder à sessão, pois precisa esperar que o firewall identifique o aplicativo, já que a regra 2 tem uma restrição de aplicativo nele.

Se a regra 2 tivesse apenas redes de origem e não fosse XFF, então teria levado 1 pacote para corresponder à sessão.

Você deve sempre colocar as regras das camadas 1 a 4 acima de todas as outras regras na política quando possível, pois essas regras normalmente exigem um pacote para tomar uma decisão. No entanto, você também pode observar que mesmo com regras das camadas 1 a 4, pode haver mais de um pacote para corresponder a uma regra de CA, e o motivo para isso é a inteligência de segurança de URL/DNS. Se você tiver uma dessas ativações, o firewall precisará determinar o aplicativo para todas as sessões que estão sendo avaliadas pela política AC, pois ele precisa determinar se são HTTP ou DNS. Em seguida, ele deve determinar se deve permitir a sessão com base nas listas negras.

Abaixo está uma saída truncada do comando **firewall-engine-debug**, que tem os campos relevantes destacados em vermelho. Observe o comando usado para obter o nome do aplicativo identificado.



#### Exemplo 2: O tráfego correspondente a uma regra de confiança está bloqueado

Em alguns cenários, o tráfego pode ser bloqueado apesar de corresponder a uma regra de Confiança no ACP. O exemplo abaixo avalia o tráfego com a mesma política de controle de acesso e hosts.

19 19 19 19 19 19 <b>[IS</b> <b>Fi</b> 19	22.168.62.3-54 12.168.62.3-54 ine sgt tag: ur 12.168.62.3-54 12.168.62.3-54 Session was his happened rewall engine 12.168.62.3-54	4650 > 10.123.1 1650 > 10.123.1 htagged, ISE sg 1650 > 10.123.1 1650 > 10.123.1 <b>deleted becaus</b> <b>before AC rule</b> will re-evaluar 1650 > 10.123.1	75.22-22 6 AS 1 75.22-22 6 AS 1 t id: 0, svc 0, par 75.22-22 6 AS 1 75.22-22 6 AS 1 se we hit a drop a was matched te from top of A 75.22-22 6 AS 1	I 10 New sessio I 0 Starting wit yload 0, client 0, I 0 pending rul I 0 Deleting se IPS rule and bl (Intrusion polic IC policy to find	n h minimum 4, 'insp misc 0, user 999999 e order 4, 'inspect', ssion lacklisted the flow. y before AC rule ma l a rule for logging o minimum 0, id 0 and	ect', and IPPro 7, icmpType 0 XFF wait for , atch dropped) decision] d IPProto first y	oto first with z icmpCode 0 AppId vith zones 1 -	cones 1 -> 2,	geo 0 -> 0, vlan ( • 0, vlan 0, inline	D,
sg 19 19 19	t tag: 0, ISE s 2.168.62.3-54 12.168.62.3-54 12.168.62.3-54 12.168.62.3-54	gt id: 0, svc -1, 1650 > 10.123.1 1650 > 10.123.1 1650 > 10.123.1 1650 > 10.123.1	payload -1, clier 75.22-22 6 AS 1 75.22-22 6 AS 1 75.22-22 6 AS 1	nt -1, misc -1, use     0 no match ru     0 no match ru     0 match rule	er 9999997, icmpTyp ule order 3, 'Trust s ule order 4, 'inspect order 5, 'trust serve	e 102, icmpCo sh for host', s ', XFF non-htt r backup', act	de 22 rc network a p tion Trust	and GEO		
Action ×	<u>Reason</u> ×	Initiator IP ×	Responder × IP	Source Port / × ICMP Type	Destination Port / × ICMP Code	Application × Protocol	<u>Client</u> ×	Intrusion × Events	Access Control × Policy	Access Control × Rule
<u>Block</u>	Intrusion Block	192.168.62.3	10.123.175.22	55654 / tcp	22 (ssh) / tcp			<b>I</b>	JG AC (all)	trust server backup

Como visto acima, a saída **firewall-engine-debug** mostra que o tráfego corresponde a uma "Confiança", enquanto os Eventos de Conexão mostram a ação de **Bloquear** devido a uma regra de Política de Intrusão (determinada porque a coluna Razão mostra **Bloco de Intrusão**).

A razão pela qual isso pode ocorrer é devido à **Política de intrusão usada antes que a regra de controle de acesso seja determinada** Configuração na guia **Avançado** no ACP. Antes que o tráfego possa ser confiável de acordo com a ação da regra, a Política de intrusão em questão identifica uma correspondência de padrão e descarta o tráfego. No entanto, a avaliação de regra ACP resulta em uma correspondência da regra de Confiança, já que os endereços IP correspondem aos critérios da regra de "backup do servidor de confiança".

Para que o tráfego não seja submetido à inspeção da política de intrusão, a regra Trust pode ser colocada acima da regra "inspect" (inspecionar), o que seria uma prática recomendada em ambos os casos. Como a identificação do aplicativo é necessária para uma correspondência e não correspondência da regra de "inspeção", a **Política de intrusão usada antes que a regra de controle de acesso seja determinada** é usada para o tráfego que é avaliado pelo mesmo. Colocar a regra de "backup do servidor de confiança" acima da regra de "inspeção" faz com que o tráfego corresponda à regra quando o primeiro pacote é visto, pois a regra é baseada no endereço IP, que pode ser determinado no primeiro pacote. Portanto, a **Política de intrusão usada antes que a** 

regra de Controle de Acesso seja determinada não precisa ser usada.

#### Cenário 3: Tráfego bloqueado pela etiqueta do aplicativo

Neste cenário, os usuários relatam que cnn.com está sendo bloqueado. No entanto, não há uma regra específica que bloqueie a CNN. Os Eventos de Conexão, juntamente com a saída **firewall-engine-debug**, mostram o motivo do bloqueio.

Primeiro, os Eventos de Conexão têm uma caixa de informações ao lado dos campos do aplicativo que mostra informações sobre o aplicativo, bem como como o Firepower categoriza esse aplicativo.

→ First Pack	et ×	Last × Packet	Action ×	Initiator IP ×	Responder ×	Source Port / × ICMP Type	Destination Port / × ICMP Code	Application × Protocol	Web × Application	Application × Risk	Business × Relevance	<u>URL</u> ×
2017-05-19 1	6:02:29		Block	192.168.62.63	151.101.65.67	<u>54308 / tcp</u>	80 (http) / tcp	HTTP HTTP	CNN.com	Medium	Medium	http://cnn.com/
	CN Turr	N.com	sting Syste	m's news website	2.			1				
	Тур	e		Wel	Application							
	Ris	K		Ver	y Low							
	Bus	iness keie	vance	Higi	1	-						
	Cat	egories		mul	timedia (TV/vide	o, news						
	Tag	S		disp	lays ads			//				
		dadas Contex	kt Explorer	W Wikipedia	G Google	Y Yahoo!	b Bing					

Com essas informações em mente, **firewall-engine-debug** é executado. Na saída de depuração, o tráfego é bloqueado com base na etiqueta de aplicativo.



Embora não haja uma regra que bloqueasse explicitamente <u>http://cnn.com</u>, os **anúncios exibidos** marcados estão sendo bloqueados na guia **Aplicativos** de uma regra ACP.

Editing	Rule	<ul> <li>block by</li> </ul>	/ tag
---------	------	------------------------------	-------

Name block	by tag			🕑 Enabled	1	Move				
Action 💢 Bl	lock with reset		• • • •	2 🖆 🔎						
Zones N	letworks VLAN Tags	🔺 Users	s Application	Ports URI	_s SGT/ISE At	tributes		Inspection	Logging	Comments
Application Fi	ilters Clear A	ll Filters 💢	Available Appl	ications (759) 🗳			Selecte	d Applications	and Filters	(1) 🧏 🕆 📀
Search by	name		🔍 Search by r	ame			Filters			
	elorrene	19	enercoyear		۳.		Tags	: displays ads		8
🔲 💽 bl	og	53	ClickTale				M rage	i displays ads		3
🕅 🔝 bu	undles software	7	Clip2Net		0					
🕅 💽 bu	usiness impact	44	Clip2Net Up	load						
📃 💽 Co	ommon Industrial Protoco	1	CloudFlare		0					
📃 💽 co	onsole gaming	25	CNBC		<u>n</u>					
🕅 💽 co	ontent provider	28	CNET							
📃 💽 de	ecrypted traffic	21								
🔽 💽 di:	splays ads	759				Add to Rule				
📃 😒 eD	Donkey	2			0					
🔳 💽 er	ncrypts communications	280			0					
🗐 💿 ev	vasive	58	CNZZ		0					
Fa	acebook	27	Cognitive M	atch						
Fa	acebook game	27	CollegeHum	ior	0					
Fa	acebook post	25	Collider		0					
E S fil	e sharing/transfer	240	Comcast							
E S FI	ash	249	Comedy Ce	ntral	0					
E 💽 FT	TP protocol	11	Commission	Junction	0.					
E Gr	nutella_protocol	•	M 4	Viewing 101-200 of 75	59 🕨 🕅					
									Save	Cancel

### Dados a fornecer ao TAC

Dados Instruções Solucionar problemas do dispositivo Firepower http://www.cisco.com/c/en/us/support/docs/security/sourcefire-defense-center/1176 que inspeciona o tráfego sistema suporta firewall-engine-debug Consulte este artigo para obter instruções e system-supporttrace output Exportação da Navegue até Sistema > Ferramentas > Importar/Exportar, selecione a Política de C política de controle botão Exportar de acesso

**Caution**: Se o ACP contiver uma política SSL, remova a política SSL do ACP antes de exportar para evitar a divulgação de informações confidenciais de PKI

# Próxima etapa: Solucionar problemas da camada de política SSL

Se uma política SSL estiver em uso e a solução de problemas da política de controle de acesso não revelar o problema, a próxima etapa será solucionar o problema da política SSL.