Configurar a política de intrusão e a configuração de assinatura no módulo Firepower (gerenciamento integrado)

Contents

Introduction **Prerequisites Requirements Componentes Utilizados** Informações de Apoio Configuração Etapa 1. Configurar política de intrusão Etapa 1.1. Criar política de intrusão Etapa 1.2. Modificar política de intrusão Etapa 1.3. Modificar política básica Etapa 1.4. Filtragem de assinatura com opção de barra Filtro Etapa 1.5. Configurar o estado da regra Etapa 1.6. Configuração do filtro de eventos Etapa 1.7. Configurar estado dinâmico Etapa 2. Configurar o NAP (Network Analysis Policy, Política de análise de rede) e conjuntos de variáveis (opcional) Passo 3: Configurar o controle de acesso para incluir a política de intrusão/ NAP/ conjuntos de variáveis Etapa 4. Implante a política de controle de acesso Etapa 5. Monitorar eventos de intrusão Verificar Troubleshoot Informações Relacionadas

Introduction

Este documento descreve a funcionalidade do sistema de prevenção de intrusão (IPS - Intrusion Prevention System)/sistema de detecção de intrusão (IDS - Intrusion Detection System) do módulo FirePOWER e vários elementos da política de intrusão que fazem uma política de detecção no módulo FirePOWER.

Prerequisites

Requirements

A Cisco recomenda que você tenha conhecimento destes tópicos:

* Conhecimento do firewall do Adaptive Security Appliance (ASA), Adaptive Security Device Manager (ASDM).

* Conhecimento do dispositivo FirePOWER.

Componentes Utilizados

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

Módulos ASA FirePOWER (ASA 5506X/5506H-X/5506W-X, ASA 5508-X, ASA 5516-X) executando a versão de software 5.4.1 e posterior.

Módulo ASA FirePOWER (ASA 5515-X, ASA 5525-X, ASA 5545-X, ASA 555-X) executando a versão de software 6.0.0 e posterior.

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. Se a rede estiver ativa, certifique-se de que você entenda o impacto potencial de qualquer comando.

Informações de Apoio

O FirePOWER IDS/IPS foi projetado para examinar o tráfego de rede e identificar quaisquer padrões mal-intencionados (ou assinaturas) que indiquem um ataque à rede/sistema. O módulo FirePOWER funciona no modo IDS se a política de serviço do ASA estiver especificamente configurada no modo de monitor (promíscuo), caso contrário, ele funcionará no modo em linha.

O FirePOWER IPS/IDS é uma abordagem de detecção baseada em assinatura. O módulo FirePOWER no modo IDS gera um alerta quando a assinatura corresponde ao tráfego malintencionado, enquanto o módulo FirePOWER no modo IPS gera um alerta e bloqueia o tráfego malintencionado.

Nota: Certifique-se de que o módulo FirePOWER tenha licença **Protect** para configurar essa funcionalidade. Para verificar a licença, navegue até **Configuration > ASA FirePOWER Configuration > License.**

Configuração

Etapa 1. Configurar política de intrusão

Etapa 1.1. Criar política de intrusão

Para configurar a Política de intrusão, faça login no Adaptive Security Device Manager (ASDM) e execute estas etapas:

Etapa 1. Navegue até Configuration > ASA FirePOWER Configuration > Policies > Intrusion Policy > Intrusion Policy.

Etapa 2. Clique em Criar política.

Etapa 3. Digite o nome da política de intrusão.

Etapa 4. Insira a **Descrição** da Política de intrusão (opcional).

Etapa 5. Especifique a opção Eliminar quando em Linha.

Etapa 6. Selecione a **política básica** na lista suspensa.

Passo 7. Clique em Create Policy para concluir a criação da Intrusion Policy.

Dica: Descartar quando a opção em linha é crucial em determinados cenários quando o sensor está configurado no modo em linha e é necessário não descartar o tráfego mesmo que ele corresponda a uma assinatura que tenha uma ação de descarte.

<u>File View Tools Wizards Window H</u> elp		Type topic to search Go	abab
😚 Home 🦓 Configuration 🔯 Monitoring 🔲 Save ASA Ch	anges 🔇 Refresh 🔇 Back 🕥 Forward 🧖 Hel	lp	CISCO
ASA FirePOWER Configuration 🗗 🌗 Configu	ration > ASA FirePOWER Configuration > Policies	s > Intrusion Policy > Intrusion Policy	
Policies Access Control Policy There Rule Editor Files SSL Actions Alarta	are no policies defined. Click Create Policy to create a poli	Compare Polic 2	Create Policy
Actions Alerts	Create Intrusion Policy	7 %	
DNS Policy Device Management Object Management Local Updates Licenses Drols Integration	Policy Information Name * 3 IPS_Policy Description 4 IPS_policy for Drop when Inline 5 Base Policy 6 Balanced Sec	or LAB	
Firewall		Create Policy Create and Edit Policy Cancel	
Remote Access VPN			
Site-to-Site VPN			
ASA FirePOWER Configuration			
Device Management			
	<admin> 15</admin>	D 2 1/4/10	6 1:17:37 AM UTC

Você pode observar que a política está configurada, no entanto, ela não é aplicada a nenhum dispositivo.

\ FirePOWER Config	uration > Policies > Intrusion Policy	> Intrusion Policy	
		Compare Policies	s Create Policy
Drop when Inline	Status	Last Modified	
Yes	<u>No access control policies use this policy</u> Policy not applied on device	2016-01-04 07:40:00 Modified by "admin"	🕒 🕞 🥒 🖯
	Drop when Inline Yes	FirePOWER Configuration > Policies > Intrusion Policy Drop when Inline Status Yes No access control policies use this policy Policy not applied on device	Vision Policies Intrusion Policy Intrusion Policy Drop when Inline Status Last Modified Yes No access control policies use this policy Policy not applied on device 2016-01-04 07:40:00 Modified by "admin"

Etapa 1.2. Modificar política de intrusão

Para modificar a política de intrusão, navegue para Configuration > ASA FirePOWER

Configuration > Policies > Intrusion Policy > Intrusion Policy e selectione Edit option.



Etapa 1.3. Modificar política básica

A página Gerenciamento de política de intrusão oferece a opção de alterar a política/derivação básica quando a opção Inline/ Salvar e descartar.

A política básica contém algumas políticas fornecidas pelo sistema, que são políticas internas.

- 1. Segurança e conectividade equilibradas: é uma política ideal em termos de segurança e conectividade. Essa política tem cerca de 7.500 regras ativadas, algumas delas geram apenas eventos, enquanto outras geram eventos e também descartam o tráfego.
- 2. Segurança sobre conectividade:Se sua preferência é segurança, você pode escolher segurança sobre política de conectividade, o que aumenta o número de regras habilitadas.
- Conectividade em relação à segurança: se sua preferência é conectividade em vez de segurança, você pode escolher conectividade em relação à política de segurança, o que reduzirá o número de regras habilitadas.
- 4. Detecção máxima Selecione esta política para obter a detecção máxima.
- 5. Nenhuma regra ativa Esta opção desativa todas as regras. É necessário ativar as regras manualmente com base na sua política de segurança.

Policy Information 🛆	Policy Information	< Back
Rules ⊕ Advanced Settings	Name IPS_Policy Description IPS_policy for LAB	
⊕ Policy Layers	Drop when Inline	
	Balanced Security and Connectivity ▼ ⊗ The base policy is up to date (Rule Update 2015-10-01-001-vrt)	1anage Base Policy
	 ➡ This policy has 7591 enabled rules ➡ 114 rules generate events X 7477 rules drop and generate events 	Manage Rules S View View
	This policy contains enabled preprocessor rules. Please read the rule docum the preprocessors have the correct settings for these rules	entation to ensure
	Commit Changes Discard Changes	

Etapa 1.4. Filtragem de assinatura com opção de barra Filtro

Navegue até a opção **Regras** no painel de navegação e a página Gerenciamento de regras será exibida. Há milhares de regras no banco de dados de regras. A barra de filtros fornece uma boa opção do mecanismo de pesquisa para pesquisar a regra de forma eficaz.

Você pode inserir qualquer palavra-chave na barra Filtro e o sistema obtém os resultados para você. Se houver um requisito para encontrar a assinatura para vulnerabilidade de bloqueio SSL (Secure Sockets Layer), você poderá pesquisar palavras-chave desgastadas na barra de filtros e ela buscará a assinatura para a vulnerabilidade heartbleed.

Dica: se várias palavras-chave forem usadas na barra de filtros, o sistema as combina usando a lógica AND para criar uma pesquisa composta.

Você também pode pesquisar as regras usando o ID de assinatura (SID), ID do gerador (GID), Categoria: dos etc.

As regras são efetivamente divididas em várias maneiras, como baseadas em Categoria/ Classificações/ Vulnerabilidades da Microsoft / Microsoft Worms/ Específico da plataforma. Essa associação de regras ajuda o cliente a obter a assinatura certa de forma fácil e a ajudar o cliente a ajustar as assinaturas com eficiência.

Policy Information	Rules		< Back
Rules	Rule Configuration	Filter: heartbleed	3 K 7
⊕ Advanced Settings	Rule Content	Filter returned 33 results	
Policy Lavers	Category	⇒ ▼	Delieu
er Policy Edyers	app-detect	Rule State Event Filtering Dynamic State Alerting Comments	Policy
	blacklist	GID SID Message	🔿 ү 🕑 🕕 🖓
	browser-chrome browser-firefox	1 30549 SERVER-OTHER OpenSSL Heartbleed masscan access exploitation attempt	×
	browser-ie	SERVER-OTHER OpenSSL SSLv3 large heartbeat response - possible ssl heartbleed attempt	• 🗙
	browser-plugins	SERVER-OTHER OpenSSL SSLv3 large heartbeat response - possible ssl heartbleed attempt	• 🗙
	browser-webkit content-replace	SERVER-OTHER OpenSSL SSLv3 large heartbeat response - possible ssl heartbleed attempt	* ×
	decoder exploit-kit	SERVER-OTHER OpenSSL SSLv3 large heartbeat response - possible ssl heartbleed attempt	* 🗙
	file-executable	SERVER-OTHER OpenSSL TLSv1 large heartbeat response - possible ssl heartbleed attempt	* 🗙
	file-flash Classifications	SERVER-OTHER OpenSSL TLSv1 large heartbeat response - possible ssl heartbleed attempt	* ×
	Microsoft Vulnerabilities	SERVER-OTHER OpenSSL TLSv1 large heartbeat response	e 🗙
	Microsoft Worms	- possible ssl heartbleed attempt	~
	Platform Specific	SERVER-OTHER OpenSSL ILSv1 large heartbeat response - possible ssl heartbleed attempt	* ×
	Preprocessors	SERVER-OTHER OpenSSL TLSv1.1 large heartbeat	
	Priority	<u> </u>	
	Rule Update		

Você também pode pesquisar com o número CVE para encontrar as regras que os cobrem. Você pode usar a sintaxe CVE: <cve-number>.



Etapa 1.5. Configurar o estado da regra

Navegar para Regras é exibida no painel de navegação e na página Gerenciamento de regras. Selecione as regras e escolha a opção Estado da regra para configurar o estado das regras. Há três estados que podem ser configurados para uma regra:

< Back

30

7 🕑 🕕

1 of 1 > >

۳

1. Gerar eventos: Essa opção gera eventos quando a regra corresponde ao tráfego.

2. Ignorar e Gerar Eventos: essa opção gera eventos e derruba o tráfego quando a regra corresponde ao tráfego.

- Policy Information Rules **Rule Configuration** Rules Filter: **Rule Content** Advanced Settings Filter returned 33 results Category • Policy Layers Policy app-detect Rule State Event Filtering Dynamic State Alerting Comments blacklist Generate Events age 🔺 \Rightarrow browser-chrome Drop and Generate Events ER-OTHER OpenSSL Heartbleed masscan access × browser-firefox itation attempt Disable ER-OTHER OpenSSL SSLv3 large heartbeat response browser-ie × possible ssl heartbleed attempt browser-other SERVER-OTHER OpenSSL SSLv3 large heartbeat response 🗙 1 30778 browser-plugins - possible ssl heartbleed attempt browser-webkit SERVER-OTHER OpenSSL SSLv3 large heartbeat response 1 30785 11 content-replace - possible ssl heartbleed attempt SERVER-OTHER OpenSSL SSLv3 large heartbeat response 🗙 decoder 1 30514 possible ssl heartbleed attempt exploit-kit SERVER-OTHER OpenSSL TLSv1 large heartbeat response 1 30779 file-executable - possible ssl heartbleed attempt file-flash SERVER-OTHER OpenSSL TLSv1 large heartbeat response 1 30780 Classifications - possible ssl heartbleed attempt **Microsoft Vulnerabilities** SERVER-OTHER OpenSSL TLSv1 large heartbeat response 1 30786 × - possible ssl heartbleed attempt Microsoft Worms SERVER-OTHER OpenSSL TLSv1 large heartbeat response 1 30515 × Platform Specific - possible ssl heartbleed attempt Preprocessors SERVER-OTHER OpenSSL TLSv1.1 large heartbeat 1 30781 Priority K < **Rule Update**
- 3. Desabilitado: Esta opção desativa a regra.

Etapa 1.6. Configuração do filtro de eventos

A importância de um evento de invasão pode ser baseada na frequência de ocorrência ou no endereço IP de origem ou de destino. Em alguns casos, talvez você não se importe com um evento até que ele tenha ocorrido várias vezes. Por exemplo, você pode não estar preocupado se alguém tentar fazer login em um servidor até que falhe um certo número de vezes. Em outros casos, talvez seja necessário apenas ver algumas ocorrências de regra atingidas para verificar se há um problema generalizado.

Há duas maneiras de você conseguir isso:

- 1. Limiar de evento.
- 2. Supressão de evento.

Limite do evento

Você pode definir limites que ditem a frequência com que um evento é exibido, com base no número de ocorrências. Você pode configurar o limite por evento e por política.

Etapas para configurar o Limite de eventos:

Etapa 1. Selecione as **Regras** para as quais deseja configurar o Limite de Eventos.

- Etapa 2. Clique em Filtragem de eventos.
- Etapa 3. Clique no Limite.
- Etapa 4. Selecione o tipo na lista suspensa. (Limite ou Limite ou Ambos).
- Etapa 5. Selecione como deseja rastrear na caixa suspensa Rastrear por. (Origem ou Destino).
- Etapa 6. Digite a **contagem** de eventos para atender ao limite.
- Passo 7. Insira os segundos a decorrer antes da contagem ser redefinida.
- Etapa 8. Clique em OK para concluir.

	GID	SIL TI	nreshold (3)				\Rightarrow	7	0	9
3	1	28t St	uppression	T 360.cn SafeG ess attempt	iuard local HTTP i	management	×			
0	1	280 Re	emove Thresholds	360.cn Safegua	rd runtime outboun	d communication	\Rightarrow			
0	1	328 Re	emove Suppressions 209.53.113	Absolute Softwa	re Computrace outb	oound connection -	\Rightarrow			
0	1	32846	APP-DETECT absolute.com	r Absolute Softwa m	re Computrace outb	oound connection -	⇒			
0	1	32847	, APP-DETECT bh.nameque	r Absolute Softwa ery.com	Set Threshold	d for 1 rule		73	¢.	
0	1	32848	APP-DETECT namequery.	r Absolute Softwa nettrace.co.za	4 Type	Limit	•			
3	1	26286	APP-DETECT search.dnss	「Absolute Softwa earch.org	6 Count	10				
0	1	26287	, APP-DETECT search.nam	r Absolute Softwa equery.com	O Seconds	60				

Depois que um filtro de eventos for adicionado a uma regra, você poderá ver um ícone de filtro ao lado da indicação de regra, que mostra que há uma filtragem de eventos habilitada para essa regra.

Supressão de evento

As notificações de eventos especificados podem ser suprimidas com base no endereço IP de origem/destino ou por regra.

Note: Quando você adiciona supressão de evento para uma regra. A inspeção de assinatura funciona normalmente, mas o sistema não gera os eventos se o tráfego corresponder à assinatura. Se você especificar uma origem/destino específico, os eventos não aparecerão somente para a origem/destino específico para esta regra. Se você optar por suprimir a regra completa, o sistema não gerará nenhum evento para essa regra.

Etapas para configurar o Limite de eventos:

- Etapa 1. Selecione as **Regras** para as quais deseja configurar o Limite de Eventos.
- Etapa 2. Clique em Filtragem de eventos.
- Etapa 3. Clique em Supressão.
- Etapa 4. Selecione Tipo de supressão na lista suspensa. (Regra ou origem ou destino).
- Etapa 5. Clique em OK para concluir.

⇒ ▼ 2 ▼ ▼ Rule State Event Filte	ring Dynamic Stat	O ▼ Ç te Alerting C	⊃ ▼ Comments		Policy		•	-
GID SID Threshold	i				⇒ <	7 🕑 🕕	∇	
🗌 1 🕄 Suppress	ion T 360 ess a	0.cn SafeGua ittempt	ard local HTTP ma	anagement	×			
1 280 Remove S	hresholds 360. Suppressions on	cn Safeguard	runtime outbound		⇒			
1 32845	APP-DETECT Abso connection - 209.	lute Software 53.113.223	Computrace outbo	und	⇒			
1 32846	APP-DETECT Abso connection - abso	lute Software lute.com	Computrace outbo	und	⇒ •	7		
Add Suppression Suppression Type 5 1 20207 1 32849	OK Cancel OK Cancel Connection - searc APP-DETECT Abso connection - searc	x uery.cor Software y.nettra Software issearch. Software ch.namequery lute Software ch.us.nameque	Add Suppression Type Network Add Suppression Type Suppression Type Network	sion for 1 4 Source 5 sion for 1 4 Destination	rule ΟΚ rule ation ▼	? X Cancel ? X		

Depois que o filtro de eventos for adicionado a esta regra, você poderá ver um ícone de filtro com a contagem dois ao lado da indicação de regra, que mostra que há dois filtros de eventos ativados para esta regra.

Etapa 1.7. Configurar estado dinâmico

Éum recurso no qual podemos alterar o estado de uma regra se a condição especificada corresponder.

Suponha um cenário de ataque de força bruta para decifrar a senha. Se uma assinatura detectar falha na tentativa de senha e a ação da regra for gerar um evento. O sistema continua gerando o alerta para tentativa de falha de senha. Para esta situação, você pode usar o **estado Dinâmico** onde uma ação de **Gerar Eventos** pode ser alterada para **Descartar e Gerar Eventos** para bloquear o ataque de força bruta.

Navegar para **Regras** no painel de navegação e na página Gerenciamento de regras é exibida. Selecione a regra para a qual deseja habilitar o estado Dinâmico e escolha as opções **Estado Dinâmico > Adicionar um Estado de Regra Base de Taxa.**

Para configurar o Estado da Regra Baseada em Taxa:

1. Selecione as **Regras** para as quais deseja configurar o Limite de Eventos.

- 2. Clique em Estado dinâmico.
- 3. Clique em Add Rate-Based Rule State.
- 4. Selecione como deseja rastrear o estado da regra na caixa suspensa **Rastrear por**. (**Regra ou Origem ou Destino**).
- 5. Entre na **rede**. Você pode especificar um único endereço IP, bloco de endereços, variável ou uma lista separada por vírgulas que seja composta por qualquer combinação deles.
- 6. Insira a Contagem de eventos e o carimbo de data e hora em segundos.
- 7. Selecione o novo estado, que você deseja definir para a regra.
- 8. Insira o tempo limite após o qual o estado da regra será revertido.
- 9. Clique em OK para concluir.



Etapa 2. Configurar o NAP (Network Analysis Policy, Política de análise de rede) e conjuntos de variáveis (opcional)

Configurar a política de análise de rede

A política de acesso à rede também é conhecida como pré-processadores. O pré-processador faz a remontagem de pacotes e normaliza o tráfego. Ele ajuda a identificar anomalias de protocolo da camada de rede e da camada de transporte na identificação de opções de cabeçalho inadequadas.

O NAP faz a desfragmentação de datagramas IP, fornece inspeção de estado TCP e remontagem de fluxo e validação de somas de verificação. O pré-processador normaliza o tráfego, valida e verifica o padrão do protocolo.

Cada pré-processador tem seu próprio número GID. Ele representa qual pré-processador foi disparado pelo pacote.

Para configurar a política de análise de rede, navegue até **Configuration > ASA FirePOWER Configuration > Policies > Access Control Policy > Advanced > Network Analysis and Intrusion Policy** A política de análise de rede padrão é a segurança e a conectividade equilibradas, que é a política recomendada ideal. Há outras três políticas NAP fornecidas pelo sistema que podem ser selecionadas na lista suspensa.

Selecione a opção Network Analysis Policy List para criar uma política NAP personalizada.

Configuration > ASA FirePOWER Configuration > Policies > Access Control Policy	
ASA FirePOWER	
custom porcy	
Pa 🛛 Status: Policy Up-to-date on device	
Identity Policy: None SSL Policy: None	
Rules Security Intellie Network Analysis and Intrusion Policies ? ×	
General Settings Intrusion Policy used before Access Control No Rules Active	<i>I</i>
Maximum URL characters rule is determined	No
Allow an Interactive Bloc Network Analysis Pules No Outom Pules Network Analysis Policy List	Ø
Retry URL cache miss loo Default Network Analysis Policy Balanced Security and Connectivity	Disabled
Inspect traffic during pol	Ø
Identity Policy Settin Revert to Defaults OK Cancel Iyze Per	5
Identity Policy None Performance Statistics - Sample Time (seconds)	300
SSL Policy Settings	Default
SSL Policy to use for inspecting encrypted connections None Regular Expression - Recursion Limit	Default
Network Analysis and Intrusion Policies 🖉 Intrusion Event Logging Limits - Max Events Stored Per Packet	8 🗸
Store ASA FirePOWER Changes Cancel	

Configurar Conjuntos de Variáveis

Os conjuntos de variáveis são usados em regras de intrusão para identificar os endereços origem e destino e as portas. As regras são mais eficazes quando as variáveis refletem seu ambiente de rede com mais precisão. A variável desempenha um papel importante no ajuste de desempenho.

Os conjuntos de variáveis já foram configurados com a opção padrão (Rede/Porta). Adicione novos Conjuntos de Variáveis se quiser alterar a configuração padrão.

Para configurar os Conjuntos de variáveis, navegue para **Configuração > Configuração do ASA Firepower > Gerenciamento de objetos > Conjunto de variáveis**. Selecione a opção **Add Variable Set** para adicionar novos conjuntos de variáveis. Insira o **Nome** dos Conjuntos de Variáveis e especifique a **Descrição**.

Se qualquer aplicativo personalizado funcionar em uma porta específica, defina o número da porta no campo Número da porta. Configure o parâmetro network.

\$Home_NET especifique a rede interna.

\$External_NET especifica a rede externa.

ASA FirePOWER Configuration	Configuration >	ASA FirePOWE	R Configurati	on > Obje	ect Management > <u>Variable Set</u>		
Policies Povice Management Object Management Anagement Network					O Add Variable Set	Silter	
Port	Name				Description		
	Default-Set				This Variable Set is system-provided.		Ø 8
	New Varia	ble Set				? :	< 1
	Name:	Custom_Variable	e_Set				
Sinkhole	Description:	Enter a descript	tion				
						💿 Add)
⊕≪] Distinguished Name ⊕.� PKI	Variable N	lame	Туре	Value			
Eccal	Customize	d Variables	24			A	
Updates	This categ	ory is empty				_	
Tools	Default V	ariables	1	0.000			
🗄 🗞 Integration	AIM_SERVE	RS	Network	[64.12.	31.136/32, 205.188.210.203/32, 6]	Ø98	
	DNS_SERV	ERS	Network	HOME_I	NET	Ø76	
	EXTERNAL	NET	Network	any		Ø76	
	FILE_DATA	PORTS	Port	[HTTP_	PORTS, 143, 110]	Ø ə 6	
Device Setup	FTP_PORTS		Port	[21, 21	00, 3535]	2 78	
💱 Firewall	GTP_PORTS	5	Port	[3386,	2123, 2152]	2 36	
Remote Access VPN	HOME_NET	60	Network	any		Ø76 _	> C
Site-to-Site VPN	4						
ASA FirePOWER Configuration							
Device Management					Store ASA FirePOWER Changes	S Cancel	

Passo 3: Configurar Controle de Acesso para incluir política de intrusão/ NAP/ conjuntos de variáveis

Navegue até **Configuration > ASA Firepower Configuration > Policies > Access Control Policy.** Você precisa concluir estas etapas:

- 1. Edite a regra da Diretiva de Acesso onde deseja atribuir a política de Intrusão.
- 2. Escolha a guia Inspeção.
- 3. Escolha a **Política de intrusão** na lista suspensa e escolha os **Conjuntos de variáveis** na lista suspensa
- 4. Click Save.

Standard Rules										
1 Access_Policy_Rule	any	any	any	any a	ny any	any	any	any	Allow	VDD0 🥖
Root Rules										0
Editing Rule - Access	s Policy F	Rule								?
Earling rate 7.0000	5_1 one / _1	ture .								
Name Access_Policy_Ru	le				Enabled		Move			
Action Allow			V IP	S: IPS Policy	Variables: (Default-Set	Files: no	inspection Lo	aaina: no l	paaina
• • • • • • • • • • • • • • • • • • • •										
Zones Networks	🔺 Users	🔺 Applicati	ons Por	ts 🔺 URLs	S 🔺 ISE A	ttributes	2 🔺 1	Inspection	Logging	Comments
Intrusion Policy	8. del	37	225	(1997)		Variable	Set			
IPS_Policy					× 🖉	Default	Set			
3										
File Policy										
None										~
								4	Save	Cancel

Como uma política de intrusão é adicionada a esta regra de política de acesso. Você pode ver o ícone de blindagem em Cor de Ouro que indica que a Política de intrusão está ativada.

										🖌 📑 Sta	tus: Access Cont	rol policy out-	of-date on devic	e
Ide	ntity Polic	ry: None		SSL Policy: <u>N</u>	one									
Ru	les Sec	curity Inte	elligence	HTTP Responses	Advanced									
									📀 Add Ca	tegory 📀 A	dd Rule Search	Rules		×
#	Name		Source Zones	Dest Zones	Source Networks	Dest Networks	Users	Applicat	Src Ports	Dest Ports	URLs	Action	V 🗈 🗊 🕫	
Adı	ninistrator	Rules		19		ст		-41			20			
Thi	s category i	is empty												
Sta	ndard Rule	es												
1	Access_Pol	licy_Rule	any	any	any	any	any	any	any	any	any	Allow	0] []	0
Roo	t Rules											1	-	
Thi	s category i	is empty												
De	fault Actio	n							Intrusion P	revention: Balan	iced Security and	Connectivity	*	\$ 📘
										Displaying	1 - 1 of 1 rules	I< < Page	1 of 1 $>$	> C
						Store	ASA FirePOW	ER Changes	Cancel					

Clique em Store ASA FirePOWER changes para salvar as alterações.

Etapa 4. Implante a política de controle de acesso

Agora, você deve implantar a política de controle de acesso. Antes de aplicar a política, você verá uma indicação Política de controle de acesso desatualizada no dispositivo. Para implantar as alterações no sensor:

- 1. Clique em Implantar.
- 2. Clique em Implantar alterações do FirePOWER.
- 3. Clique em Implantar na janela pop-up.





Nota: Na versão 5.4.x, para aplicar a política de acesso ao sensor, clique em Aplicar alterações do ASA FirePOWER

Note: Navegue até **Monitoring > ASA Firepower Monitoring > Task Status.** Verifique se a tarefa deve ser concluída para aplicar a alteração de configuração.

Etapa 5. Monitorar eventos de intrusão

Para ver os eventos de intrusão gerados pelo módulo FirePOWER, navegue para **Monitoramento** > **Monitoramento do ASA FirePOWER > Eventos em tempo real.**

V V						
Gaurav_Connection_Eve	ents × All ASA FirePOWER E	vents Connection	Intrusion	File	Malware File	Security Intelliger
ilter						
Rule Action=Block * reaso	n=Intrusion Block 🗱					
Pause Refresh	Rate 5 seconds	• 1/10/16 6:13	:42 PM (IST)			
Pause Receive Times	Rate 5 seconds Action	 1/10/16 6:13 Event Type 	:42 PM (IST)	In	line Result	Reason
Pause Refresh I Receive Times 1/10/16 6:11:50 PM	Rate 5 seconds Action Block	1/10/16 6:13 Event Type ASA FirePOWER Co	:42 PM (IST)	In	line Result	Reason Intrusion Bloc
Pause Refresh I Receive Times 1/10/16 6:11:50 PM 1/10/16 6:09:52 PM	Rate 5 seconds Action Block Block	1/10/16 6:13 Event Type ASA FirePOWER Co ASA FirePOWER Co	:42 PM (IST) onnection	In	line Result	Reason Intrusion Bloc Intrusion Bloc

Verificar

No momento, não há procedimento de verificação disponível para esta configuração.

Troubleshoot

Etapa 1. Verifique se o Estado das regras está configurado corretamente.

Etapa 2. Verifique se a política de IPS correta foi incluída nas regras de acesso.

Etapa 3. Verifique se os conjuntos de variáveis estão configurados corretamente. Se os conjuntos de variáveis não estiverem configurados corretamente, as assinaturas não corresponderão ao tráfego.

Etapa 4. Certifique-se de que a implantação da política de controle de acesso seja concluída com êxito.

Etapa 5. Monitore os eventos de conexão e de intrusão para verificar se o fluxo de tráfego está atingindo a regra correta ou não.

Informações Relacionadas

- Guia de início rápido do módulo Cisco ASA FirePOWER
- Suporte Técnico e Documentação Cisco Systems