Configuración de la política de intrusiones y la configuración de firmas en el módulo Firepower (administración integrada)

Contenido

Introducción **Prerequisites Requirements Componentes Utilizados Antecedentes** Configuración Paso 1. Configuración de la política de intrusiones Paso 1.1. Crear una política de intrusiones Paso 1.2. Modificar la política de intrusiones Paso 1.3. Modificar política base Paso 1.4. Filtrado de firmas con opción de barra de filtro Paso 1.5. Configuración del estado de regla Paso 1.6. Configuración del filtro de eventos Paso 1.7. Configuración del estado dinámico Paso 2. Configuración de los conjuntos de variables y políticas de análisis de red (NAP) (opcional) Paso 3: Configurar el control de acceso para incluir la política de intrusiones/ conjuntos de variables Paso 4. Implementación de la política de control de acceso Paso 5. Supervisar eventos de intrusión Verificación Troubleshoot Información Relacionada

Introducción

Este documento describe la funcionalidad del sistema de prevención de intrusiones (IPS)/sistema de detección de intrusiones (IDS) del módulo FirePOWER y varios elementos de la política de intrusiones que hacen una política de detección en el módulo FirePOWER.

Prerequisites

Requirements

Cisco recomienda que tenga conocimiento sobre estos temas:

* Conocimiento del firewall Adaptive Security Appliance (ASA), Adaptive Security Device Manager (ASDM).

* Conocimiento del dispositivo FirePOWER.

Componentes Utilizados

La información que contiene este documento se basa en las siguientes versiones de software y hardware.

Módulos ASA FirePOWER (ASA 5506X/5506H-X/5506W-X, ASA 5508-X, ASA 5516-X) que ejecutan la versión de software 5.4.1 y superiores.

Módulo ASA FirePOWER (ASA 5515-X, ASA 5525-X, ASA 5545-X, ASA 5555-X) que ejecuta la versión de software 6.0.0 y superior.

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. Si tiene una red en vivo, asegúrese de entender el posible impacto de cualquier comando.

Antecedentes

FirePOWER IDS/IPS está diseñado para examinar el tráfico de red e identificar cualquier patrón (o firmas) malicioso que indique un ataque a la red o al sistema. El módulo FirePOWER funciona en modo IDS si la política de servicio del ASA está configurada específicamente en modo monitor (promiscuo) si no, funciona en modo en línea.

FirePOWER IPS/IDS es un enfoque de detección basado en firmas. El módulo FirePOWER en modo IDS genera una alerta cuando la firma coincide con el tráfico malintencionado, mientras que el módulo FirePOWER en modo IPS genera una alerta y bloquea el tráfico malintencionado.

Nota: Asegúrese de que el módulo FirePOWER tenga la licencia **Protect** para configurar esta funcionalidad. Para verificar la licencia, navegue hasta **Configuration > ASA FirePOWER Configuration > License.**

Configuración

Paso 1. Configuración de la política de intrusiones

Paso 1.1. Crear una política de intrusiones

Para configurar la política de intrusiones, inicie sesión en Adaptive Security Device Manager (ASDM) y complete estos pasos:

Paso 1. Vaya a Configuration > ASA FirePOWER Configuration > Policies > Intrusion Policy > Intrusion Policy.

Paso 2. Haga clic en Crear política.

Paso 3. Introduzca el **nombre** de la política de intrusiones.

Paso 4. Introduzca la descripción de la política de intrusiones (opcional).

Paso 5. Especifique la opción Drop when Inline.

Paso 6. Seleccione la **Política base** de la lista desplegable.

Paso 7. Haga clic en Crear política para completar la creación de la política de intrusiones.

Sugerencia: Soltar cuando la opción En línea es crucial en ciertos escenarios cuando el sensor se configura en el modo En línea y se requiere no descartar el tráfico aunque coincida con una firma que tenga una acción de descarte.

<u>File View Tools Wizards Window Help</u>		Type topic to search Go	ahaha
😽 Home 🦓 Configuration 🔯 Monitoring 🗐 Save ASA Cha	iges 🔇 Refresh 🔇 Back 🔘 Forward 🢡 Helj	p	CISCO
ASA FirePOWER Configuration 🛛 🕤 🚺 Configur	tion > ASA FirePOWER Configuration > Policies	> Intrusion Policy > Intrusion Policy	
Policies Access Control Policy Intrusion Policy Rule Editor Files SSL Actions Alerts	e no policies defined. Click Create Policy to create a polic	Compare Polic 2	Create Policy
Identity Policy	Create Intrusion Policy	2.8	
Divis Policy Device Management	Policy Information		
Object Management Local	Name * 3 IPS_Policy		
System Information	Description 4 IPS_policy for	r LAB	
Licenses	Drop when Inline 5		
tools ⊡ ∿ Integration	Base Policy 6 Balanced Sec	urity and Connectivity	
Device Setup	* Required	Create Policy Create and Edit Policy Cancel	
Remote Access VPN			
Site-to-Site VPN			
ASA FirePOWER Configuration			
Device Management			
»			
	<admin> 15</admin>	1/4	16 1:17:37 AM UTC

Puede observar que la política está configurada, sin embargo, no se aplica a ningún dispositivo.

Configuration > ASA FirePOWER Configuration > Policies > Intrusion Policy > Intrusion Policy Image: Compare Policies Image: Compare Policies Image: Compare Policies Intrusion Policy Drop when Inline Status Last Modified IPS_Policy Yes No access control policies use this policy 2016-01-04 07:40:00 Image: Compare Policies IPS_policy for LAB Yes No access control policies use this policy 2016-01-04 07:40:00 Image: Compare Policies Image: Compare Policies						
Configuration > ASA FirePOWER Col Intrusion Policy Drop when Inl IPS_Policy Yes IPS_policy for LAB Yes			Compare Policies	S O Create Policy		
Intrusion Policy	Drop when Inline	Status	Last Modified			
IPS_Policy IPS_policy for LAB	Yes	<u>No access control policies use this policy</u> Policy not applied on device	2016-01-04 07:40:00 Modified by "admin"	8 🖓 6		

Paso 1.2. Modificar la política de intrusiones

Para modificar la política de intrusiones, navegue hasta **Configuration > ASA FirePOWER Configuration > Policies > Intrusion Policy > Intrusion Policy** y seleccione la **opción Edit**.



Paso 1.3. Modificar política base

La página Intrusion Policy Management (Administración de directivas de intrusiones) ofrece la opción de cambiar la política base/ descartar cuando está en línea/ Guardar y descartar.

La política básica contiene algunas políticas proporcionadas por el sistema, que son políticas integradas.

- 1. Conectividad y seguridad equilibradas: se trata de una política óptima en términos de seguridad y conectividad. Esta política tiene habilitadas alrededor de 7500 reglas, algunas solo generan eventos mientras que otras generan eventos y descartan el tráfico.
- 2. Seguridad en lugar de conectividad: si prefiere la seguridad, puede elegir la seguridad en lugar de la política de conectividad, lo que aumenta el número de reglas activadas.
- 3. Conectividad sobre seguridad: si su preferencia es la conectividad en lugar de la seguridad, puede elegir la conectividad en lugar de la política de seguridad, lo que reducirá el número de reglas activadas.
- 4. Maximum Detection (Detección máxima): Seleccione esta política para obtener la máxima detección.
- 5. Sin regla activa: esta opción desactiva todas las reglas. Debe activar las reglas manualmente en función de su política de seguridad.

Policy Information 🖄	Policy Information	< Back
Rules ⊕ Advanced Settings	Name IPS_Policy	
Policy Layers	Drop when Inline	
⊕ Policy Layers	Base Policy Balanced Security and Connectivity ▼ The base policy is up to date (Rule Update 2)	Manage Base Policy 015-10-01-001-vrt)
	 ➡ This policy has 7591 enabled rules ➡ 114 rules generate events X 7477 rules drop and generate events 	🖉 Manage Rules 🔍 View 🤍 View
	This policy contains enabled preprocessor rules. Pl the preprocessors have the correct settings for the	lease read the rule documentation to ensure ese rules
	Commit Changes	Discard Changes

Paso 1.4. Filtrado de firmas con opción de barra de filtro

Navegue hasta la opción **Reglas** en el panel Navegación y aparecerá la página Administración de reglas. Hay miles de reglas en la base de datos de reglas. La barra de filtros proporciona una buena opción de motor de búsqueda para buscar la regla de forma eficaz.

Puede insertar cualquier palabra clave en la barra de filtros y el sistema obtiene los resultados. Si hay un requisito para encontrar la firma para la vulnerabilidad de la capa de conexión segura (SSL), puede buscar la cadena de palabras clave en la barra de filtros y obtendrá la firma para la vulnerabilidad de la hemorragia cardiaca.

Sugerencia: si se utilizan varias palabras clave en la barra de filtros, el sistema las combina utilizando la lógica AND para crear una búsqueda compuesta.

También puede buscar las reglas mediante la ID de firma (SID), la ID de generador (GID) y la Categoría: dos, etc.

Las reglas se dividen de forma eficaz en varias formas, por ejemplo, en función de categorías/clasificaciones/vulnerabilidades de Microsoft/gusanos de Microsoft/plataforma específica. Esta asociación de reglas ayuda al cliente a obtener la firma adecuada de una manera sencilla y ayuda al cliente a ajustar las firmas de forma eficaz.

Policy Information	Rules		< Back
Rules	Rule Configuration	Filter: heartbleed	× ?
⊕ Advanced Settings	Rule Content		
⊕ Policy Layers	Category app-detect	⇔ ▼ ▼ ▼	Policy 🔻
	browser-chrome browser-firefox	GID SID Message ▲ 1 30549 SERVER-OTHER OpenSSL Heartbleed masscan access exploitation attempt	→ ♥ © 0 ♥ × ^
	browser-ie browser-other	1 30777 SERVER-OTHER OpenSSL SSLv3 large heartbeat response - possible ssl heartbleed attempt	×
	browser-plugins	1 30778 SERVER-OTHER OpenSSL SSLv3 large heartbeat response - possible ssl heartbleed attempt	×
	browser-webkit content-replace	1 30785 SERVER-OTHER OpenSSL SSLv3 large heartbeat response - possible ssl heartbleed attempt	×
	decoder exploit-kit	1 30514 SERVER-OTHER OpenSSL SSLv3 large heartbeat response - possible ssl heartbleed attempt	×
	file-executable	1 30779 SERVER-OTHER OpenSSL TLSv1 large heartbeat response - possible ssl heartbleed attempt	×
	Classifications	1 30780 SERVER-OTHER OpenSSL TLSv1 large heartbeat response - possible ssl heartbleed attempt	×
	Microsoft Vulnerabilities Microsoft Worms	SERVER-OTHER OpenSSL TLSv1 large heartbeat response - possible ssl heartbleed attempt	×
	Platform Specific	1 30515 SERVER-OTHER OpenSSL TLSv1 large heartbeat response - possible ssl heartbleed attempt	×
	Preprocessors	SERVER-OTHER OpenSSL TLSv1.1 large heartbeat	¥
	Rule Update	K	< 1 of 1 > >

También puede buscar con el número CVE para encontrar las reglas que los cubren. Puede utilizar la sintaxis **CVE: <cve-number>.**

Policy Information 🔺	Rules		< Back
Rules	Rule Configuration	Filter: CVE:"2013-2135"	× ?
⊕ Advanced Settings	Rule Content	Filter returned 2 results	
	Message 🔺	⇒▼ ▼ O ▼ O ▼ Poli Rule State Event Filtering Dynamic State Alerting Comments Poli	cy 🔻
	GID	📃 GID SID Message 🔺 🔿	7 🕑 🕕 🖓
	Reference CVE ID	1 27575 SERVER-APACHE Apache Struts arbitrary OGNL remote code execution attempt	
	URL Bugtrag ID	1 27574 SERVER-APACHE Apache Struts OGNL getRuntime.exec static method access attempt	
	Nessus ID Arachnids ID Mcafee ID Action Protocol Direction Source IP		
	Category		
	Classifications		
	Microsoft Vulnerabilities		
	Microsoft Worms		
	Platform Specific		
	Preprocessors		
	Priority		
	Rule Update	K K	1 of 1 > >

Paso 1.5. Configuración del estado de regla

Vaya a **Reglas** en el panel de navegación y aparece la página Administración de reglas.. Seleccione las reglas y elija la opción **Estado de regla** para configurar el estado de las reglas. Hay tres estados que se pueden configurar para una regla:

1. Generar eventos: Esta opción genera eventos cuando la regla coincide con el tráfico.

2. **Drop and Generate Events:** Esta opción genera eventos y descarta tráfico cuando la regla coincide con el tráfico.

3. Desactivar: Esta opción inhabilita la regla.

Policy Information	Rules		< E	Back
Rules	Rule Configuration	Filter:		2 2
⊕ Advanced Settings	Rule Content	Filter returned 33 results		
Advanced Settings Policy Layers	Category app-detect blacklist browser-chrome browser-firefox browser-ie browser-other browser-plugins browser-webkit content-replace decoder exploit-kit file-flash Microsoft Vulnerabilities Microsoft Worms Platform Specific Preprocessors	Filter returned 33 results Filter returned 33 results Rule State Event Filtering Dynamic State Alerting Comments Generate Events Generate Events Drop and Generate Events DR-OTHER OpenSSL SSLv3 large heartbeat response - possible ssl heartbleed attempt Drop 30778 SERVER-OTHER OpenSSL SSLv3 large heartbeat response - possible ssl heartbleed attempt 1 30785 SERVER-OTHER OpenSSL SSLv3 large heartbeat response - possible ssl heartbleed attempt 1 30779 SERVER-OTHER OpenSSL TLSv1 large heartbeat response - possible ssl heartbleed attempt 1 30780 SERVER-OTHER OpenSSL TLSv1 large heartbeat response - possible ssl heartbleed attempt 1 30786 SERVER-OTHER OpenSSL TLSv1 large heartbeat response - possible ssl h	Policy ⇒ ▼ × × × × × × × × × × × × × × ×	
	Priority	K	< 1 of 1 > >	×
	Rule Update			

Paso 1.6. Configuración del filtro de eventos

La importancia de un evento de intrusión puede basarse en la frecuencia de aparición, o en la dirección IP de origen o de destino. En algunos casos, es posible que no le importe un evento hasta que haya ocurrido un determinado número de veces. Por ejemplo, es posible que no le preocupe si alguien intenta iniciar sesión en un servidor hasta que se produzcan fallos un determinado número de veces. En otros casos, es posible que sólo tenga que ver algunas incidencias de la regla para comprobar si existe un problema generalizado.

Hay dos maneras de lograr esto:

- 1. Umbral de evento.
- 2. Supresión de eventos.

Umbral de evento

Puede establecer umbrales que dicten la frecuencia con la que se muestra un evento, en función del número de eventos. Puede configurar el umbral por evento y por política.

Pasos para configurar el umbral de evento:

Paso 1. Seleccione las reglas para las que desea configurar el umbral de evento.

- Paso 2. Haga clic en Event Filtering.
- Paso 3. Haga clic en el Umbral.
- Paso 4. Seleccione el tipo de la lista desplegable. (Límite, Umbral o Ambos).
- Paso 5. Seleccione cómo desea realizar el seguimiento en el cuadro de lista desplegable Track

By. (Origen o Destino).

Paso 6. Introduzca el **recuento** de eventos para cumplir el umbral.

Paso 7. Introduzca los segundos que deben transcurrir antes de que se reinicie el recuento.

Paso 8. Haga clic en **Aceptar** para completarlo.

	GID	SII Thresho	old 3				\Rightarrow	70	0 5
	1	28 Suppres	ssion	T 360.cn SafeG ess attempt	uard local HTTP n	nanagement	×		
	1	280 Remove	Thresholds	360.cn Safegua	rd runtime outbound	d communication	\Rightarrow		
	1	32	Suppressions 209.53.113	Absolute Softwa	re Computrace outbo	ound connection -	\Rightarrow		
	1	32846	APP-DETECT absolute.com	r Absolute Softwa m	re Computrace outbo	ound connection -	⇒		
	1	32847	APP-DETECT	r Absolute Softwa ery.com	Set Threshold	for 1 rule		7 X	
	1	32848	APP-DETECT namequery.	r Absolute Softwa nettrace.co.za	4 Type	Limit •	- -		
	1	26286	APP-DETECT search.dnss	F Absolute Softwa search.org	6 Count	10			
3	1	26287	APP-DETECT search.nam	r Absolute Softwa equery.com	C Seconds	60		2	

Después de agregar un filtro de evento a una regla, debería poder ver un icono de filtro junto a la indicación de regla, que muestra que hay un filtrado de eventos habilitado para esta regla.

Supresión de eventos

Las notificaciones de eventos especificados se pueden suprimir en función de la dirección IP de origen/ destino o por regla.

Nota: Cuando agrega supresión de eventos para una regla. La inspección de firma funciona como siempre, pero el sistema no genera los eventos si el tráfico coincide con la firma. Si especifica un origen/destino específico, los eventos no aparecen sólo para el origen/destino específico de esta regla. Si opta por suprimir la regla completa, el sistema no generará ningún evento para esta regla.

Pasos para configurar el umbral de evento:

Paso 1. Seleccione las reglas para las que desea configurar el umbral de evento.

Paso 2. Haga clic en Event Filtering.

Paso 3. Haga clic en Supresión.

Paso 4. Seleccione Suppression Type en la lista desplegable. (Regla, Origen o Destino).

Paso 5. Haga clic en **Aceptar** para completarlo.

⇒ ▼ 2 ▼ ▼ Rule State Event Filtering	⊙ ▼	Policy		•
GID SID Threshold		⇒	7 🕑 🕕	9
1 Suppression	T 360.cn SafeGuard local HTTP management ess attempt	×		-
1 280 Remove Suppre	nolds 360.cn Safeguard runtime outbound essions on	⇒		
1 32845 APP- Conn	DETECT Absolute Software Computrace outbound nection - 209.53.113.223	\Rightarrow		
✓ 1 32846 APP- conn	DETECT Absolute Software Computrace outbound nection - absolute.com	⇒	•	
Add Suppression for Suppression Type 4 Rule 5 Or 1 20207 conn 1 32849 APP- conn	1 rule * Software uery.cor Add Suppression for 1 Software v.nettrai Suppression 4 Source Software v.nettrai Software ssearch. Network 5 DETECT Absolute Software section - search.us.namequery 6 6 Suppression 4 Source Software section - search.us.namequery 5 Metwork 5 6 Suppression 4 Desti Network 5 6 Suppression 4 Desti Network 5 6 Suppression 4 Desti Network 5 6	L rule	? X	

Después de agregar el filtro de eventos a esta regla, debería poder ver un icono de filtro con el recuento dos junto a la indicación de regla, que muestra que hay dos filtros de eventos habilitados para esta regla.

Paso 1.7. Configuración del estado dinámico

Es una función en la que podemos cambiar el estado de una regla si coincide la condición especificada.

Suponga un escenario de ataque de fuerza bruta para descifrar la contraseña. Si una firma detecta un intento de error de contraseña y la acción de regla es generar un evento. El sistema continúa generando la alerta para el intento de error de contraseña. Para esta situación, puede utilizar el **estado Dinámico** donde una acción de **Generar eventos** se puede cambiar a **Abandonar y Generar eventos** para bloquear el ataque de fuerza bruta.

Vaya a **Reglas** en el panel de navegación y en la página Administración de reglas. Seleccione la regla para la que desea habilitar el estado Dinámico y elija las opciones **Estado dinámico > Agregar un estado de regla base de velocidad.**

Para configurar el estado de regla basado en velocidad:

- 1. Seleccione las **reglas** para las que desea configurar el umbral de evento.
- 2. Haga clic en el estado dinámico.
- 3. Haga clic en Agregar estado de regla basado en velocidad.
- 4. Seleccione cómo desea realizar el seguimiento del estado de regla en el cuadro de lista desplegable **Track By**. (**Regla, Origen o Destino**).
- 5. Introduzca la **red**. Puede especificar una única dirección IP, bloque de direcciones, variable o una lista separada por comas que esté compuesta por cualquier combinación de estos.
- 6. Introduzca el **recuento** de eventos y la marca de tiempo en segundos.
- 7. Seleccione el estado nuevo, que desea definir para la regla.
- 8. Introduzca el tiempo de espera después del cual se revierte el estado de la regla.
- 9. Haga clic en **Aceptar** para completarlo.

Policy Information	Rules		< Back
Rules	Rule Configuration	Filter:	x 7
⊕ Advanced Settings	Rule Content	1 selected rule of 33	
@ Policy Lowers	mation Rules < Back		
Policy Layers	app-detect	Rule State Event Filtering Dynamic State Alerting Comments	•
	blacklist	□ GID SID M3 Add Rate-Based Rule State → 💎 🕑	0 🖓
	browser-chrome	SER Remove Rate-Based Rule States ed masscan access	
	browser-firefox	0 1 30349 expl	
alicy Information Rules Rules Rules Rule Configuration Rule Content Category app-detect blacklist browser-chrome browser-chrome browser-ie browser-ie browser-ie browser-ie browser-other browser-other browser-other browser-other browser-usebkit content-replace decoder exploit-kit file-executable file-fiash Classifications Microsoft Vulnerabilities Microsoft Vulnerabilities Microsoft Vulnerabilities Platform Specific Preprocessors Priority Rule Update Rule Update Filter: Filt	SERVER-OTHER OpenSSL SSLv3 large heartbeat response		
	browser-other	Add Rate-Based Rule State for 1 rule	
	browser-plugins		
	browser-webkit		
	content-replace	1 30783 5 Network 192.168.20.3	
	decoder	1 30514 New State	
	exploit-kit	Timeout 20	
	file-executable	1 30779 1 1 30779	
	file-flash 🔻	0 OK Cancel	
	Classifications		
	Microsoft Vulnerabilities	SERVER-OTHER OpenSSL TLSv1 large heartbeat response	
	Microsoft Worms	- possible ssi neartbleed attempt	
	Platform Specific	- 1 30515 - possible ssl heartbleed attempt	
	Preprocessors	SERVER-OTHER OpenSSL TLSv1.1 large heartbeat	
	Priority		
	Rule Update	K K 1 of 1	- 2 N

Paso 2. Configuración de los conjuntos de variables y políticas de análisis de red (NAP) (opcional)

Configuración de la política de análisis de red

La política de acceso a la red también se conoce como preprocesadores. El preprocesador realiza el reensamblado de paquetes y normaliza el tráfico. Ayuda a identificar anomalías en la capa de red y el protocolo de capa de transporte al identificar opciones de encabezado inapropiadas.

NAP realiza la desfragmentación de los datagramas IP, proporciona la inspección con estado de TCP y el reensamblado de flujo y la validación de las sumas de comprobación. El preprocesador normaliza el tráfico, valida y verifica el estándar de protocolo.

Cada preprocesador tiene su propio número GID. Representa el preprocesador que el paquete ha disparado.

Para configurar la política de análisis de red, vaya a **Configuración > Configuración de ASA** FirePOWER > Políticas > Política de control de acceso > Avanzado > Análisis de red y Política de

intrusión

La política de análisis de red predeterminada es Equilibrio entre seguridad y conectividad, lo que constituye una política óptima recomendada. Hay otras tres políticas NAP proporcionadas por el sistema que se pueden seleccionar en la lista desplegable.

Seleccione la opción Network Analysis Policy List para crear una política NAP personalizada.

Configuration > ASA Fire	POWER Configuration > Policies > Access	Control Policy			
ASA ASA FirePO	WER				
Default Allow A	II Traffic				
custom policy					
			J Status: Policy Up-to-date on device		
Identity Policy: None	SSL Policy: None				
Rules Security Intellig	Network Analysis and Intrusion Pol	icies	? ×		
General Settings	Intrusion Policy used before Access Control	No Pules Active		Ø	
Maximum URL characters	rule is determined	NO Rules Acuve		No	
Allow an Interactive Bloc	Intrusion Policy Variable Set	Default-Set	▼ Ø	Ø	
Retry URL cache miss loo	Network Analysis Rules	No Custom Rules	Network Analysis Policy List	Disabled	
Inspect traffic during pol	Default Network Analysis Policy	Balanced Security	and Connectivity	A	
Identity Policy Setting					
identicy rule, etc.	Revert to Defaults		OK Cancel Jyze Per	5	
Identity Policy		None	Performance Statistics - Sample Time (seconds)	300	
SSL Policy Settings		Ø	Regular Expression - Limit	Default	
SSL Policy to use for inspe	cting encrypted connections	None	Regular Expression - Recursion Limit	Default	
Network Analysis and	Intrusion Policies	Ø	Intrusion Event Longing Limits - Max Events Stored Per Packet	8	
			ER-Changes Cancel		

Configurar conjuntos de variables

Los conjuntos de variables se utilizan en las reglas de intrusión para identificar las direcciones de origen y destino y los puertos. Las reglas son más eficaces cuando las variables reflejan su entorno de red con mayor precisión. La variable desempeña un papel importante en el ajuste del rendimiento.

Los conjuntos de variables ya se han configurado con la opción predeterminada (Red/Puerto). Agregue nuevos conjuntos de variables si desea cambiar la configuración predeterminada.

Para configurar los conjuntos de variables, navegue hasta **Configuration > ASA Firepower Configuration > Object Management > Variable Set**. Seleccione la opción **Añadir conjunto de variables** para agregar nuevos conjuntos de variables. Introduzca el **nombre** de los conjuntos de variables y especifique la **descripción**.

Si alguna aplicación personalizada funciona en un puerto específico, defina el número de puerto en el campo Número de puerto. Configure el parámetro de red.

\$Home_NET especifique la red interna.

\$External_NET especifique la red externa.

ASA FirePOWER Configuration	<u>Configuration ></u>	ASA FirePOWER	Configurati	on > Obje	ect Management > <u>Variable Set</u>		
Policies Solution Policies Solution Solution Solution Solution Solution Policies Solution Solution Policies Policies	_				Add Variable Set	Silter	
Port Security Zones	Name				Description		
Application Filters URL GeoLocation	Default-Set New Varia	ble Set			This Variable Set is system-provided.	? :	×
Variable Set	Name:	Custom_Variable_	Set]
Sinkhole	Description:	Enter a description	n				1
- Gipher Suite List						🕢 Add)
⊕	Variable N	lame	Туре	Value			1
Object Management Add Variable Set Hitter Network Port Description Security Zones Application Filters URL Object Management URL Description Security Zones Application Filters URL Object Management URL Description Security Zones Application Filters URL Security Intelligence Sinkhole Enter a description FileList Custom_Variable_Set Description Object Management Variable Mame Type Value Polication Customized Variables Customized Variables Operation Object Management This category is empty Default Variables Operation Updates Ucale Minegration Ons_SERVERS Network HOME_NET Operation Disconservers Network Integration Port (117P_PORTS, 143, 110) Operation periode Access VPN Site-to-Site VPN Port (3386, 2123, 2152) Operation							
Updates	This catego	ory is empty				_	
Elcenses	Default Va	ariables					
🗄 🖏 Integration	AIM_SERVE	RS	Network	[64.12.	31.136/32, 205.188.210.203/32, 6]	2 36	
	DNS_SERV	ERS	Network	HOME_I	NET	/>B	
	EXTERNAL_	NET	Network	any		2 76	
	FILE_DATA	_PORTS	Port	[HTTP_	PORTS, 143, 110]	Ø 9 6	
Device Setup	FTP_PORTS		Port	[21, 21	00, 3535]	0 28	
Firewall	GTP_PORTS	5	Port	[3386,	2123, 2152]	23 6	
Remote Access VPN	HOME_NET	ee	Network	any		Ø78 _	> 0
Site-to-Site VPN	4					•	
ASA FirePOWER Configuration							
Device Management					Store ASA FirePOWER Changes	Cancel	

Paso 3: Configurar el control de acceso para incluir conjuntos de políticas de intrusión/ NAP/ Variable

Vaya a Configuration > ASA Firepower Configuration > Policies > Access Control Policy . Debe completar estos pasos:

- 1. Edite la regla de directiva de acceso donde desea asignar la directiva de intrusión.
- 2. Elija la pestaña Inspección.
- 3. Elija la **política de intrusiones** de la lista desplegable y elija los **conjuntos de variables** de la lista desplegable
- 4. Click Save.

tanuaru kules												
Access_Policy_Rule	any	any	any	any	any	any	any	any	any	Allow	UDD0	Ø
oot Rules											1	
diting Rule - Access	s Policy R	ule										?
Name Access_Policy_Ru	le				🕑 Enab	led		Move				
Action Allow			▼ IF	S: IPS Po	licv Va	riables: D	efault-Set	Files: no i	inspection Lo	aaina: no l	paaina	
- HIGH										-		
Zones Networks	🔺 Users	🔺 Applicatio	ns Poi	rts 🔺 l	JRLs	ISE At	tributes	2 🔺 1	Inspection	Logging	Commen	nts
ntrusion Policy				1999			Variable	Set				
IPS_Policy						× 🥜	Default	Set				
File Policy												
None											-	-
												268
									-		L	
									4	Save	Cancel	

Puesto que se agrega una política de intrusiones a esta regla de directiva de acceso. Puede ver el icono de escudo en Color dorado que indica que la política de intrusiones está activada.

									🖌 📑 Sta	tus: Access Cont	rol policy out-	of-date on devic	e
Ide	ntity Policy: Nor	e	SSL Policy: <u>N</u>	lone									
Ru	les Security I	ntelligence	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				či – S	2	24) · · · · ·		54	2		- 44 	
Thi	s category is empl	У											
Sta	ndard Rules												
1	Access_Policy_Ru	le any	any	any	any	any	any	any	any	any	Allow	0 [] (] 🔍	0
Roo	t Rules										/	·	
Thi	s category is empl	Y											
De	fault Action							Intrusion P	revention: Balan	ced Security and	Connectivity	*	\$ 📕
									Displaying	1 - 1 of 1 rules	I< < Page	1 of 1 $>$	> c
					Store	ASA FirePOV	VER Changes	Cancel					

Haga clic en Store ASA FirePOWER changes para guardar los cambios.

Paso 4. Implementación de la política de control de acceso

Ahora, debe implementar la política de control de acceso. Antes de aplicar la política, verá una indicación de Directiva de control de acceso desactualizada en el dispositivo. Para implementar los cambios en el sensor:

- 1. Haga clic en Implementar.
- 2. Haga clic en Implementar cambios de FirePOWER.
- 3. Haga clic en Implementar en la ventana emergente.



Deploy FirePOWER Changes	X
Deploy Policies Version:2016-01-05 09:09 AM	?
System Policy: Default	
Sensor Policy: firepower	
Access Control Policy: Default Allow All Traffic	
Intrusion Policy: Balanced Security and Connectivity	
J Intrusion Policy: IPS_Policy	
ONS Policy: Default DNS Policy	
3 Deploy C	ancel
C Deploy	ancel

Nota: En la versión 5.4.x, para aplicar la política de acceso al sensor, debe hacer clic en Aplicar cambios de ASA FirePOWER

Nota: Vaya a **Monitoring > ASA Firepower Monitoring > Task Status**. Asegúrese de que la tarea debe completarse para aplicar el cambio de configuración.

Paso 5. Supervisar eventos de intrusión

Para ver los eventos de intrusión generados por el módulo FirePOWER, vaya a **Monitoring > ASA FirePOWER Monitoring > Real Time Event.**

Gaurav_Connection	n_Events × All ASA FireP	OWER Events Connectio	n Intrusion	File	Malware File	Security Intelligen
Filter						
Rule Action=Block * n	reason=Intrusion Block ×					
		-				
		-				
Pause Refr	resh Rate 5 seconds	- 1/10/16 6:	13:42 PM (IST)			
Pause Refr Receive Times Refr	resh Rate 5 seconds Action	 1/10/16 6: Event Type 	13:42 PM (IST)	In	ine Result	Reason
Refr Receive Times 1/10/16 6:11:50 PM	resh Rate 5 seconds Action Block	 1/10/16 6: Event Type ASA FirePOWER 	13:42 PM (IST) Connection	In	ine Result	Reason Intrusion Block
Receive Times	resh Rate 5 seconds Action Block	 1/10/16 6: Event Type ASA FirePOWER 	13:42 PM (IST) Connection	In	ine Result	Reason Intrusion Bloc

Verificación

Actualmente, no hay un procedimiento de verificación disponible para esta configuración.

Troubleshoot

Paso 1. Asegúrese de que el estado de regla de las reglas está configurado correctamente.

Paso 2. Asegúrese de que la política IPS correcta se ha incluido en las reglas de acceso.

Paso 3. Asegúrese de que los conjuntos de variables estén configurados correctamente. Si los conjuntos de variables no están configurados correctamente, las firmas no coincidirán con el tráfico.

Paso 4. Asegúrese de que la implementación de la política de control de acceso se complete correctamente.

Paso 5. Supervise los eventos de conexión y los eventos de intrusión para verificar si el flujo de tráfico está llegando a la regla correcta o no.

Información Relacionada

- Guía de inicio rápido del módulo Cisco ASA FirePOWER
- Soporte Técnico y Documentación Cisco Systems