Configurazione della policy di intrusione e della configurazione delle firme in Firepower Module (gestione integrata)

Sommario

Introduzione Prerequisiti **Requisiti** Componenti usati Premesse Configurazione Passaggio 1. Configurare i criteri per le intrusioni Passaggio 1.1. Creazione di una policy di intrusione Passaggio 1.2. Modifica criteri intrusioni Passaggio 1.3. Modifica criteri di base Passaggio 1.4. Filtro della firma con l'opzione della barra Filtro Passaggio 1.5. Configurazione dello stato della regola Passaggio 1.6. Configurazione del filtro eventi Passaggio 1.7. Configurazione dello stato dinamico Passaggio 2. Configurare i set di variabili e criteri di analisi della rete (facoltativo) Passaggio 3: Configurare il controllo di accesso per includere i set di criteri/variabili di Protezione accesso alla rete/Intrusion Passaggio 4. Distribuire i criteri di controllo di accesso Passaggio 5. Monitoraggio degli eventi di intrusione Verifica Risoluzione dei problemi Informazioni correlate

Introduzione

In questo documento viene descritta la funzionalità IPS (Intrusion Prevention System)/IDS (Intrusion Detection System) del modulo FirePOWER e vari elementi della policy di intrusione che creano una policy di rilevamento nel modulo FirePOWER.

Prerequisiti

Requisiti

Cisco raccomanda la conoscenza dei seguenti argomenti:

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

* Conoscenza dell'appliance FirePOWER.

Componenti usati

Le informazioni fornite in questo documento si basano sulle seguenti versioni software e hardware:

Moduli ASA FirePOWER (ASA 5506X/5506H-X/5506W-X, ASA 5508-X, ASA 5516-X) con software versione 5.4.1 e successive.

Modulo ASA FirePOWER (ASA 5515-X, ASA 5525-X, ASA 5545-X, ASA 5555-X) con software versione 6.0.0 e successive.

Le informazioni discusse in questo documento fanno riferimento a dispositivi usati in uno specifico ambiente di emulazione. Su tutti i dispositivi menzionati nel documento la configurazione è stata ripristinata ai valori predefiniti. Se la rete è operativa, valutare attentamente eventuali conseguenze derivanti dall'uso dei comandi.

Premesse

FirePOWER IDS/IPS è progettato per esaminare il traffico di rete e identificare eventuali modelli dannosi (o firme) che indicano un attacco alla rete o al sistema. Il modulo FirePOWER funziona in modalità IDS se la policy dei servizi dell'ASA è configurata in modo specifico in modalità monitor (promiscua), altrimenti funziona in modalità Inline.

FirePOWER IPS/IDS è un approccio di rilevamento basato su firma. Il modulo FirePOWER in modalità IDS genera un avviso quando la firma corrisponde al traffico dannoso, mentre il modulo FirePOWER in modalità IPS genera un avviso e blocca il traffico dannoso.

Nota: Verificare che il modulo FirePOWER disponga della licenza **Protect** per configurare questa funzionalità. Per verificare la licenza, selezionare **Configurazione > ASA FirePOWER Configuration > Licenza**.

Configurazione

Passaggio 1. Configurare i criteri per le intrusioni

Passaggio 1.1. Creazione di una policy di intrusione

Per configurare la policy sulle intrusioni, accedere a Adaptive Security Device Manager (ASDM) e completare i seguenti passaggi:

Passaggio 1. Passare a Configurazione > ASA FirePOWER Configuration > Policies > Intrusion Policy > Intrusion Policy.

Passaggio 2. Fare clic su Crea criterio.

Passaggio 3. Inserire il **nome** della policy di intrusione.

Passaggio 4. Inserire la descrizione della politica sulle intrusioni (facoltativo).

Passaggio 5. Specificare l'opzione Elimina quando in linea.

Passaggio 6. Selezionare il criterio di base dall'elenco a discesa.

Passaggio 7. Fare clic su Crea criterio per completare la creazione dei criteri di intrusione.

Suggerimento: l'opzione Rilascia quando inline è fondamentale in alcuni scenari quando il sensore è configurato in modalità inline ed è richiesto di non rilasciare il traffico anche se corrisponde a una firma che ha un'azione di rilascio.

<u>File View Tools Wizards Window H</u> elp	[Type topic to search Go	ababa
🐔 Home 🦓 Configuration 🔯 Monitoring 🔲 Save A	ASA Changes 🔇 Refresh 🔇 Back 🕥 Forward 🧖 Help		CISCO
ASA FirePOWER Configuration 🛛 🗗 🖸	configuration > ASA FirePOWER Configuration > Policies >	> Intrusion Policy > Intrusion Policy	
Policies Policy Access Control Policy Thrusion Policy Rule Editor Files SSL Actions Alerts	There are no policies defined. Click Create Policy to create a policy	Compare Polic 2	Create Policy
Identity Policy DNS Policy Diject Management Object Management Local System Information Updates Licenses Tools Tools Tools Tools Tools	Create Intrusion Policy Policy Information Name * Description Drop when Inline Base Policy Base Policy Create Intrusion Policy Drop when Solution Drop when Inline Drop	? ×	
Pevice Setup	* Required	reate Policy Create and Edit Policy Cancel	
Remote Access VPN			
Site-to-Site VPN			
ASA FirePOWER Configuration			
Device Management			
	<admin> 15</admin>	I /4/10	5 1:17:37 AM UTC

Èpossibile notare che il criterio è configurato, ma non viene applicato ad alcun dispositivo.

Configuration > AS/	A FirePOWER Config	uration > Policies > Intrusion Policy :	> Intrusion Policy	
			Compare Policies	G 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"	🕒 🕞 🥒 🙃

Passaggio 1.2. Modifica criteri intrusioni

Per modificare la policy di intrusione, selezionare **Configurazione > ASA FirePOWER Configuration > Policies > Intrusion Policy > Intrusion Policy** (Configurazione ASA FirePOWER > Criteri di intrusione), quindi selezionare l'opzione **Edit** (Modifica).



Passaggio 1.3. Modifica criteri di base

La pagina Gestione dei criteri per le intrusioni consente di modificare l'opzione Criteri di base/Elimina in linea/Salva e Elimina.

I criteri di base contengono alcuni criteri forniti dal sistema, ovvero criteri incorporati.

- 1. Sicurezza e connettività equilibrate: è una politica ottimale in termini di sicurezza e connettività. Questa politica ha attivato circa 7500 regole, alcune delle quali generano solo eventi, mentre altre generano eventi e scaricano il traffico.
- 2. Protezione rispetto alla connettività: se si preferisce la protezione, è possibile scegliere la protezione rispetto al criterio di connettività, che aumenta il numero di regole abilitate.
- 3. Connettività anziché sicurezza: se la preferenza è la connettività anziché la sicurezza, è possibile scegliere la connettività anziché i criteri di sicurezza che ridurranno il numero di regole abilitate.
- 4. Rilevamento massimo: selezionare questo criterio per ottenere il rilevamento massimo.
- 5. Nessuna regola attiva: questa opzione disattiva tutte le regole. È necessario attivare le regole manualmente in base ai criteri di protezione.

Policy Information	Policy Information	< Back
Rules ⊕ Advanced Settings	Name IPS_Policy	
⊕ Policy Layers	Drop when Inline	
	Balanced Security and Connectivity ▼ Solution Security and Connectivity ▼ Solution Connectivity ■ Solution Connectivi	Manage Base Policy 1-vrt)
	 ➡ This policy has 7591 enabled rules ➡ 114 rules generate events X 7477 rules drop and generate events 	Manage Rules
	This policy contains enabled preprocessor rules. Please read the r the preprocessors have the correct settings for these rules	rule documentation to ensure
	Commit Changes Discard Changes)

Passaggio 1.4. Filtro della firma con l'opzione della barra Filtro

Passare all'opzione **Regole** nel pannello di navigazione e viene visualizzata la pagina Gestione regole. Nel database delle regole sono presenti migliaia di regole. La barra dei filtri fornisce un'opzione valida per il motore di ricerca per eseguire ricerche efficaci nella regola.

Èpossibile inserire qualsiasi parola chiave nella barra Filtro e il sistema acquisisce automaticamente i risultati. Se è necessario trovare la firma per la vulnerabilità heartbleed SSL (Secure Sockets Layer), è possibile cercare la parola chiave heartbleed nella barra del filtro e recupererà la firma per la vulnerabilità heartbleed.

Suggerimento: se nella barra Filtro vengono utilizzate più parole chiave, il sistema le combina utilizzando la logica AND per creare una ricerca composta.

Èinoltre possibile cercare le regole utilizzando Signature ID (SID), Generator ID (GID), Category: dos ecc.

Le regole sono effettivamente suddivise in più modi, ad esempio in base a categoria/classificazioni/vulnerabilità Microsoft/Microsoft Worm/specifiche della piattaforma. Tale associazione di regole consente al cliente di ottenere la firma corretta in modo semplice e aiuta il cliente a ottimizzare efficacemente le firme.

Policy Information	Rules							<	Back
Rules	Rule Configuration	Filter:	heartbleed					2	× ?
⊕ Advanced Settings	Rule Content			Filter returned 33 resu	ts				
Policy Layers	Category		T •			Policy			
W Folicy Edyclo	app-detect	Rule State	Event Filtering	Dynamic State Alerting Comments		Policy			
	blacklist	📃 GID SID	D Mes	ssage 🔺			70	0 🤉	2
	browser-chrome browser-firefox	1 30	1549 SEI ext	RVER-OTHER OpenSSL Heartbleed mass loitation attempt	can access	×			
	browser-ie	1 30	1777 SEI - p	RVER-OTHER OpenSSL SSLv3 large hear ossible ssl heartbleed attempt	rtbeat response	×			
	browser-plugins	1 30	778 SEI - p	RVER-OTHER OpenSSL SSLv3 large hear ossible ssl heartbleed attempt	rtbeat response	×			
	browser-webkit content-replace	1 30	785 SEI	RVER-OTHER OpenSSL SSLv3 large hear ossible ssl heartbleed attempt	rtbeat response	×			
	decoder exploit-kit	1 30	514 SE	RVER-OTHER OpenSSL SSLv3 large hear ossible ssl heartbleed attempt	rtbeat response	×			
	file-executable	1 30	1779 SEI - p	RVER-OTHER OpenSSL TLSv1 large hear ossible ssl heartbleed attempt	tbeat response	×			
	file-flash Classifications	1 30	1780 SEI - p	RVER-OTHER OpenSSL TLSv1 large hear ossible ssl heartbleed attempt	tbeat response	×			
	Microsoft Vulnerabilities	1 30)786 SEI	RVER-OTHER OpenSSL TLSv1 large hear	tbeat response	×			
	Microsoft Worms		- p	ossible ssl heartbleed attempt					
	Platform Specific	1 30)515 - p	RVER-OTHER OpenSSL TLSV1 Targe near ossible ssl heartbleed attempt	tbeat response	×			
	Preprocessors		SE	RVER-OTHER OpenSSL TLSv1.1 large he	artbeat				-
	Priority		/81		1				
	Rule Update	A			14		1 or	1 7 1	2

Èinoltre possibile eseguire ricerche con il numero CVE per trovare le regole che li riguardano. È possibile utilizzare la sintassi **CVE: <numero-cve>.**



Passaggio 1.5. Configurazione dello stato della regola

Passa a **Regole** nel pannello di navigazione e viene visualizzata la pagina Gestione regole. Selezionare le regole e scegliere l'opzione **Stato regola** per configurare lo stato delle regole. È possibile configurare tre stati per una regola:

1. Genera eventi: Questa opzione genera eventi quando la regola corrisponde al traffico.

2. **Elimina e genera eventi:** questa opzione genera eventi e rilascia traffico quando la regola corrisponde al traffico.

3.	Disabilitazione:	Questa	opzione	disattiva	la regola.	
----	------------------	--------	---------	-----------	------------	--

Policy Information	Rules		< Back
Rules	Rule Configuration	Filter:	x ?
⊕ Advanced Settings	Rule Content	Filter returned 33 results	
 Advanced Settings Policy Layers 	Rule Content Category app-detect blacklist browser-chrome browser-chrome browser-firefox browser-other browser-other browser-plugins browser-webkit content-replace decoder exploit-kit file-flash Microsoft Vulnerabilities Microsoft Worms Platform Specific	Filter returned 33 results Filter returned 33 results Rule State Event Filtering Dynamic State Alerting Comments Generate Events Image A Image A Image A Drop and Generate Events Image A Image A Image A Disable ER-OTHER OpenSSL Heartbleed masscan access itation attempt Image A 1 30778 SERVER-OTHER OpenSSL SSLv3 large heartbeat response - possible ssl heartbleed attempt 1 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 SSLv3 large heartbeat response - possible ssl heartbleed attempt 1 30779 SERVER-OTHER OpenSSL TLSv1 large heartbeat response - possible ssl heartbleed attempt 1 30780 - possible ssl heartbleed attempt 1 30786 SERVER-OTHER OpenSSL TLSv1 large heartbeat response - possible ssl heartbleed attempt 1 30786 SERVER-OTHER OpenSSL TLSv1 large heartbeat response - possible ssl heartbleed attempt 1 30786 SERVER-OTHER OpenSSL TLSv1 large heartbeat response - possible ss	Policy ▼ ● ● × ● ● ● × ● ● ● × ● ● ● × ● ● ● × ● ● ● × ● ● ● × ● ● ● × ● ● ● × ● ● ● × ● ● ● × ● ● ● × ● ● ● × ● ● ● × ● ● ● × ● ● ● × ● ● ● × ● ● ● ● × ● ● ● ● × ● ● ● ● × ● ● ● ● × ● ● ● ● ×
	Priority	SERVER-OTHER OpenSSL TLSv1.1 large heartbeat	* *
	Rule Update	к	< 1 of 1 > >

Passaggio 1.6. Configurazione del filtro eventi

L'importanza di un evento di intrusione può essere basata sulla frequenza dell'evento oppure sull'indirizzo IP di origine o di destinazione. In alcuni casi è possibile che un evento non sia rilevante fino a quando non si è verificato un determinato numero di volte. È possibile, ad esempio, che il problema non si verifichi se un utente tenta di accedere a un server fino a quando il tentativo non riesce per un determinato numero di volte. In altri casi, potrebbe essere necessario visualizzare solo alcune occorrenze della regola per verificare se il problema è molto diffuso.

A tale scopo, è possibile procedere in due modi:

- 1. Soglia evento.
- 2. Eliminazione degli eventi.

Soglia evento

Èpossibile impostare soglie che determinano la frequenza di visualizzazione di un evento, in base al numero di occorrenze. È possibile configurare la soglia per evento e per criterio.

Passaggi per la configurazione della soglia eventi:

Passaggio 1. Selezionare le **regole** per le quali si desidera configurare la soglia evento.

Passaggio 2. Fare clic su Filtro eventi.

Passaggio 3. Fare clic su Soglia.

Passaggio 4. Selezionare il Tipo dall'elenco a discesa. (Limite o Soglia o Entrambi).

Passaggio 5. Selezionare la modalità di registrazione dalla casella di riepilogo **Traccia per**. (Origine o Destinazione).

Passaggio 6. Inserire il conteggio degli eventi per raggiungere la soglia.

Passaggio 7. Inserire i secondi che devono trascorrere prima della reimpostazione dell'inventario.

Passaggio 8. Fare clic su **OK** per completare l'operazione.

	GID	SII Thresho	old 3				⇒	7	•	0 5
	1	28t Suppres	ssion	T 360.cn Safe@ ess attempt	Guard local HTTP n	nanagement	×			
	1	280 Remove	Thresholds	360.cn Safegua	rd runtime outboun	d communication	\Rightarrow			
	1	328 Remove	Suppressions 209.53.113	Absolute Softwa	re Computrace outb	ound connection -	⇒			
•	1	32846	APP-DETECT absolute.com	ົ Absolute Softwa ກ	re Computrace outb	ound connection -	⇒			
	1	32847	APP-DETECT	⁻ Absolute Softwa ery.com	Set Threshold	l for 1 rule		7	×	
	1	32848	APP-DETECT namequery.	⁻ Absolute Softwa nettrace.co.za	4 Type	Limit	•			
	1	26286	APP-DETECT search.dnss	Absolute Softwa earch.org	6 Count	10				
	1	26287	APP-DETECT search.nam	⁻ Absolute Softwa equery.com	5econds	60				

Dopo l'aggiunta di un filtro di eventi a una regola, dovrebbe essere possibile visualizzare un'icona di filtro accanto all'indicazione della regola, che indica che per la regola è abilitato il filtro di eventi.

Eliminazione eventi

Le notifiche degli eventi specificati possono essere eliminate in base all'indirizzo IP di origine/destinazione o in base a una regola.

Nota: Quando si aggiunge l'eliminazione di eventi per una regola. L'ispezione della firma funziona normalmente ma il sistema non genera gli eventi se il traffico corrisponde alla firma. Se si specifica un'origine o una destinazione specifica, gli eventi non vengono visualizzati solo per l'origine o la destinazione specifica per questa regola. Se si sceglie di sopprimere la regola completa, il sistema non genera alcun evento per questa regola.

Passaggi per la configurazione della soglia eventi:

Passaggio 1. Selezionare le **regole** per le quali si desidera configurare la soglia evento.

Passaggio 2. Fare clic su Filtro eventi.

Passaggio 3. Fare clic su Soppressione.

Passaggio 4. Selezionare **Tipo di soppressione** dall'elenco a discesa. (Regola, Origine o Destinazione).

Passaggio 5. Fare clic su OK per completare l'operazione.

⇒ ▼ 2 ▼ ▼ Rule State Event Filt	ering Dynamic Sta	€ Alerting Co) ▼ omments		Policy			•
GID SID Threshol	d				⇒ 🔻	۵ ()	9	
1 3 Suppres	sion T 36	0.cn SafeGua attempt	rd local HTTP ma	anagement	×			-
1 280 Remove	Thresholds 360. Suppressions on	.cn Safeguard r	untime outbound		⇒			
1 32845	APP-DETECT Abso connection - 209	olute Software (.53.113.223	Computrace outbo	und	⇒			
1 32846	APP-DETECT Abso connection - abso	olute Software (olute.com	Computrace outbo	und	⇒			
Add Suppression Suppression Type 1 20207 1 32849	n for 1 rule ? Rule OK Cance Connection - sear APP-DETECT Abso connection - sear	Software uery.cor Software y.nettra Software ssearch. Software ch.namequery olute Software ch.us.nameque	Add Suppression Type Network Add Suppression Type Suppression Type Network	sion for 1 ru 4 Source 5 5 4 Destination 5	Ile ▼ ок ule оп ▼	? × Cancel ? × Cancel		

Dopo aver aggiunto il filtro eventi a questa regola, dovrebbe essere possibile visualizzare un'icona di filtro con il conteggio due accanto all'indicazione della regola, che indica che sono disponibili due filtri eventi abilitati per questa regola.

Passaggio 1.7. Configurazione dello stato dinamico

Si tratta di una funzionalità che consente di modificare lo stato di una regola se la condizione specificata corrisponde.

Si supponga di avere uno scenario di attacco di forza bruta per violare la password. Se una firma rileva un tentativo di errore della password e l'azione della regola consiste nel generare un evento. Il sistema continua a generare l'avviso per il tentativo di mancato superamento della password. In questo caso, potete utilizzare lo **stato Dinamico** in cui un'azione di **Genera eventi** (Generate Events) può essere modificata in **Elimina (Drop) e Genera eventi (Generate Events)** per bloccare l'attacco di forza bruta.

Passa a **Regole** nel pannello di navigazione e viene visualizzata la pagina Gestione regole. Selezionare la regola per la quale si desidera abilitare lo stato Dinamico e scegliere le opzioni **Stato dinamico > Aggiungi uno stato regola base tasso.**

Per configurare lo stato della regola basata sulla velocità:

- 1. Selezionare le **regole** per le quali si desidera configurare la soglia evento.
- 2. Fare clic su Stato dinamico.
- 3. Fare clic su Aggiungi stato regola basata su tasso.
- 4. Selezionare come si desidera tenere traccia dello stato della regola dalla casella di riepilogo **Rileva per**. (**regola, origine o destinazione**).
- 5. Accedere alla **rete**. È possibile specificare un singolo indirizzo IP, un blocco di indirizzi, una variabile o un elenco separato da virgole costituito da una combinazione di questi elementi.
- 6. Immettere il conteggio degli eventi e il timestamp in secondi.
- 7. Selezionare il Nuovo stato che si desidera definire per la regola.
- 8. Immettere il timeout dopo il quale lo stato della regola viene ripristinato.
- 9. Fare clic su **OK** per completare l'operazione.

Policy Information	Rules	< B
Rules	Rule Configuration	Filter: ×
⊕ Advanced Settings	Rule Content	1 selected rule of 33
Policy Layers	Category	
E Policy Layers	app-detect	Rule State Event Filtering Dynamic State Alerting Comments
	blacklist	🔲 GID SID M 🗿 Add Rate-Based Rule State 🛛 🔿 💎 🕑 🕕 🖓
	browser-chrome browser-firefox	1 30549 SER Remove Rate-Based Rule States ad masscan access
	browser-ie	SERVER-OTHER OpenSSL SSLv3 large heartbeat response
	browser-other	Add Rate-Based Rule State for 1 rule
	browser-plugins	1 30778
	browser-webkit content-replace	4 Track By Destination ▼ 1 30785 5 Network 192.168.20.3
	decoder exploit-kit	6 Rate 10 Count / 5 Seconds 1 30514 7 New State Drop and Generate Events Image: Second Se
	file-executable	1 30779 3 Timeout 30
	file-flash 🔹	0 1 30780 OK Cancel
	Classifications	
	Microsoft Vulnerabilities	SERVER-OTHER OpenSSL TLSv1 large heartbeat response
	Microsoft Worms	SERVER-OTHER OpenSSL TLSv1 large heartbeat response
	Platform Specific	- possible ssl heartbleed attempt
	Preprocessors	□ 1 30781 SERVER-OTHER OpenSSL TLSv1.1 large heartbeat
	Priority	K (1 of 1)
	Rule Update	

Passaggio 2. Configurare i set di variabili e criteri di analisi della rete (facoltativo)

Configura criteri di analisi della rete

I criteri di accesso alla rete sono noti anche come preprocessori. Il preprocessore riassembla il pacchetto e normalizza il traffico. Aiuta a identificare le anomalie del protocollo del livello di rete e del livello di trasporto nell'identificazione di opzioni di intestazione inappropriate.

Protezione accesso alla rete esegue la deframmentazione dei datagrammi IP, fornisce l'ispezione con conservazione dello stato TCP e il riassemblaggio dei flussi e la convalida dei checksum. Il preprocessore normalizza il traffico, convalida e verifica lo standard del protocollo.

Ogni preprocessore dispone di un proprio numero GID. Indica il preprocessore attivato dal pacchetto.

Per configurare i criteri di analisi della rete, selezionare **Configurazione > ASA FirePOWER Configuration > Policy > Access Control Policy > Advanced > Network Analysis and Intrusion Policy**

Il criterio di analisi della rete predefinito è Protezione e connettività bilanciate, il criterio consigliato

ottimale. Esistono altri tre criteri di Protezione accesso alla rete forniti dal sistema che è possibile selezionare dall'elenco a discesa.

Selezionare l'opzione **Network Analysis Policy** List per creare un criterio di Protezione accesso alla rete personalizzato.

Configuration > ASA FireP	OWER Configuration > Policies > Access	s Control Policy			
ASA ASA FirePO Default Allow A	wer II Traffic				
custom poncy			January Status: Policy Up-to-date on device		
Identity Policy: None	SSL Policy: None				
Rules Security Intellig	Network Analysis and Intrusion Pol	icies	2 ×		
General Settings	Network Analysis and Inclusion For	icies		<i>a</i>	-
Maximum URL characters	Intrusion Policy used before Access Control rule is determined	No Rules Active	×	No	
Allow on Interactive Plac	Intrusion Policy Variable Set	Default-Set	✓ Ø	110	
Anow an interactive bloc	Network Analysis Rules	No Custom Rules	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 Settine	Revert to Defaults		OK Cancel lyze Per	F	
Identity Policy		None		5	
SSI Policy Settings		<i>li</i>	Performance Statistics - Sample Time (seconds)	300	
CCL Pulling to use for imme		News	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 Logging Limits - Max Events Stored Per Packet	8	-
		Store ASA FirePOW	ER Changes Cancel		

Configura set di variabili

I set di variabili vengono utilizzati nelle regole di intrusione per identificare le porte e gli indirizzi di origine e di destinazione. Le regole sono più efficaci quando le variabili riflettono l'ambiente di rete in modo più accurato. La variabile svolge un ruolo importante nel tuning delle prestazioni.

I set di variabili sono già stati configurati con l'opzione predefinita (Rete/Porta). Aggiungere nuovi set di variabili se si desidera modificare la configurazione predefinita.

Per configurare i set di variabili, selezionare **Configurazione > ASA Firepower Configuration > Object Management > Set di variabili**. Selezionare l'opzione **Add Variable Set** (Aggiungi set di variabili) per aggiungere nuovi set di variabili. Immettere il **nome** degli insiemi di variabili e specificare la **descrizione**.

Se un'applicazione personalizzata funziona su una porta specifica, definire il numero di porta nel campo Numero porta. Configurare il parametro network.

\$Home_NET specifica la rete interna.

\$External_NET specifica la rete esterna.

ASA FirePOWER Configuration	<u>Configuration ></u>	ASA FirePOWER	Configurati	on > Obje	ect Management > <u>Variable Set</u>		
Policies Device Management Object Management Notwork					O Add Variable Set	Rilter	
Port	Name				Description		
Application Filters	Default-Set				This Variable Set is system-provided.		Ø 8
	New Varia	ble Set				?	×
Variable Set	Name:	Custom_Variable_	Set				1
SecurityIntelligence	Description:	Enter a descriptio	n				Ĩ.
						Add 🕥	Ĵ
🕀 🚰 Distinguished Name	Variable N	lame	Туре	Value			
Local	Customize	d Variables	24. 	24			
Updates	This catego	ory is empty					
Elicenses	Default Va	ariables					
🗄 🔩 Integration	AIM_SERVE	RS	Network	[64.12.	31.136/32, 205.188.210.203/32, 6]	Ø78	
	DNS_SERV	ERS	Network	HOME_N	NET	Ø96	
	EXTERNAL	NET	Network	any		Ø78	
	FILE_DATA	PORTS	Port	[HTTP_I	PORTS, 143, 110]	Ø76	
Device Setup	FTP_PORTS		Port	[21, 21	00, 3535]	Ø96	
Firewall	GTP_PORTS	5	Port	[3386,	2123, 2152]	Ø76	
Remote Access VPN	HOME_NET	÷0	Network	any		Ø76 _	> 0
Site-to-Site VPN	4					+	1
ASA FirePOWER Configuration							
Device Management					Store ASA FirePOWER Changes	Cancel	

Passaggio 3: Configurare il controllo di accesso per includere i set di criteri/variabili di Protezione accesso alla rete per le intrusioni

Selezionare Configuration > ASA Firepower Configuration > Policies > Access Control Policy (Configurazione di ASA Firepower > Criteri > Policy di controllo dell'accesso). Eseguire i seguenti passaggi:

- 1. Modificare la regola dei criteri di accesso a cui si desidera assegnare i criteri per le intrusioni.
- 2. Scegliere la scheda Ispezione.
- 3. Selezionare il **criterio** di **intrusione** dall'elenco a discesa e scegliere **Set di variabili** dall'elenco a discesa

4. Fare clic su Salva.



Name Access_Policy_Rule					E	nabled	Move		
Action	Allow 🖉		~	IPS:	IPS_Policy	Variables: Default-Set	Files: no inspection	Logging: no lo	gging
Zones	Networks	🔺 Users	Applications	Ports	🔺 URLs	🔺 ISE Attributes	2 🔺 Inspection	Logging	Comments
ntrusion P	olicy					Variable	Set		
PS_Policy						💌 🦉 🛛 Default	Set		
le Policy									
lone									~

Poiché a questa regola dei criteri di accesso è stato aggiunto un criterio di intrusione. È possibile vedere l'icona a forma di scudo in Colore dorato che indica che la policy sulle intrusioni è attivata.

										M 📑 Sta	tus: Access	s Control policy out-	of-date on devi	ce
Ide	entity P	Policy: None		SSL Policy: N	lone									
Ru	les	Security Inte	elligence	HTTP Responses	Advanced									
ĺ.	1000		10		11.	2.X.			🗿 Add Ca	itegory 📀 A	dd Rule S	earch Rules		×
#	Name	e	Source Zones	Dest Zones	Source Networks	Dest Networks	Users	Applicat	Src Ports	Dest Ports	URLs	Action	V 🗈 🗊 🖓	
Adı	ninistra	ator Rules	2 	14			2	26) - 24			00			- 24
Th	s catego	ory is empty												
Sta	ndard I	Rules												
1	Access	_Policy_Rule	any	any	any	any	any	any	any	any	any	Allow	0 [] (]	0
Ro	t Rules	5										/	1	
Th	s catego	ory is empty												
Default Action						Intrusion Prevention: Balanced Security and Connec					ty and Connectivity	×.	\$ 🔳	
										Displaying	1 - 1 of 1	rules 🛛 🔾 🖌 Page	e 1 of 1 >	> c
						Store	ASA FirePOV	VER Changes	Cancel					

Fare clic su Store ASA FirePOWER changes per salvare le modifiche.

Passaggio 4. Distribuire i criteri di controllo di accesso

A questo punto è necessario distribuire i criteri di controllo di accesso. Prima di applicare il criterio, nel dispositivo verrà visualizzata un'indicazione relativa ai criteri di controllo di accesso non aggiornata. Per distribuire le modifiche al sensore:

- 1. Fare clic su **Distribuisci**.
- 2. Fare clic su Distribuisci modifiche FirePOWER.
- 3. Fare clic su Distribuisci nella finestra popup.



Deploy FirePOWER Changes	
Deploy Policies Version:2016-01-05 09:09 AM	1
System Policy: Default	
Sensor Policy: firepower	
D Access Control Policy: Default Allow All Traffic	
Intrusion Policy: Balanced Security and Connectivity	
Intrusion Policy: IPS_Policy	
ONS Policy: Default DNS Policy	
3 Deploy	Cancel

Nota: Nella versione 5.4.x, per applicare la policy di accesso al sensore, è necessario fare clic su Apply ASA FirePOWER Changes (Applica modifiche FirePOWER ASA)

Nota: Passare a **Monitoraggio > Monitoraggio ASA Firepower > Stato task. Per** applicare la modifica alla configurazione, verificare che il task debba essere completato.

Passaggio 5. Monitoraggio degli eventi di intrusione

Per visualizzare gli eventi Intrusion generati dal modulo FirePOWER, passare a **Monitoraggio** > ASA FirePOWER Monitoring > Eventi in tempo reale.

V Chilling						
Gaurav_Connection_Eve	ents × All ASA FirePOWER E	events Connection	Intrusion	File	Malware File	Security Intelligent
ïlter						
Rule Action=Block * reaso	n=Intrusion Block 🗱					
121 E						
Pause Refresh F	Rate 5 seconds	▼ 1/10/16 6:13	8:42 PM (IST)			
Pause Receive Times	Rate 5 seconds Action	 1/10/16 6:13 Event Type 	8:42 PM (IST)	Inl	ine Result	Reason
Refresh F Receive Times 1/10/16 6:11:50 PM	Rate 5 seconds Action Block	1/10/16 6:13 Event Type ASA FirePOWER Co	9:42 PM (IST)	Inl	ine Result	Reason Intrusion Block
Pause Refresh F 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 	3:42 PM (IST) onnection onnection	Inl	ine Result	Reason Intrusion Block Intrusion Block

Verifica

Attualmente non è disponibile una procedura di verifica per questa configurazione.

Risoluzione dei problemi

Passaggio 1. Verificare che lo stato delle regole sia configurato correttamente.

Passaggio 2. Verificare che nelle regole di accesso sia stato incluso il criterio IPS corretto.

Passaggio 3. Verificare che i set di variabili siano configurati correttamente. Se i set di variabili non sono configurati correttamente, le firme non corrisponderanno al traffico.

Passaggio 4. Verificare che la distribuzione dei criteri di controllo di accesso venga completata correttamente.

Passaggio 5. Monitorare gli eventi di connessione e gli eventi di intrusione per verificare se il flusso di traffico sta violando la regola corretta.

Informazioni correlate

- Guida introduttiva al modulo Cisco ASA FirePOWER
- Documentazione e supporto tecnico Cisco Systems