Configurazione e test dei criteri dei file AMP tramite FDM

Sommario

Introduzione
Prerequisiti
Requisiti
Componenti usati
Istruzione
Licenze
Configurazione
<u>Test</u>
Risoluzione dei problemi

Introduzione

In questo documento viene descritto come configurare e provare una policy sui file di Advanced Malware Protection (AMP) tramite Firepower Device Manager (FDM).

Prerequisiti

Requisiti

Cisco raccomanda la conoscenza dei seguenti argomenti:

- Firepower Device Manager (FDM)
- Firepower Threat Defense (FTD)

Componenti usati

- Cisco virtual FTD versione 7.0 gestito tramite FDM
- Licenza di valutazione (la licenza di valutazione viene utilizzata a scopo dimostrativo. Si consiglia a Cisco di acquistare e utilizzare una licenza valida)

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.

Istruzione

Licenze

1. Per abilitare la licenza malware, passare alla pagina DEVICE nell'interfaccia utente di FDM.



2. Individuare la casella Smart License e fare clic su View Configuration.



Pagina Dispositivo FDM

3. Abilitare la licenza Malware.



Licenza per malware

Configurazione

1. Passare alla pagina CRITERI in FDM.

|--|

Scheda Criteri FDM

2. In Criteri di sicurezza, passare alla sezione Controllo di accesso.

Manager	MONITORING	POLICIES	OBJECTS	DEVICE: FTD			Ø	۵ ک) (?)	admin Administrator	2)~
ø Secur	ity Policies											
$\Box \ \rightarrow$	SSL Decryption	\rightarrow O Identity	ightarrow Secu	urity Intelligence \rightarrow	🔗 NAT $ ightarrow$ 🖌 🖌 Ac	cess Control 💛	Intrusion					
5 rules						Q Search	h			(0	+

Scheda Controllo accesso di FDM

3. Individuare o creare una regola di accesso per configurare il criterio file. Fare clic sull'editor Regole di accesso. Per istruzioni su come creare una regola di accesso, fare riferimento a questo <u>collegamento.</u>

Manager	MON	ITORING	POLICIES	OBJECTS	DEVICE: FTD				6	3 🙆 () admi Admi	n inistrator	۹~
ø S	ecurity Pol	icies											
Ð	\rightarrow () SSL	Decryptior	$n \rightarrow \bigcirc$ Ident	ity $ ightarrow$ 📀 Se	curity Intelligence	-> 🕗 NAT	→ 🖌 Access	Control $ ightarrow$	Intrusion				
5 rules								Q Search				0	+
			SOURCE			DESTINATION							
н	NAME	ACTION	ZONES	NETWORKS	PORTS	ZONES	NETWORKS	PORTS/PROTO	APPLICATIONS	URLS	USERS		ACTIONS
> 1	Inside_Outside	€	inside_zone	ANY	ANY	outside_zone	ANY	ANY	ANY	ANY	ANY	🗞 D.	00
		Allow											Edit

Regola di controllo di accesso FDM

4. Fare clic sulla sezione Criterio file nella regola di accesso e selezionare l'opzione Criterio file preferito dall'elenco a discesa. Fare clic su OK per salvare le modifiche apportate alla regola.

Edit Access Rule		@ ×
Order Title 1 Inside_Outside_Rule Source/Destination Applications URLs I Users I	Action Allow Intrusion Policy	File policy Description Logging
Evaluation Period This feature needs a license to be purchased. For more details, go to Sma SELECT THE FILE POLICY Block Malware All None Block Malware All Cloud Lookup All Block Office Document and PDF Upload, Block Malware Others Block Office Documents Upload, Block Malware Others	rt License.	CONTROLLING FILES AND MALWARE Use file policies to detect malicious software, or malware, using Advanced Malware Protection for Firepower (AMP for Firepower.) You can also use file policies to perform file control, which allows control over all files of a specific type regardless of whether the files contain malware
Show Diagram () 582 Reset () 2023-08-30 09:55:26		CANCEL

Scheda Criterio file delle regole di controllo d'accesso FDM

5. Verificare che il criterio file sia stato applicato alla regola di accesso verificando se l'icona Criterio file è attivata.

Icona Criterio	> 1	Inside_Outside	→ Allow	inside_zone	ANY	ANY	outside_zone	ANY	ANY	ANY	ANY	ANY	Block Malware All
file abilitata													

6. Salvare e distribuire le modifiche al dispositivo gestito.

Test

Per verificare il corretto funzionamento dei criteri file configurati per la protezione da malware, utilizzare questo scenario di test per tentare di scaricare un file di test malware dal browser Web di un host finale.

Come mostrato in questa schermata, il tentativo di scaricare un file di test malware dal Web browser non è riuscito.

6			Problem loading page — Mozilla Firefox				• -	• ×
٠	Problem loading	page ×	+					\sim
~	→ C	③ 10.122.	149.2:8080/eicar/eicar_com.zip	\$	9	\pm	Û	
	The col The col • The • If yo • If yo to a	CONNEC nnection to site could b ou are unable our compute ccess the w	tion was reset while the page was the server was reset while the page was e temporarily unavailable or too busy. Try again e to load any pages, check your computer's net r or network is protected by a firewall or proxy, eb.	loading. in a few moments. work connection. make sure that Firefox is perm Try Age	itted			

Test di download browser

Dalla CLI di FTD, la traccia di supporto del sistema indica che il download del file è stato bloccato dall'elaborazione del file. Per istruzioni su come eseguire una traccia di supporto del sistema tramite la CLI FTD, fare riferimento a questo <u>collegamento</u>.

192.168.0.10-40016 > 10.122.149.2-8080 6 AS 1 I 0 File signature verdict Reject and flags 0x00005A00 for 2546d
cffc5ad854d4ddc64fbf056871cd5a00f2471cb7a5bfd4ac23b6e9eedad of instance 0
192.168.0.10-40016 > 10.122.149.2-8080 6 File Process: drop /eicar/eicar_com.zip
192.168.0.10-40016 > 10.122.149.2-8080 6 IPS Event: gid 147, sid 1, drop
192.168.0.10-40016 > 10.122.149.2-8080 6 AS 1 I 0 File malware event for 2546dcffc5ad854d4ddc64fbf056871cd5a00
f2471cb7a5bfd4ac23b6e9eedad named eicar_com.zip with disposition Malware and action Block Malware
192.168.0.10-40016 > 10.122.149.2-8080 6 AS 1 I 0 Archive childs been processed No
192.168.0.10-40016 > 10.122.149.2-8080 6 Snort detect_drop: gid 147, sid 1, drop
192.168.0.10-40016 > 10.122.149.2-8080 6 AS 1 I 0 deleting firewall session
192.168.0.10-40016 > 10.122.149.2-8080 6 Snort id 0, NAP id 2, IPS id 0, Verdict BLACKLIST
192.168.0.10-40016 > 10.122.149.2-8080 6 ===> Blocked by File Process
verdict reason is sent to DAQ

Test di traccia supporto di sistema

Ciò conferma che la configurazione dei criteri file è riuscita a bloccare il malware.

Risoluzione dei problemi

Se il malware non viene bloccato correttamente durante l'utilizzo delle configurazioni precedenti, fare riferimento ai seguenti suggerimenti per la risoluzione dei problemi:

- 1. Verificare che la licenza malware non sia scaduta.
- 2. Verificare che la regola di controllo di accesso sia destinata al traffico corretto.

3. Conferma che l'opzione criterio file selezionata è corretta per il traffico di destinazione e la protezione da malware desiderata.

Se il problema persiste, contattare Cisco TAC per ulteriore supporto.

Informazioni su questa traduzione

Cisco ha tradotto questo documento utilizzando una combinazione di tecnologie automatiche e umane per offrire ai nostri utenti in tutto il mondo contenuti di supporto nella propria lingua. Si noti che anche la migliore traduzione automatica non sarà mai accurata come quella fornita da un traduttore professionista. Cisco Systems, Inc. non si assume alcuna responsabilità per l'accuratezza di queste traduzioni e consiglia di consultare sempre il documento originale in inglese (disponibile al link fornito).