Konfigurieren von IP-Blacklisting unter Verwendung von Cisco Security Intelligence über ASDM (integriertes Management)

Inhalt

Einführung Voraussetzungen Anforderungen Verwendete Komponenten Hintergrundinformationen Übersicht über Security Intelligence Feed Manuelles Hinzufügen von IP-Adressen zu Global-Blacklist und Global-Whitelist Erstellen der benutzerdefinierten Liste der Blacklist-IP-Adresse Konfigurieren der Sicherheitsintelligenz Bereitstellung einer Zugriffskontrollrichtlinie Ereignisüberwachung durch Security Intelligence Überprüfen Fehlerbehebung Zugehörige Informationen

Einführung

Dieses Dokument beschreibt die Reputation von Cisco Security Intelligence/IP-Adressen und die Konfiguration von IP-Blacklisting (Blockierung) unter Verwendung benutzerdefinierter/automatischer Feeds mit IP-Adressen mit niedriger Reputation.

Voraussetzungen

Anforderungen

Cisco empfiehlt, über Kenntnisse in folgenden Bereichen zu verfügen:

- Kenntnis der ASA-Firewall (Adaptive Security Appliance), ASDM (Adaptive Security Device Manager)
- Fachkenntnis der FirePOWER-Appliance

Hinweis: Für die Filterung von Sicherheitsinformationen ist eine Schutzlizenz erforderlich.

Verwendete Komponenten

Die Informationen in diesem Dokument basieren auf den folgenden Software- und Hardwareversionen:

- ASA FirePOWER-Module (ASA 5506X/5506H-X/5506W-X, ASA 5508-X, ASA 5516-X) mit Softwareversion 5.4.1 und höher
- ASA FirePOWER-Modul (ASA 5515-X, ASA 5525-X, ASA 5545-X, ASA 555-X) mit Softwareversion 6.0.0 und höher

Die Informationen in diesem Dokument wurden von den Geräten in einer bestimmten Laborumgebung erstellt. Alle in diesem Dokument verwendeten Geräte haben mit einer leeren (Standard-)Konfiguration begonnen. Wenn Ihr Netzwerk in Betrieb ist, stellen Sie sicher, dass Sie die potenziellen Auswirkungen eines Befehls verstehen.

Hintergrundinformationen

Cisco Security Intelligence besteht aus mehreren regelmäßig aktualisierten Auflistungen von IP-Adressen, die vom Cisco TALOS-Team als schlecht bekannt eingestuft werden. Das Cisco TALOS-Team ermittelt die geringe Reputation, wenn schädliche Aktivitäten von IP-Adressen wie Spam, Malware, Phishing-Angriffe usw. ausgehen.

Cisco IP Security Intelligence Feed verfolgt die Datenbank von Angreifern, Bogon, Bots, CnC, DGA, ExploitKit, Malware, Open_Proxy, Open_Relay, Phishing, Response, Spam, Verdächtig. Das FirePOWER-Modul bietet die Möglichkeit, einen benutzerdefinierten Feed mit IP-Adresse in niedriger Reputation zu erstellen.

Übersicht über Security Intelligence Feed

Im Folgenden finden Sie einige weitere Informationen über den Typ der IP-Adresserfassungen, die in den Sicherheitsinformationen als unterschiedliche Kategorien klassifiziert werden können.

Angreifer: Eine Sammlung von IP-Adressen, die ständig nach Schwachstellen durchsucht werden oder versuchen, andere Systeme auszunutzen.

Malware: Eine Sammlung von IP-Adressen, die versuchen, Malware zu verbreiten, oder aktiv jeden angreifen, der sie besucht.

Phishing: Sammlung von Hosts, die Benutzer aktiv dazu verleiten sollen, vertrauliche Informationen wie Benutzernamen und Kennwörter einzugeben.

Spam: Sammlung von Hosts, die als Quelle für das Senden von Spam-E-Mail-Nachrichten identifiziert wurden.

Bots: Eine Auflistung von Hosts, die aktiv als Teil eines Botnets beteiligt sind und von einem bekannten Botnet-Controller gesteuert werden.

CnC: Sammlung von Hosts, die als die Kontrollserver für ein bekanntes Botnet identifiziert wurden.

OpenProxy: Eine Auflistung von Hosts, die bekannte Open Web Proxies ausführen und anonyme Webbrowserdienste anbieten.

OpenRelay: Eine Sammlung von Hosts, die bekannte anonyme E-Mail-Weiterleitungsdienste anbieten, die von Spam- und Phishing-Angreifern verwendet werden.

TorExitNode: Sammlung von Hosts, die bekanntermaßen Exit Node Services für das Tor Anonymizer Netzwerk anbieten.

Bogon: Sammlung von IP-Adressen, die nicht zugewiesen sind, aber Datenverkehr senden.

Verdächtig: Erfassung von IP-Adressen, die verdächtige Aktivitäten anzeigen und aktiv untersucht werden.

Antwort: Sammlung von IP-Adressen, die wiederholt bei verdächtigem oder schädlichem Verhalten beobachtet wurden.

Manuelles Hinzufügen von IP-Adressen zu Global-Blacklist und Global-Whitelist

Mit dem FirePOWER-Modul können Sie Global-Blacklist bestimmte IP-Adressen hinzufügen, wenn Sie wissen, dass diese Teil einer bösartigen Aktivität sind. IP-Adressen können auch Global-Whitelist hinzugefügt werden, wenn Sie den Datenverkehr an bestimmte IP-Adressen zulassen möchten, die von Blacklist-IP-Adressen blockiert werden. Wenn Sie Global-Blacklist/Global-Whitelist eine IP-Adresse hinzufügen, wird diese sofort wirksam, ohne dass die Richtlinie angewendet werden muss.

Um die IP-Adresse Global-Blacklist/Global-Whitelist hinzuzufügen, navigieren Sie zu **Monitoring > ASA FirePOWER Monitoring > Real Time Event**, bewegen Sie die Maus über Verbindungsereignisse, und wählen Sie **Details anzeigen aus**.

Sie können der Global-Blacklist/Global-Whitelist entweder die Quell- oder Ziel-IP-Adresse hinzufügen. Klicken Sie auf die Schaltfläche **Bearbeiten** und wählen Sie **Whitelist Now/Blacklist Now**, um die IP-Adresse der entsprechenden Liste hinzuzufügen, wie im Bild gezeigt.

All ASA FirePOWER EV	ents Connection Intrusion	File Malware File	Security Intelligence	
Filter				
Rule Action=Allow *				
(
R Paulas - Paríod	5.1. (F			
Refrest	Rate 5 seconds	* 1/25/16 9:11:2	5 AM (151)	
Receive Times	Action	First Packet	Last Packet	Reaso
1/25/16 9:09:50 AM	Allow	1/25/16 9:09:48 AM	1/25/16 9:09:49 AM	
1/25/16 9:07:36 AM	Allow	View de 1/25/16 9:07:03 AM	tails 1/25/16 9:07:03 AM	
1/25/16 0.07.07 AM	411	1/25/15 0.07-05 114	1/25/16 0.07.05 114	
	Allow	1/25/16 9:07:06 AM	1/25/16 9:07:06 AM	
1/25/16 9:07:07 AM				
oring > ASA FirePOWER M	onitoring > Real Time Even	tina		
oring > ASA FirePOWER Mo	onitoring > Real Time Even	ting		
ime Eventing	onitoring > Real Time Even	ting Responder	Edit	
ime Eventing Initiator Initiator IP	nitoring > Real Time Event	ting Responder Responder IP	Edit 10.106.44.5	•
ime Eventing Initiator Initiator IP Initiator Country and Continent	192.168.20.3 not available Blacklist Now	ting Responder Responder IP Responder Count Continent	Edit 10.106.44.5 try and <i>not available</i>	

Um zu überprüfen, ob die Quell- oder Ziel-IP-Adresse der Global-Blacklist/Global-Whitelist hinzugefügt wurde, navigieren Sie zu **Configuration > ASA Firepower Configuration > Object Management > Security Intelligence > Network Lists and Feeds** und bearbeiten Sie Global-Blacklist/Global Whitelist. Sie können auch die Schaltfläche Löschen verwenden, um alle IP-Adressen aus der Liste zu entfernen.

Erstellen der benutzerdefinierten Liste der Blacklist-IP-Adresse

Mit FirePOWER können Sie eine benutzerdefinierte Netzwerk-/IP-Adressenliste erstellen, die in Blacklists (Blockierungen) verwendet werden kann. Sie haben drei Möglichkeiten:

- Sie können die IP-Adressen in eine Textdatei schreiben (eine IP-Adresse pro Leitung) und die Datei in das FirePOWER-Modul hochladen. Um die Datei hochzuladen, navigieren Sie zu Configuration > ASA FirePOWER Configuration > Object Management > Security Intelligence > Network Lists and Feeds und klicken Sie dann auf Add Network Lists and Feeds (Netzwerklisten und -Feeds hinzufügen). Name: Geben Sie den Namen der benutzerdefinierten Liste an. Typ: Wählen Sie List aus der Dropdown-Liste aus. Upload-Liste: Wählen Sie Durchsuchen, um die Textdatei in Ihrem System zu suchen. Wählen Sie die Option Hochladen aus, um die Datei hochzuladen.
- Sie können eine beliebige IP-Datenbank eines Drittanbieters für die benutzerdefinierte Liste verwenden, für die das FirePOWER-Modul den Drittanbieter-Server kontaktiert, um die IP-Adressliste abzurufen. Um dies zu konfigurieren, navigieren Sie zu Configuration > ASA

FirePOWER Configuration > Object Management > Security Intelligence > Network Lists and Feeds und klicken Sie dann auf Add Network Lists and Feeds (Netzwerklisten und -Feeds hinzufügen).

Name: Geben Sie den Namen des benutzerdefinierten Feeds an.

Typ: Wählen Sie Option Feed aus der Dropdown-Liste aus.

Feed-URL: Geben Sie die URL des Servers an, zu dem das FirePOWER-Modul eine Verbindung herstellen soll, und laden Sie den Feed herunter.

MD5-URL: Geben Sie den Hashwert an, um den URL-Pfad für den Feed zu validieren.

Aktualisierungshäufigkeit: Geben Sie das Zeitintervall an, in dem das System eine Verbindung zum URL-Feed-Server herstellt.

		Update Feeds	d Fe
Name	Security Intell	igence for Network List / Feed	1
Cisco-Intelligence-Feed Last Updated: 2016-01-22 05:56.	Name:	Custom_Feed	
Custom_Feed	Type:	List	
Global-Blacklist	Upload	C: (lakepath (custom_IP_reed.	wse
Global-Whitelist			
iguration > ASA FirePOWER Configurat	ion > Object Managemer	Store ASA FirePOWER Changes Car nt > SecurityIntelligence > Network Lists and F	ncel Fee
iguration > ASA FirePOWER Configurat	ion > Object Managemer	Store ASA FirePOWER Changes Car Ant > SecurityIntelligence > Network Lists and F Jpdate Feeds O Add Network Lists and general for Network List / Feed	Feed Feed
iguration > ASA FirePOWER Configurat	ion > Object Managemer	Store ASA FirePOWER Changes Car nt > SecurityIntelligence > Network Lists and F Jpdate Feeds O Add Network Lists and gence for Network List / Feed	Feed Feed
iguration > ASA FirePOWER Configurat Name Cisco-Intelligence-Feed Last Updated: 2016-01-22 05:56:	ion > Object Managemer Security Intelli Name:	Store ASA FirePOWER Changes Car Ant > SecurityIntelligence > Network Lists and F Jpdate Feeds O Add Network Lists and gence for Network List / Feed Custom_Network_Feed	Feed d Feed
iguration > ASA FirePOWER Configurat Name Cisco-Intelligence-Feed Last Updated: 2016-01-22 05:56: Custom_Feed	ion > Object Managemen Security Intelli Name: Type:	Store ASA FirePOWER Changes Car Ant > SecurityIntelligence > Network Lists and F Jpdate Feeds Add Network Lists and gence for Network List / Feed Custom_Network_Feed Feed	Feed d Feed
iguration > ASA FirePOWER Configurat Name Cisco-Intelligence-Feed <i>Last Updated: 2016-01-22 05:56:</i> Custom_Feed Global-Blacklist	ion > Object Managemen Security Intelli Name: Type: Feed URL:	Store ASA FirePOWER Changes Car Int > SecurityIntelligence > Network Lists and F Update Feeds Add Network Lists and gence for Network List / Feed Custom_Network_Feed Feed http://192.168.30.1/blacklist-IP.txt	ncel Feed
iguration > ASA FirePOWER Configurat Name Cisco-Intelligence-Feed <i>Last Updated: 2016-01-22 05:56:</i> Custom_Feed Global-Blacklist	ion > Object Managemen Security Intelli Name: Type: Feed URL: MD5 URL:	Store ASA FirePOWER Changes Car Int > SecurityIntelligence > Network Lists and R Jpdate Feeds Add Network Lists and gence for Network List / Feed Custom_Network_Feed Feed http://192.168.30.1/blacklist-IP.txt (optional)	Feed d Feed

Konfigurieren der Sicherheitsintelligenz

Navigieren Sie zum Konfigurieren von Sicherheitsinformationen zu Configuration > ASA

FirePOWER Configuration > Policies > Access Control Policy (Konfiguration > ASA FirePOWER-Konfiguration > Richtlinien > Zugriffskontrollrichtlinie), und wählen Sie die Registerkarte Security Intelligence aus.

Wählen Sie den Feed aus dem Network Available Object (Netzwerk verfügbar) aus, und wechseln Sie zur Whitelist/Blacklist-Spalte, um die Verbindung zur schädlichen IP-Adresse zuzulassen/zu blockieren.

Sie können auf das Symbol klicken und die Protokollierung aktivieren, wie im Bild angegeben.

Wenn Sie das Ereignis nur für schädliche IP-Verbindungen generieren möchten, statt die Verbindung zu blockieren, klicken Sie mit der rechten Maustaste auf den Feed, und wählen Sie **Monitor-only (Nur Monitor) (nicht blockieren)** aus, wie im Bild gezeigt:

efault Allow All Traffic			You have unsaved chan
	1	Status: Policy Up-to-date on device	
Initity Policy: None SSL Policy: Default SSL Policy Initity Policy: None HTTP Responses Initity Policy: None HTTP Responses Advance Available Zones	ed	DNS Policy: Default DNS Policy	
Search for a Network		Whitelist (2)	Blacklist (7) Enable loggi
Networks URLs		Networks	Networks 📄
Attackers	()	😴 Global-Whitelist (Any Zone) 📋	🔞 Global-Blacklist (Any Zone) 💢
Bogon	Add to Whitelist		Pata (Any Zone)
Bots	Add to	Global-Whitelist-for-URL (Any	Bots (Any Zone)
P CnC	Blacklist		Block
			Monitor-only (do not bloc
Open_proxy Open_relay			UR Logging Options
Phishing			Select All
· · · · · · · · · · · · · · · · · · ·			Delete

Wählen Sie Option Store ASA FirePOWER Changes, um die Änderungen an AC-Richtlinien zu speichern.

Bereitstellung einer Zugriffskontrollrichtlinie

Damit die Änderungen wirksam werden, müssen Sie die Zugriffskontrollrichtlinie bereitstellen. Bevor Sie die Richtlinie anwenden, sehen Sie einen Hinweis darauf, dass die Zugriffskontrollrichtlinie auf dem Gerät veraltet ist.

Um die Änderungen am Sensor bereitzustellen, cKlicken Sie auf **Deploy** und wählen Sie **Deploy FirePOWER Changes aus.** Wählen Sie anschließend **Deploy** im Popup-Fenster aus, um die Änderungen bereitzustellen.

File View Tools Wizards Window	Help
Add Delete Connect Find:	2 Deploy FirePOWER Changes Ctrl+D Save Running Configuration to Flash Ctrl+S
Deploy FirePOWER Changes	
Deploy Policies Version:2016-03 System Policy: Default Sensor Policy: firepower Access Control Policy: Default Allow A Access Control Policy: Default Allow A - Intrusion Policy: Balanced Security - Intrusion Policy: IPS_Policy DNS Policy: Default DNS Policy	I -05 09:09 AM ?
	3 Deploy Cancel

Hinweis: In Version 5.4.x müssen Sie auf ASA FirePOWER-Änderungen anwenden klicken, um die Zugriffsrichtlinie auf den Sensor anzuwenden.

Hinweis: Navigieren Sie zu Monitoring > ASA FirePOWER Monitoring > Task Status. Stellen Sie sicher, dass die Aufgabe

abgeschlossen sein muss, um die Konfigurationsänderungen anzuwenden. Ereignisüberwachung durch

Security Intelligence Um die Sicherheitsintelligenz des FirePOWER-Moduls anzuzeigen, navigieren Sie zu Monitoring > ASA FirePOWER Monitoring > Real Time Event. Wählen Sie die Registerkarte Sicherheitsintelligenz aus. Es werden die Ereignisse angezeigt, wie im Bild gezeigt:

oring > ASA FirePOWER Monit	oring > Real Time Eve	enting				
Time Eventing						
All A FirePOWER Event	s Connection Intrusi	ion File Malware File	Security Intelligence			
Filter						
Enter filter criteria						
Pause Refresh Ra	te 5 seconds	• 2/9/16 1:03:31	PM (IST)			
Receive Times	Action	First Packet	Last Packet	Reason	Initiator IP	Responder IP
2/9/16 1:01:48 PM	Block	2/9/16 1:01:47 PM		IP Block	192.168.20.3	184.26.162.43

ÜberprüfenFür diese Konfiguration ist derzeit kein Überprüfungsverfahren

verfügbar. FehlerbehebungUm sicherzustellen, dass die Sicherheitsinformations-Feeds

auf dem neuesten Stand sind, navigieren Sie zu Configuration > ASA FirePOWER Configuration > Object Management > Security Intelligence > Network Lists and Feeds und überprüfen Sie die Uhrzeit, zu der der Feed zuletzt aktualisiert wurde. Sie können die Schaltfläche Bearbeiten auswählen, um die Häufigkeit der Feed-Updates

festzulegen.

Update Feeds O Add Network Lists and Feeds				
Name	Туре			
Cisco-Intelligence-Feed Last Updated: 2016-02-08 10:03:14	Feed	Ø		
Custom_Feed	Feed	Ø		
Global-Blacklist	List	Ø		
Global-Whitelist	List	0		

Stellen Sie sicher, dass die Bereitstellung der Zugriffskontrollrichtlinie erfolgreich abgeschlossen wurde. Überwachen Sie die Sicherheitsinformationen, um festzustellen, ob der Datenverkehr blockiert wird oder nicht. **Zugehörige Informationen**

- Cisco ASA FirePOWER-Modul Kurzreferenz
- Technischer Support und Dokumentation Cisco Systems