Bestimmen des von einer bestimmten Snort-Instanz verarbeiteten Datenverkehrs

Inhalt

 Einleitung

 Voraussetzungen

 Anforderungen

 Verwendete Komponenten

 1. Verwenden von CLI-Befehlen

 2. Verwendung von FirePOWER Management Center (FMC)

 3. Verwenden von Syslog und SNMP

 4. Verwenden der benutzerdefinierten Skripte

Einleitung

In diesem Dokument wird beschrieben, wie der Datenverkehr bestimmt wird, der von einer bestimmten Snort-Instanz in einer Cisco FirePOWER Threat Defense (FTD)-Umgebung verarbeitet wird.

Voraussetzungen

Anforderungen

Cisco empfiehlt, dass Sie mit den folgenden Produkten vertraut sind:

- Secure FirePOWER Management Center (FMC)
- Sicherer Schutz vor Bedrohungen mit Firepower (FTD)
- Syslog und SNMP
- REST-API

Verwendete Komponenten

Die Informationen in diesem Dokument beziehen sich auf Geräte in einer speziell eingerichteten Testumgebung. Alle in diesem Dokument verwendeten Geräte begannen mit einer gelöschten (Standard-)Konfiguration. Wenn Ihr Netzwerk in Betrieb ist, stellen Sie sicher, dass Sie die möglichen Auswirkungen aller Befehle kennen.

1. Verwenden von CLI-Befehlen

Über die Befehlszeilenschnittstelle (CLI) Ihres FTD-Geräts können Sie auf detaillierte Informationen über Snort-Instanzen und den von ihnen verarbeiteten Datenverkehr zugreifen.

• Dieser Befehl liefert die Details zu den ausgeführten Snort-Prozessen.

show snort instances

Hier ist ein Beispiel für die Befehlsausgabe.

> show snort instances

Total number of instances available - 1 +-----+ | INSTANCE | PID | +----+ | 1 | 4765 | <<<< One instance available and its process ID +-----+

• Für detailliertere Informationen zu den von Snort-Instanzen verarbeiteten Datenverkehrsstatistiken können diese Befehle verwendet werden. Es werden verschiedene Statistiken angezeigt, z. B. die Anzahl der verarbeiteten und verworfenen Pakete sowie die von jeder Snort-Instanz generierten Warnungen.

show snort statistics

Hier ist ein Beispiel für die Befehlsausgabe.

> show snort statistics Packet Counters: Passed Packets			3791881977 Blocked					
Packets 707722 Injected Packets			87 Packets bypassed (Snort					
Down) 253403701 <<< Packets by		<	d Packets bypassed (Snort Busy) 0 Flow C					
Forwarded Flows		294816 Blacklisted Flows	227 Miscellar	neous Counters: Start-of-Flow				
events 0 End-of-Flow events			317032 Denied flow events142					
Frames forwarded to	Snort before drop	0 Inject packets dropped	0 TCP Ack bypas	SS				
Packets	6412936 T	CP Meta-Ack Packets	2729907 Portscan Events	s 0				
Packet decode optim	nized	21608793 Packet decode leg	acy 6558642					

show asp inspect-dp snort

Hier ist ein Beispiel für die Befehlsausgabe.

> show asp inspect-dp snort

SNORT Inspect Instance Status Info Id Pid ------0 16450 8% (7% 0%) 2.2 K 0 READY 1 16453 9% (8% 0%) 2.2 K 0 READY 2 16451 6% (5% | 1%) 2.3 READY 3 16454 5% (5% 0%) 2.2 K 1 READY 4 16456 6% (6% | 0%) 2.3 K 0 0 READY 5 16457 6% (Κ READY 6 16458 6% (5% | 0%) 2.2 K 1 READY 7 16459 4% (4% 0%) 2.3 K 0 6% 0%) 2.3 K 0 **READY 8** 16452 9% (8% 1%) 2.2 K 0 READY 9 16455 100% (100% 0%) 2.2 K 5 READY <<<< High CPU utilization 10 16460 7% (6% 0%) 2.2 K 0 READY -- ---- Summary 15% (14% 0%) 24.6 K 7

2. Verwendung von FirePOWER Management Center (FMC)

Wenn Sie Ihre FTD-Geräte über FMC verwalten, können Sie über die Webschnittstelle detaillierte Informationen und Berichte zum Datenverkehr und zu Snort-Instanzen abrufen.

• Überwachung

FMC Dashboard: Navigieren Sie zum Dashboard, wo Sie eine Übersicht über den Systemstatus einschließlich der Snort-Instanzen sehen können.

Health Monitoring: Im Abschnitt Health Monitoring können Sie detaillierte Statistiken zu Snort-Prozessen abrufen, einschließlich des verarbeiteten Datenverkehrs.

Analyse

Analyse: Navigieren Sie zu Analyse > Verbindungsereignisse.

Filter: Verwenden Sie Filter, um die Daten auf die jeweilige Snort-Instanz oder den Datenverkehr einzugrenzen, für den Sie sich interessieren.

	Firewall Ma Analysis / Conr	anageme nections / Ev	ent Cent	ter	Overview	Analysis	Policie	s Devices	s Objects	Integratio	n
								Book	mark This Page	e Reporting Da	ashboard
Con	Connection Events (switch workflow)										
No Se	No Search Constraints (Edit Search)										
Con	Connections with Application Details Table View of Connection Events										
Jum	Jump to										
) ↓ First Packet ×	Last Packet ×	Action ×	Reason ×	Initiator × IP	Initiator × Country ×	Initiator × User ×	Responder _X IP	Responder × Country	Security Intelligence × Category	Ingress Security Zone

Verbindungsereignisse

Firewall Manageme	Overview	Analysis	Policies	Devices	Objects	Integration	
Connection Events	Search						
Sections	(unnamed s	earch)					
General Information	Device						
Geolocation		Device*				device1.examp	le.com, *.example.com, 192.1
Device		Ingress Interface				s1p1	
Application		Egress Interface				s1p1	
URL	Ingress	/ Egress Interface				s1p1	
Netflow	Г						
QoS		Snort Instance ID					

Snort-Instanz-ID

3. Verwenden von Syslog und SNMP

Sie können Ihren FTD so konfigurieren, dass er Syslog-Meldungen oder SNMP-Traps an ein externes Überwachungssystem sendet, wo Sie die Datenverkehrsdaten analysieren können.

Syslog-Konfiguration

Geräte: Navigieren Sie in FMC zu Geräte > Plattformeinstellungen.

Erstellen oder Bearbeiten einer Richtlinie: Wählen Sie die entsprechende Richtlinie für die Plattformeinstellungen aus.

Syslog: Konfigurieren Sie die Syslog-Einstellungen so, dass sie Snort-Warnungen und -Statistiken enthalten.

Firewall Managemer	nt Center Over	view Analysis	Policies	Devices Obj	ects Integ	ration	Deploy	Q 🧬 🌣	admin ✓ intervent secure secure
test									Save Cancel
Enter Description									
									Policy Assignments (0
ARP Inspection	Logging Setup L	ogging Destinations	Email Setup	Event Lists	Rate Limit	Syslog Settings	Syslog Se	rvers	
Banner	Basic Logging Settin	igs							
DNS	Enable Logging								
External Authentication	Enable Logging on	the failover standby uni	t						
Fragment Settings	Send syslogs in EM	IBLEM format							
HTTP Access	Send debug messa	iges as syslogs							
ICMP Access	Memory Size of the Inte	ernal Buffer							
SSH Access	4096								
SMTP Server									
SNMP									
SSL	VPN Logging Setting	js							
Syslog	Enable Logging to F	Firewall Management C	enter						
Timeouts	Logging Level								
Time Synchronization	errors	▼							
Time Zone	Specify ETD Server	nformation							
UCAPL/CC Compliance	Specity PTP Server I	mormation							

SNMP-Konfiguration

SNMP-Einstellungen: Ähnlich wie bei Syslog müssen Sie die SNMP-Einstellungen unter Geräte > Plattformeinstellungen konfigurieren.

Traps: Stellen Sie sicher, dass die erforderlichen SNMP-Traps für die Snort-Instanzstatistik aktiviert sind.

Firewall Managemen	t Center Overview	Analysis	Policies	Devices	Objects	Integration
test						
Enter Description						
ARP Inspection	Enable SNMP Servers	7				
Banner	Read Community String	_				
DNS						
External Authentication	Confirm					
Fragment Settings						
HTTP Access	System Administrator Name	•				
ICMP Access						
SSH Access	Location					
SMTP Server						
SNMP	Listen Port					
SSL	161					

SNMP-Konfiguration

4. Verwenden der benutzerdefinierten Skripte

Für fortgeschrittene Benutzer können Sie benutzerdefinierte Skripte schreiben, die die FTD REST API verwenden, um Statistiken über Snort-Instanzen zu sammeln. Für diesen Ansatz müssen Sie mit Skripting und der API-Verwendung vertraut sein.

REST-API

API-Zugriff: Stellen Sie sicher, dass der API-Zugriff auf Ihrem FMC aktiviert ist.

API-Aufrufe: Verwenden Sie die entsprechenden API-Aufrufe, um Snort-Statistiken und Datenverkehrsdaten abzurufen.

Dadurch werden JSON-Daten zurückgegeben, die Sie analysieren und so den von bestimmten Snort-Instanzen verarbeiteten Datenverkehr bestimmen können.

Durch die Kombination dieser Methoden erhalten Sie ein umfassendes Verständnis des Datenverkehrs, der von jeder Snort-Instanz in Ihrer Cisco FTD-Bereitstellung verarbeitet wird.

Informationen zu dieser Übersetzung

Cisco hat dieses Dokument maschinell übersetzen und von einem menschlichen Übersetzer editieren und korrigieren lassen, um unseren Benutzern auf der ganzen Welt Support-Inhalte in ihrer eigenen Sprache zu bieten. Bitte beachten Sie, dass selbst die beste maschinelle Übersetzung nicht so genau ist wie eine von einem professionellen Übersetzer angefertigte. Cisco Systems, Inc. übernimmt keine Haftung für die Richtigkeit dieser Übersetzungen und empfiehlt, immer das englische Originaldokument (siehe bereitgestellter Link) heranzuziehen.