Inloggen van FirePOWER-module voor systeem/verkeersgebeurtenissen configureren met ASDM (on-box beheer)

Inhoud

Inleiding Voorwaarden Vereisten Gebruikte componenten Achtergrondinformatie Configureren Een uitvoerbestemming configureren Stap 1. Configuratie van Syrische server Stap 2.SNMP-serverconfiguratie Configuratie voor het verzenden van verkeersgebeurtenissen Schakel externe loggen in voor verbindingsgebeurtenissen Schakel externe houtkap in voor inbraakgebeurtenissen Schakel externe vastlegging voor IP-beveiligingsinlichtingen/DNS-beveiligingsinlichtingen/URLbeveiligingsinlichtingen in Schakel extern loggen op SSL-gebeurtenissen in Configuratie voor het verzenden van de systeemgebeurtenissen Schakel externe loggen in voor systeemgebeurtenissen Verifiëren Problemen oplossen Gerelateerde informatie Gerelateerde Cisco Support Community-discussies

Inleiding

In dit document worden het systeem/de verkeersgebeurtenissen van de Firepower Module beschreven en verschillende manieren beschreven om deze gebeurtenissen naar een externe logserver te sturen.

Voorwaarden

Vereisten

Cisco raadt kennis van de volgende onderwerpen aan:

 Kennis van ASA (adaptieve security applicatie) firewall, ASDM (adaptieve security applicatie Manager).

- Kennis van FirePOWER-apparaat.
- Syslog, SNMP protocol kennis.

Gebruikte componenten

De informatie in dit document is gebaseerd op de volgende software- en hardware-versies:

- ASA 5506X/5506H-X/5506W-X, ASA 5508-X, ASA 5516-X) software versie 5.4.1 en hoger.
- ASA 5515-X, ASA 5525-X, ASA 5545-X, ASA 5555-X) software versie 6.0.0 en hoger.
- ASDM 7.5(1) en hoger.

De informatie in dit document is gebaseerd op de apparaten in een specifieke laboratoriumomgeving. Alle apparaten die in dit document worden beschreven, hadden een opgeschoonde (standaard)configuratie. Als uw netwerk live is, moet u de potentiële impact van elke opdracht begrijpen.

Achtergrondinformatie

Soort gebeurtenissen

Gebeurtenissen in de FirePOWER Module kunnen in twee typen worden gecategoriseerd:-

- 1. Verkeersgebeurtenissen (Connection gebeurtenissen/inbraakgebeurtenissen/security inlichtingengebeurtenissen/SSL-gebeurtenissen/Malware/File Events).
- 2. systeemgebeurtenissen (Firepower Operating System (OS)).

Configureren

Een uitvoerbestemming configureren

Stap 1. Configuratie van Syrische server

Als u een Syrische server wilt configureren voor verkeersgebeurtenissen, navigeer dan naar Configuration > ASA Firepower Configuration > Policy > Actions en klik op het vervolgkeuzemenu Maken en kies optie Syslog Alert maken. Voer de waarden in voor de snelserver.

Naam: Specificeer de naam die uniek de systeemserver identificeert.

Host: Specificeer het IP-adres/hostnaam van de Syrische server.

Poorten: Specificeer het poortnummer van de Syrische server.

Faciliteit: Selecteer een voorziening die is ingesteld op uw Syrische server.

Ernst: Selecteer een prioriteit die op de systeemserver is ingesteld.

Markering: Geef een tag op die u met het waarschuwingsbericht wilt weergeven.

Gisco ASDM 7.5(2) for ASA - 192.168.20.1						• 🗙
File View Tools Wizards Window	Help		Type topic to sear	ch	Go	aha
Home 🖏 Configuration 🔯 Monitoring	g 🔚 Deploy 👻 🔇 Refresh 🚺 B	ack 🔘 Forward 🖓 Help			CIS	co
Device List Bookmarks Cont	figuration > ASA FirePOWER Configura	ation > Policies > Actions Alerts				
Device List D P X						
🕈 Add 📋 Delete 🚿 Connect	Alerts					
Find: Go				0	Create Alert	Ŧ
	Name		Туре	In Use	Enabled	
ASA FirePOWER Configur 🗇 🕂						
Policies	Edit Syslog	Alert Configuration		? X		
Access Control Policy						
	Name	Syslog_Server				
	Host	192.168.20.3				
Files	Port	514		_		
Actions Alerts	Facility	ALERT		T		
DNS Policy	Severity					
Device Management	Sevency					
Device	Tag			_		
Device Setup						
Firewall		Store ASA FirePOWE	R Changes Ca	ancel		

Stap 2.SNMP-serverconfiguratie

Als u een SNMP-trap-server voor verkeersgebeurtenissen wilt configureren, navigeer dan naar ASDM-configuratie > ASA Firepower Configuration > Policy > Action Alerts en klik op het vervolgkeuzemenu Waarschuwen kies optie SNMP-waarschuwing maken.

Naam: Specificeer de naam die uniek de SNMP Trap server identificeert.

Trap Server: Specificeer IP-adres/hostnaam van SNMP-valserver.

Versie: Firepower Module ondersteunt SNMP v1/v2/v3. Selecteer de SNMP versie in het uitrolmenu.

Community-string: Als u v1 of v2 selecteert in de optie **Versie**, geeft u de SNMP-community-naam op.

Gebruikersnaam: Als u v3 in de optie **Versie** selecteert, wordt het **veld Gebruikersnaam** gevraagd. Specificeer de gebruikersnaam.

Verificatie: Deze optie maakt deel uit van de SNMP v3-configuratie. Het biedt authenticatie gebaseerd op Hash

algoritme met MD5 of SHA. Selecteer in **het** uitrolmenu **Protocol** de hashalgoritme en voer het volgende in

Wachtwoord in optie Wachtwoord. Als u deze optie niet wilt gebruiken, selecteert u geen optie.

Privacy: Deze optie maakt deel uit van de SNMP v3-configuratie. Het verstrekt encryptie met DES algoritme. Selecteer in **het** vervolgkeuzemenu de optie als **DES** en voer een wachtwoord in het veld **Wachtwoord in**. Als u geen coderingsfunctie wilt gebruiken, kiest u **geen** optie.

Alerts	ç			-	
	Edit SNMP AI	ert Configuration SNMP Version V1/V2	? ×	•	Create Alert 🔹
Name	Name	SNMP_SERVER_1		Use	Enabled
Syslog_Server	Trap Server	192.168.20.4		t Used	~
	Version	v2	T		
	Community String	Secret			
		Store ASA FirePOWER Changes	Cancel		
Alerts					
	Edit SNMP AI	ert Configuration SNMP Version V3	? ×	0	Create Alert 🔹
Name	Name	SNMP_SERVER_1		Use	Enabled
Syslog_Server	Trap Server	192.168.20.4		t Used	
	Version	v3	•		
	User Name	user1			
	Authenticatio	n			
	Protocol	MD5	•		
	Password	•••••			
	Privacy				
	Protocol	DES	T		
	Password	•••••			
	Engine ID	Europela: 122456780a			
	Lingine ID	Example: 123456789a			
		Store ASA FIREPOWER Changes	10		

Configuratie voor het verzenden van verkeersgebeurtenissen

Schakel externe loggen in voor verbindingsgebeurtenissen

Er worden verbindingsgebeurtenissen gegenereerd wanneer het verkeer een toegangsregel raakt met de mogelijkheid van het registreren. Om de externe houtkap voor verbindingsgebeurtenissen mogelijk te maken, navigeer naar (ASDM Configuration > ASA Firepower Configuration > Policy > Access Control Policy) de toegangsregel en navigeer naar logging optie.

Selecteer de logoptie **loggen aan het begin en eind van de verbinding** of **loggen aan het eind van de verbinding**. Navigeer om **verbindingsgebeurtenissen naar** optie **te verzenden** en specificeer waar u gebeurtenissen wilt verzenden.

Als u gebeurtenissen naar een externe Syrische server wilt doorsturen, selecteert u **Syslog** en vervolgens selecteert u een waarschuwingsrespons in de vervolgkeuzelijst. U kunt desgewenst een waarschuwingsbericht toevoegen door op het **pictogram** toevoegen te klikken.

Als u verbindingsgebeurtenissen naar een SNMP-valserver wilt doorsturen, selecteert u **SNMPtrap** en vervolgens selecteert u een SNMP-alarmrespons in de vervolgkeuzelijst. U kunt desgewenst een SNMP-alarmrespons toevoegen door op het **pictogram** toevoegen te klikken.

ASA HIPPOWER	
Editing Rule - WebsiteBlock	
Name WebsiteBlock 🕑 Enabled Move	
Action X Block with reset IPS: no policies Variables: n/a Files: no inspection Logging: connections: Event Viewer, s	syslog,
Zones Networks 🔺 Users Applications Ports URLs 🔺 ISE Attributes Inspection Log	ging
Log at Beginning and End of Connection	
O Log at End of Connection	
O No Logging at Connection	
File Events:	
Log Files	
Send Connection Events to:	
✓ Event Viewer	
Syslog (Connection Event only) Syslog_Server	
SNMP Trap SNMP_SERVER_1	
Save	

Schakel externe houtkap in voor inbraakgebeurtenissen

Inbraakgebeurtenissen worden gegenereerd wanneer een signatuur (korte regels) met een of ander kwaadaardig verkeer overeenkomt. Om de externe houtkap voor inbraakgebeurtenissen mogelijk te maken, kunt u navigeren naar **ASDM Configuration > ASA Firepower Configuration > Policy > Inbraakbeleid > Inbraakbeleid.** Maak een nieuw inbraakbeleid of bewerk het bestaande inbraakbeleid.Navigeer naar **geavanceerde instelling > Externe reacties.**

Als u inbraakgebeurtenissen naar een externe SNMP-server wilt doorsturen, selecteert u de optie **Ingeschakeld** in **SNMP-signalering** en vervolgens klikt u op de optie **Bewerken**.

Type trap: Het type val wordt gebruikt voor IP-adressen die in de waarschuwingen verschijnen. Als uw netwerkbeheersysteem correct het INET_IPV4 adrestype teruggeeft, kunt u als Binair selecteren. Anders selecteert u als string.

SNMP versie: Selecteer een van Versie 2 of Versie 3 radioknop.

SNMP v2-optie

Trap Server: Specificeer het IP-adres/hostname van SNMP Trap server, zoals in deze afbeelding.

Gemeenschap-string: Specificeer de community-naam.

SNMP v3-optie

Trap Server: Specificeer het IP-adres/hostname van SNMP Trap server, zoals in deze afbeelding.

Verificatiewachtwoord: Opgevenwachtwoord vereist voor verificatie. SNMP v3 gebruikt de hashfunctie om het wachtwoord te authentiseren.

Private Wachtwoord: Wachtwoord voor codering opgeven. SNMP v3 maakt gebruik van het

blokalgoritme Data Encryption Standard (DES) om dit wachtwoord te versleutelen.

Gebruikersnaam: Specificeer de gebruikersnaam.

onfiguration > ASA FirePOWER Config	iguration > Policies > Intrusion Policy > Intrusion Policy		
Policy Information	SNMP Alerting	< Back	
Rules	Settings		
 Advanced Settings 	Trap Type 💿 as Binary 🔘 as String		
Global Rule Thresholding	SNMP Version Version Version 3		
SNMP Alerting			
Policy Layers	SNMP v2		
	Trap Server 192.168.20.3		
	Community String Secret		
Policy Information 🖄	SNMP Alerting	< Back	
Policy Information	SNMP Alerting	< Back	
Advanced Settings	Settings		
Global Rule Thresholding	Trap Type 💿 as Binary 🔘 as String		
SNMP Alerting	SNMP Version O Version2 Version3		
Policy Layers	SNMP v3		
	Trap Server 192.168.20.3		
	Authentication Password		
	Private Password (SNMP v3 passwords must be 8 or more characters)		
	Username user3		
	Revert to Defaults		

Selecteer de optie om inbraakgebeurtenissen naar een externe SLOG-server te verzenden **Ingeschakeld** in **Syslog waarschuwing** klik vervolgens op **Bewerken** zoals in deze afbeelding.

Logging Host: Specificeer het IP-adres/hostnaam van de Syrische server.

Faciliteit: Selecteer een faciliteit dat is ingesteld op uw Syslog-server.

Ernst: Selecteer een prioriteit die op de systeemserver is ingesteld.

Policy Information 🛆	Syslog Alerting	< Back
Rules	Settings	
 Advanced Settings Global Rule Thresholding 	Logging Hosts 192.168.20.3 (Single IP address or comma-separated	d list)
SNMP Alerting Svsloa Alertina	Priority EMERG T	
Policy Layers	Revert to Defaults	

Schakel externe vastlegging voor IP-beveiligingsinlichtingen/DNS-beveiligingsinlichtingen/URL-

beveiligingsinlichtingen in

IP Security Intelligence/DNS Security Intelligence/URL Security Intelligence gebeurtenissen worden gegenereerd wanneer verkeer met elke IP-adres/domeinnaam/URL security Intelligencedatabase overeenkomt. Om de externe houtkap mogelijk te maken voor IP/URL/DNS security Intelligence-gebeurtenissen, navigeer naar (ASDM Configuration > ASA Firepower Configuration > beleid > Access Control Policy > Security Intelligence),

Klik op het **pictogram** zoals in het afbeelding, om de vastlegging voor IP/DNS/URL security intelligentie mogelijk te maken. Wanneer u op het pictogram klikt, wordt een dialoogvenster geopend om loggen en opties mogelijk te maken om de gebeurtenissen naar de externe server te verzenden.

Als u gebeurtenissen naar een externe Syrische server wilt doorsturen, selecteert u **Syslog** en vervolgens selecteert u een waarschuwingsrespons in de vervolgkeuzelijst. U kunt desgewenst een waarschuwingsbericht toevoegen door op het pictogram toevoegen te klikken.

Als u verbindingsgebeurtenissen naar een SNMP-trap-server wilt doorsturen, selecteert u **SNMPtrap** en vervolgens selecteert u een SNMP-alarmrespons in de vervolgkeuzelijst. U kunt desgewenst een SNMP-alarmrespons toevoegen door op het pictogram toevoegen te klikken.



Schakel extern loggen op SSL-gebeurtenissen in

SSL gebeurtenissen worden gegenereerd wanneer het verkeer om het even welke regel in SSL beleid aanpast, waarin het registreren wordt toegelaten. Om de externe houtkap voor SSL-verkeer in te schakelen, navigeer naar ASDM Configuration > ASA Firepower Configuration > Policy > SSL. Bewerk het bestaande of maak een nieuwe regel en navigeer naar logging optie.Selecteer log aan einde van verbinding optie.

navigeer dan om **verbindingsgebeurtenissen naar** en specificeer waar te om de gebeurtenissen te verzenden.

Als u gebeurtenissen naar een externe Syrische server wilt doorsturen, selecteert u **Syslog** en vervolgens selecteert u een waarschuwingsrespons in de vervolgkeuzelijst. U kunt desgewenst een waarschuwingsbericht toevoegen door op het pictogram toevoegen te klikken.

Als u verbindingsgebeurtenissen naar een SNMP-valserver wilt doorsturen, selecteert u **SNMPtrap** en vervolgens selecteert u een SNMP-alarmrespons in de vervolgkeuzelijst. U kunt desgewenst een SNMP-alarmrespons toevoegen door op het pictogram toevoegen te klikken.

Configuration > ASA FirePOWER Configuration > Policies > <u>SSL</u>	đ
Default SSL Policy SSL Policy	
Editing Rule - SSL_Re_Sign	
Name SSL_Re_Sign Move into Category	Stand
Action 🙆 Decrypt - Resign 🔹 with Servertest 🔹 C <table-cell> Replace Key</table-cell>	
Zones Networks Users Applications Ports Category Certificate DN Cert Status Cipher Suite Version	
✓ Log at End of Connection	
Send Connection Events to:	
C Event Viewer	
Syslog_Server	
SNMP_SERVER_1	

Configuratie voor het verzenden van de systeemgebeurtenissen

Schakel externe loggen in voor systeemgebeurtenissen

De systeemgebeurtenissen tonen de status van het besturingssysteem Firepower. SNMP Manager kan worden gebruikt om deze systeemgebeurtenissen te bekijken.

Om SNMP server te configureren om systeemgebeurtenissen van de Firepower Module te kunnen opvragen, moet u een systeembeleid configureren dat de informatie beschikbaar maakt in de vuurkracht MIB (Management Information Base), die kan worden opgevraagd door de SNMP server.

Navigeer naar ASDM Configuration > ASA Firepower Configuration > Local > System Policy en klik op SNMP.

SNMP versie: Firepower Module ondersteunt SNMP v1/v2/v3. Specificeer de SNMP versie.

Community-string: Als u v1/v2 selecteert in SNMP-versieoptie, typt u de SNMP-community-naam in het veld Community String.

Username: Als u de optie v3 selecteert, verschijnt deze optie. Klik op de knop Gebruiker toevoegen en specificeer de gebruikersnaam in het veld Gebruikersnaam.

Verificatie: Deze optie maakt deel uit van de SNMP v3-configuratie. Het biedt verificatie op basis van de Hashed Message Verifier-code met MD5- of SHA-algoritmen. Kies **Protocol** voor algoritme hash en voer het wachtwoord in

in het veld Wachtwoord. Als u geen echtheidsfunctie wilt gebruiken, selecteert u Geen optie.

Privacy: Deze optie maakt deel uit van de SNMP v3-configuratie. Het verstrekt encryptie met DES/AES algoritme. Selecteer een protocol voor codering en voer een wachtwoord in het veld **Wachtwoord** in. Als u geen optie voor gegevenscodering wilt hebben, kiest u **geen** optie.

quration > ASA FirePOWER Conf	iguration > Local > System Policy	Ľ
Policy Name	Default	
Policy Description	Default Custom Delinu	
Policy Description	Derault System Polic	-y
Status: System policy out-of-dat	e on device	
	SNMP Version V1/V2	
Access List	SNMP Version Version 2	
Email Notification	Community String Count	
SNMP	Community String Secret	
STIG Compliance		
Time Synchronization		
Save Policy and Evit Cancel	· · · · ·	
Save Folicy and Exc Concord	figuration & Local & Custom Dalia	
Policy Description Status: System policy out-of-da	Default System Poli te on device SNMP Version V3	icy
Access List		
Email Notification	Username	user2
▶ SNMP	Authentication Protocol	SHA 🔻
STIG Compliance		
Time Synchronization	Authentication Password Verify Password	
Save Policy and Exit Cancel	Privacy Protocol	DES V
	Privacy Password	•••••
	Verify Password	•••••
		Add

Opmerking: Een management information base (MIB) is een verzameling informatie die hiërarchisch is georganiseerd. Het MIB bestand (DCEALERT.MIB) voor Firepower Module is beschikbaar op directory location (/etc/sf/DCEALERT.MIB), die vanaf deze directory locatie kan worden opgehaald.



Er is momenteel geen verificatieprocedure beschikbaar voor deze configuratie.

Problemen oplossen

Er is momenteel geen specifieke troubleshooting-informatie beschikbaar voor deze configuratie.

Gerelateerde informatie

• Technische ondersteuning en documentatie – Cisco Systems