# Configureer de FirePOWER-module voor AMP van het netwerk of bestandscontrole met ASDM.

## Inhoud

Inleiding Voorwaarden Vereisten Gebruikte componenten Achtergrondinformatie Configuratie van het bestandsbeleid voor IP-beheer/netwerk Bestandstoegangscontrole instellen Network Malware Protection configureren Toegangsbeheerbeleid voor bestanden configureren Toegangsbeheerbeleid implementeren Monitorverbinding voor gebeurtenissen in het bestandsbeleid Verifiëren Problemen oplossen Gerelateerde informatie

## Inleiding

In dit document wordt de functionaliteit voor Network Advanced Malware Protection (AMP)/bestandstoegang van de FirePOWER-module beschreven, evenals de methode om deze te configureren met Adaptieve Security Devices Manager (ASDM).

## Voorwaarden

## Vereisten

Cisco raadt kennis van de volgende onderwerpen aan:

- Kennis van de adaptieve security applicatie (ASA) firewall en ASDM.
- Kennis van FirePOWER-apparaat.

### 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, ASA 5555-X) die software versie 6.0.0 en hoger uitvoeren.
- 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

Kwaadaardige software/malware kan op meerdere manieren in het netwerk van een organisatie worden ingevoerd. Om de effecten van deze kwaadaardige software en malware te identificeren en te verzachten, kunnen de AMP-functies van FirePOWER worden gebruikt om de transmissie van kwaadaardige software en malware in het netwerk te detecteren en optioneel te blokkeren.

Met functionaliteit voor bestandscontrole kunt u ervoor kiezen om bestanden te controleren (detecteren), te blokkeren of de overdracht van het uploaden en downloaden van bestanden toe te staan. Een bestandsbeleid kan bijvoorbeeld worden uitgevoerd waardoor het downloaden van uitvoerbare bestanden door de gebruiker wordt geblokkeerd.

Dankzij de AMP-functie van het netwerk kunt u bestandstypen selecteren die u wilt bewaken via algemeen gebruikte protocollen en SHA 256-hashes, metagegevens uit de bestanden of zelfs kopieën van de bestanden zelf naar de Cisco Security Intelligence Cloud sturen voor malware analyse. Cloud retourneert dispositie voor bestandshashes als schoon of kwaadaardig, gebaseerd op bestandsanalyse.

Bestandscontrole en AMP voor Firepower kunnen worden ingesteld als bestandsbeleid en worden gebruikt als onderdeel van de configuratie van uw algemene toegangscontrole. Bestandsbeleid dat is gekoppeld aan toegangscontroleregels, inspecteert netwerkverkeer dat voldoet aan regelvoorwaarden.

Opmerking: Zorg ervoor dat de FirePOWER-module een Protect/Control/Malware-licentie heeft om deze functie te configureren. Selecteer **Configuration > ASA FirePOWER Configuration > Licentie** om de licenties te controleren.

## Configuratie van het bestandsbeleid voor IP-beheer/netwerk

#### Bestandstoegangscontrole instellen

Meld u aan bij ASDM en kies **Configuratie > ASA Firepower Configuration > Policy > Files.** Het dialoogvenster **Nieuw bestandsbeleid** verschijnt.

Voer een naam en optionele beschrijving in voor uw nieuwe beleid en klik vervolgens op **Store ASA Firepower Change** optie. De pagina Bestandsbeleid wordt weergegeven.

ASA FirePOWER Configur 🗗 🗜	Configuration > AS/	FirePOWER Conf	figuration > Policies > Files			
Policies	7					
					Compare Policies	New File Policy
📑 Files	- 10 Maria da maria				200	
	File Policy	Now File Do	licy	2 × ie	d	
🔯 Actions Alerts		New The Po	псу			
		Name			Add a new policy	
DNS Policy		Name	File_Access_Control		add a new policy	
		Description	Network file Access Control			
🗄 🧑 Object Management						
E- Cocal						
Configuration		Store AS	5A FirePOWER Changes Ca	ancel		
1 Information						

Klik op **Bestandsregel toevoegen** om een regel aan het bestandsbeleid toe te voegen. De bestandregel geeft u de granulaire controle over bestandstypen die u wilt loggen, blokkeren of scannen voor malware.

**Toepassingsprotocol:** Specificeer het toepassingsprotocol als **Any** (standaard) of het specifieke protocol (HTTP, MTP, IMAP3, POP3, FTP, MKB).

**Richting van overdracht:** Specificeer de richting van bestandsoverdracht. Het kan zijn, of Upload/Download zijn op basis van het Toepassingsprotocol. U kunt het protocol (HTTP, IMAP, POP3, FTP, MKB) inspecteren voor het downloaden van bestanden en het protocol (HTTP, MTP, FTP, MKB) voor het uploaden van bestanden. Gebruik de optie Any optie om bestanden te detecteren via meerdere toepassingsprotocollen, ongeacht of gebruikers het bestand verzenden of ontvangen.

Actie: Specificeer de actie voor de functie Bestandstoegangscontrole. Handeling moet Bestanden detecteren of Bestanden blokkeren. Detect File action genereert de gebeurtenis en Block Files actie genereert de gebeurtenis en blokkeert de bestandsoverdracht. Met de actie Block Files kunt u optioneel Reset Connection selecteren om de verbinding te beëindigen.

**Categorieën bestandstypen:** selecteer de categorieën bestandstype waarvoor u het bestand wilt blokkeren of de waarschuwing wilt genereren.

**Bestandstypen:** Selecteer de bestandstypen. De optie Bestandstypen biedt een meer gedetailleerde optie om het specifieke bestandstype te kiezen.

Kies de optie ASA FirePOWER Verandert om de configuratie op te slaan.

Application Protocol	Any		
phration Protocol	АПУ	Action X Block Files Y	
Direction of Transfer	Any	✓ Reset Connection	
ile Type Categories		File Types	Selected File Categories and Types
Office Documents	20	Search name and description	Category: Multimedia
Archive	18		Category: Archive
Multimedia	30	All types in selected Categories	Category: Office Documents
Executables	11	TZ (7-Zip compressed file)	·
PDF files	2	ACCDB (Microsoft Access 2007 file)	Add
Encoded	2	AMF (Advanced Module Format for digita	
Graphics	6	AMR (Adaptive Multi-Rate Codec File)	
System files	12	ARJ (Compressed archive file)	
		ASF (Microsoft Windows Media Audio/Vid	
		BZ (bzip2 compressed archive)	

#### Network Malware Protection configureren

Meld u aan bij ASDM en navigeer naar **Configuration > ASA Firepower Configuration > Policy > Files.** De pagina Bestandsbeleid wordt weergegeven. Klik nu op het dialoogvenster Nieuw bestandsbeleid.

Voer een **naam** en optionele **Description in** voor uw nieuwe beleid en klik vervolgens op de optie **Store ASA Firepower Wijzigingen**. De pagina Bestandsbeleidsregels verschijnt.

ASA FirePOWER Configur 🗗 🕂	Configuration > ASA Fire	POWER Configura	tion > Policies > Files			
Policies     Policies     Policies     Thrusion Policy     Policy     Policies     Intrusion Policy     Policies     SSL	Default SSL SSL Policy	Policy				
Actions Alerts     Jentity Policy     DNS Policy		New File Pol	icy	? ×		Compare Policies
Device Management	File Policy	Name	Network_Malware_Protection		_	
E	File Assess Control	Description	Network AMP		20.52	
Configuration Information	Network file Access C	Store AS	A FirePOWER Changes Car	ncel	1in"	

Klik op de optie **Bestandsregel toevoegen** om een regel aan bestandsbeleid toe te voegen. Bestandsregel geeft u de granulaire controle over bestandstypen die u wilt loggen, blokkeren of scannen voor malware.

**Toepassingsprotocol:** Specificeer of om het even welk (standaard) of specifiek protocol (HTTP, MTP, IMAP3, POP3, FTP, MKB)

**Richting van overdracht:** Specificeer de richting van bestandsoverdracht. Het kan zijn, of Upload/ Download zijn op basis van het Toepassingsprotocol. U kunt het protocol (HTTP, IMAP, POP3, FTP, MKB) inspecteren voor het downloaden van bestanden en het protocol (HTTP, mtp, FTP, MKB) voor het uploaden van bestanden. Gebruik **een** optie om bestanden te detecteren via meerdere toepassingsprotocollen, ongeacht of gebruikers het bestand verzenden of ontvangen.

Actie: Voor de functionaliteit voor Network Malware Protection is Action Malware Cloud Cloud

Cloud or **Block Malware**. Action **Malware Cloud Upload** genereert slechts een gebeurtenis terwijl Action **Block Malware** de gebeurtenis genereert en de malware bestandsoverdracht blokkeert.

Opmerking: Met **de** regels **van de Cloud en de** Blok van **Malware** staat de Firepower toe om de SHA-256 hash te berekenen en het voor het proces van de cloud te verzenden om te bepalen of bestanden die het netwerk oversteken malware bevatten.

Categorieën bestandstypen: selecteer de specifieke bestandscategorieën.

Bestandstypen: Selecteer de specifieke bestandstypen voor meer gedetailleerde bestanden.

Kies optie ASA Firepower Wijzigingen opslaan om de configuratie op te slaan.

Application Protocol	Any	Action Block Malware		
Direction of Transfer	Any	Connection		
File Type Categories Office Documents Archive Multimedia Executables PDF files Encoded Graphics System files	16 17 2 7 1 0 0 0 2	File Types  Search name and description  All types in selected Categories  7Z (7-Zip compressed file)  ARJ (Compressed archive file)  BINARY_DATA (Universal Binary/Java Byl BINHEX (Macintosh BinHex 4 Compresse BZ (bzip2 compressed archive)	Selected File Categories and Type Category: PDF files Category: Executables Categòry: Archive	s
		CPIO_CRC (Archive created with the cpio CPIO_NEWC (Archive created with the cp		

Opmerking: Bestandsbeleid behandelt bestanden in de volgende regel-actieregel: Blokkeren heeft voorrang op malware inspectie, wat voorrang heeft op eenvoudige detectie en vastlegging.

Als u op netwerk gebaseerde Advanced Malware Protection (AMP) configureren en Cisco Cloud de verwerking van een bestand onjuist detecteert, kunt u het bestand aan een lijst toevoegen met een SHA-256-hashwaarde om de bestandsindeling in de toekomst te verbeteren. Afhankelijk van het type bestandslijst kunt u:

- Als u een bestand wilt behandelen alsof de cloud een schone locatie heeft toegewezen, voegt u het bestand toe aan de lijst met regels.
- Als u een bestand wilt behandelen alsof de cloud een slechte dispositie heeft toegewezen, voegt u het bestand toe aan de aangepaste lijst.

Om dit te configureren navigeer u naar **Configuratie > ASA FirePOWER Configuration > Objectbeheer > Bestandslijst** en bewerkt de lijst om SHA-256 toe te voegen.

ASA FirePOWER Configur 리 무	Configuration > ASA FirePOWER Configuration	<u>1 &gt; Object Management</u> > <u>FileList</u>	
Device Management			🤍 Filter
Object Management     Object Management	Name	Number of Entries	
Port     Security Zones	Clean-List	0	Ø 8
Application Filters URL Individual Objects Object Groups GeoLocation Variable Set SecurityIntelligence Network Lists and Feed DNS Lists and Feeds Sinkhole Ide let	Custom-Detection-List	2	

## Toegangsbeheerbeleid voor bestanden configureren

Navigeer naar **Configuratie > ASA Firepower Configuration > Policy > Access Control Policy**, en maak een nieuwe **toegangsregel** of bewerk bestaande **toegangsregel**, zoals in deze afbeelding wordt getoond.

Om het bestandsbeleid aan te passen, dient actie **toegestaan** te zijn. Navigeer naar het tabblad **Inspectie** en selecteer het **Bestandsbeleid** in het vervolgkeuzemenu.

Om loggen mogelijk te maken, navigeer de optie **loggen** en selecteer de gewenste logoptie en optie **Log bestanden**. Klik op de knop **Opslaan/toevoegen** om de configuratie op te slaan.

Kies optie ASA Firepower Wijzigingen opslaan om de wijzigingen in het AC-beleid op te slaan.

nfiguration	> ASA FirePO	WER Configur	ation > Policies	> <u>Access</u>	Control P	<u>olicy</u>					
ASA	ASA FirePOV	VER									
Default	t Allow	All Traff	fic								
Add Rule											
Name Ne Action	etwork-AMP Allow			▼ IPS	5: no poli	✓ Enabled cies Variables: n/a	Insert Files: Network_N	below rule 1alware_Pro Log	▼ 1 ging: files: Event	: Viewer	
Zones	Networks	🔺 Users	Applications	Ports	URLs	🔺 ISE Attributes	]		Inspection	Logging	Comr
Intrusion P	olicy					V	ariable Set				
None						<b>Y</b>	Default Set				
File Policy											

## Toegangsbeheerbeleid implementeren

Navigeer naar de **optie** van ASDM **implementeren** en kies de optie **Firepower Change** implementeren in het uitrolmenu. Klik op de optie Importeren om de wijzigingen in te voeren.

Deploy Policies Version:2016-01-07 11:57 AM	
Access Control Policy: Default Allow All Traffic	
Intrusion Policy: Balanced Security and Connectivity	
🖸 Intrusion Policy: No Rules Active	
Intrusion Policy: IPS_Policy	
DNS Policy: Default DNS Policy	
ວ System Policy: Default	
D Sensor Policy: firepower	

Navigeer naar **bewaking > ASA FirePOWER Monitoring > Task Status.** Zorg ervoor dat deze taak voltooid moet zijn om de configuratie verandering toe te passen.

Opmerking: In versie 5.4.x moet u om het toegangsbeleid op de sensor toe te passen klikken om ASA FirePOWER Wijzigingen toepassen.

## Monitorverbinding voor gebeurtenissen in het bestandsbeleid

Om de gebeurtenissen te zien die door de Firepower Module met betrekking tot bestandsbeleid worden gegenereerd, navigeer naar **bewaking > ASA Firepower Monitoring > Real Time Eventing.** 

ing > ASA FirePOWER Mor	nitoring > Real Time Ev	<u>venting</u>					
e Eventing							
All ASA FirePOWER Eve	nts Connection Intru	ision File Malware File	Security Intelligence				
ter							
Reason=File Monitor 🕷							
Pause Refresh	Rate 5 seconds	• 1/7/16 12:06:30	) PM (IST)	•			±Ш
Receive Times	Action	First Packet	Last Packet	Reason	Initiator IP	Responder IP	S
1/6/16 1:29:48 PM	Allow	1/6/16 11:38:29 AM	1/6/16 1:26:46 PM	File Monitor	192.168.20.3	10.76.76.160	e
1/6/16 2:21:23 AM	Allow	1/6/16 2:16:47 AM	1/6/16 2:18:21 AM	File Monitor	192.168.20.3	13.107.4.50	5
1/5/16 9:22:57 PM	Allow	1/5/16 9:16:21 PM	1/5/16 9:22:56 PM	File Monitor	192.168.20.3	46.43.34.31	5
1/5/16 9:21:27 PM	Allow	1/5/16 9:15:15 PM	1/5/16 9:21:26 PM	File Monitor	192.168.20.3	46.43.34.31	5

# Verifiëren

Er is momenteel geen verificatieprocedure beschikbaar voor deze configuratie.

## Problemen oplossen

Zorg ervoor dat het bestandsbeleid correct is geconfigureerd met protocol/richting/actie/bestandstypen. Zorg ervoor dat het juiste bestandsbeleid in toegangsregels is opgenomen.

Zorg ervoor dat de implementatie van het toegangsbeheerbeleid is voltooid.

Controleer de Connection gebeurtenissen & File events (**bewaking > ASA FirePOWER-bewaking > Real Time Eventing**) om te controleren of de verkeersstroom de juiste regel heeft of niet.

## Gerelateerde informatie

• Technische ondersteuning en documentatie - Cisco Systems