IPS 5.x en hoger: De handtekening instellen met Event Action Filter met behulp van CLI en IDM

Inhoud

Inleiding Voorwaarden Vereisten Gebruikte componenten Conventies Event Action Filters De betekenis van Event Action Filters Configuratie van Event Action Filters met CLI Configuratie van Event Action Filters met IDM Configuratie van gebeurtenis-variabele Gerelateerde informatie

Inleiding

Dit document beschrijft hoe de handtekening met het Event Action Filter in Cisco Inbraakpreventiesysteem (IPS) moet worden afgestemd op de Opdracht Line Interface (CLI) en IDS Apparaatbeheer (IDM).

Voorwaarden

Vereisten

Dit document gaat ervan uit dat Cisco IPS is geïnstalleerd en correct werkt.

Gebruikte componenten

De informatie in dit document is gebaseerd op Cisco 4200 Series IDS/IPS-apparaat waarmee softwareversie 5.0 en hoger wordt uitgevoerd.

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.

Conventies

Raadpleeg Cisco Technical Tips Conventions (Conventies voor technische tips van Cisco) voor

Event Action Filters

De betekenis van Event Action Filters

De actiefilters van de gebeurtenis worden verwerkt als een geordende lijst en u kunt filters omhoog of omlaag in de lijst verplaatsen.

Filters laten de sensor bepaalde handelingen uitvoeren als reactie op het voorval zonder dat de sensor alle handelingen hoeft uit te voeren of het hele voorval verwijderen. Filters werken door handelingen uit een evenement te verwijderen. Een filter dat alle handelingen uit een gebeurtenis verwijdert, verwerkt de gebeurtenis effectief.

N.B.: Wanneer u handtekening filtert, raadt Cisco u aan de doeladressen niet te filteren. Als er meerdere doeladressen zijn, wordt alleen het laatste adres gebruikt om het filter aan te passen.

U kunt actiefilters voor gebeurtenissen configureren om specifieke handelingen uit een gebeurtenis te verwijderen of een hele gebeurtenis weg te gooien en verdere verwerking door de sensor te voorkomen. U kunt de gebeurtenis actievariabelen gebruiken die u aan groepadressen voor uw filters definieert. Zie de sectie Werkingsvariabelen <u>toevoegen, bewerken en verwijderen</u> van <u>de</u> gebeurtenis <u>Variabelen</u>.

Opmerking: U moet de variabele voorkeuren met een dollarteken (\$) om aan te geven dat u een variabele in plaats van een string gebruikt. Anders ontvangt u de foutmelding 'slechte bron' en 'doelfout'.

Configuratie van Event Action Filters met CLI

Voltooi deze stappen om actiefilters van de gebeurtenis te configureren:

- 1. Meld u aan bij de CLI met een account met beheerrechten.
- 2. Modus actieregels voor gebeurtenis invoeren:
 sensor#configure terminal
 sensor(config)#service event-action-rules rules1
 sensor(config-eve)#
- 3. Maak de filternaam: sensor(config-eve)#filters insert name1 begin

Gebruik **name1**, **name2**, etc. om uw gebeurtenis actiefilters te noemen. Gebruik het **begin | Einde | inactief | eerder | na** zoekwoorden om aan te geven waar u het filter wilt plaatsen.

4. Specificeer de waarden voor dit filter:Specificeer het bereik van de handtekening: sensor(config-eve-fil)#signature-id-range 1000-1005

De standaardinstelling is 900 tot 65535.Specificeer het bereik van de onderhandtekening: sensor(config-eve-fil)#subsignature-id-range 1-5

De standaardinstelling is 0 tot 255.Specificeer het adresbereik van de hacker: sensor(config-eve-fil)#attacker-address-range 10.89.10.10-10.89.10.23

De standaardinstelling is 0.0.0.0 tot 25.255.255.255.255.Geef het adresbereik van het

slachtoffer op: sensor(config-eve-fil)#victim-address-range 192.56.10.1-192.56.10.255

De standaardinstelling is 0.0.0.0 tot 25.255.255.255.255.Geef het bereik van de slachtofferpoort op: sensor(config-eve-fil)#victim-port-range 0-434

De standaardinstelling is 0 tot 65535.Specificeer de relevantie van het besturingssysteem: sensor(config-eve-fil)#os-relevance relevant

De standaardinstelling is 0 tot 100.Specificeer het bereik van de risicoclassificatie. sensor(config-eve-fil)#**risk-rating-range 85-100**

De standaardinstelling is 0 tot 100.Specificeer de te verwijderen acties: sensor(config-eve-fil)#actions-to-remove reset-tcp-connection

Als u een ontkende actie filtert, stelt u het percentage ontkennende acties in dat u wilt: sensor(config-eve-fil)#deny-attacker-percentage 90

De standaard is 100.Specificeer de status van het filter uitgeschakeld of ingeschakeld. sensor(config-eve-fil)#filter-item-status {enabled | disabled}

Het standaard is ingeschakeld.Specificeer de parameter stop op match. sensor(config-eve-fil)#stop-on-match {true | false}

True vertelt de sensor om te stoppen met het verwerken van filters als dit item overeenkomt met het resultaat. **False** vertelt de sensor om door te gaan met het verwerken van filters zelfs als dit item overeenkomt.Voeg eventuele opmerkingen toe die u wilt gebruiken om dit filter uit te leggen:

sensor(config-eve-fil)#user-comment NEW FILTER

5. Controleer de instellingen voor het filter:

```
stop-on-match: True default: False
user-comment: NEW FILTER default:
os-relevance: relevant default: relevant|not-relevant|unknown
```

senor(config-eve-fil)#

- 6. Zo bewerkt u een bestaand filter: sensor(config-eve)#filters edit name1
- 7. Bewerk de parameters en zie stappen 4a tot en met 4l voor meer informatie.
- 8. Zo verplaatst u een filter naar boven of beneden in de filterlijst: sensor(config-eve-fil)#exit sensor(config-eve)#filters move name5 before name1

Sensor (config eve)#1110015 move numes selore num

9. Controleer of u de filters hebt verplaatst:

sensor(config-eve-fil)#exit
sensor(config-eve)#show settings

```
filters (min: 0, max: 4096, current: 5 - 4 active, 1 inactive)
_____
ACTIVE list-contents
_____
  NAME: name5
   _____
    signature-id-range: 900-65535 <defaulted>
    subsignature-id-range: 0-255 <defaulted>
    attacker-address-range: 0.0.0.0-255.255.255.255 <defaulted>
    victim-address-range: 0.0.0.0-255.255.255.255 <defaulted>
    attacker-port-range: 0-65535 <defaulted>
    victim-port-range: 0-65535 <defaulted>
    risk-rating-range: 0-100 <defaulted>
    actions-to-remove: <defaulted>
    filter-item-status: Enabled <defaulted>
    stop-on-match: False <defaulted>
    user-comment: <defaulted>
    _____
   _____
```

```
NAME: name1
```

_____ signature-id-range: 900-65535 <defaulted> subsignature-id-range: 0-255 <defaulted> attacker-address-range: 0.0.0.0-255.255.255.255 <defaulted> victim-address-range: 0.0.0.0-255.255.255.255 <defaulted> attacker-port-range: 0-65535 <defaulted> victim-port-range: 0-65535 <defaulted> risk-rating-range: 0-100 <defaulted> actions-to-remove: <defaulted> filter-item-status: Enabled <defaulted> stop-on-match: False <defaulted> user-comment: <defaulted> _____ _____ NAME: name2 ----signature-id-range: 900-65535 <defaulted> subsignature-id-range: 0-255 <defaulted> attacker-address-range: 0.0.0.0-255.255.255.255 <defaulted> victim-address-range: 0.0.0.0-255.255.255.255 <defaulted> attacker-port-range: 0-65535 <defaulted> victim-port-range: 0-65535 <defaulted> risk-rating-range: 0-100 <defaulted> actions-to-remove: <defaulted> filter-item-status: Enabled <defaulted> stop-on-match: False <defaulted> user-comment: <defaulted> _____ _____ _____

sensor(config-eve)#

10. Zo verplaatst u een filter naar de inactieve lijst: sensor(config-eve)#filters move name1 inactive

11. Controleer dat het filter naar de inactieve lijst is verplaatst: sensor(config-eve-fil)#**exit**

sensor(config-eve)#show settings

_____ INACTIVE list-contents _____ _____ NAME: name1 ----signature-id-range: 900-65535 <defaulted> subsignature-id-range: 0-255 <defaulted> attacker-address-range: 0.0.0.0-255.255.255.255 <defaulted> victim-address-range: 0.0.0.0-255.255.255.255 <defaulted> attacker-port-range: 0-65535 <defaulted> victim-port-range: 0-65535 <defaulted> risk-rating-range: 0-100 <defaulted> actions-to-remove: <defaulted> filter-item-status: Enabled <defaulted> stop-on-match: False <defaulted> user-comment: <defaulted> _____ _____

sensor(config-eve)#

- 12. Modus actie-regels voor gebeurtenis afsluiten: sensor(config-eve)#exit Apply Changes:?[yes]:
- 13. Druk op **Voer** in om uw veranderingen toe te passen of **geef** een **nee op** om deze weg te gooien.

Configuratie van Event Action Filters met IDM

Voltooi deze stappen om actiefilters voor gebeurtenissen toe te voegen, te bewerken, te

verwijderen, in te schakelen en te verplaatsen:

- 1. Meld u aan bij IDM met een account met beheerder- of exploitatierechten.
- Kies Configuration > Policy > Event Action Regels > regels0 > Event Action Filters als de softwareversie 6.x is. Kies voor de softwareversie 5.x Configuration > Event Action Rules > Event Action Filters. Het tabblad Event Action Filters verschijnt zoals



- 3. Klik op **Add** om een evenement actiefilter toe te voegen.Het dialoogvenster Event Action Filter toevoegen verschijnt.
- 4. Typ in het veld Naam een naam als **naam1** voor het filter van de gebeurtenis.Er wordt een standaardnaam bijgeleverd, maar u kunt deze wel wijzigen in een betekenisvollere naam.
- 5. Klik in het veld Actief op de knop **Ja** om dit filter aan de lijst toe te voegen, zodat het effect op filtergebeurtenissen is.
- 6. Klik in het veld Ingeschakeld op de knop Ja om het filter in te schakelen.Opmerking: U moet ook het aanvinkvakje Event Action Filters gebruiken controleren op het tabblad Event Action Filters of geen van de gebeurtenis actiefilters wordt ingeschakeld, ongeacht of u het aanvinkvakje Ja in het dialoogvenster Bijvoegen actiefilter aankruist.
- 7. Voer in het veld Handtekening-ID de handtekening-ID's in van alle handtekeningen waarop dit filter moet worden toegepast. U kunt een lijst gebruiken, bijvoorbeeld 1000, 1005 of een bereik, bijvoorbeeld 1000-1005 of een van de SIG variabelen indien u ze definieert op het tabblad Event Variables. Voordruk de variabele met \$.
- 8. Voer in het veld SubSignature ID de onderhandtekening-ID's in van de onderhandse handtekeningen waarop dit filter moet worden toegepast. Bijvoorbeeld, **1-5**.

- Voer in het veld Adres aanmaakster het IP-adres van de bronhost in.U kunt één van de variabelen gebruiken als u ze definieert op het tabblad Event Variables. Voordruk de variabele met \$. U kunt ook een scala aan adressen invoeren, bijvoorbeeld 10.89.10.10-10.89.10.23. Standaard is 0.0.0-255.255.255.255.
- 10. Voer in het veld poort op de aanvaller het poortnummer in dat door de aanvaller wordt gebruikt om het aangetaste pakje te verzenden.
- 11. Voer in het veld Victim Address het IP-adres van de ontvangende host in.U kunt één van de variabelen gebruiken als u ze definieert op het tabblad Event Variables. Voordruk de variabele met \$. U kunt ook een scala aan adressen invoeren, bijvoorbeeld 192.56.10.1-192.56.10.255. Standaard is 0.0.0-255.255.255.255.
- 12. Voer in het veld Victim Port het havennummer in dat door de slachtoffergastheer wordt gebruikt om het aanstekende pakket te ontvangen. Bijvoorbeeld, **0-434**.
- 13. Voer in het veld Risicobeoordeling een RR-bereik voor dit filter in. Bijvoorbeeld, **85-100**.Als de RR voor een gebeurtenis binnen het gebied valt dat u specificeert, wordt de gebeurtenis verwerkt tegen de criteria van dit filter.
- 14. Kies in de vervolgkeuzelijst Handelingen om af te trekken de handelingen die u wilt dat dit filter uit de gebeurtenis verwijdert. Kies bijvoorbeeld de TCP-verbinding opnieuw instellen.Tip: Houd de Ctrl-toets ingedrukt om in de lijst meer dan één event te kiezen.
- 15. Kies in de vervolgkeuzelijst OS Relevantie of u wilt weten of de waarschuwing relevant is voor het besturingssysteem dat voor het slachtoffer is geïdentificeerd. Kies bijvoorbeeld **Relevant**.
- 16. In het veld Percentage ontkennen, voer het percentage pakketten in om te ontkennen voor aanmaakoptie. Bijvoorbeeld, **90**.De standaard is 100 procent.
- 17. Kies een van deze radioknoppen in het veld Stop op overeenkomsten: Ja Als u wilt dat de component Event Action Filters de verwerking stoppen nadat de handelingen van dit specifieke filter zijn verwijderdAlle resterende filters worden niet verwerkt; daarom kunnen geen extra acties van het evenement worden uitgesloten .Nee Als u extra filters wilt blijven verwerken
- 18. Typ in het veld Opmerkingen alle opmerkingen die u met dit filter wilt opslaan, zoals het doel van dit filter of de reden dat u dit filter op een bepaalde manier hebt ingesteld. Bijvoorbeeld NIEUW FILTER.Tip: Klik op Annuleren om de wijzigingen ongedaan te maken en het dialoogvenster Event Action Filter toevoegen te sluiten.

🕵 Add Event Action	n Filter	×
Name:	name1	
Active:	⊙ Yes C No	
Enabled:	• Yes C No	
Signature ID:	1000-1005	
Subsignature ID:	1-5	
Attacker Address:	10.89.10.10-10.89.10.23	
Attacker Port:	0-65535	
Victim Address:	0.0.0.0-255.255.255.255	
Victim Port:	0-434	
Risk Rating:	Minimum Maximum 85 - 100	
Actions to Subtract:	Request Block Connection Request Block Host Request Rate Limit Request Snmp Trap Reset Top Connection]
OS Relevance:	Not Relevant Relevant Unknown	
Deny Percentage:	90	
Stop on Match:	C Yes 💿 No	
Comments:	NEW FILTER	
	OK Cancel Help	

19. Klik op **OK**.Het nieuwe filter van de gebeurtenis verschijnt nu in de lijst op het tabblad Event Action Filters, zoals weergegeven.

E Cisco IDM 6	.0 - 10.77.241.14	2							
File Help	· · · · · · · · · · · · · · · · · · ·								
Home	Configuration	Monitoring	Be	ock For	ward Ref	🖻 🤗 resh Help			cisco
Sensor Setu Network	P A	rules0 Event Actio	n Override	s Target \	/alue Rating E	vent Action Filte	rs OS Identifications Eve	nt Variables	General Settings
G SSH Auth Auth	norized Keys	Use Ev	ent Action	Filters					
Sen:	sor Key	Name	Active	Enabled	Sig ID	SubSig ID	Attacker (address/port)		Select All
Trus Serv	ted Hosts ver Certificate	name1	Yes	Yes	1000-1005	1-5	10.89.10.10-10.89.10.23 0-65535	0.0.0	Add
D Time									Edit
Interface Cor	nfiguration								Move Up
Interface	y IS								Move Down
VLAN Pa	e Pairs airs							- 1	Enable
VLAN G	roups								Disable
Analysis Eng	low Notificativ								Delete

20. Controleer de optie Event Action Overrijdt met de optie Aangepaste installatie zoals

aangegev	en.							
🕼 Cisco IDM 6	.0 - 10.77.241.14	12						
File Help								
Home	Configuration	Monitoring	Back	Forward	@ Refresh	? Help		cisco
Network Allowed Allowed SSH SSH	Hosts norized Keys wm Host Key: sor Key tes ted Hosts ver Certificate	Event Action O An Event Act RR value for select Use Even	Overrides Ti ion Override that event fail vent Action Over t Action Over Event Act Inline	arget Value Ra lets you assign ls within the de verrides to use mides	ting Event A n a Risk Rating sfined range fi e any override	ction Filters OS k (RR) range to eac or a particular action that is currently en Enabled Yes	dentifications Event Variables th event action type. If an even on, that action is added to the e nabled. Risk Rating 90-100	General Settings t occurs and the went. You must Select All Add

Opmerking: U moet het aanvinkvakje **Use Event Action Overrijdes** aankruisen op het tabblad Event Action Overrides of geen van de gebeurtenissen-actie overtreedt wordt ingeschakeld, ongeacht de waarde die u in het dialoogvenster Actiefilter toevoegen instelt.

21. Klik in de lijst op een bestaand actiefilter voor gebeurtenissen om het te bewerken en klik op **Bewerken**.Het dialoogvenster Event Action Filter bewerken

Name:	name1	
Active:	€ Yes C No	
Enabled:	€ Yes C No	
Signature ID:	1000-1005	
Subsignature ID:	1-5	
Attacker Address:	10.89.10.10-10.89.10.23	
Attacker Port:	0-65535	
Victim Address:	192.56.10.1-192.56.10.255	-
Victim Port:	0-434	
Risk Rating:	Minimum Maximum 85 - 100	
Actions to Subtract	Request Block Connection Request Block Host Request Rate Limit Request Snmp Trap Reset Top Connection	*
OS Relevance:	Not Relevant Relevant Unknown	
Deny Percentage:	100	
Stop on Match:	C Yes @ No	
		_

verschijnt.

- 22. Verandert elke waarde in de velden die u moet wijzigen. Zie stappen 4 tot en met 18 voor informatie over het invullen van de velden. **Tip:** Klik op **Annuleren** om de wijzigingen ongedaan te maken en het dialoogvenster Event Action Filter bewerken te sluiten.
- 23. Klik op **OK**.Het filter van de bewerkte gebeurtenis verschijnt nu in de lijst op het tabblad Event Action Filters.
- 24. Controleer de optie **Event Action Overrijdt** met de knop **Use** Event.**Opmerking:** U moet het aanvinkvakje **Use Event Action Overrijdes** controleren in het tabblad Event Action Overrides of er is geen van de regeltoetsen van de gebeurtenis ingeschakeld, ongeacht de waarde die u in het dialoogvenster Activeringsfilter bewerken hebt ingesteld.
- 25. Klik in de lijst op een actiefilter voor gebeurtenissen om het te verwijderen en klik vervolgens op **Verwijderen**.Het filter van de gebeurtenis verschijnt niet langer in de lijst op het tabblad Event Action Filters.

- 26. Filter omhoog of omlaag in de lijst om een gebeurtenis actie te bewegen, kies het, en klik dan **Beweeg omhoog** of **Beweeg omlaag**. **Tip:** Klik op **Beginwaarden** om de wijzigingen te verwijderen.
- 27. Klik op **Toepassen** om de wijzigingen toe te passen en de herziene configuratie op te slaan.

Configuratie van gebeurtenis-variabele

Voltooi deze stappen om gebeurtenis variabelen toe te voegen, te bewerken en te verwijderen:

- 1. Inloggen. Gebruik bijvoorbeeld een account met een beheerder of een beheerder.
- Kies Configuration > Policy > Event Action Regels > regels0 > Event Variables als de softwareversie 6.x is. Kies voor de softwareversie 5.x Configuration > Event Action Rules > Event Variables.Het tabblad Event Variables verschiint.

Cisco IDM 6.0 - 10.77.241.1	12			de Vec I		
File Help						
Home Configuration	Monitoring	Back F	orward Refresh	? Help		cisco
Sensor Setup Network Allowed Hosts SSH Authorized Keys Known Host Keys Known Host Keys Sensor Key Certificates Trusted Hosts Server Certificate Time Users Interface Configuration Summary Interface Configuration Summary Interface Pairs VLAN Pairs VLAN Groups Bypass Traffic Flow Notification Signature Definitions Signature Definitions Signature Definitions Signature Definitions Signature Definitions Signature Definitions	rules0 Event Action O Event Variable use that variak dollar sign (\$) 1 N	verrides Target is let you use the ble are updated w to indicate the va lame	Value Rating Event same value within m with the new value. If lue is a variable and r Type	Action Filters O atiple filters. When you use a variable tot a literal string.	S Identifications Event Variables in you change the value of a variable in a filter, be sure to preface the v Value	General Settings le, all filters that variable with a Add Edit Delete

- 3. Klik op **Add** om een variabele te maken.Het dialoogvenster Variabele toevoegen verschijnt.
- Typ in het veld Naam een naam voor deze variabele. Opmerking: de geldige naam kan alleen nummers of letters bevatten. U kunt ook een koppelteken (-) of een underscore (_) gebruiken.
- 5. Typ in het veld Waarde de waarden voor deze variabele.Specificeer het volledige IP-adres of het volledige bereik of de reeks bereiken. Bijvoorbeeld:10.89.10.10-10.89.10.2310.90.1.1192.168.10.1-192.168.10.255**Opmerking:** U kunt komma's als scheidingstekens gebruiken. Zorg ervoor dat er na de komma geen trailverende ruimtes zijn. Anders ontvangt u een mislukt foutbericht voor validatie.**Tip:** Klik op **Annuleren** om de wijzigingen ongedaan te maken en het dialoogvenster Event Variable toevoegen te

🎼 Ad	d Event Variable	×
Nam	e: variable1]
Туре	e: address 💌	
Valu	ie: 10.89.10.10-10.89.10.23 10.90.1.1 192.168.10.1-192.168 10.255	
	OK Cancel Help	

sluiten.

6. Klik op **OK**.De nieuwe variabele verschijnt in de lijst op het tabblad Event Variables.

Cisco IDM	6.0 - 10.77.241.14	2							
ile Help									
Home	Configuration	Montoring	Back	Forward	@ Refresh	🤗 Help			cisco
Allown	rk ed Hosts uthorized Keys nown Host Key: ensor Key	Event Action Ov Event Variables use that variable dollar sign (\$) to	errides To slet you use le are updat o indicate th	arget Value Rat e the same valu ted with the ne ne value is a va	ing Event A se within mult w value. If yo riable and no	ction Filters pie filters. Wh u use a varial t a literal string	OS Identifications ien you change the ble in a filter, be su g.	Event Variables e value of a varia are to preface the	General Setting: ble, all filters that variable with a
Certific	cates	Ne	ame	1 1	ype		Value		Add
Time	usted Hosts erver Certificate	variable1		ad	dress	10.89.10.10-1 10.90.1.1 192.168.10.1	10.89.10.23		Edit
Interface (Configuration								Delete

- 7. Kies de bestaande variabele in de lijst om deze te bewerken en klik vervolgens op **Bewerken**.Het dialoogvenster Event Variable bewerken verschijnt.
- 8. Voer in het veld Waarde de wijzigingen in de waarde in.
- 9. Klik op **OK**.De variabele bewerkte gebeurtenissen verschijnt nu in de lijst in het tabblad Event Variables.**Tip:** Kies **Reset** om uw wijzigingen te verwijderen.
- 10. Klik op **Toepassen** om de wijzigingen toe te passen en de herziene configuratie op te slaan.

Gerelateerde informatie

- <u>Categoriepagina voor Cisco-inbraakpreventiesysteem</u>
- <u>Technische ondersteuning en documentatie Cisco Systems</u>