CS-MARS - Voeg een IPS-sensor toe en configureren als rapportageapparaat

Inhoud

Inleiding

Dit document legt uit hoe u een Cisco Secure Inbraakpreventiesysteem (IPS)-apparaat en elke geconfigureerde virtuele sensoren kunt voorbereiden om als rapportageapparaat te fungeren voor Cisco Security Monitoring, Analysis, and Response System (CS-MARS).

Voorwaarden

Vereisten

Voor Cisco IPS 45.x, 6.x en 7.x apparaten, trekt MARS de logs in via SDEE over SSL. Daarom moet MARS toegang hebben tot de sensor. Om de sensor voor te bereiden moet u de HTTP server op de sensor inschakelen, TLS in staat stellen om toegang tot HTTPS toe te staan, en zorgen dat het IP adres van MARS wordt gedefinieerd als een toegestane host, die toegang heeft tot de sensor en gebeurtenissen kan trekken. Als de sensoren zijn geconfigureerd om toegang te verlenen van beperkte hosts of subnetten op het netwerk, kunt u de opdracht **ip_adres/netmask** gebruiken om deze toegang mogelijk te maken.

Gebruikte componenten

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

- Cisco Secure MARS-apparaat dat softwareversie 4.2.x en hoger uitvoert
- Cisco 4200 Series IPS-apparaat waarmee softwareversie 6.0 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.

Verwante producten

Deze configuratie kan ook met deze sensoren worden gebruikt:

- IPS-4240 sensor
- IPS-4255 switch
- IPS-4260 sensor
- IPS-4270-20 switch

Conventies

Raadpleeg de Cisco Technical Tips Convention voor meer informatie over documentconventies.

Configureren

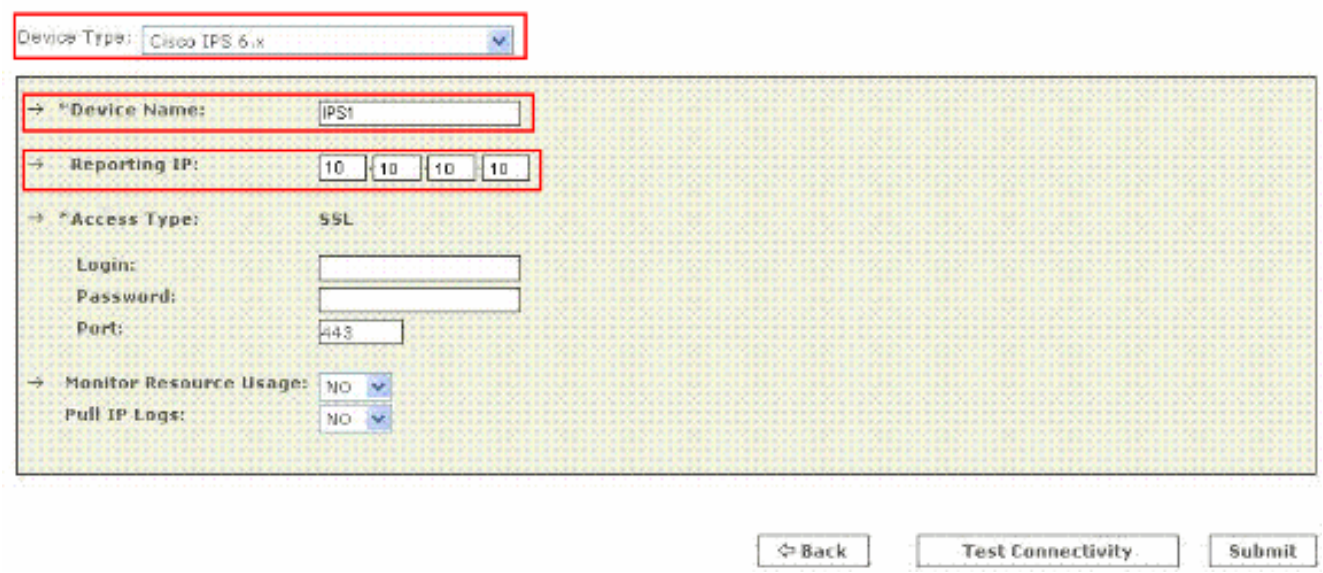
In deze sectie, wordt u voorgesteld met de informatie over hoe u een Cisco Secure Inbraakpreventiesysteem (IPS) sensor aan een Cisco Security Monitoring, Analysis, and Response System (CS-MARS) apparaat kunt toevoegen en configureren.

Een Cisco IPS 6.x of 7.x-apparaat in MARS toevoegen en configureren

Wanneer u een Cisco IPS 6.x of 7.x apparaat in MARS definieert, kunt u elke virtuele sensoren ontdekken die op het apparaat zijn geconfigureerd. Wanneer je deze virtuele sensoren ontdekt, stelt MARS in staat om de gemelde gebeurtenissen te scheiden door een virtuele sensor. Hiermee kunt u ook de lijst met gecontroleerde netwerken op elke virtuele sensor instellen, waardoor de nauwkeurigheid van de gewenste rapportage wordt verbeterd.

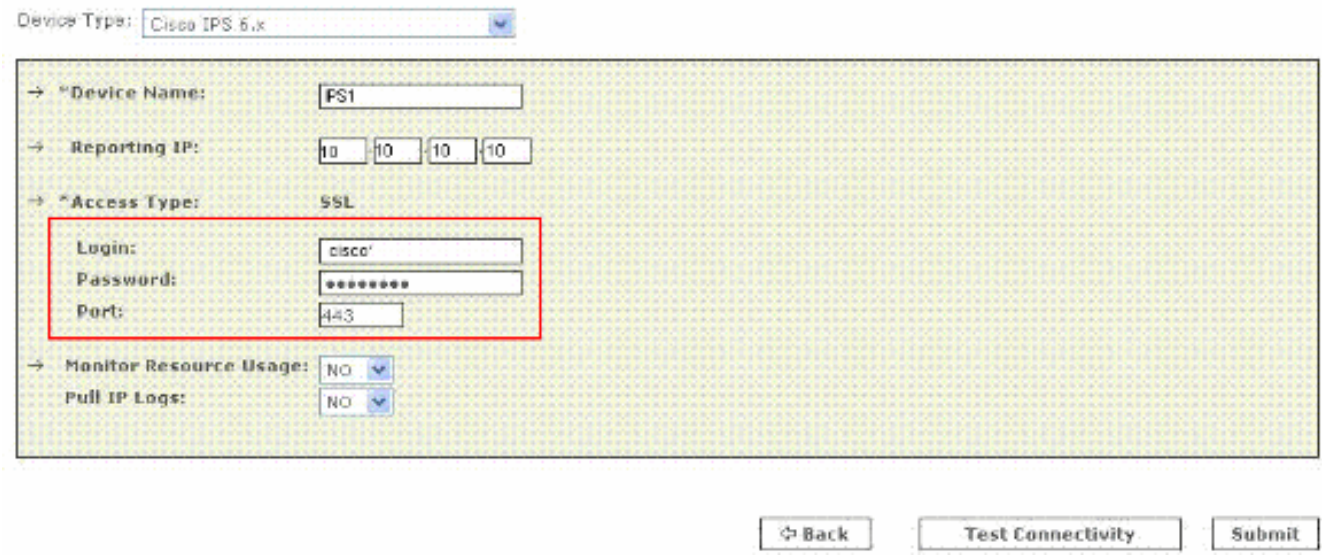
Voltooi deze stappen om een Cisco IPS 6.x of 7.x apparaat in MARS toe te voegen en te configureren:

1. Kies **Admin > System Setup > Security and Monitor Devices**. Klik vervolgens op **Toevoegen**.
2. Kies **Cisco IPS 6.x of Cisco IPS 7.x** in de lijst met apparaattype. Voer nu de hostnaam van de sensor in het veld **Apparaatnaam** in zoals hier wordt getoond. IPS1 is de Apparaatnaam die in dit voorbeeld wordt gebruikt. De waarde van de apparaatnaam moet identiek zijn aan de ingestelde naam van de
sensor.



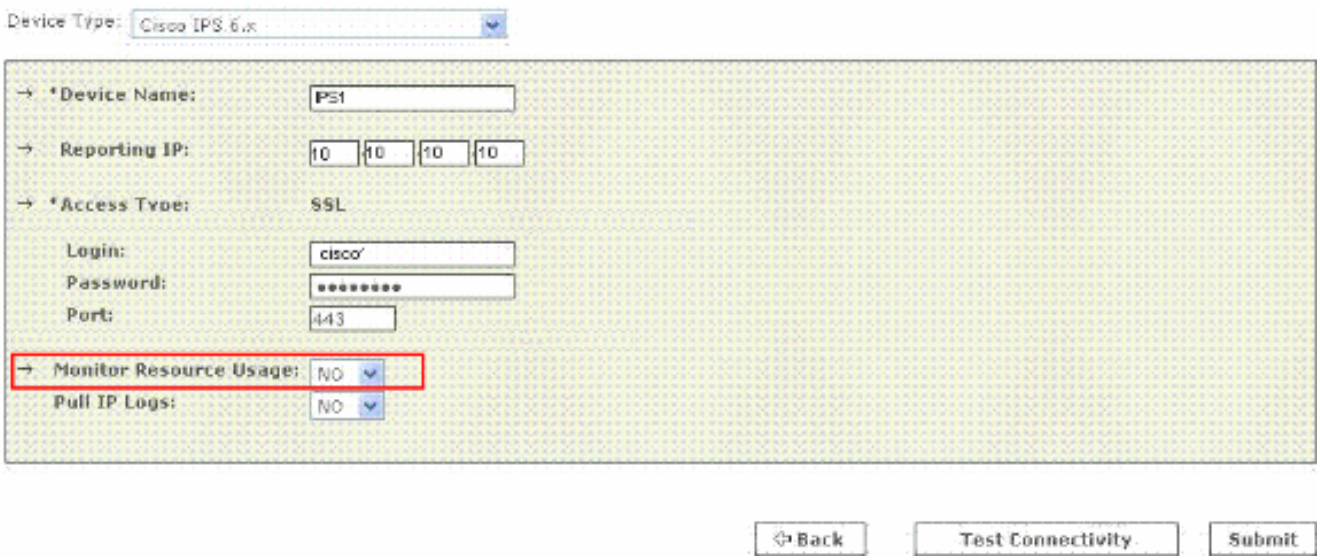
Voer nu het administratieve IP-adres in het veld **Rapportage IP in**. Het IP-adres van de rapportage is hetzelfde adres als het IP-adres van de administratie.

3. Voer in het **veld Aanmelden** de gebruikersnaam in die is gekoppeld aan de administratieve account die wordt gebruikt voor toegang tot het rapportageapparaat. Typ nu in het **veld Wachtwoord** het wachtwoord dat gekoppeld is aan de gebruikersnaam die in het **veld Aanmelden** is gespecificeerd. De **gebruikersnaam** is **Cisco** en het **wachtwoord** dat wordt gebruikt is **cisco123** in dit voorbeeld. Voer ook het TCP poortnummer in waarop de webserver die op de sensor draait, luistert in het **Port-veld**. De standaard HTTPS poort is 443.

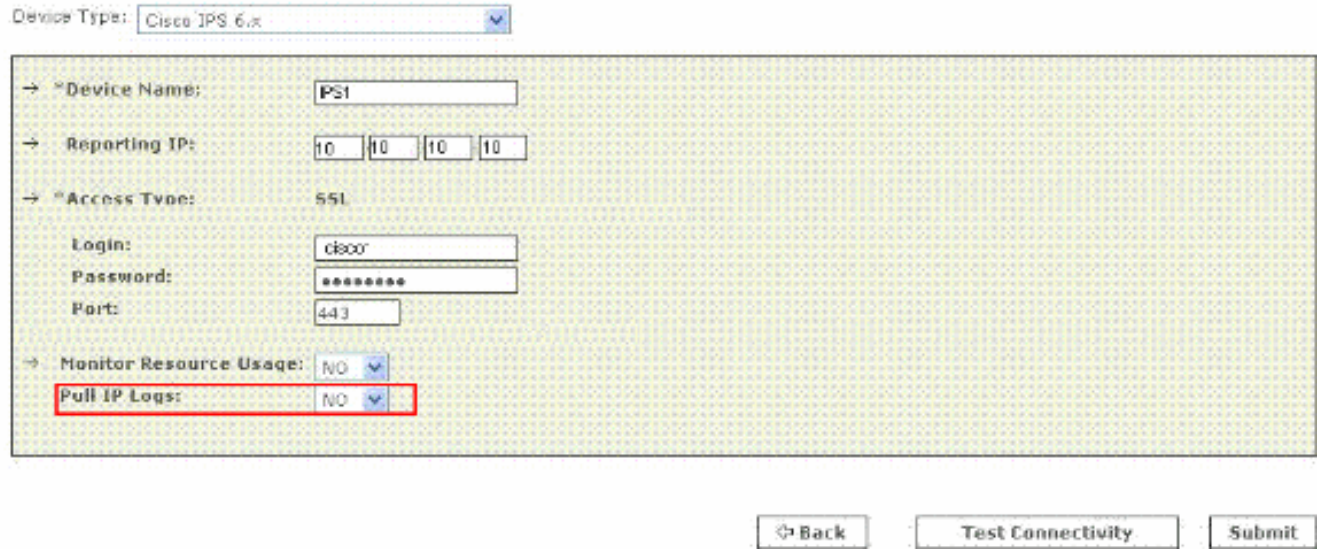


Opmerking: hoewel het mogelijk is om HTTP alleen te configureren heeft MARS HTTPS nodig.

4. Controleer nu of **er geen** geluid is geselecteerd in de lijst **Gebruik bewakingsresource**. Terwijl de optie Gebruik van de monitor op deze pagina verschijnt, werkt het niet voor Cisco IPS.

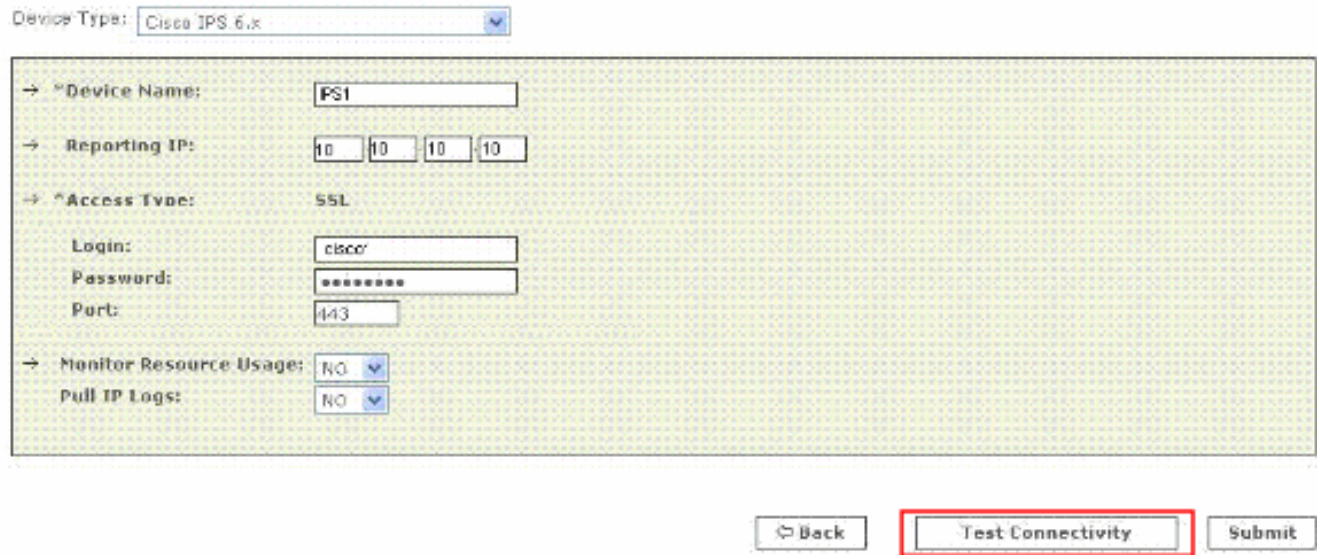


5. Om de IP-logbestanden uit de sensor te halen, kiest u **Ja** uit de lijst **Pull IP-Logs**. Dit is een optionele functie die indien nodig kan worden gebruikt.

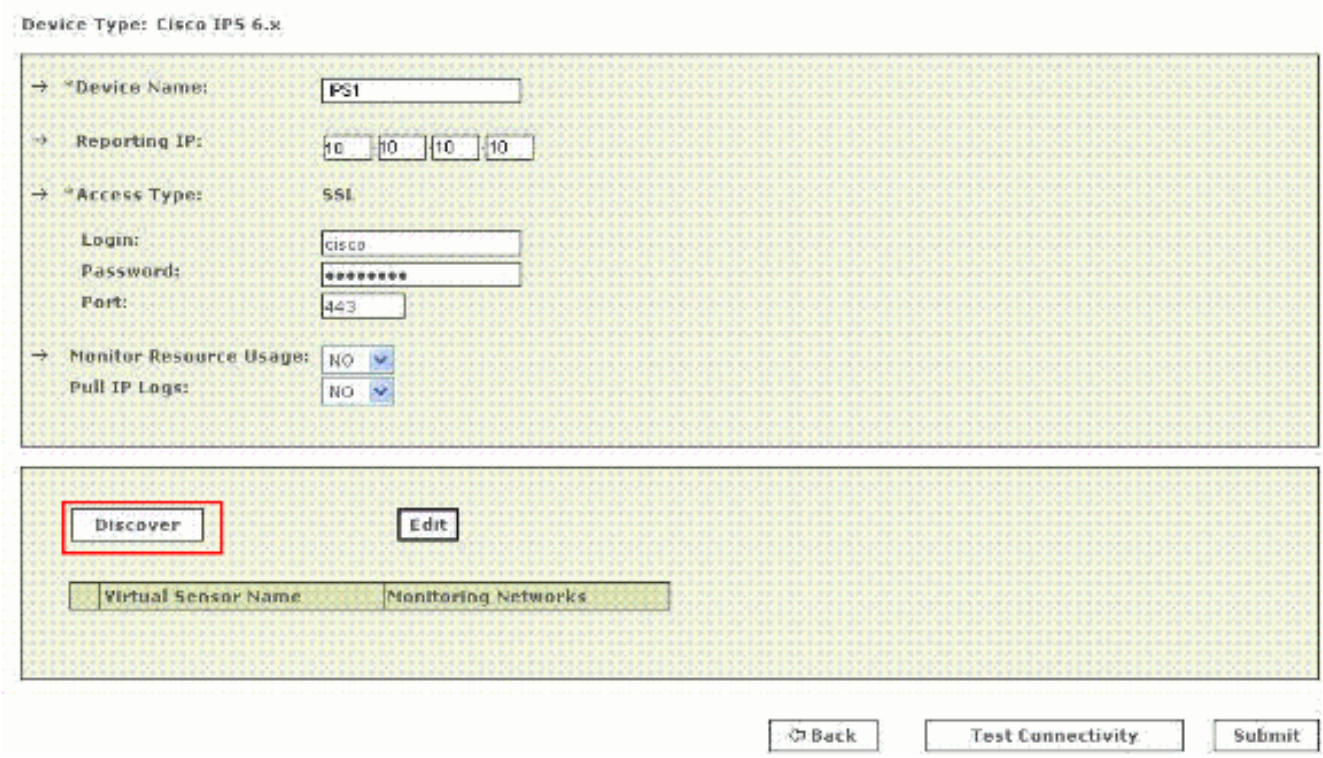


Deze instelling is van toepassing op de hele sensor, met inbegrip van de stammen die gegenereerd zijn voor virtuele sensoren.

6. Klik op **Test Connectivity** om de configuratie te verifiëren en de ontdekking van virtuele sensoren mogelijk te maken.

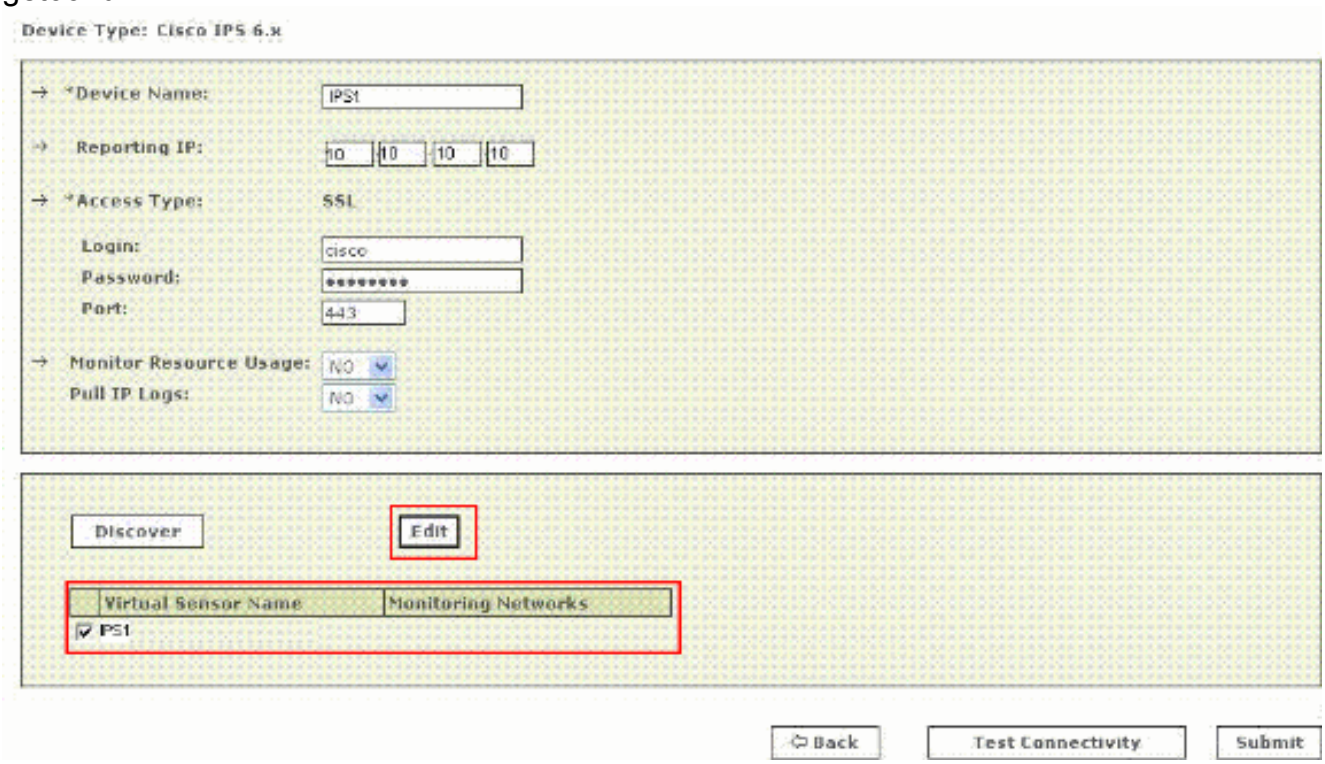


7. Klik op **Discover** om gedefinieerde virtuele sensoren te ontdekken.



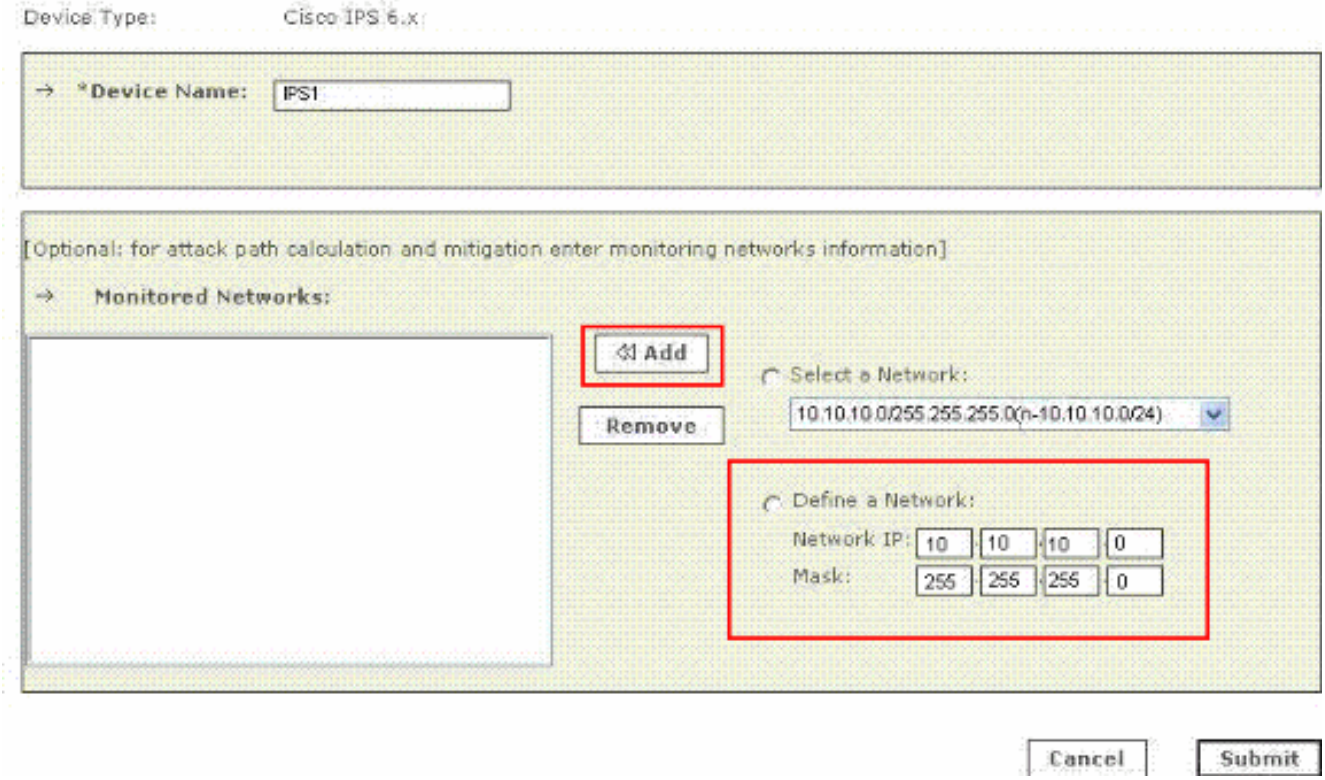
Opmerking: MARS is zich niet bewust van de wijzigingen die in de sensor zijn aangebracht. Als u wijzigingen aanbrengt in de virtuele sensorinstellingen, moet u op **Discover** klikken op de configuratiescherm van de sensor om de virtuele sensorgegevens in MARS op te frissen.

8. Kies het selectieteken naast de naam van de virtuele sensor en klik op **Bewerken** om de gecontroleerde netwerken voor elke virtuele sensor te definiëren. Nu verschijnt de pagina met de IPS-module zoals hier wordt getoond.



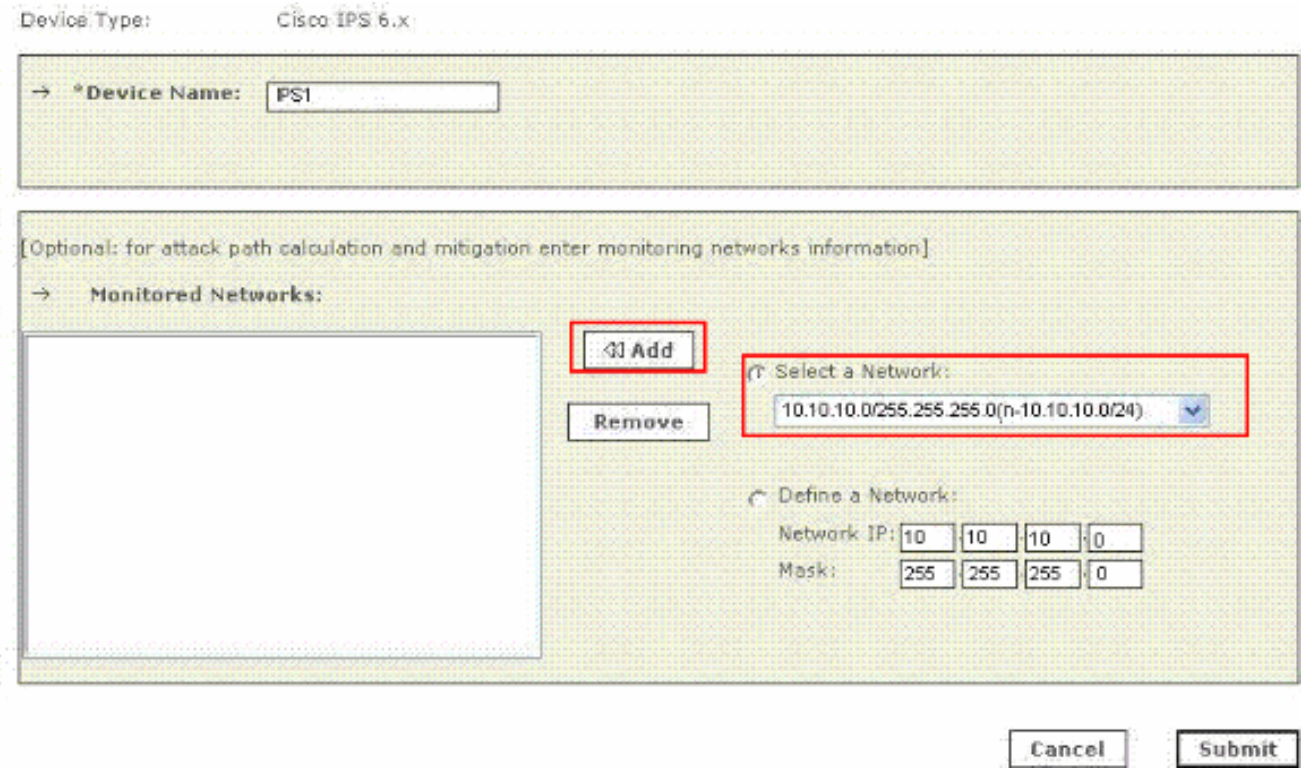
9. Specificeer voor berekening en beperking van de aanvalspad de netwerken die door de sensor worden bewaakt. Kies de knop **Netwerk** definiëren om het netwerk handmatig te definiëren. Voltooi vervolgens deze stappen om een netwerk te definiëren:Voer het

netwerkadres in het veld **IP-netwerk** in.Voer de corresponderende netwerkmaskerwaarde in in het veld **masker**.Klik op **Add** om het gespecificeerde netwerk naar het veld Gemonitord netwerken te verplaatsen.Herhaal de vorige stappen als er meer netwerken moeten worden gedefinieerd.



Opmerking: deze optie is optioneel beschikbaar en kan, indien niet vereist, worden overgeslagen.

10. Klik op de knop **Een netwerk selecteren** om de netwerken te selecteren die aan het apparaat gekoppeld zijn. Voltooi vervolgens deze stappen om de netwerken te kiezen:Selecteer een netwerk in de lijst **Netwerk selecteren**.Klik op **Add** om het gespecificeerde netwerk naar het veld Gemonitord netwerken te verplaatsen.Herhaal de vorige stappen als er meer netwerken moeten worden geselecteerd.



Opmerking: deze optie is optioneel beschikbaar en kan, indien niet vereist, worden overgeslagen.

11. Herhaal **stap 8** tot en met **stap 10** voor elke virtuele sensor.
12. Klik op **Inzenden** om de wijzigingen op te slaan. De naam van het apparaat verschijnt onder de Informatielijst Beveiliging en Toezicht. De opdracht verzenden registreert de wijzigingen in de tabellen van de gegevensbank. Maar de veranderingen in het werkgeheugen van het MARS-apparaat worden er niet door geladen. De actieve lading heeft veranderingen in het werkgeheugen ingediend.
13. Klik op **Activeren** om MARS in staat te stellen om de gebeurtenissen van dit apparaat te beginnen.MARS begint de door deze module gegenereerde gebeurtenissen te sijpelen en evalueert deze gebeurtenissen met behulp van de vastgestelde inspectie- en uitrolregels. Alle gebeurtenissen die door het apparaat vóór de activering naar MARS zijn gepubliceerd, kunnen met het rapporterende IP-adres van het apparaat worden bevraagd als een matchcriterium. Raadpleeg het gedeelte Rapportage en beperking van het apparaat activeren. voor meer informatie over de activeringsactie .

Controleer dat MARS gebeurtenissen van een Cisco IPS-apparaat oproept

Het is gemeenschappelijk om gunstige gebeurtenissen op het netwerk te creëren om de gegevensstroom te verifiëren. Voltooi deze stappen om de gegevensstroom tussen een Cisco IPS-apparaat en een MARS te controleren:

1. Schakel op het Cisco IPS-apparaat de handtekeningen 2000 en 2004 in en waarschuwen. De handtekeningen volgen ICMP berichten (pings).
2. Pingen een apparaat op het voorwerp op het voorwerp waarop het apparaat van Cisco IPS luistert. De gebeurtenissen worden gegenereerd en door MARS.
3. Controleer dat de gebeurtenissen in de MARS-webinterface verschijnen. U kunt een query uitvoeren met het Cisco IPS-apparaat.

4. Nadat de gegevensstroom is geverifieerd, kunt u de handtekeningen van 2000 en 2004 op het Cisco IPS-apparaat uitschakelen.**Opmerking:** Als de Test Connectivity-handeling niet mislukt tijdens de configuratie van een Cisco IPS-apparaat in de MARS-webinterface, zijn de communicatie ingeschakeld. Met deze taak kunt u verder controleren of de waarschuwingen correct gegenereerd en getrokken zijn.

Problemen oplossen

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

Gerelateerde informatie

- Ondersteuning van Cisco-systeem voor beveiligingsbewaking, analyse en respons
- Categoriepagina voor Cisco-inbraakpreventiesysteem
- Cisco-systeem voor beveiligingsbewaking, analyse en respons - compatibiliteitsinformatie
- Verzoeken om opmerkingen (RFC's)
- Technische ondersteuning en documentatie – Cisco Systems