CS-MARS: Agregue el sensor del IPS de Cisco como dispositivo de informe al ejemplo de la configuración CS-MARS

Contenido

Introducción

Este documento explica cómo preparar un dispositivo seguro del Sistema de prevención de intrusiones (IPS) de Cisco y cualquier sensor virtual configurado para actuar como dispositivos de informe a vigilar del Cisco Security, al análisis, y al sistema de la respuesta (CS-MARS).

Prerequisites

Requisitos

Para los dispositivos 5.x, 6.x, y 7.x del IPS de Cisco, MARTE tira de los registros usando SDEE sobre el SSL. Por lo tanto, MARTE debe tener acceso HTTPS al sensor. Para preparar el sensor, usted debe activar el servidor HTTP en el sensor, permite a TLS permitir el acceso HTTPS, y se asegura de que la dirección IP de MARTE esté definida como host permitido, uno que pueda tener acceso al sensor y tirar de los eventos. Si los sensores se han configurado para permitir el acceso de los host o de las subredes limitados en la red, usted puede utilizar los **ip_address de la acceso-lista/el** comando de la **máscara de red** para activar este acceso.

Componentes usados

La información que contiene este documento se basa en las siguientes versiones de software y hardware.

- Dispositivo seguro de Cisco MARTE que funciona con la versión de software 4.2.x y más adelante
- Dispositivo IPS de las Cisco 4200 Series que funciona con la versión de software 6.0 y más adelante

La información que contiene este documento se creó a partir de los dispositivos en un ambiente de laboratorio específico. Todos los dispositivos que se utilizan en este documento se pusieron en funcionamiento con una configuración verificada (predeterminada). Si la red está funcionando, asegúrese de haber comprendido el impacto que puede tener cualquier comando.

Productos relacionados

Esta configuración se puede también utilizar con estos sensores:

- IPS-4240
- IPS-4255
- IPS-4260
- IPS-4270-20

Convenciones

Consulte Convenciones de Consejos Técnicos de Cisco para obtener más información sobre las convenciones sobre documentos.

Configurar

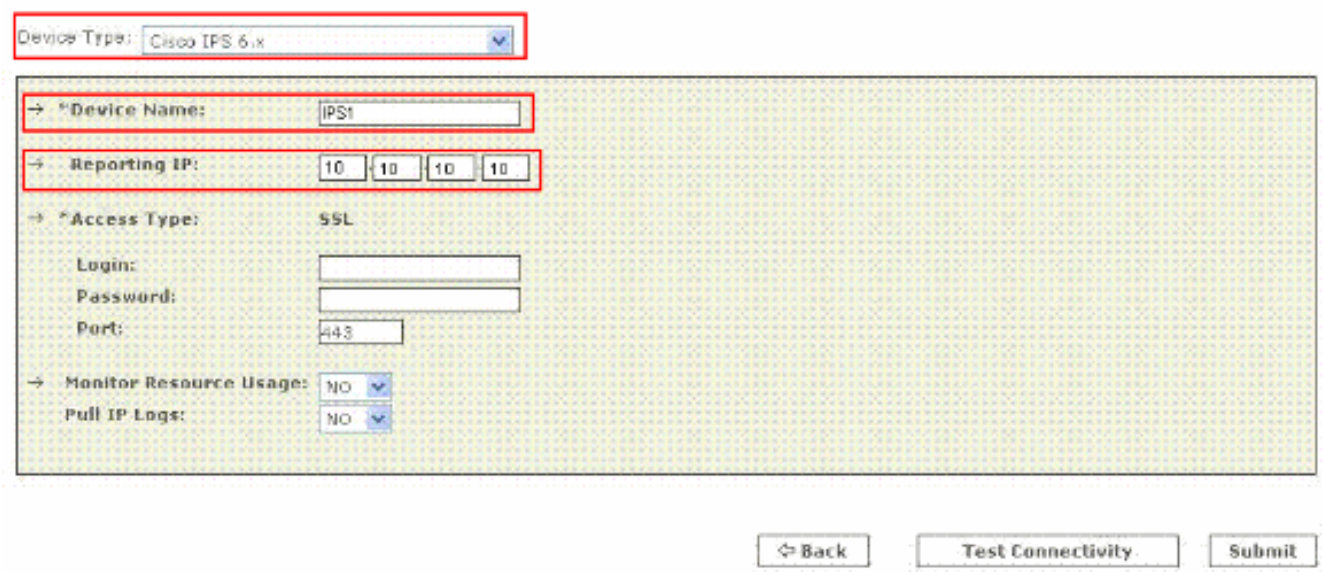
En esta sección, le presentan con la información sobre cómo agregar y configurar un sensor seguro del Sistema de prevención de intrusiones (IPS) de Cisco a vigilar de un Cisco Security, al análisis, y al dispositivo del sistema de la respuesta (CS-MARS).

Agregue y configure un dispositivo 6.x o 7.x del IPS de Cisco en MARTE

Cuando usted define un dispositivo 6.x o 7.x del IPS de Cisco en MARTE, usted puede descubrir cualquier sensor virtual configurado en el dispositivo. Cuando usted descubre estos sensores virtuales, esto permite que MARTE separe los eventos señalados por el sensor virtual. También permite que usted adapte la lista de redes vigiladas a cada sensor virtual, que mejora la exactitud de la información deseada.

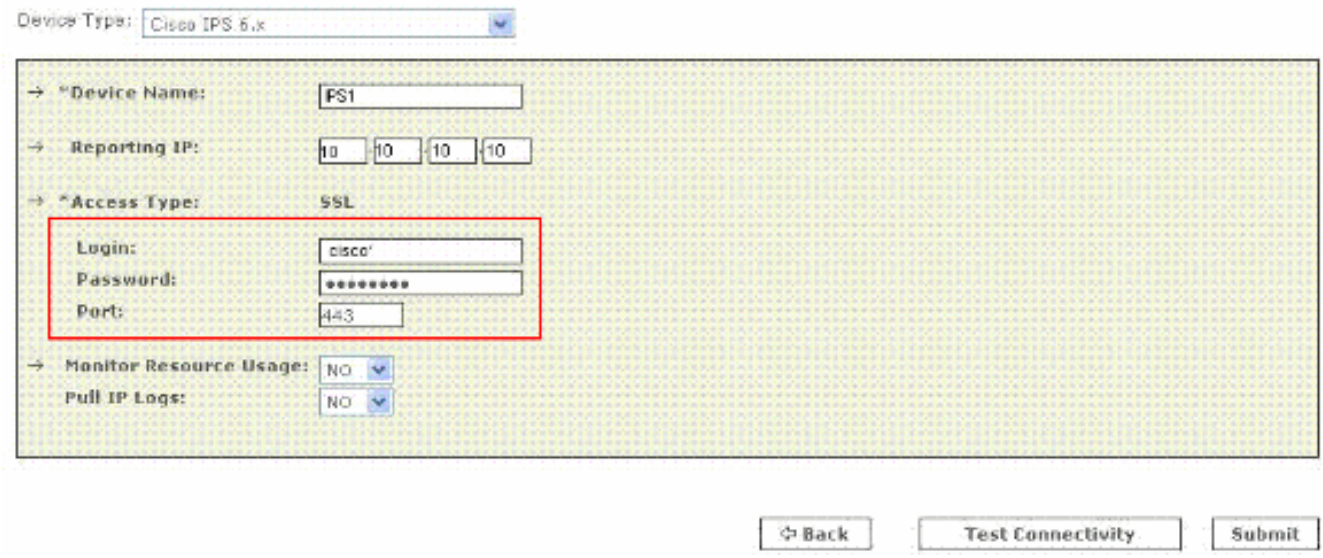
Complete estos pasos para agregar y configurar un dispositivo 6.x o 7.x del IPS de Cisco en MARTE:

1. Elija **> Security (Seguridad) de la disposición Admin > del sistema y vigile los dispositivos**. Entonces, haga clic en **agregan**.
2. Elija el **IPS de Cisco 6.x o el IPS de Cisco 7.x de la** lista del tipo de dispositivo. Ahora ingrese el hostname del sensor en el campo de **Nombre del dispositivo** como se muestra aquí. IPS1 es el Nombre del dispositivo usado en este ejemplo. El valor del Nombre del dispositivo debe ser idéntico al nombre configurado del sensor.



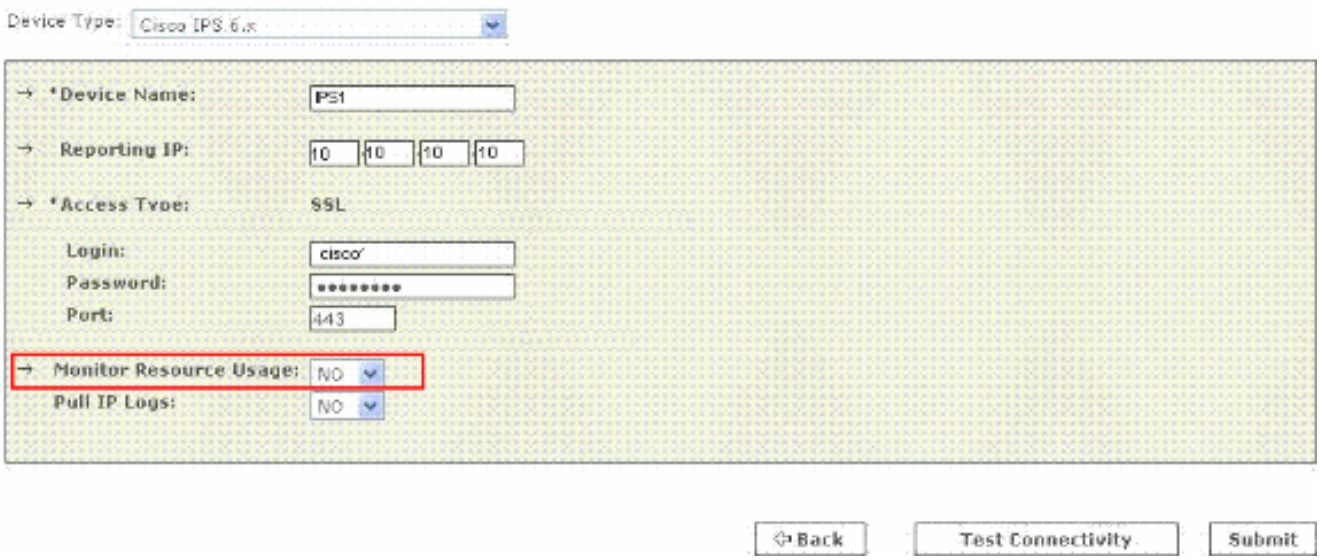
Ahora ingrese el IP address administrativo en el campo **IP que señala**. La dirección IP de la información es el mismo direccionamiento que la dirección IP administrativa.

3. En el **campo de la clave**, ingrese el username asociado a la cuenta administrativa que se utiliza para tener acceso al dispositivo de informe. Ahora, en el **campo de contraseña**, ingrese la contraseña asociada al username especificado en el **campo de la clave**. **El username** es **Cisco** y la **contraseña** usada es **cisco123** en este ejemplo. También ingrese el número del puerto TCP en el cual el web server que se ejecuta en el sensor escucha en el **campo de puerto**. El puerto del valor por defecto HTTPS es
443.

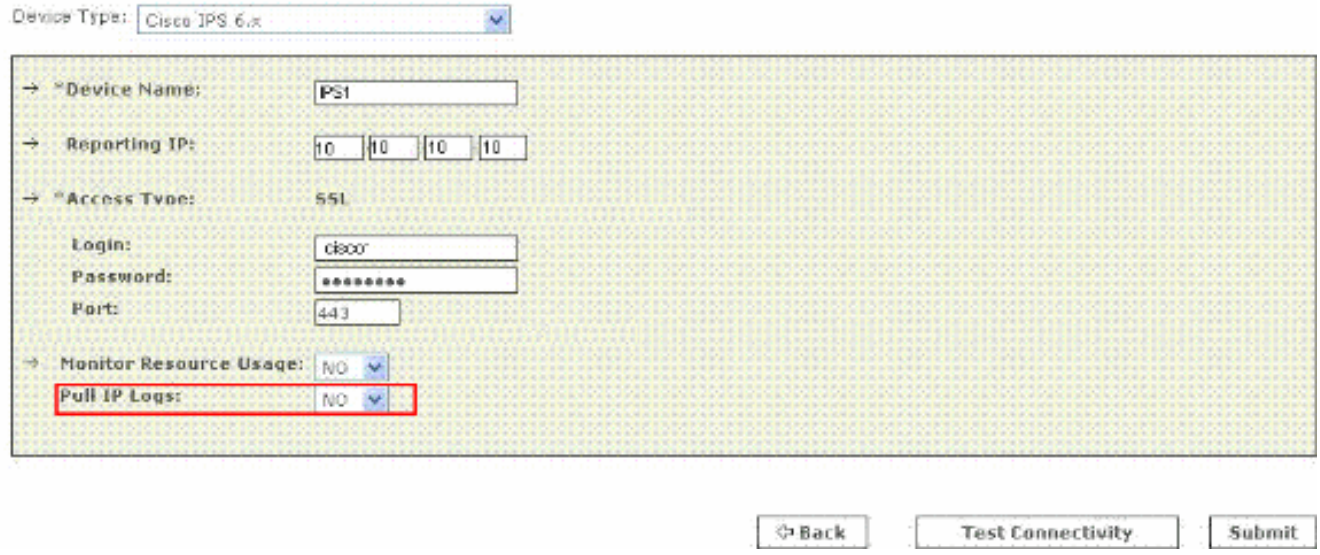


Note: Mientras que es posible configurar el HTTP solamente, MARTE requiere el HTTPS.

4. Ahora verifique que **NINGÚN** chosed en la lista del **USO de recurso del monitor**. Mientras que la opción del USO de recurso del monitor aparece en esta página, no funciona para el IPS de
Cisco.

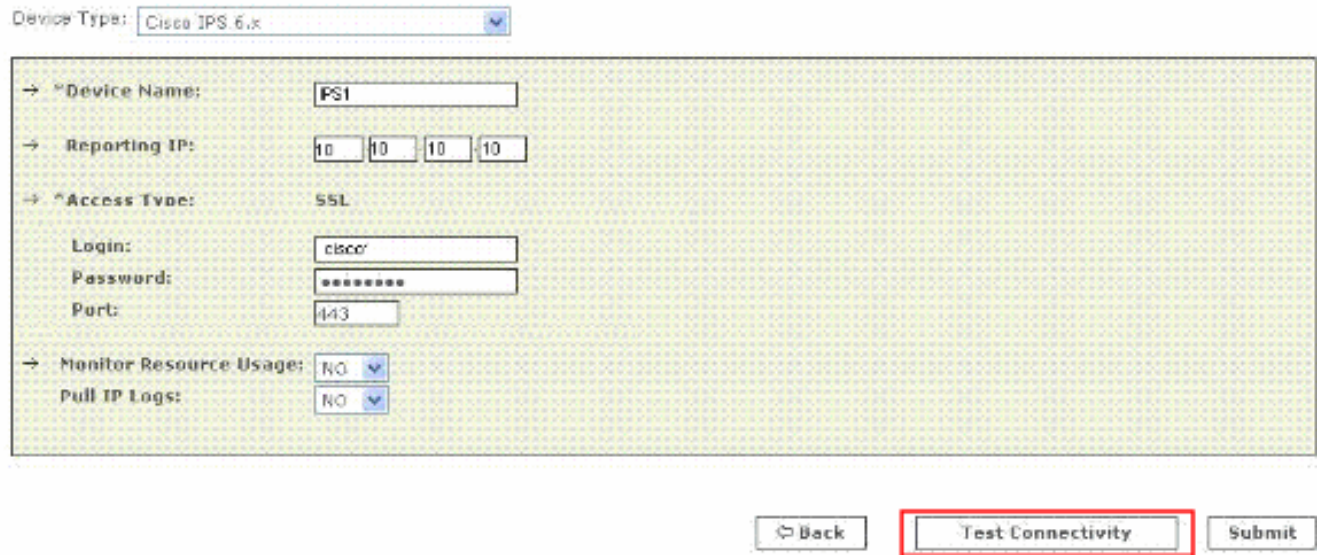


5. Para tirar de los registros IP del sensor, elija **sí de la** lista de **registros IP de la extracción**. Ésta es una característica opcional, que se puede utilizar si procede.

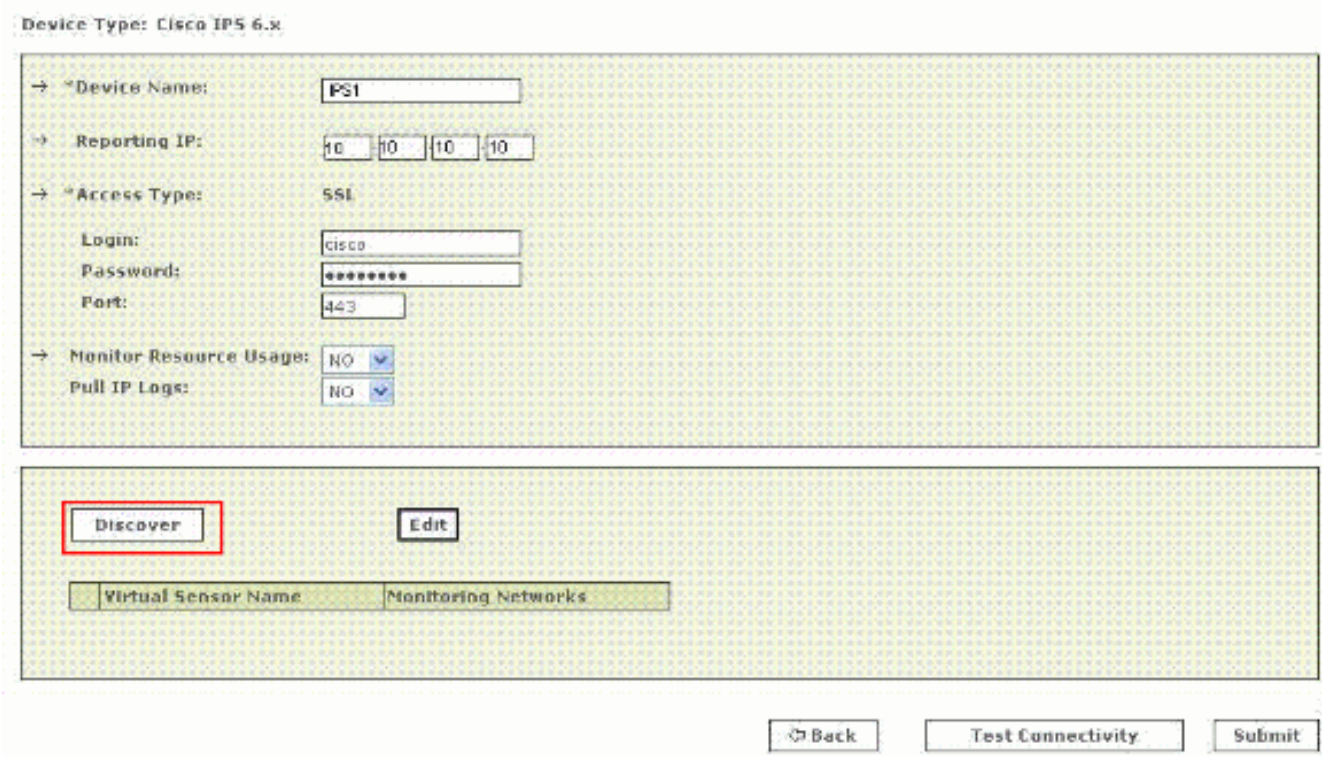


Esta configuración se aplica al sensor entero, que incluye esos registros generados para las alertas virtuales de los sensores.

6. Haga clic la **Conectividad de la prueba** para verificar la configuración y activar el descubrimiento de los sensores virtuales.

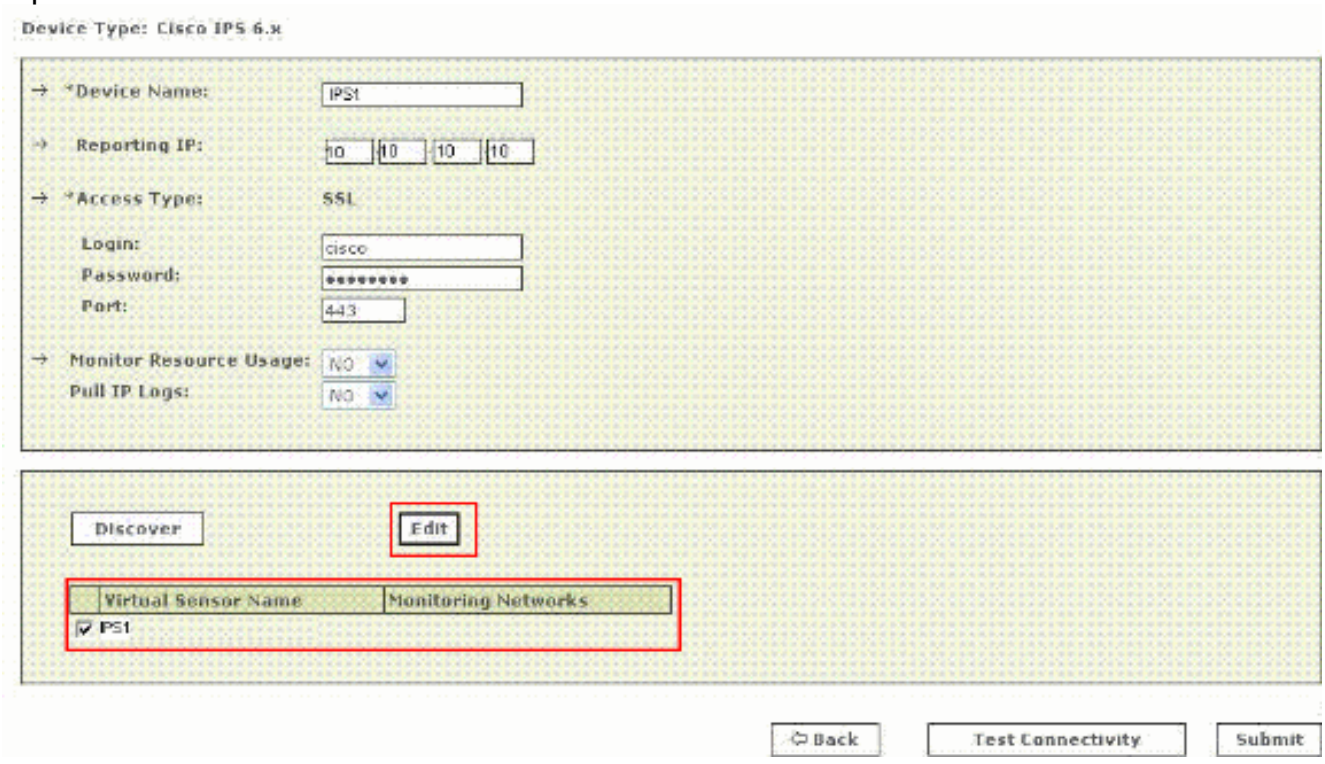


7. El tecleo **descubre** para descubrir cualquier sensor virtual definido.



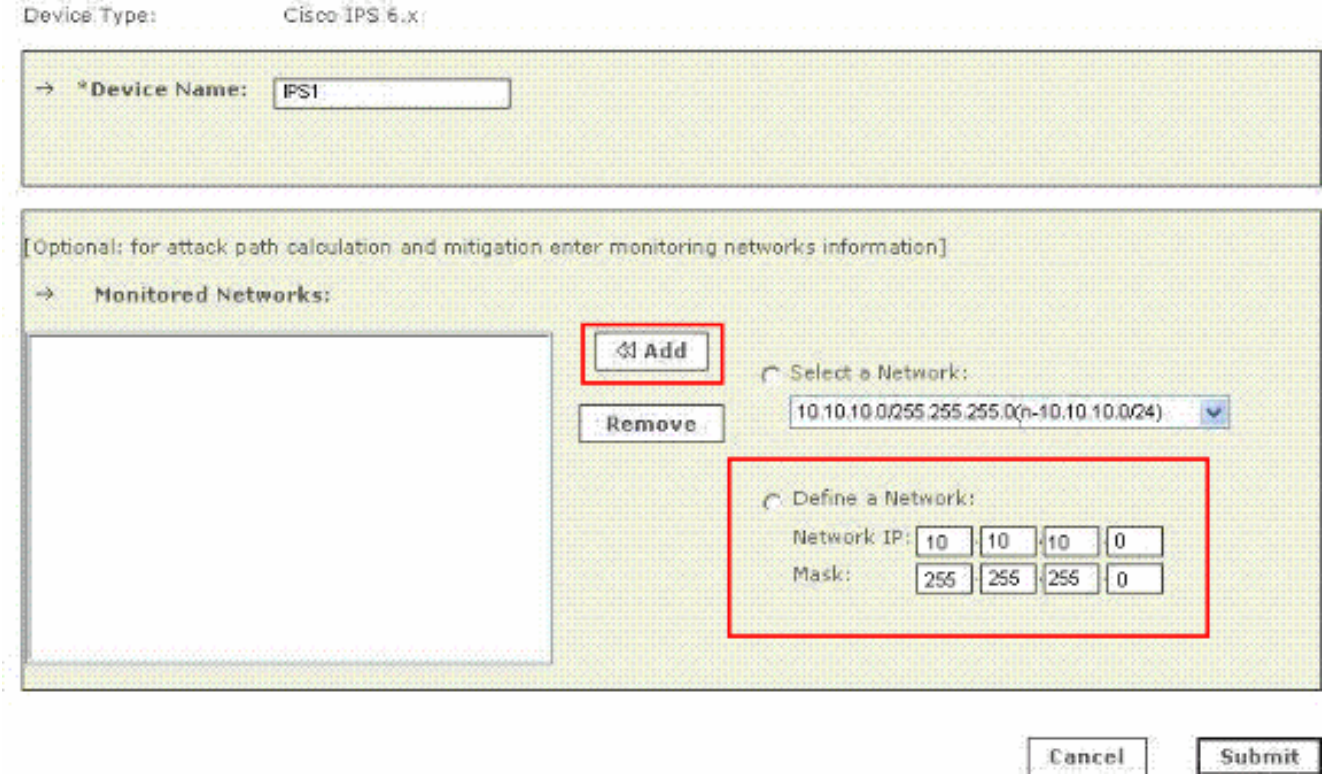
Note: MARTE está inconsciente de los cambios realizados al sensor. Siempre usted realiza los cambios a las configuraciones virtuales del sensor, usted debe hacer clic **descubre** en esa página de la Configuración del sensor para restaurar los detalles virtuales del sensor en MARTE.

8. Elija el checkbox al lado del nombre virtual del sensor y el tecleo **corrige** para definir las redes vigiladas para cada sensor virtual. Ahora la página del módulo ips aparece como se muestra
aquí.



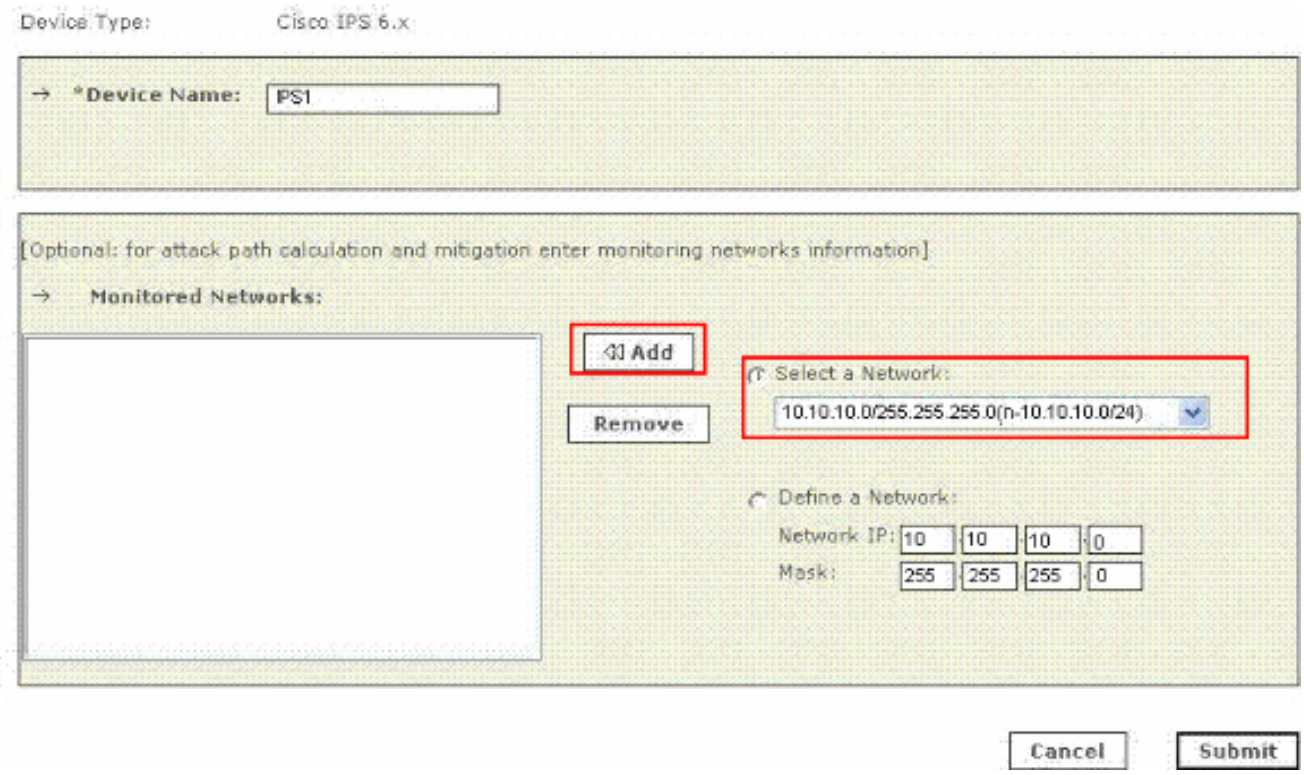
9. Para el cálculo y la mitigación de la trayectoria del ataque, especifique las redes que son vigiladas por el sensor. Elija la **definición un** botón de radio de la **red** para definir

manualmente la red. Entonces complete estos pasos para definir una red:Ingrese a la dirección de red en el campo del **IP de la red**.Ingrese el valor correspondiente de la máscara de la red en el campo de la **máscara**.El tecleo **agrega** para trasladarse la red específicada al campo vigilado de las redes.Relance los pasos anteriores si hay una necesidad de definir más
redes.



Note: Esto es una característica opcional disponible y se puede saltar si no requirió.

10. Haga clic el **selecto un** botón de radio de la **red** en la orden seleccionan las redes que se asocian al dispositivo. Entonces complete estos pasos para elegir las redes:Elija una red del **selecto una lista de red**.El tecleo **agrega** para trasladarse la red específicada al campo vigilado de las redes.Relance los pasos anteriores si hay una necesidad de elegir más redes.



Note: Esto es una característica opcional disponible y se puede saltar si no requirió.

11. Relance el **paso 8** al **paso 10** para cada sensor virtual.
12. El tecleo **somete** para salvar sus cambios. El Nombre del dispositivo aparece conforme a la Seguridad y a la lista de la información de la supervisión. La operación del someter registra los cambios en las tablas de base de datos. Pero, no carga los cambios en memoria de trabajo del dispositivo de MARTE. Las cargas de la operación del activar sometieron los cambios en memoria de trabajo.
13. El tecleo **activa** para permitir a MARTE comenzar a sessionize los eventos de este dispositivo.MARTE comienza a sessionize los eventos generados por este módulo y a evaluar esos eventos usando las reglas definidas del examen y del descenso. Cualquier eventos publicados por el dispositivo a MARTE antes de que la activación se pueda preguntar con la dirección IP de la información del dispositivo como criterio de la coincidencia. Refiérase activan la información y los dispositivos de la mitigación. para más información sobre la acción del activar.

Verifique que MARTE tire de los eventos de un dispositivo del IPS de Cisco

Es común crear los eventos benignos en la red para verificar el flujo de datos. Complete estos pasos para verificar el flujo de datos entre un dispositivo del IPS de Cisco y un MARTE:

1. En el dispositivo del IPS de Cisco, active y alerte en las firmas 2000 y 2004. Los mensajes ICMP del monitor de las firmas (pings).
2. Haga ping un dispositivo en la subred en la cual el dispositivo del IPS de Cisco está escuchando. Los eventos son generados y tirados por MARTE.
3. Verifique que los eventos aparezcan en la interfaz Web de MARTE. Usted puede realizar una interrogación con el dispositivo del IPS de Cisco.
4. Una vez que se verifica el flujo de datos, usted puede inhabilitar las 2000 y 2004 firmas en el dispositivo del IPS de Cisco.**Note**: Si la operación de la Conectividad de la prueba no falla

durante la configuración de un dispositivo del IPS de Cisco en la interfaz Web de MARTE, después se activan las comunicaciones. Esta tarea permite que usted verifique más lejos las alertas estén generadas y tiradas correctamente.

Troubleshooting

No hay actualmente información disponible específica del troubleshooting para esta configuración.

Información Relacionada

- Página de soporte del Cisco Security Monitoring, Analysis and Response System
- Página de soporte del Cisco Intrusion Prevention System
- Cisco Security Monitoring, Analysis and Response System - Información sobre compatibilidad
- Pedidos los comentarios (RFC)
- Soporte técnico y documentación - Cisco Systems