CS-MARS - Aggiunta e configurazione di un sensore IPS come dispositivo di reporting

Sommario

[Introduzione](#)
[Prerequisiti](#)
[Requisiti](#)
[Componenti usati](#)
[Prodotti correlati](#)
[Convenzioni](#)
[Configurazione](#)
[Aggiunta e configurazione di un dispositivo Cisco IPS 6.x o 7.x in MARS](#)
[Verificare che MARS esegua il pull di eventi da un dispositivo IPS Cisco](#)
[Risoluzione dei problemi](#)
[Informazioni correlate](#)

Introduzione

Questo documento spiega come preparare un dispositivo Cisco Secure Intrusion Prevention System (IPS) e tutti i sensori virtuali configurati per agire come dispositivi di report per Cisco Security Monitoring, Analysis, and Response System (CS-MARS).

Prerequisiti

Requisiti

Per i dispositivi Cisco IPS 5.x, 6.x e 7.x, MARS estrae i log utilizzando SDEE su SSL. Pertanto, MARS deve avere accesso HTTPS al sensore. Per preparare il sensore, è necessario abilitare il server HTTP sul sensore, abilitare TLS per consentire l'accesso HTTPS e assicurarsi che l'indirizzo IP di MARS sia definito come host consentito, in grado di accedere al sensore e di eseguire il pull degli eventi. Se i sensori sono stati configurati per consentire l'accesso da host o subnet limitati sulla rete, è possibile usare il comando **access-list ip_address/netmask** per abilitare questo accesso.

Componenti usati

Le informazioni fornite in questo documento si basano sulle seguenti versioni software e hardware:

- Dispositivo Cisco Secure MARS con software versione 4.2.x e successive
- Cisco serie 4200 IPS Device con software versione 6.0 e successive

Le informazioni discusse in questo documento fanno riferimento a dispositivi usati in uno specifico ambiente di emulazione. Su tutti i dispositivi menzionati nel documento la configurazione è stata ripristinata ai valori predefiniti. Se la rete è operativa, valutare attentamente eventuali conseguenze derivanti dall'uso dei comandi.

Prodotti correlati

Questa configurazione può essere utilizzata anche con i seguenti sensori:

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

Convenzioni

Fare riferimento a Cisco Technical Tips Conventions per ulteriori informazioni sulle convenzioni dei documenti.

Configurazione

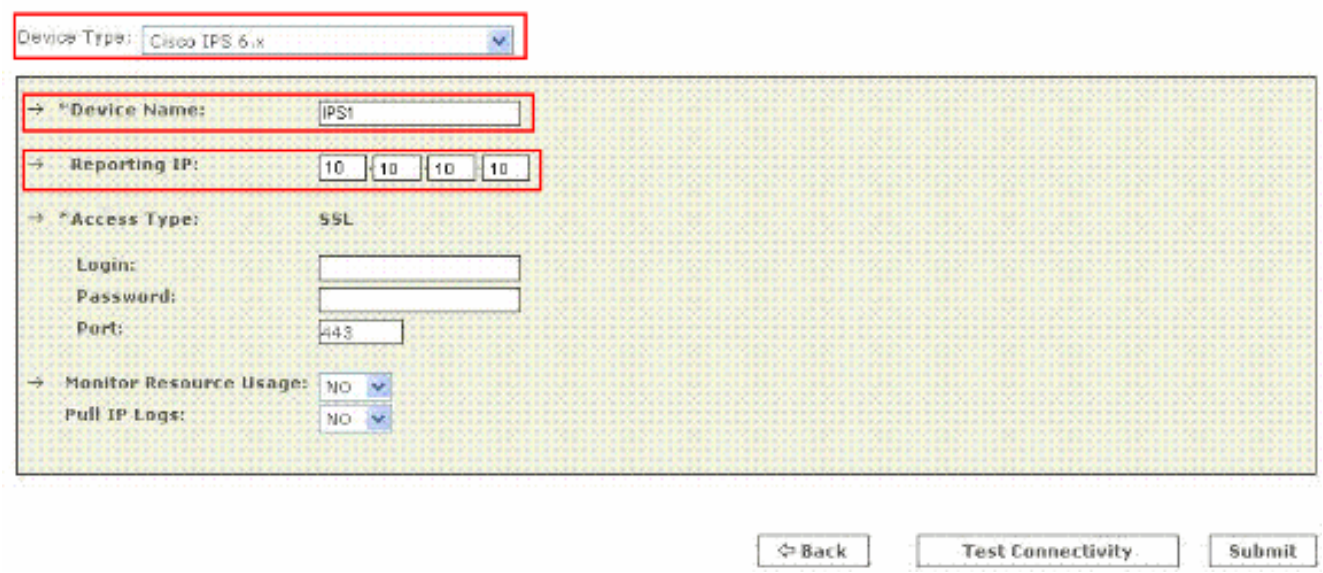
In questa sezione vengono presentate le informazioni su come aggiungere e configurare un sensore Cisco Secure Intrusion Prevention System (IPS) a un dispositivo Cisco Security Monitoring, Analysis, and Response System (CS-MARS).

Aggiunta e configurazione di un dispositivo Cisco IPS 6.x o 7.x in MARS

Quando si definisce un dispositivo Cisco IPS 6.x o 7.x in MARS, è possibile rilevare qualsiasi sensore virtuale configurato sul dispositivo. Quando si rilevano questi sensori virtuali, MARS è in grado di separare gli eventi segnalati per sensore virtuale. Consente inoltre di regolare l'elenco delle reti monitorate per ogni sensore virtuale, migliorando l'accuratezza del report desiderato.

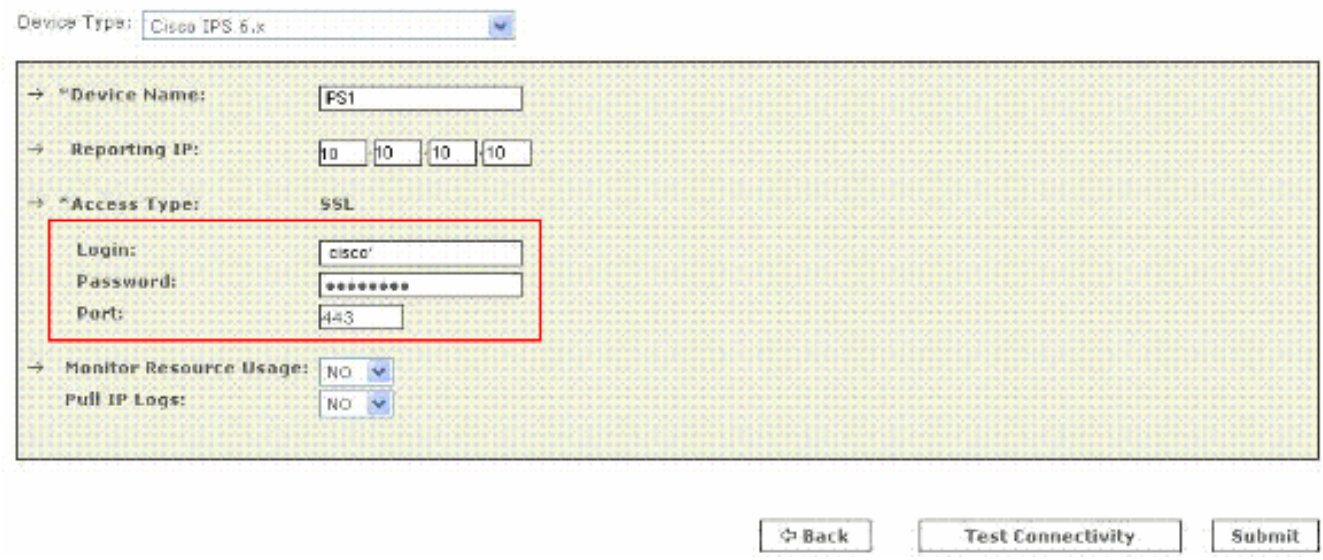
Completare questa procedura per aggiungere e configurare un dispositivo Cisco IPS 6.x o 7.x in MARS:

1. Scegliere **Amministrazione > Configurazione di sistema > Protezione e monitoraggio dispositivi**. Quindi fai clic su **Aggiungi**.
2. Selezionare **Cisco IPS 6.x o Cisco IPS 7.x** dall'elenco Tipo di dispositivo. Immettere il nome host del sensore nel campo **Device Name** (Nome dispositivo), come mostrato di seguito. IPS1 è il nome del dispositivo utilizzato nell'esempio. Il valore di Nome dispositivo deve essere identico al nome del sensore configurato.



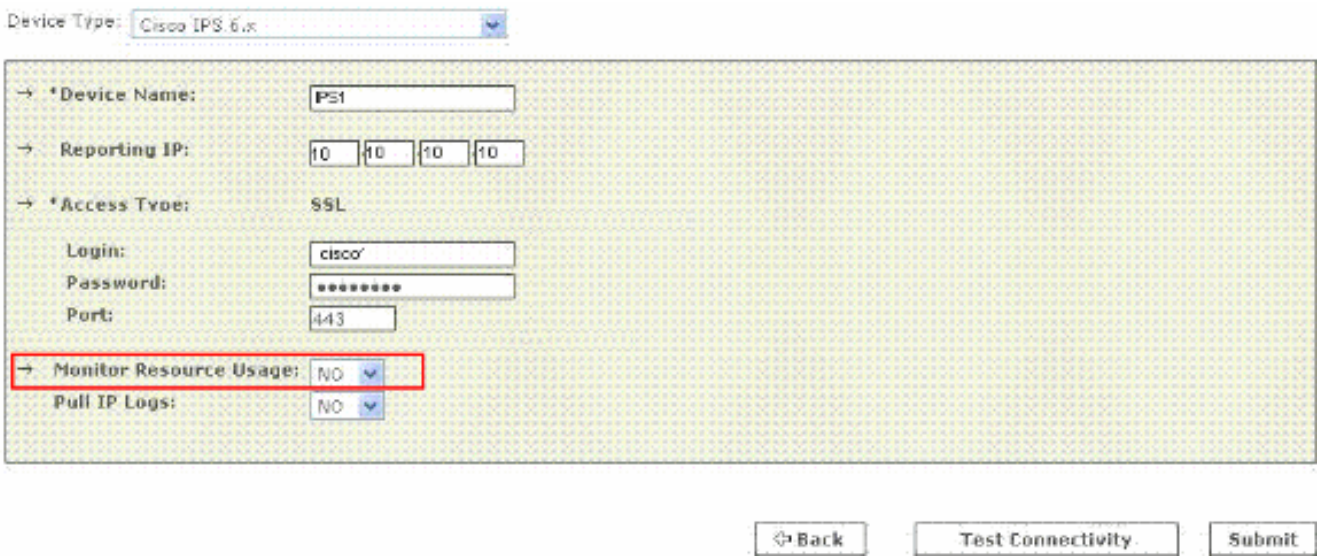
Immettere l'indirizzo IP amministrativo nel campo **IP di reporting**. L'indirizzo IP di report corrisponde all'indirizzo IP amministrativo.

3. Nel **campo Login**, immettere il nome utente associato all'account amministrativo utilizzato per accedere al dispositivo di report. A questo punto, nel **campo Password**, immettere la password associata al nome utente specificato nel **campo Login**. Il **nome utente** è **cisco** e la **password** usata è **cisco123** nell'esempio. Nel **campo Porta** immettere anche il numero della porta TCP su cui è in ascolto il server Web in esecuzione sul sensore. La porta HTTPS predefinita è
   443.

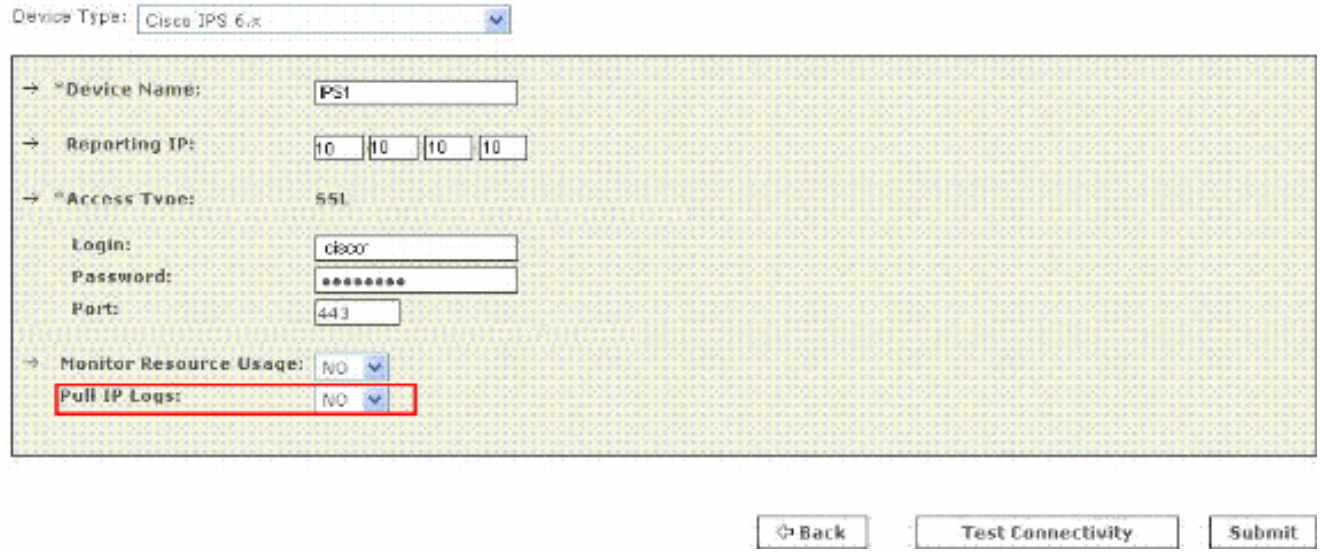


Nota: sebbene sia possibile configurare solo HTTP, MARS richiede HTTPS.

4. Verificare ora che **NO** sia selezionato nell'elenco **Controlla utilizzo risorse**. In questa pagina viene visualizzata l'opzione Controlla uso risorse, ma non funziona per Cisco
   IPS.

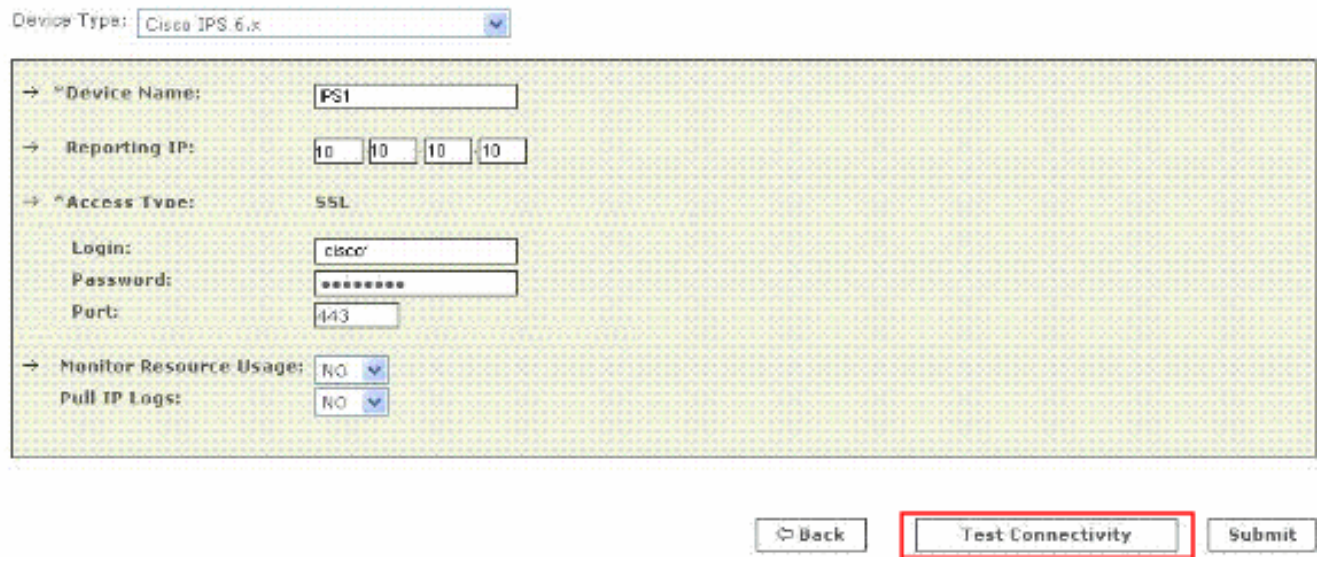


5. Per estrarre i log IP dal sensore, scegliere **Yes** (Sì) dall'elenco **Pull** dei **log IP**. Si tratta di una funzione opzionale che può essere utilizzata se necessario.

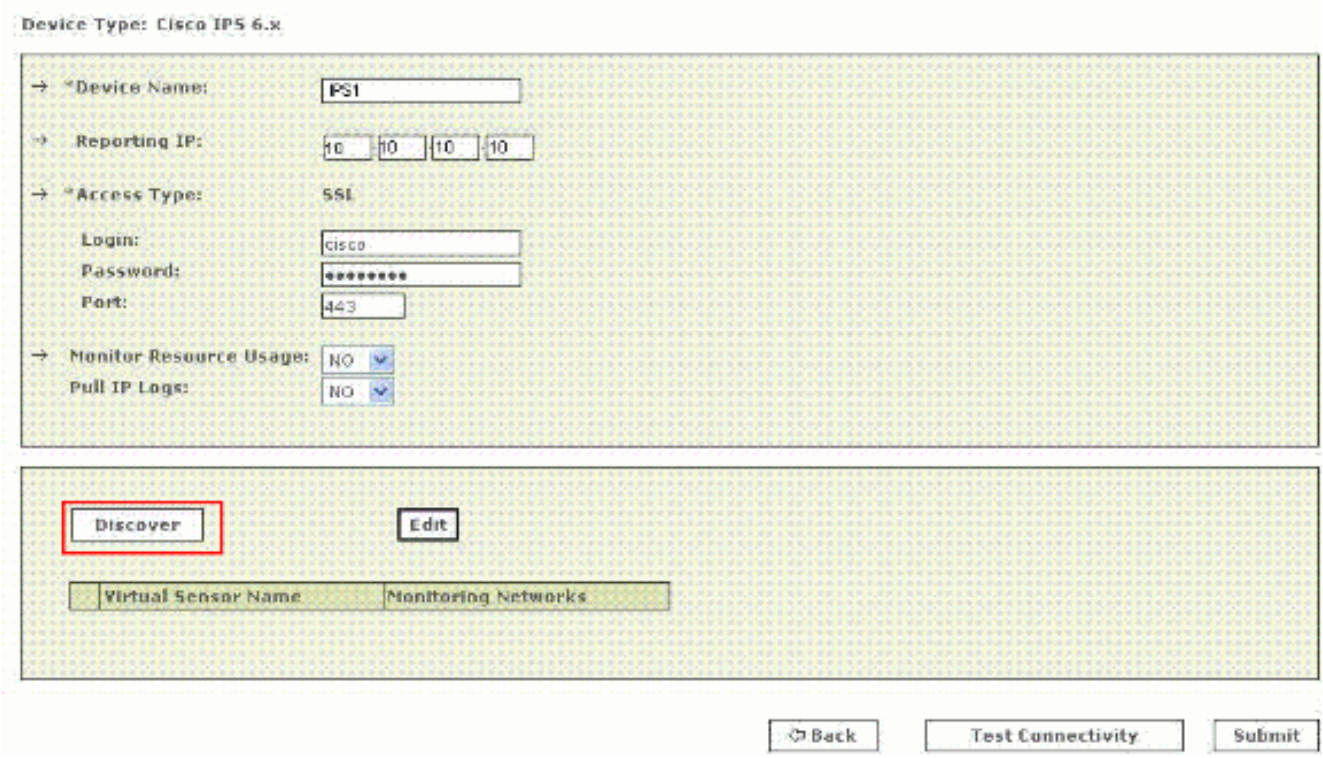


Questa impostazione si applica all'intero sensore, che include i registri generati per gli avvisi dei sensori virtuali.

6. Fare clic su **Test connettività** per verificare la configurazione e abilitare il rilevamento di sensori virtuali.

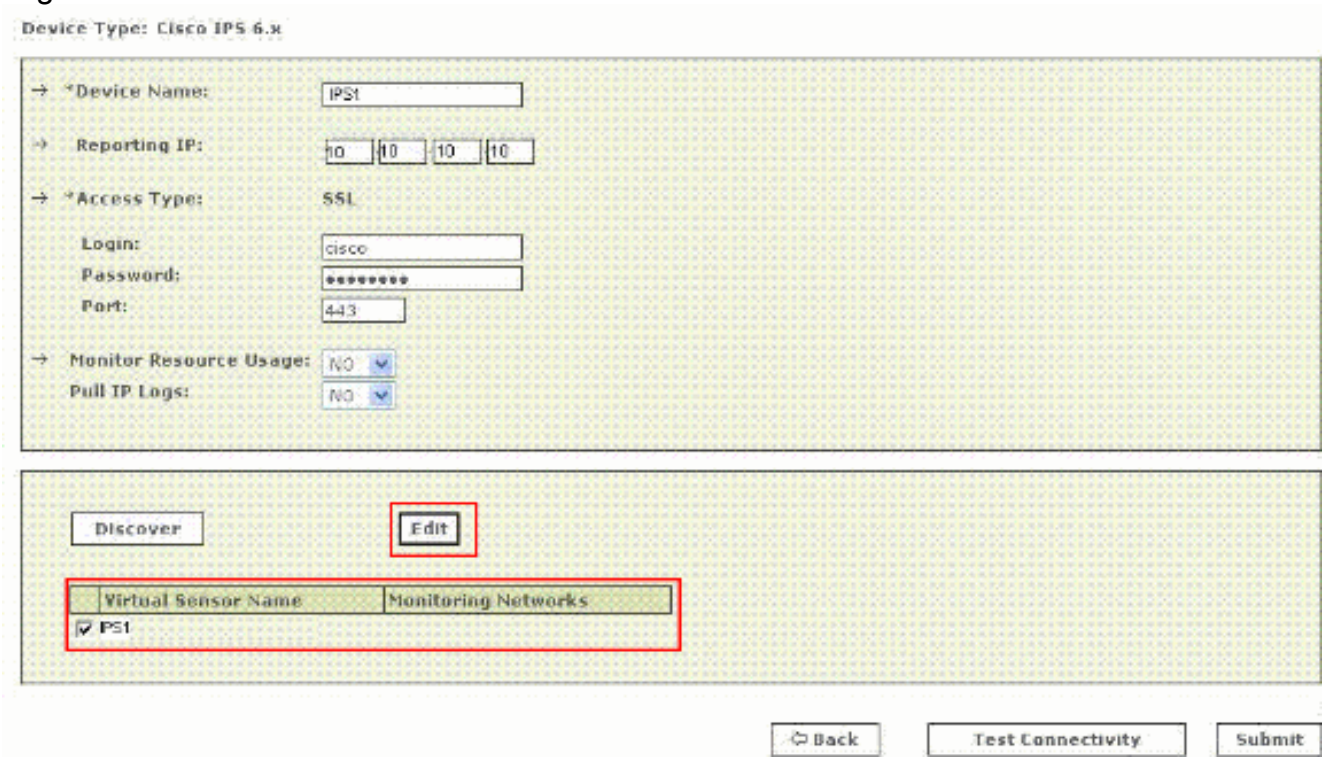


7. Fare clic su **Discover** per individuare eventuali sensori virtuali definiti.



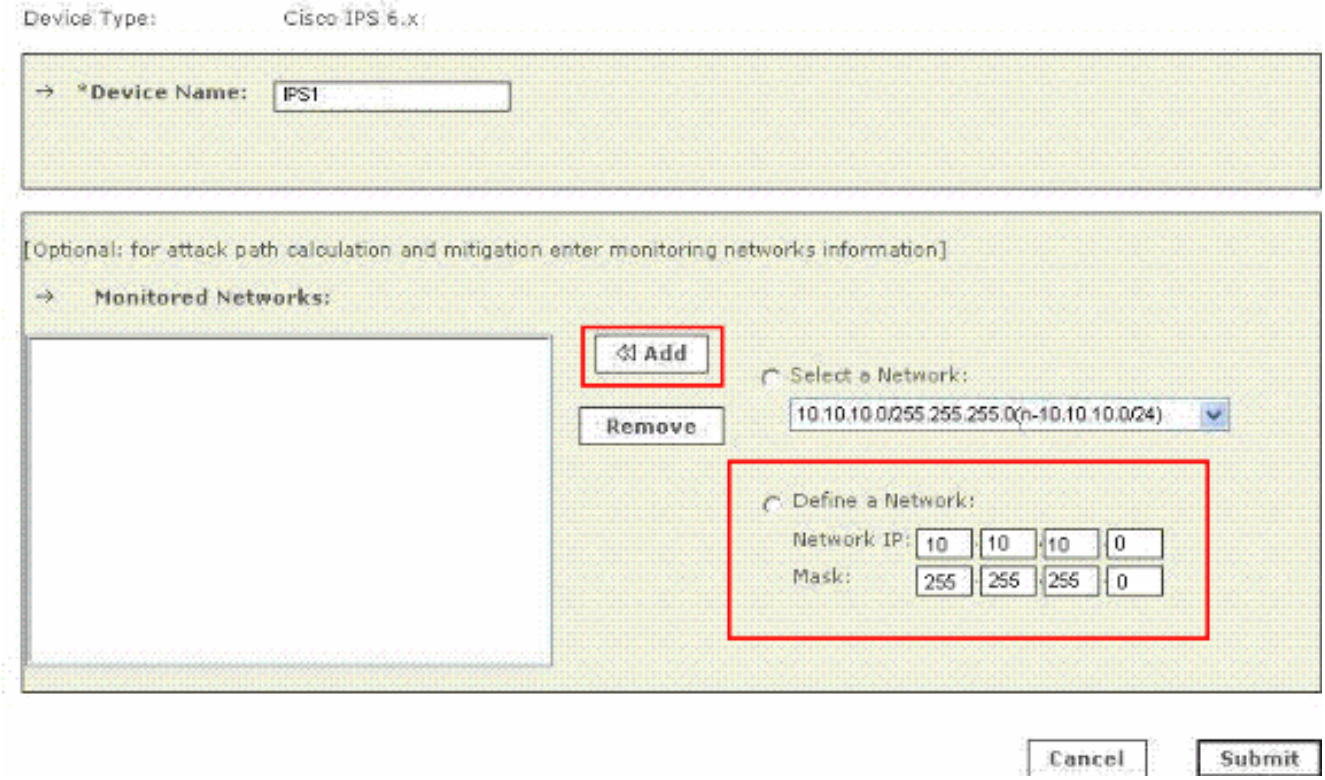
Nota: MARS non è a conoscenza delle modifiche apportate al sensore. Ogni volta che si apportano modifiche alle impostazioni del sensore virtuale, è necessario fare clic su **Discover** nella pagina di configurazione del sensore per aggiornare i dettagli del sensore virtuale in MARS.

8. Selezionare la casella di controllo accanto al nome del sensore virtuale e fare clic su **Modifica** per definire le reti monitorate per ciascun sensore virtuale. A questo punto, viene visualizzata la pagina Modulo IPS, come mostrato di seguito.



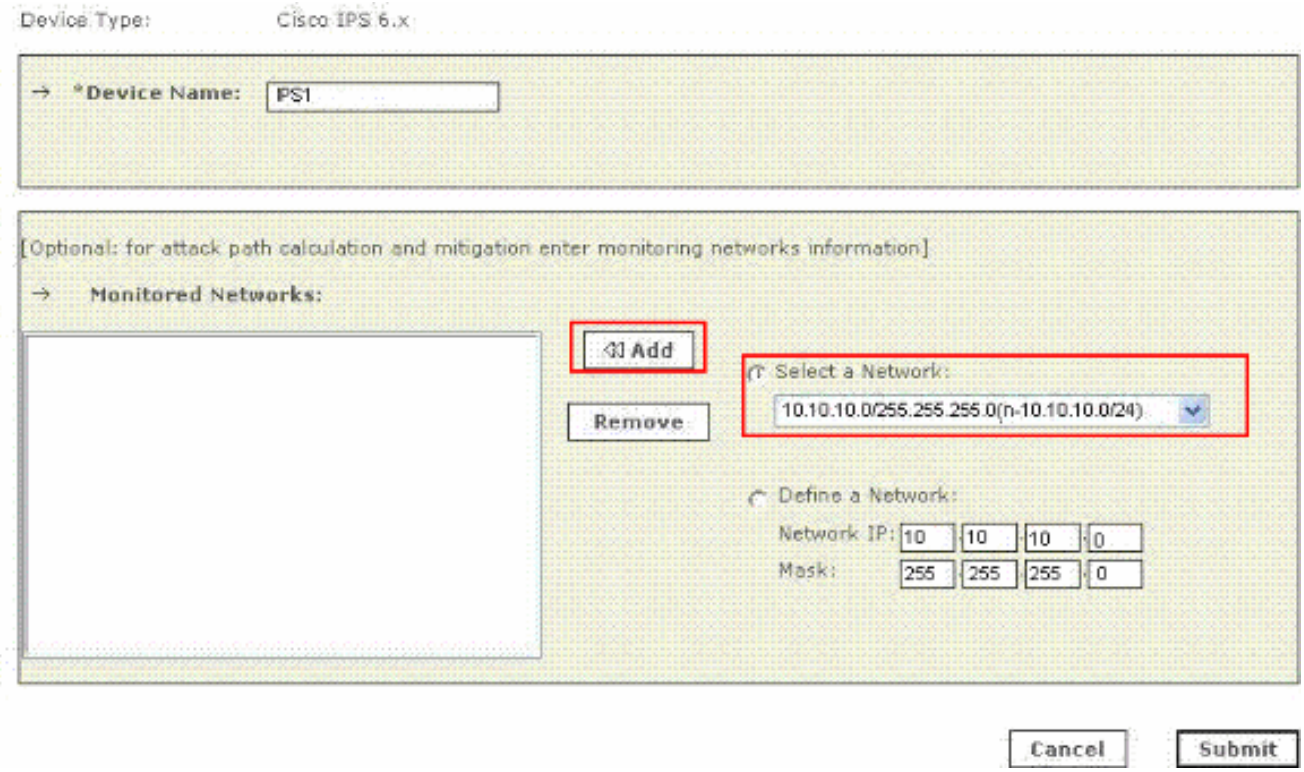
9. Per il calcolo e la mitigazione del percorso di attacco, specificare le reti monitorate dal sensore. Per definire manualmente la rete, selezionare il pulsante di opzione **Definisci una**

rete. Quindi, per definire una rete, completare i seguenti passaggi:Immettere l'indirizzo di rete nel campo **IP rete**.Immettere il valore della maschera di rete corrispondente nel campo **Maschera**.Per spostare la rete specificata nel campo Reti monitorate, fare clic su **Add** (Aggiungi).Ripetere i passaggi precedenti se è necessario definire più reti.



Nota: si tratta di una funzione opzionale disponibile che può essere ignorata se non necessaria.

10. Fare clic sul pulsante di scelta **Seleziona una rete** per selezionare le reti collegate al dispositivo. Quindi, per scegliere le reti, completare i seguenti passaggi:Scegliere una rete dall'elenco **Selezionare una rete**.Per spostare la rete specificata nel campo Reti monitorate, fare clic su **Add** (Aggiungi).Ripetere i passaggi precedenti se è necessario scegliere più reti.



Nota: si tratta di una funzione opzionale disponibile che può essere ignorata se non necessaria.

11. Ripetere i **passaggi da 8** a **10** per ciascun sensore virtuale.
12. Per salvare le modifiche, fare clic su **Submit** (Invia). Il nome del dispositivo viene visualizzato nell'elenco Informazioni su monitoraggio e protezione. L'operazione di invio registra le modifiche nelle tabelle del database. Tuttavia, non carica le modifiche nella memoria di lavoro dell'accessorio MARS. L'operazione di attivazione carica le modifiche inviate nella memoria di lavoro.
13. Fare clic su **Activate** per abilitare MARS per avviare la sessione degli eventi dal dispositivo.MARS inizia a sessionalizzare gli eventi generati da questo modulo e valuta tali eventi utilizzando le regole di ispezione e rilascio definite. Tutti gli eventi pubblicati dal dispositivo su MARS prima dell'attivazione possono essere interrogati con l'indirizzo IP di reporting del dispositivo come criterio di corrispondenza. Fare riferimento alla sezione Attivazione dei dispositivi di reporting e mitigazione. per ulteriori informazioni sull'azione attiva.

Verificare che MARS esegua il pull di eventi da un dispositivo IPS Cisco

Ècomune creare eventi benigni sulla rete per verificare il flusso di dati. Completare questa procedura per verificare il flusso di dati tra un dispositivo Cisco IPS e MARS:

1. Sul dispositivo Cisco IPS, abilitare le firme 2000 e 2004 e inviare un avviso. Le firme monitorano i messaggi ICMP (ping).
2. Eseguire il ping di un dispositivo nella subnet su cui il dispositivo Cisco IPS è in ascolto. Gli eventi sono generati e tirati da MARS.
3. Verificare che gli eventi vengano visualizzati nell'interfaccia Web MARS. È possibile eseguire una query con il dispositivo Cisco IPS.
4. Una volta verificato il flusso di dati, è possibile disabilitare le firme 2000 e 2004 sul

dispositivo Cisco IPS.**Nota:** se l'operazione Test connettività non ha esito negativo durante la configurazione di un dispositivo IPS Cisco nell'interfaccia Web MARS, le comunicazioni vengono abilitate. Questa attività consente di verificare ulteriormente che gli avvisi vengano generati ed estratti correttamente.

Risoluzione dei problemi

Al momento non sono disponibili informazioni specifiche per la risoluzione dei problemi di questa configurazione.

Informazioni correlate

- Pagina di supporto per Cisco Security Monitoring, Analysis and Response System
- Pagina di supporto di Cisco Intrusion Prevention System
- Cisco Security Monitoring, Analysis and Response System - Informazioni sulla compatibilità
- RFC (Requests for Comments)
- Documentazione e supporto tecnico – Cisco Systems