

# CS-MARS: Adicionar o sensor de Cisco IPS como um dispositivo de relatório ao exemplo de configuração CS-MARS

## Índice

[Introdução](#)

[Pré-requisitos](#)

[Requisitos](#)

[Componentes Utilizados](#)

[Produtos Relacionados](#)

[Convenções](#)

[Configurar](#)

[Adicionar e configurar Cisco o dispositivo 6.x ou 7.x IPS em MARTE](#)

[Verifique que MARTE puxa eventos de um dispositivo de Cisco IPS](#)

[Troubleshooting](#)

[Informações Relacionadas](#)

## [Introdução](#)

Este original explica como preparar um dispositivo seguro do Intrusion Prevention System (IPS) de Cisco e todos os sensores virtuais configurados para atuar como dispositivos de relatório à monitoração, à análise, e ao sistema de resposta do Cisco Security (CS-MARS).

## [Pré-requisitos](#)

### [Requisitos](#)

Para Cisco os dispositivos 5.x, 6.x, e 7.x IPS, MARTE puxam os logs usando SDEE sobre o SSL. Conseqüentemente, MARTE deve ter o acesso HTTPS ao sensor. A fim preparar o sensor, você deve permitir o Server do HTTP no sensor, permite o TLS de permitir o acesso HTTPS, e certifica-se que o IP address de MARTE está definido como um host permitido, de um que pode alcançar o sensor e puxar eventos. Se os sensores foram configurados para permitir o acesso dos anfitriões ou das sub-redes limitadas na rede, você pode usar o comando da **lista de acesso ip\_address/netmask** a fim permitir este acesso.

### [Componentes Utilizados](#)

As informações neste documento são baseadas nestas versões de software e hardware:

- Dispositivo seguro de Cisco MARTE que executa a versão de software 4.2.x e mais tarde

- Dispositivo IPS do Cisco 4200 Series que executa a versão de software 6.0 e mais atrasado

As informações neste documento foram criadas a partir de dispositivos em um ambiente de laboratório específico. Todos os dispositivos usados neste original começaram com uma configuração cancelada (do padrão). Se sua rede está viva, certifique-se de que você compreende o impacto potencial do comando any.

## Produtos Relacionados

Esta configuração pode igualmente ser usada com estes sensores:

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

## Convenções

Consulte as [Convenções de Dicas Técnicas da Cisco](#) para obter mais informações sobre convenções de documentos.

## Configurar

Nesta seção, você é apresentado com a informação em como adicionar e configurar um sensor seguro do Intrusion Prevention System (IPS) de Cisco ao dispositivo da monitoração, da análise, e do sistema de resposta de um Cisco Security (CS-MARS).

### Adicionar e configurar Cisco o dispositivo 6.x ou 7.x IPS em MARTE

Quando você define Cisco o dispositivo 6.x ou 7.x IPS em MARTE, você pode descobrir todos os sensores virtuais configurados no dispositivo. Quando você descobre estes sensores virtuais, este permite que MARTE separe os eventos relatados pelo sensor virtual. Igualmente permite que você ajuste a lista de redes monitoradas a cada sensor virtual, que melhora a precisão do relatório desejado.

Termine estas etapas a fim adicionar e configurar Cisco o dispositivo 6.x ou 7.x IPS em MARTE:

1. Escolha > **segurança da instalação Admin > de sistema e monitore dispositivos**. Então, clique sobre **Add**.
2. Escolha **Cisco IPS 6.x** ou **Cisco IPS 7.x** da lista do tipo de dispositivo. Inscreva agora o hostname do sensor no campo de **nome de dispositivo** como mostrado aqui. IPS1 é o nome de dispositivo usado neste exemplo. O valor do nome de dispositivo deve ser idêntico ao nome configurado do sensor.

Device Type: Cisco IPS 6.x

\*Device Name: IPS1

Reporting IP: 10 10 10 10

\*Access Type: SSL

Login:

Password:

Port: 443

Monitor Resource Usage: NO

Pull IP Logs: NO

Back Test Connectivity Submit

Incorpore agora o IP address administrativo ao campo de **relatório IP**. O IP address do relatório é o mesmo endereço que o IP address administrativo.

3. No campo do início de uma sessão, incorpore o username associado com a conta administrativa que é usada para alcançar o dispositivo de relatório. Agora, no campo de senha, incorpore a senha associada com o username especificado no campo do início de uma sessão. O username é Cisco e a senha usada é cisco123 neste exemplo. Igualmente entre no número de porta de TCP em que o web server que é executado no sensor escuta no campo de porta. A porta do padrão HTTPS é 443.

Device Type: Cisco IPS 6.x

\*Device Name: IPS1

Reporting IP: 10 10 10 10

\*Access Type: SSL

Login: cisco

Password: cisco123

Port: 443

Monitor Resource Usage: NO

Pull IP Logs: NO

Back Test Connectivity Submit

**Note:** Quando for possível configurar o HTTP somente, MARTE exige HTTPS.

4. Verifique agora que **NENHUM** chosed na lista do **USO de recurso do monitor**. Quando a opção do USO de recurso do monitor aparecer nesta página, não funciona para Cisco IPS.

Device Type: Cisco IPS 6.x

→ \*Device Name: PS1

→ Reporting IP: 10 10 10 10

→ \*Access Type: SSL

Login: cisco

Password: \*\*\*\*\*

Port: 443

→ Monitor Resource Usage: NO

Pull IP Logs: NO

Back Test Connectivity Submit

5. A fim puxar os logs IP do sensor, escolha **sim** da lista de **logs IP da tração**. Este é uns recursos opcionais, que possam ser usados se for necessário.

Device Type: Cisco IPS 6.x

→ \*Device Name: PS1

→ Reporting IP: 10 10 10 10

→ \*Access Type: SSL

Login: cisco

Password: \*\*\*\*\*

Port: 443

→ Monitor Resource Usage: NO

Pull IP Logs: NO

Back Test Connectivity Submit

Este ajuste aplica-se ao sensor inteiro, que inclui aqueles logs gerados para alertas virtuais dos sensores.

6. Clique a **Conectividade do teste** a fim verificar a configuração e permitir a descoberta de sensores virtuais.

Device Type: Cisco IPS 6.x

→ \*Device Name: PS1

→ Reporting IP: 10 10 10 10

→ \*Access Type: SSL

Login: cisco

Password: \*\*\*\*\*

Port: 443

→ Monitor Resource Usage: NO

Pull IP Logs: NO

Back Test Connectivity Submit

7. O clique **descobre** a fim descobrir todos os sensores virtuais definidos.

Device Type: Cisco IPS 6.x

→ \*Device Name:

→ Reporting IP:

→ \*Access Type: SSL

Login:

Password:

Port:

→ Monitor Resource Usage:  ▼

Pull IP Logs:  ▼

| Virtual Sensor Name          | Monitoring Networks |
|------------------------------|---------------------|
| <input type="checkbox"/> PS1 |                     |

**Note:** MARTE é inconsciente das mudanças feitas ao sensor. Quando você faz mudanças aos ajustes virtuais do sensor, você deve clicar **descobre** nessa página da configuração de sensor a fim refrescar os detalhes virtuais do sensor em MARTE.

8. Escolha a caixa de seleção ao lado do nome virtual do sensor e o clique **edita** a fim definir as redes monitoradas para cada sensor virtual. Agora a página do módulo ips publica-se como mostrado aqui.

Device Type: Cisco IPS 6.x

→ \*Device Name:

→ Reporting IP:

→ \*Access Type: SSL

Login:

Password:

Port:

→ Monitor Resource Usage:  ▼

Pull IP Logs:  ▼

| Virtual Sensor Name                      | Monitoring Networks |
|--|---------------------|
| <input checked="" type="checkbox"/> IPS1 |                     |

9. Para o cálculo e a mitigação do trajeto do ataque, especifique as redes que estão sendo monitoradas pelo sensor. Escolha a **definição** um botão de rádio da **rede** a fim definir manualmente a rede. Termine então estas etapas a fim definir uma rede: Incorpore o

endereço de rede ao campo do **IP de rede**. Incorpore o valor correspondente da máscara de rede ao campo da **máscara**. O clique **adiciona** a fim mover a rede especificada no campo monitorado das redes. Repita as etapas precedentes se há uma necessidade de definir mais redes.

Device Type: Cisco IPS 6.x

→ \*Device Name:

[Optional: for attack path calculation and mitigation enter monitoring networks information]

→ Monitored Networks:

Select a Network:

Define a Network:  
Network IP:      
Mask:

**Note:** Este é uns recursos opcionais disponíveis e pode ser saltado se não exigiu.

10. Clique o **seleto um** botão de rádio da **rede** em ordem selecionam as redes que são anexadas ao dispositivo. Termine então estas etapas a fim escolher as redes: Escolha uma rede do **seleto um liste de redes**. O clique **adiciona** a fim mover a rede especificada no campo monitorado das redes. Repita as etapas precedentes se há uma necessidade de escolher mais redes.

Device Type: Cisco IPS 6.x

→ \*Device Name:

[Optional: for attack path calculation and mitigation enter monitoring networks information]

→ Monitored Networks:

Select a Network:

Define a Network:  
Network IP:      
Mask:

**Note:** Este é uns recursos opcionais disponíveis e pode ser saltado se não exigiu.

11. Repita **etapa 8** com a **etapa 10** para cada sensor virtual.
12. O clique **submete-se** a fim salvar suas mudanças. O nome de dispositivo aparece sob a Segurança e a lista da informação da monitoração. A operação da submissão grava as mudanças nas tabelas de base de dados. Mas, não carrega as mudanças na memória de funcionamento do dispositivo de MARTE. As cargas da operação da ativação submeteram mudanças na memória de funcionamento.
13. O clique **ativa** a fim permitir MARTE de começar sessionize eventos deste dispositivo. MARTE começa a sessionize os eventos gerados por este módulo e a avaliar aqueles eventos usando as regras definidas da inspeção e da gota. Alguns eventos publicados pelo dispositivo a MARTE antes que a ativação puder ser perguntada com o IP address do relatório do dispositivo como um critério do fósforo. Consulte [para ativar o relatório e os dispositivos da mitigação](#). para obter mais informações sobre da ação da ativação.

## [Verifique que MARTE puxa eventos de um dispositivo de Cisco IPS](#)

É comum criar eventos benignos na rede a fim verificar o fluxo de dados. Termine estas etapas a fim verificar o fluxo de dados entre um dispositivo de Cisco IPS e um MARTE:

1. No dispositivo de Cisco IPS, permita e alerta nas assinaturas 2000 e 2004. Os mensagens ICMP do monitor das assinaturas (sibilos).
2. Sibile um dispositivo na sub-rede em que o dispositivo de Cisco IPS está escutando. Os eventos são gerados e puxados por MARTE.
3. Verifique que os eventos aparecem na interface da WEB de MARTE. Você pode executar uma pergunta com o dispositivo de Cisco IPS.
4. Uma vez que o fluxo de dados é verificado, você pode desabilitar as 2000 e 2004 assinaturas no dispositivo de Cisco IPS. **Note:** Se a operação da Conectividade do teste não falha durante a configuração de um dispositivo de Cisco IPS na interface da WEB de MARTE, a seguir as comunicações estão permitidas. Esta tarefa permite que você verifique mais os alertas estão gerados e puxados corretamente.

## [Troubleshooting](#)

Atualmente, não existem informações disponíveis específicas sobre Troubleshooting para esta configuração.

## [Informações Relacionadas](#)

- [Página de suporte do Sistema de monitoramento de segurança, análise e resposta da Cisco](#)
- [Página de suporte do Sistema de prevenção de intrusões da Cisco](#)
- [Sistema de monitoramento de segurança, análise e resposta da Cisco - Informação de compatibilidade](#)
- [Request for comments \(RFC\)](#)
- [Suporte técnico & documentação - Cisco Systems](#)