Configurar o registro no FTD usando o FMC

Contents

Introdução

Este documento descreve a configuração de registro para um FirePOWER Threat Defense (FTD) por meio do Firepower Management Center (FMC).

Pré-requisitos

Requisitos

A Cisco recomenda que você tenha conhecimento destes tópicos:

- Tecnologia FirePOWER
- Dispositivo de segurança adaptável (ASA)
- protocolo de Syslog

Componentes Utilizados

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

- Imagem do ASA Firepower Threat Defense para ASA (5506X/5506H-X/5506W-X, ASA 5508-X, ASA 5516-X) com software versão 6.0.1 e posterior
- Imagem do ASA Firepower Threat Defense para ASA (5515-X, ASA 5525-X, ASA 5545-X, ASA 5555-X, ASA 5585-X) com software versão 6.0.1 e posterior
- FMC Versão 6.0.1 e posterior

As informações neste documento foram criadas a partir de dispositivos em um ambiente de laboratório específico. Todos os dispositivos utilizados neste documento foram iniciados com uma configuração

(padrão) inicial. Se a rede estiver ativa, certifique-se de que você entenda o impacto potencial de qualquer comando.

Informações de Apoio

Os registros do sistema FTD fornecem as informações para monitorar e solucionar problemas do dispositivo FTD.

Os registros são úteis na solução de problemas de rotina e no tratamento de incidentes. O dispositivo de FTD oferece suporte a registro local e externo.

O registro local pode ajudá-lo a solucionar os problemas em tempo real. O registro externo é um método de coleta de registros do dispositivo FTD para um servidor Syslog externo.

O registro em um servidor central ajuda na agregação de registros e alertas. O registro externo pode ajudar na correlação de registros e no tratamento de incidentes.

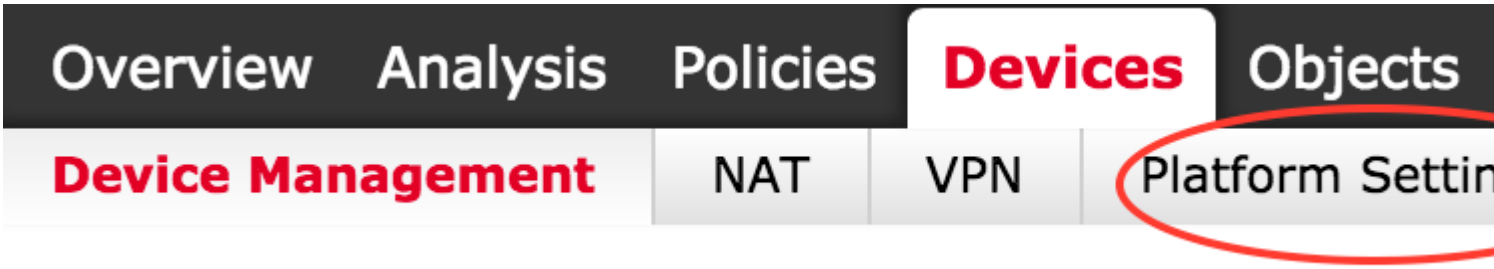
Para o registro local, o dispositivo FTD suporta console, opção de buffer interno e o registro de sessão Secure Shell (SSH).

Para registro externo, o dispositivo FTD oferece suporte ao servidor Syslog externo e ao servidor de retransmissão de e-mail.

> **Observação**: se um grande volume de tráfego passar pelo dispositivo, preste atenção no tipo de registro/gravidade/limitação de taxa. Faça isso para limitar o número de logs, o que evita o impacto no firewall.

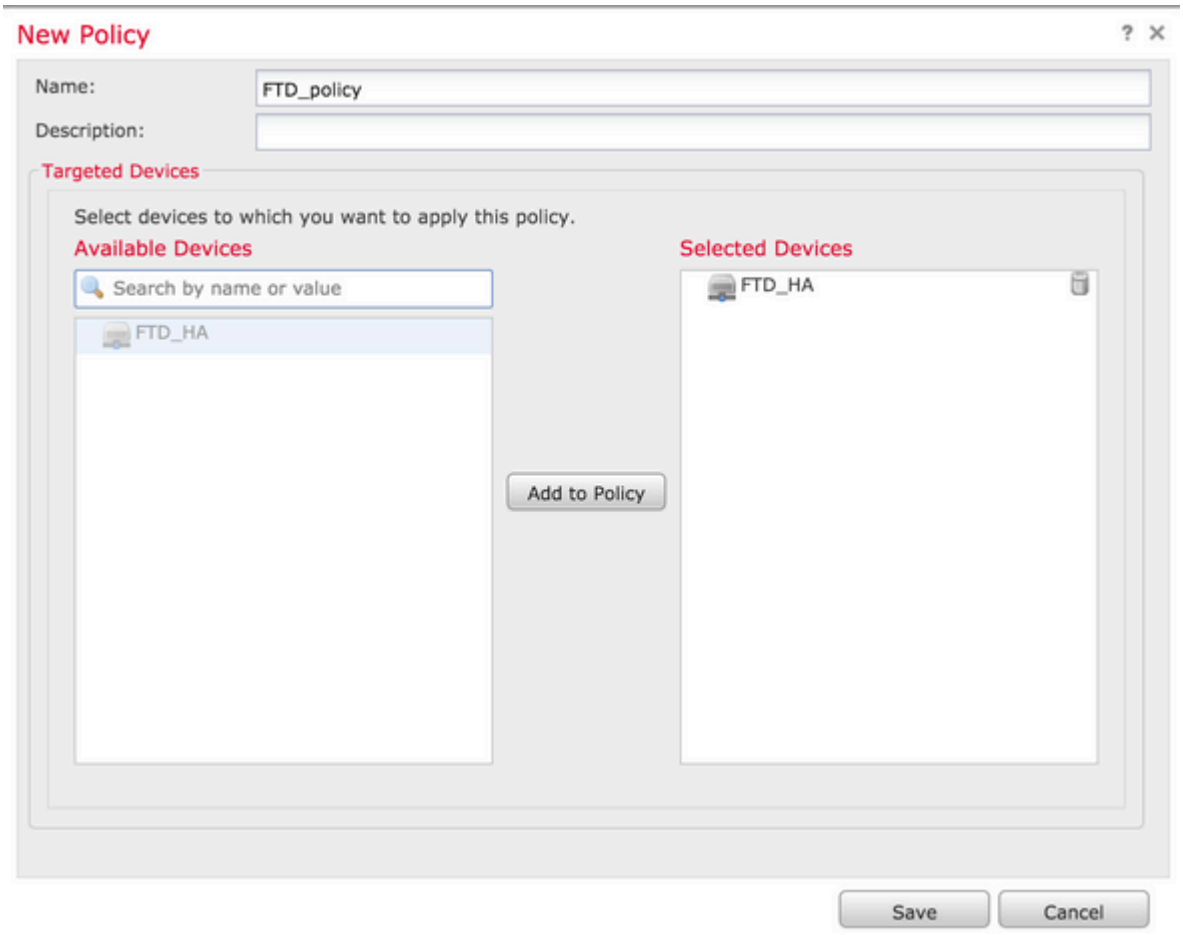
Configurar

Todas as configurações relacionadas ao registro podem ser configuradas quando você navega para a Platform Settings sob a guia Devices guia. Escolher Devices > Platform Settings como mostrado nesta imagem.



Clique no ícone do lápis para editar a diretiva existente ou clique em **New Policy**e escolha **Threat Defense Settings**para criar uma nova política de FTD como mostrado nesta imagem.

Escolha o dispositivo FTD para aplicar esta política e clique em **Save** como mostrado nesta imagem.



Configurar a configuração global do Syslog

Há certas configurações que são aplicáveis para o registro local e externo. Esta seção trata dos parâmetros obrigatórios e opcionais que podem ser configurados para Syslog.

Configuração de registro

As opções de configuração de registro são aplicáveis para registro local e externo. Para configurar a configuração de Log, escolha **Devices > Platform Settings.**

Escolher **Syslog > Logging Setup.**

Configuração básica de registro

- Enable Logging: Verifique o **Enable Logging** para habilitar o registro em log. Essa é uma opção obrigatória.
- Enable Logging on the failover standby unit: Verifique o **Enable Logging on the failover standby unit** para configurar o registro no FTD de espera que faz parte de um cluster de alta disponibilidade do FTD.
- Send syslogs in EMBLEM format: Verifique o **Send syslogs in EMBLEM format** para habilitar o formato de Syslog como EMBLEM para cada destino. O formato EMBLEM é usado principalmente para o analisador de Syslog do CiscoWorks Resource Manager Essentials (RME). Esse formato corresponde ao formato Syslog do Cisco IOS Software produzido pelos roteadores e pelos switches. Ele está disponível somente para servidores UDP Syslog.
- Send debug messages as syslogs: Verifique o **Send debug messages as syslogs** para enviar os logs de depuração como mensagens de Syslog ao servidor Syslog.
- Memory size of the Internal Buffer: insira o tamanho do buffer de memória interna em que o FTD pode salvar os dados de log. Os dados de log serão girados se o limite de buffer for atingido.

Informações do Servidor FTP (Opcional)

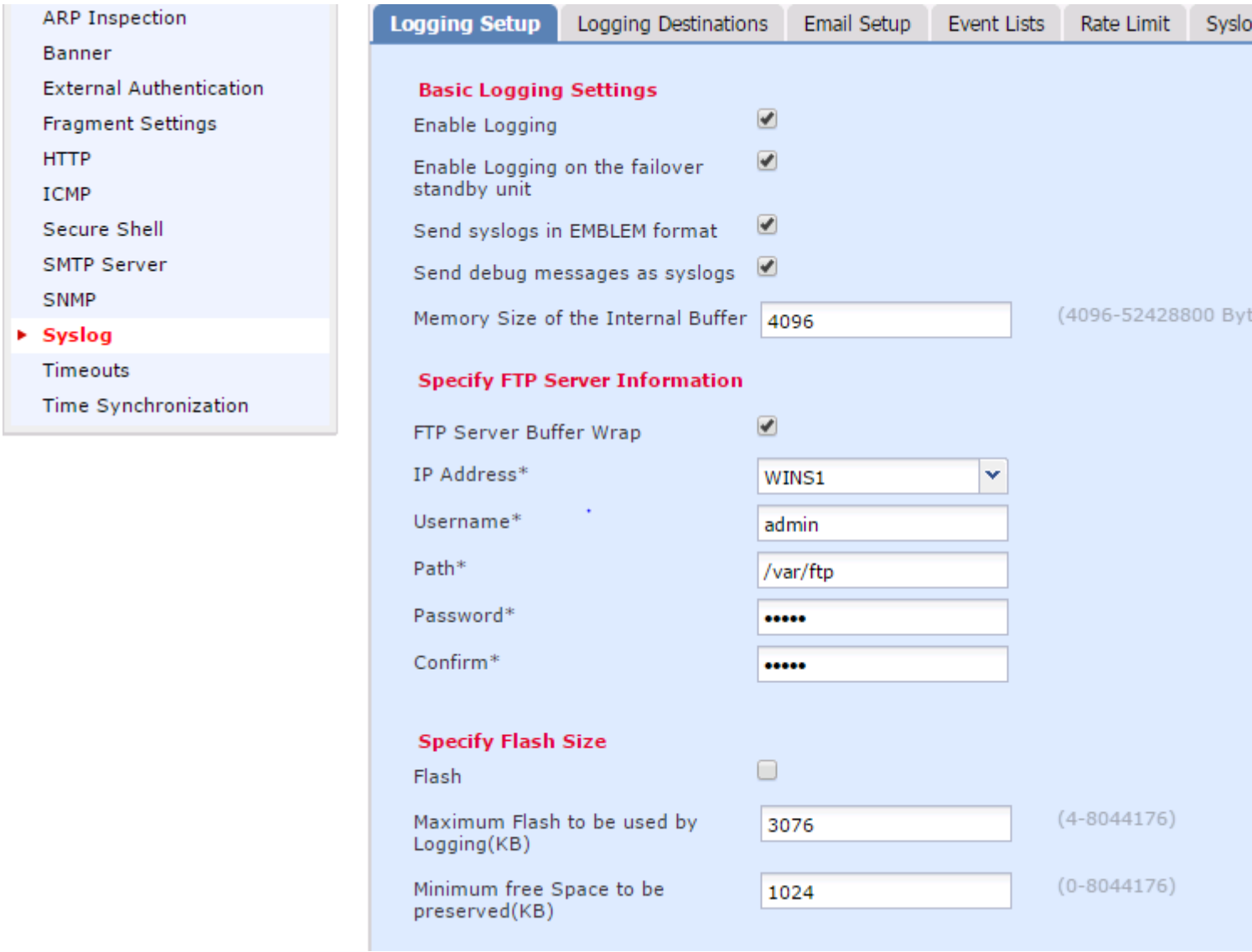
Especifique os detalhes do servidor FTP se quiser enviar os dados de log ao servidor FTP antes que ele substitua o buffer interno.

- FTP Server Buffer Wrap: Verifique o **FTP Server Buffer Wrap** para enviar os dados de log do buffer ao servidor FTP.
- IP Address: insira o endereço IP do servidor FTP.
- Username: insira o nome de usuário do servidor FTP.
- Path: insira o caminho do diretório do servidor FTP.
- Password: digite a senha do servidor FTP.
- Confirm: digite a mesma senha novamente.

Tamanho do Flash (Opcional)

Especifique o tamanho da memória flash se quiser salvar os dados de log na memória flash depois que o buffer interno estiver cheio.

- Flash: Verifique o **Flash** para enviar os dados de registro para a memória flash interna.
- Maximum Flash to be used by Logging(KB): insira o tamanho máximo em KB de memória flash que pode ser usado para registro em log.
- Minimum free Space to be preserved(KB): insira o tamanho mínimo em KB da memória flash que precisa ser preservada.



Clique em **Save** para salvar a configuração da plataforma. Escolha o **Deploy** selecione o dispositivo FTD onde deseja aplicar as alterações e clique em **Deploy** para iniciar a implantação da configuração da plataforma.

Listas de eventos

A opção Configurar Listas de Eventos permite criar/editar uma lista de eventos e especificar quais dados de log incluir no filtro da lista de eventos. Listas de eventos podem ser usadas quando você configura Filtros de registro em Destinos de registro.

O sistema permite duas opções para usar a funcionalidade de listas de eventos personalizadas.

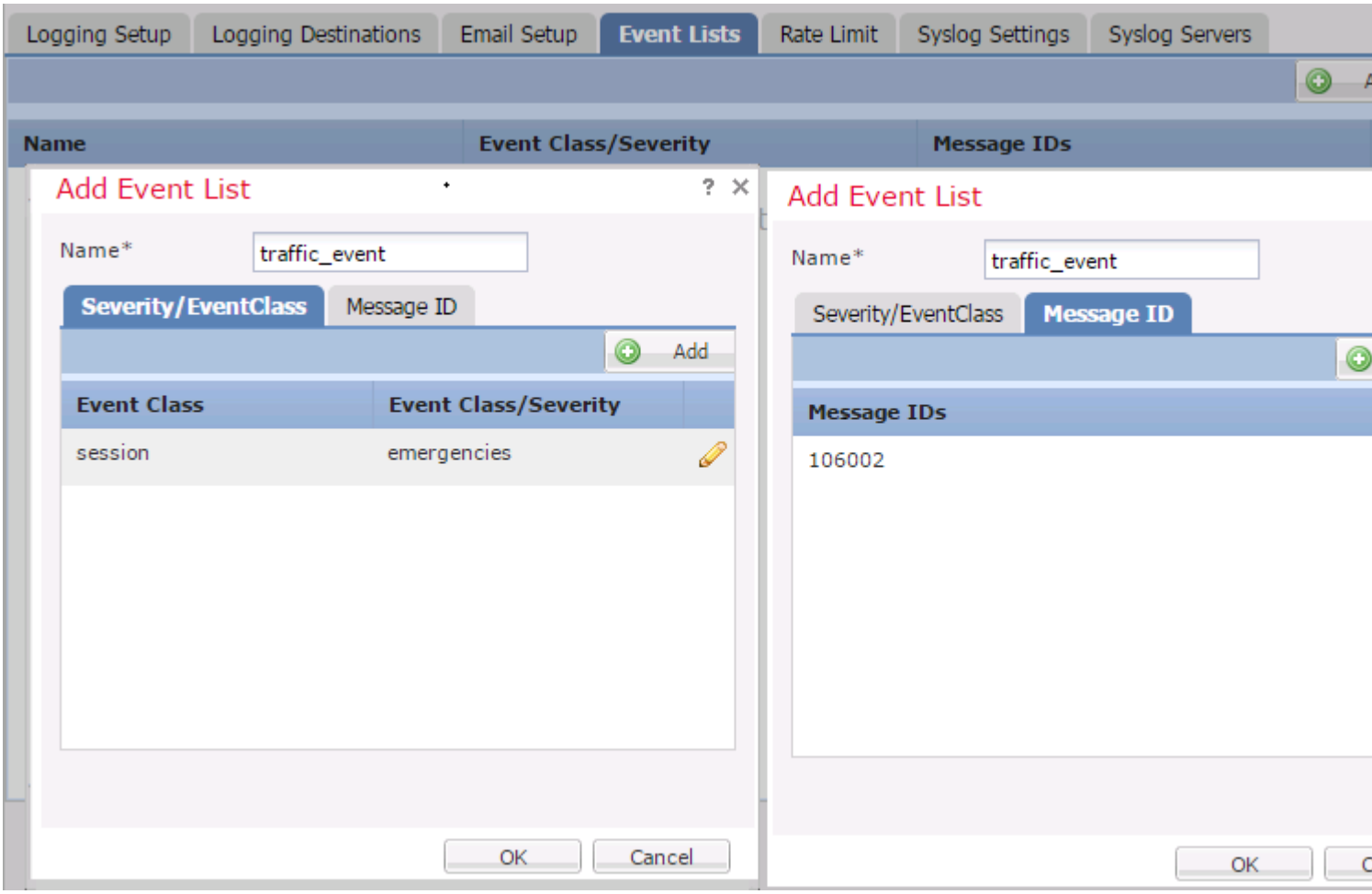
- Classe e gravidade
- ID da mensagem

Para configurar listas de eventos personalizadas, escolha **Device** > **Platform Setting** > **Threat Defense Policy** > **Syslog** > **Event List** e clique em **Add**. Estas são as opções:

- Name: digite o nome da lista de eventos.
- Severity/Event Class: na seção Severidade/Classe de Evento, clique em **Add**.
- Event Class: escolha a classe de evento na lista suspensa para o tipo de dados de log desejado. Uma classe Event define um conjunto de regras de Syslog que representam os mesmos recursos.

Por exemplo, há uma classe de evento para a sessão que inclui todos os Syslogs relacionados à sessão.

- Syslog Severity: escolha a gravidade na lista suspensa para a classe de evento escolhida. A gravidade pode variar de 0 (emergência) a 7 (depuração).
- Message ID: Se estiver interessado em dados de log específicos relacionados a uma ID de mensagem, clique em **Add** para colocar um filtro com base no ID da mensagem.
- Message IDs: Especifique o ID da mensagem como formato individual/ de intervalo.



Clique em **OK** para salvar a configuração.

Clique em **Save** para salvar a configuração da plataforma. Escolha entre **Deploy**, escolha o dispositivo FTD onde deseja aplicar as alterações e clique em **Deploy**para iniciar a implantação da configuração da plataforma.

Syslog de limitação de taxa

A opção Limite de taxa define o número de mensagens que podem ser enviadas a todos os destinos configurados e define a gravidade da mensagem à qual você deseja atribuir limites de taxa.

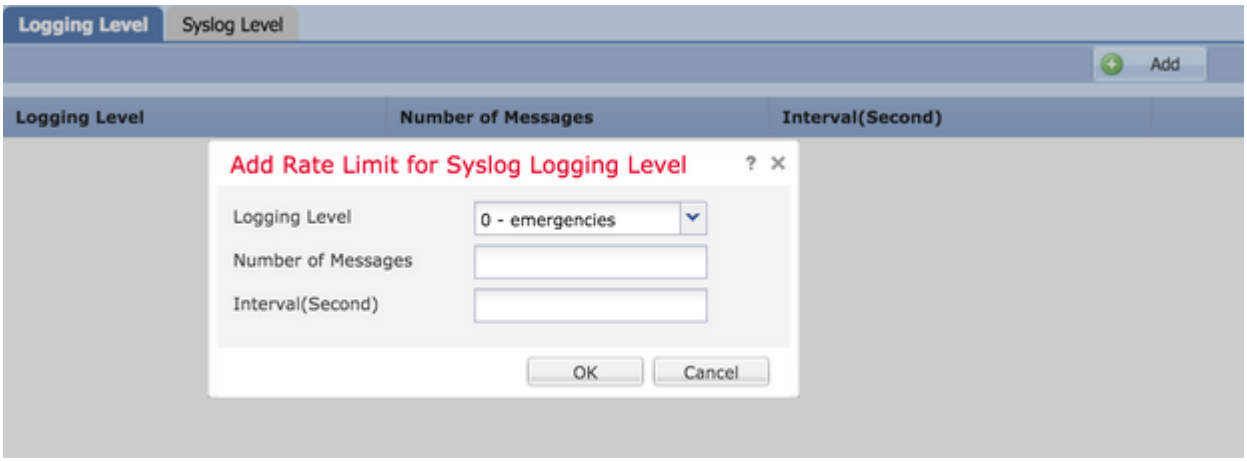
Para configurar listas de eventos personalizadas, escolha **Device > Platform Setting > Threat Defense Policy > Syslog > Rate Limit.** Você tem duas opções com base nas quais pode especificar o limite de taxa:

- Nível de registro
- Níveis de Syslog

Para habilitar o limite de taxa baseado em nível de registro, escolha **Logging Level** e clique em **Add.**

- Logging Level:Nos **Logging Level** selecione o nível de log para o qual deseja executar a limitação de taxa.
- Number of Messages: insira o número máximo de mensagens de Syslog a serem recebidas dentro do intervalo especificado.
- Interval(Second): com base no parâmetro Número de mensagens configurado anteriormente, insira o intervalo de tempo no qual um conjunto fixo de mensagens de Syslog pode ser recebido.

A taxa de Syslog é o número de mensagens/intervalos.



Clique em **OK** para salvar a configuração do nível de registro.

Para habilitar o limite de taxa baseado no nível de registro, escolha **Logging Level** e clique em **Add**.

- Syslog ID: as IDs de Syslog são usadas para identificar exclusivamente as mensagens de Syslog. Nos **Syslog ID** selecione o ID do Syslog.
- Number of Messages: insira o número máximo de mensagens de syslog a serem recebidas dentro do intervalo especificado.
- Interval(Second): com base no parâmetro Número de mensagens configurado anteriormente, insira o intervalo de tempo no qual um conjunto fixo de mensagens de Syslog pode ser recebido.

A taxa de Syslog é o número de mensagens/intervalo.

Clique em **OK** para salvar a configuração de nível de Syslog.

Clique em **Save** para salvar a configuração da plataforma. Escolha entre **Deploy**, escolha o dispositivo FTD onde deseja aplicar as alterações e clique em **Deploy** para iniciar a implantação da configuração da plataforma.

Configurações de Syslog

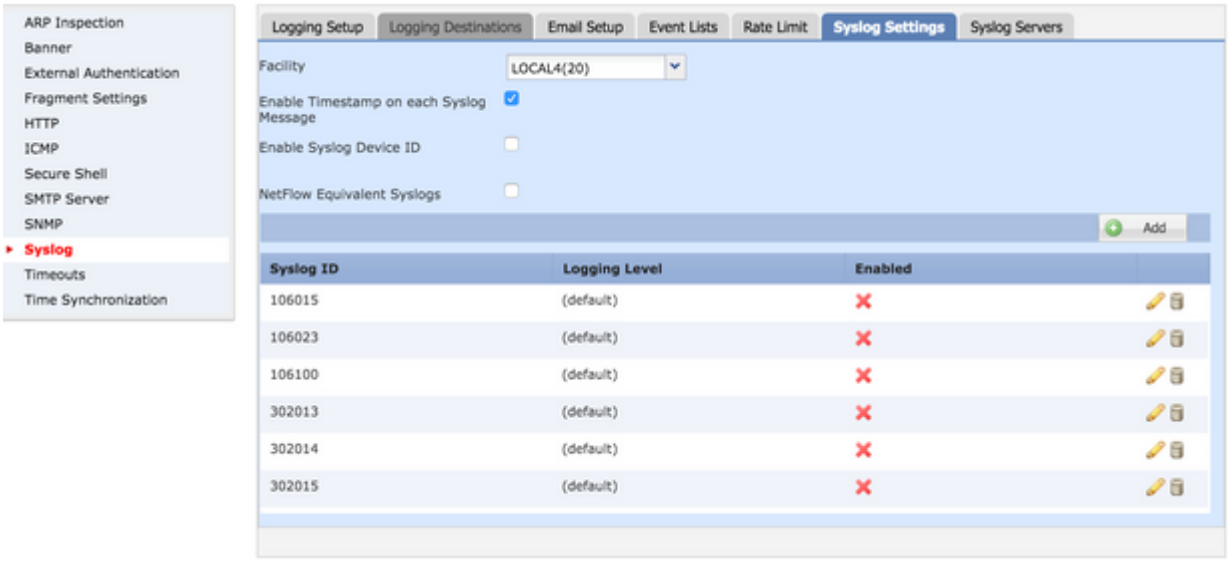
As configurações de Syslog permitem que a configuração dos valores de Facilidade seja incluída nas mensagens de Syslog. Você também pode incluir o timestamp em mensagens de log e outros parâmetros específicos do servidor Syslog.

Para configurar listas de eventos personalizadas, escolha **Device > Platform Setting > Threat Defense Policy > Syslog > Syslog Settings.**

- Facility

: um código de recurso é usado para especificar o tipo de programa que está registrando a mensagem. As mensagens com diferentes recursos podem ser tratadas de forma diferente. Nos **Facility** selecione o valor do recurso.

- Enable Timestamp on each Syslog Message: Verifique o **Enable Timestamp on each Syslog Message** para incluir o carimbo de data/hora nas mensagens Syslog.
- Enable Syslog Device ID: Verifique o **Enable Syslog Device ID** para incluir um ID de dispositivo em mensagens Syslog fora do formato EMBLEM.
- Netflow Equivalent Syslogs: Verifique o **Netflow Equivalent Syslogs** para enviar Syslogs equivalentes do NetFlow. Ele pode afetar o desempenho do dispositivo.
- Add Specific Syslog ID (Adicionar ID de Syslog específico): para especificar o ID de Syslog adicional, clique em **Add** e especificar o **Syslog ID/ Logging Level** caixa de seleção.



Clique em **Save** para salvar a configuração da plataforma. Escolha entre **Deploy**, escolha o dispositivo FTD onde deseja aplicar as alterações e clique em **Deploy** para iniciar a implantação da configuração da plataforma.

Configurar registro local

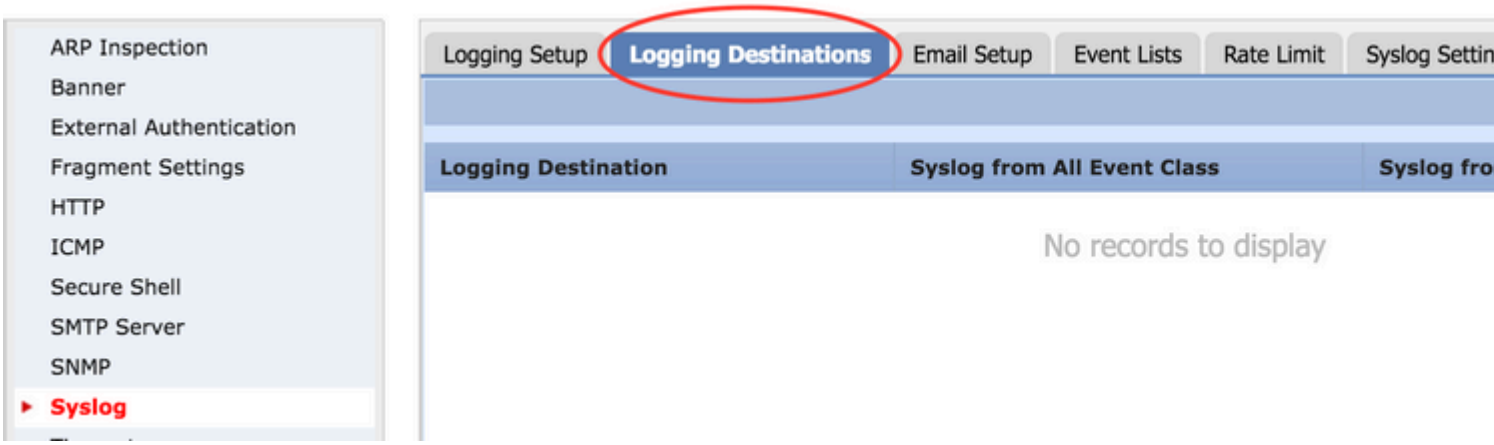
A seção Logging Destination pode ser usada para configurar o registro em destinos específicos.

Os destinos de registro interno disponíveis são:

- Buffer Interno: Registra para o buffer de registro interno (logging buffered)
- Console: Envia registros ao console (console de registro)
- Sessões SSH: registra o Syslog nas sessões SSH (monitor de terminal)

Há três etapas para configurar o registro local.

Etapa 1. Escolher **Device > Platform Setting > Threat Defense Policy > Syslog > Logging Destinations.**



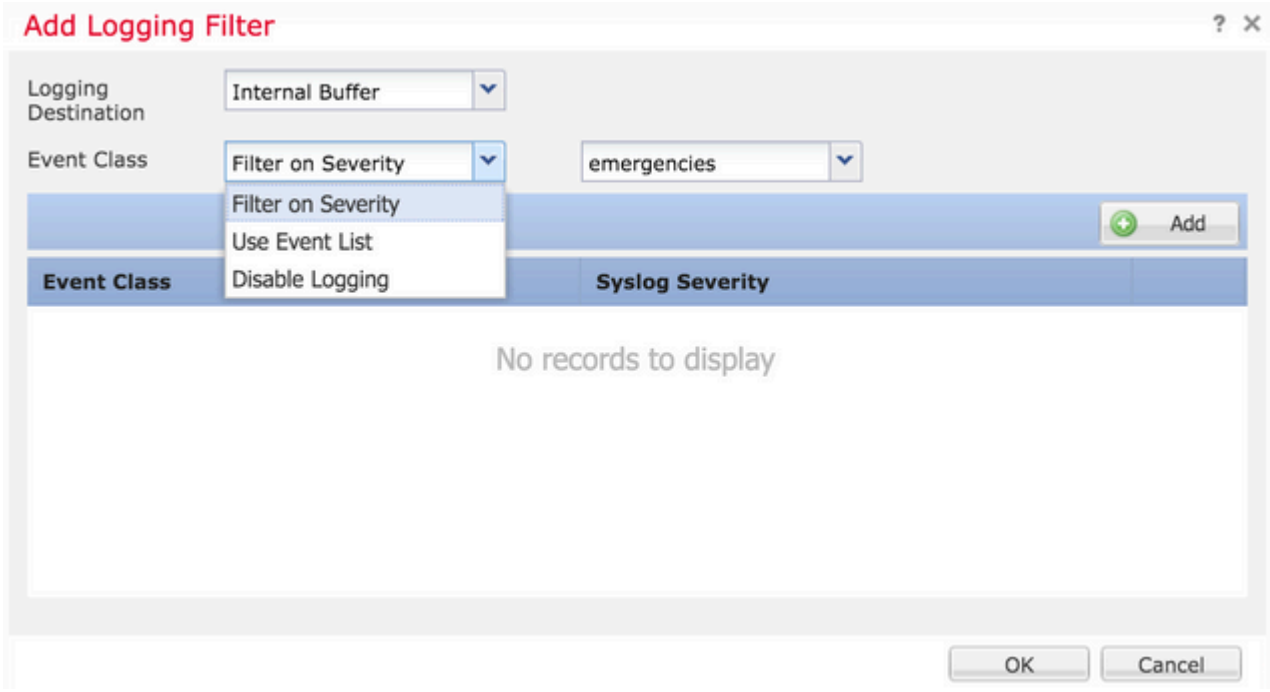
Etapa 2. Clique em **Add** para adicionar um filtro de registro para um **logging destination.**

Destino de Log: Escolha o destino de log necessário no **Logging Destination** como sessões internas de Buffer, Console ou SSH.

Classe de Evento: no menu **Event Class** selecione uma classe Event. Conforme descrito anteriormente, as Classes de Evento são um conjunto de Syslogs que representam os mesmos recursos. As classes de evento podem ser selecionadas das seguintes maneiras:

- Filter on Severity: Classes de evento filtram com base na gravidade dos Syslogs.
- User Event List: os administradores podem criar Listas de eventos específicas (descritas anteriormente) com suas próprias classes de eventos personalizadas e referenciá-las nesta seção.
- Disable Logging: use esta opção para desabilitar o registro em log para o destino de registro em log e o nível de registro em log escolhidos.

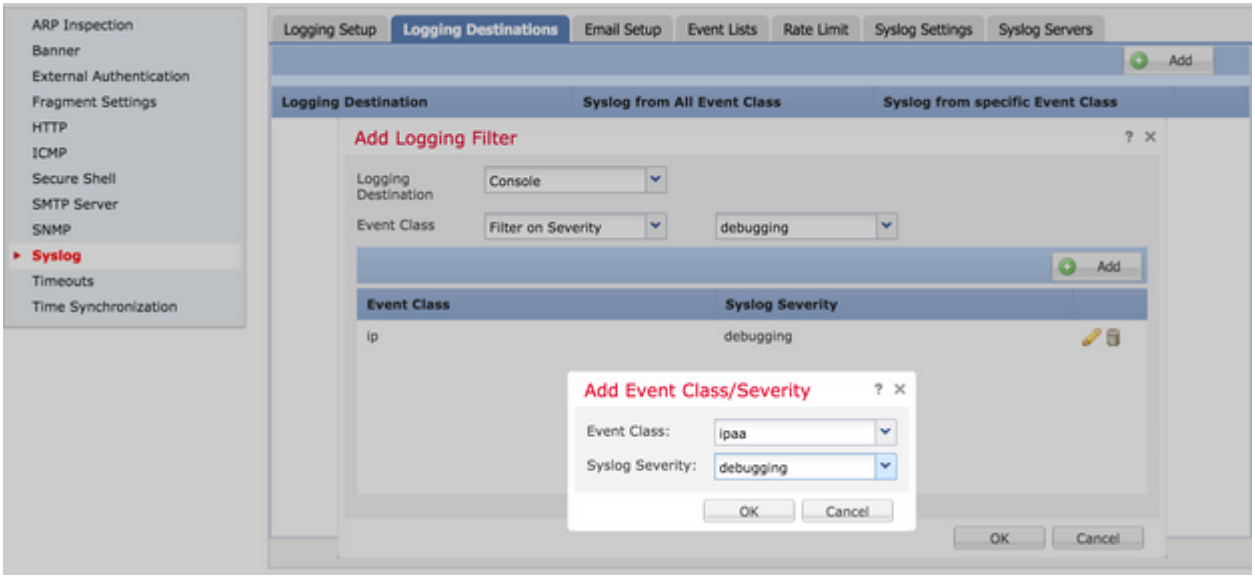
Nível de Log: Escolha o nível de log na lista suspensa. O intervalo do nível de registro é de 0 (Emergências) a 7 (depuração).



Etapa 3. Para adicionar uma classe Event separada a este filtro de registro, clique em **Add**.

Event Class: Escolha a classe de evento no **Event Class** lista suspensa.

Syslog Severity: Escolha a gravidade Syslog no **Syslog Severity** lista suspensa.



Clique em **OK** depois que o Filtro estiver configurado para adicionar o Filtro para um destino de registro específico.

Clique em **Save** para salvar a configuração da plataforma. Escolher **Deploy**, escolha o dispositivo FTD onde deseja aplicar as alterações e clique em **Deploy** para iniciar a implantação da configuração da plataforma.

Configurar o registro externo

Para configurar o registro externo, escolha **Device > Platform Setting > Threat Defense Policy > Syslog > Logging Destinations.**

O FTD suporta esses tipos de registro externo.

- Servidor Syslog: envia logs ao servidor Syslog remoto.
- Interceptação SNMP: envia os logout como uma interceptação SNMP.
- E-Mail: Envia os logs por e-mail com um servidor de retransmissão de e-mail pré-configurado.

A configuração para o registro externo e o registro interno são os mesmos. A seleção de destinos de registro decide o tipo de registro implementado. É possível configurar Classes de Evento com base em listas de Eventos Personalizados para o servidor remoto.

Servidor Syslog Remoto

Os servidores de syslog podem ser configurados para analisar e armazenar logs remotamente do FTD.

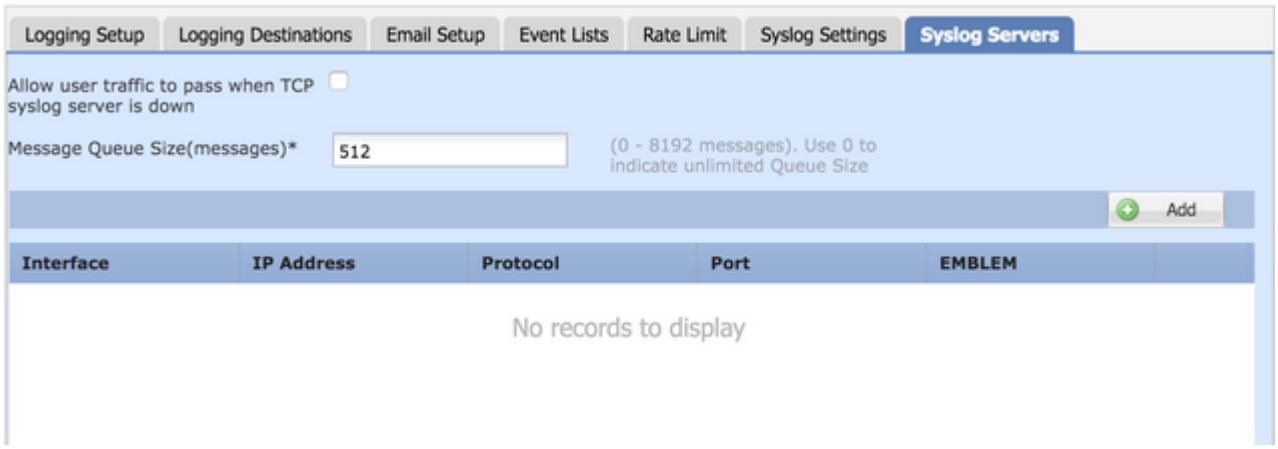
Há três etapas para configurar servidores Syslog remotos.

Etapa 1. Escolher **Device > Platform Setting > Threat Defense Policy > Syslog > Syslog Servers.**

Etapa 2. Configure o parâmetro relacionado ao servidor Syslog.

- Permitir que o tráfego do usuário passe quando o Servidor syslog TCP estiver inoperante: se um Servidor syslog TCP tiver sido implantado na rede e não estiver acessível, o tráfego de rede através do ASA será negado. Isso se aplica somente quando o protocolo de transporte entre o ASA e o servidor Syslog é TCP. Marque a caixa **Allow user traffic to pass when TCP syslog server is down** para permitir que o tráfego passe pela interface quando o Servidor Syslog estiver inoperante.

- Tamanho da Fila de Mensagens: O tamanho da fila de mensagens é o número de mensagens que são enfileiradas no FTD quando o servidor Syslog remoto está ocupado e não aceita nenhuma mensagem de log. O default é 512 mensagens e o mínimo é 1 mensagem. Se 0 for especificado nessa opção, o tamanho da fila será considerado ilimitado.



Etapa 3. Para adicionar servidores Syslog remotos, clique em **Add**.

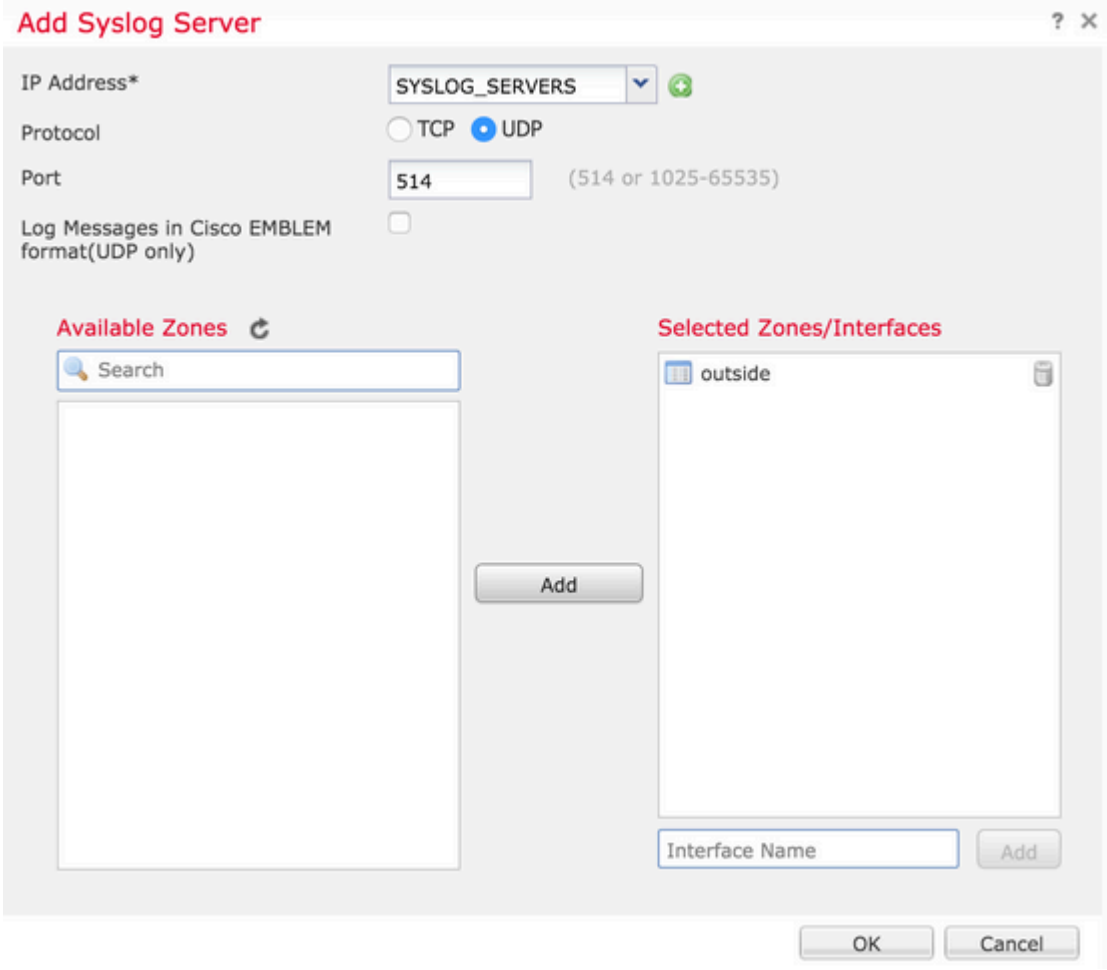
IP Address:Nos **IP Address** escolha um objeto de rede que tenha os servidores Syslog listados. Se você não tiver criado um objeto de rede, clique no ícone de adição (+) para criar um novo objeto.

Protocol: Clique no botão **TCP** or **UDP** para comunicação Syslog.

Port: insira o número da porta do servidor Syslog. Por padrão, é 514.

Log Messages in Cisco EMBLEM format(UDP only): Clique no botão **Log Messages in Cisco EMBLEM format (UDP only)** para habilitar esta opção se for necessário registrar mensagens no formato EMBLEM da Cisco. Isso se aplica somente a Syslog baseado em UDP.

Available Zones: insira as zonas de segurança sobre as quais o servidor Syslog pode ser acessado e mova-o para a coluna Zonas/Interfaces selecionadas.



Clique em **OK** e **Save** para salvar a configuração.

Clique em **Save** para salvar a configuração da plataforma. Escolher **Deploy**, escolha o dispositivo FTD onde deseja aplicar as alterações e clique em **Deploy** para iniciar a implantação da configuração da plataforma.

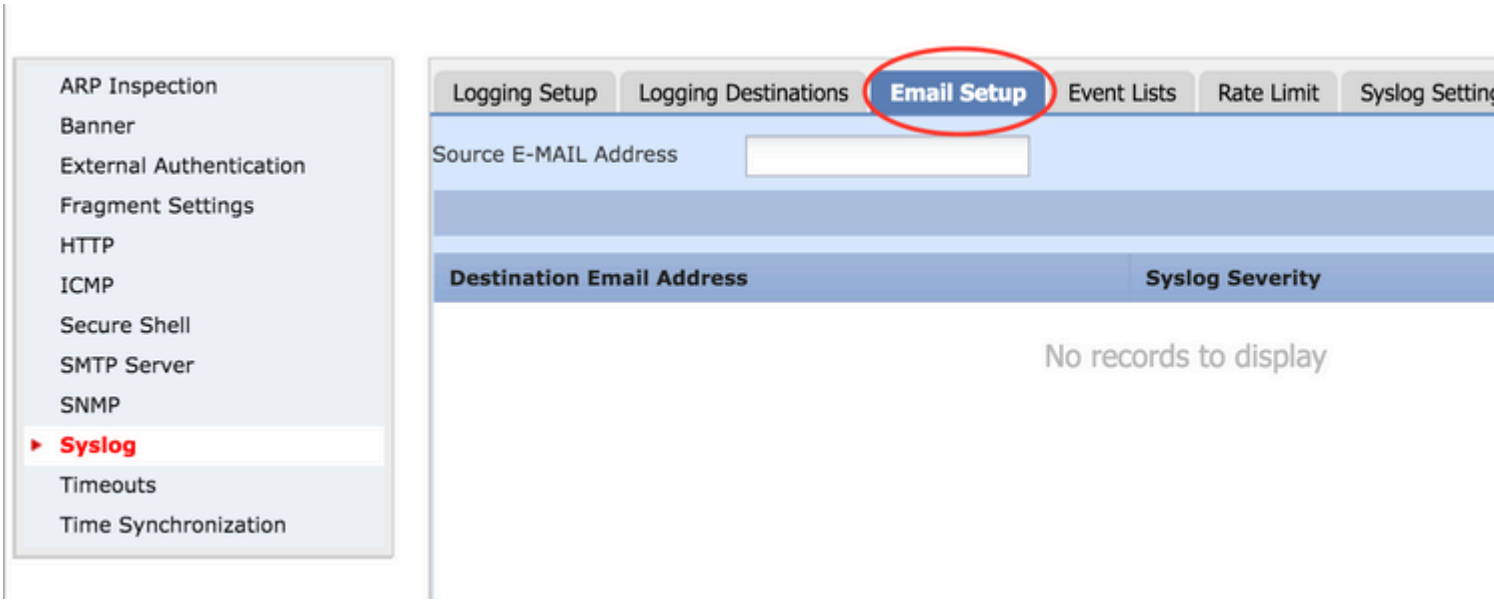
Configuração de e-mail para registro

O FTD permite enviar o Syslog para um endereço de e-mail específico. O e-mail pode ser usado como um destino de registro em log somente se um servidor de retransmissão de e-mail já tiver sido configurado.

Há duas etapas para definir as configurações de e-mail para os Syslogs.

Etapa 1. Escolher **Device** > **Platform Setting** > **Threat Defense Policy** > **Syslog** >**Email Setup.**

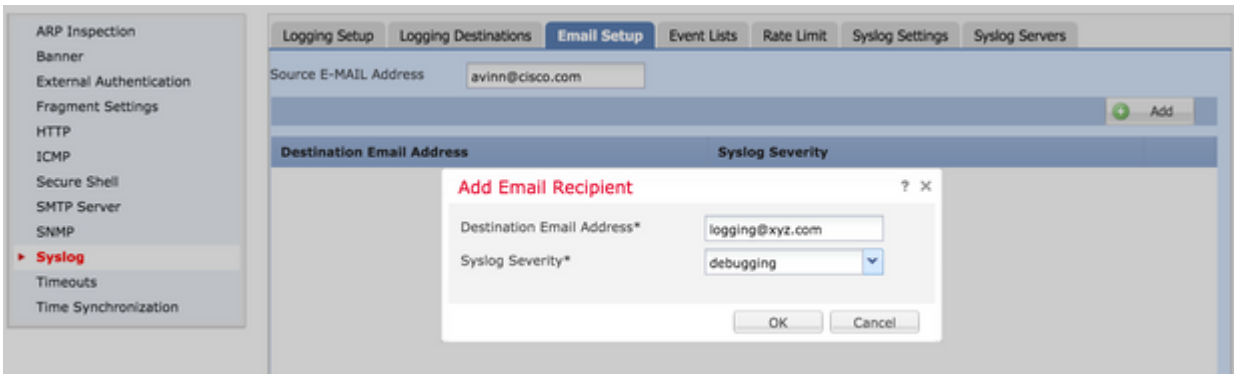
Source E-MAIL Address: insira o endereço de email de origem que aparece em todos os emails enviados do FTD que contêm os Syslogs.



Etapa 2. Para configurar o endereço de e-mail de destino e a gravidade do Syslog, clique em **Add**.

Destination Email Address: insira o endereço de e-mail de destino para onde as mensagens de Syslog são enviadas.

Syslog Severity: Escolha a gravidade Syslog no **Syslog Severity** lista suspensa.



Clique em **OK** para salvar a configuração.

Clique em **Save** para salvar a configuração da plataforma. Escolher **Deploy**, escolha o dispositivo FTD onde deseja aplicar as alterações e clique em **Deploy** para iniciar a implantação da configuração da plataforma.

Verificar

No momento, não há procedimento de verificação disponível para esta configuração.

Troubleshooting

Esta seção disponibiliza informações para a solução de problemas de configuração.

- Verifique a configuração do Syslog de FTD na CLI de FTD. Inicie a sessão na interface de gerenciamento do FTD e insira o **system support diagnostic-cli** para usar o console na CLI de diagnóstico.

```
> system support diagnostic-cli
Attaching to ASA console ... Press 'Ctrl+a then d' to detach.
Type help or '?' for a list of available commands.
```

```
><Press Enter>
firepower# sh run logging
logging enable
logging console emergencies
logging buffered debugging
logging host inside 192.168.0.192
logging flash-minimum-free 1024
logging flash-maximum-allocation 3076
logging permit-hostdown
```

- Certifique-se de que o servidor Syslog esteja acessível a partir do FTD. Faça login na interface de gerenciamento do FTD via SSH e verifique a conectividade com o **ping** comando.

```
Copyright 2004-2016, Cisco and/or its affiliates. All rights reserved.
Cisco is a registered trademark of Cisco Systems, Inc.
All other trademarks are property of their respective owners.
Cisco Fire Linux OS v6.0.1 (build 37)
Cisco Firepower Threat Defense for VMWare v6.0.1 (build 1213)

> system support diagnostic-cli
Attaching to ASA console ... Press 'Ctrl+a then d' to detach.
Type help or '?' for a list of available commands.
firepower> en
Password:
firepower# ping 192.168.0.192
```

- Você pode fazer uma captura de pacote para verificar a conectividade entre o FTD e o servidor Syslog. Inicie a sessão na interface de gerenciamento do FTD via SSH e insira o comando **system support diagnostic-cli**. Para os comandos de captura de pacotes, consulte Exemplo de Configuração de Capturas de Pacotes do ASA com CLI e ASDM.
- Verifique se a implantação da política foi aplicada com êxito.

Informações Relacionadas

- Guia de início rápido do Cisco Firepower Threat Defense para o ASA
- Suporte Técnico e Documentação - Cisco Systems

Sobre esta tradução
A Cisco traduziu este documento com a ajuda de tecnologias de tradução automática e humana para oferecer conteúdo de suporte aos seus usuários no seu próprio idioma, independentemente da localização.

Observe que mesmo a melhor tradução automática não será tão precisa quanto as realizadas por um tradutor profissional.

A Cisco Systems, Inc. não se responsabiliza pela precisão destas traduções e recomenda que o documento original em inglês (link fornecido) seja sempre consultado.