Implementar configurações de plataforma para solução de problemas de VPN

Contents

Introdução

Este documento descreve como organizar e identificar facilmente logs de depuração de VPN usando o Secure Firewall Management Center e o Secure Firewall Threat Defense.

Pré-requisitos

Requisitos

A Cisco recomenda que você tenha conhecimento destes tópicos:

- Defesa contra ameaças de firewall (FTD) segura
- Centro de gerenciamento seguro de firewall (FMC)

- Noções básicas de navegação na GUI do FMC e na CLI do FTD
- Atribuição de política existente para Configurações de Plataforma

Componentes Utilizados

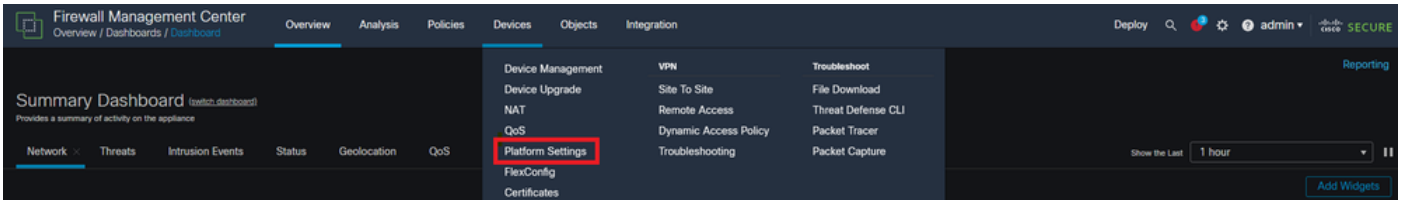
As informações neste documento são baseadas nestas versões de software e versões de hardware:

- Firewall Management Center versão 7.3
- Firewall Threat Defense versão 7.3

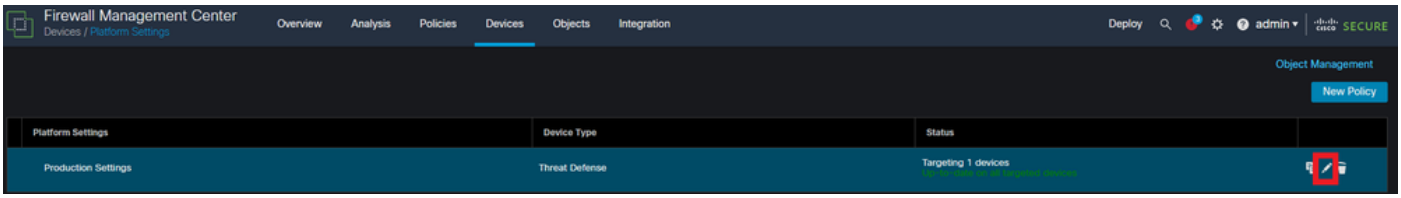
As informações neste documento foram criadas a partir de dispositivos em um ambiente de laboratório específico. Todos os dispositivos utilizados neste documento foram iniciados com uma configuração (padrão) inicial. Se a rede estiver ativa, certifique-se de que você entenda o impacto potencial de qualquer comando.

Centro de gerenciamento de firewall

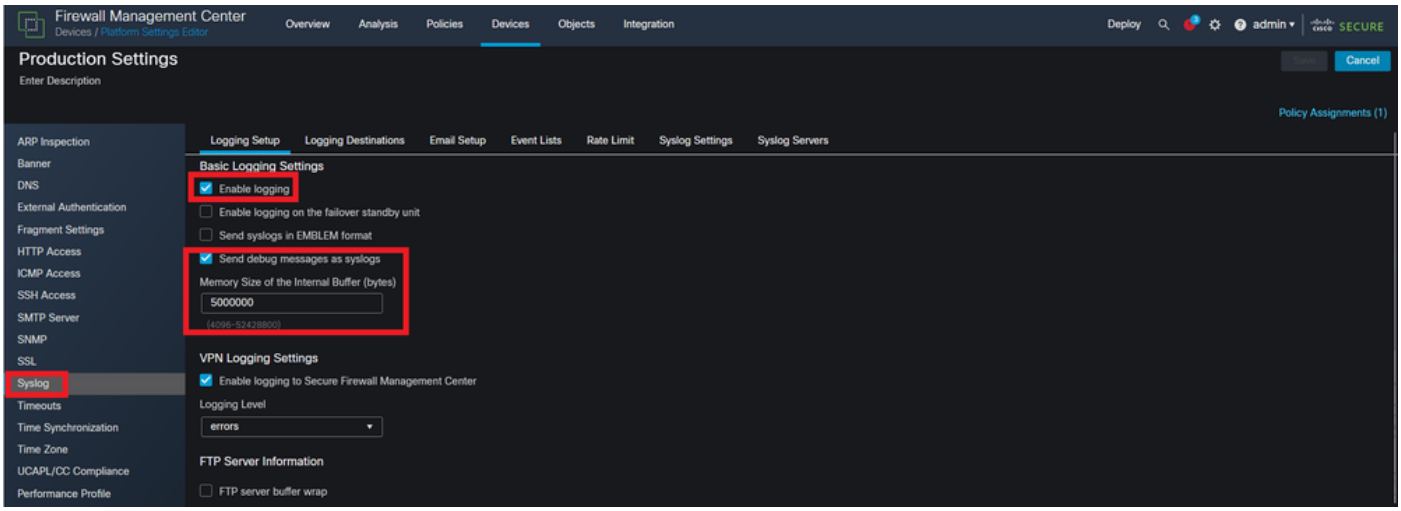
Navegue até Devices > Platform Settings.



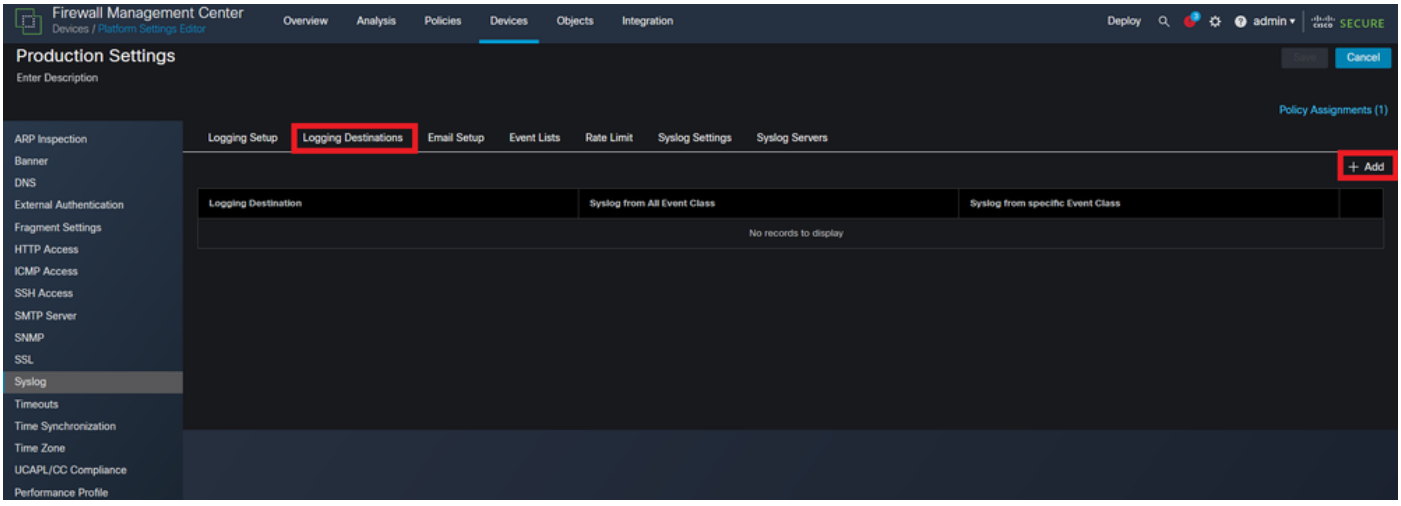
Clique no **pencil** entre copy e excluir icon.



Navegue até Syslogna coluna esquerda de opções e verifique se **Enable Logging**, e **Send debug messages as syslog** estão ativados. Além disso, certifique-se de que o Memory Size of the Internal Buffer esteja definido com um valor adequado para fins de solução de problemas.

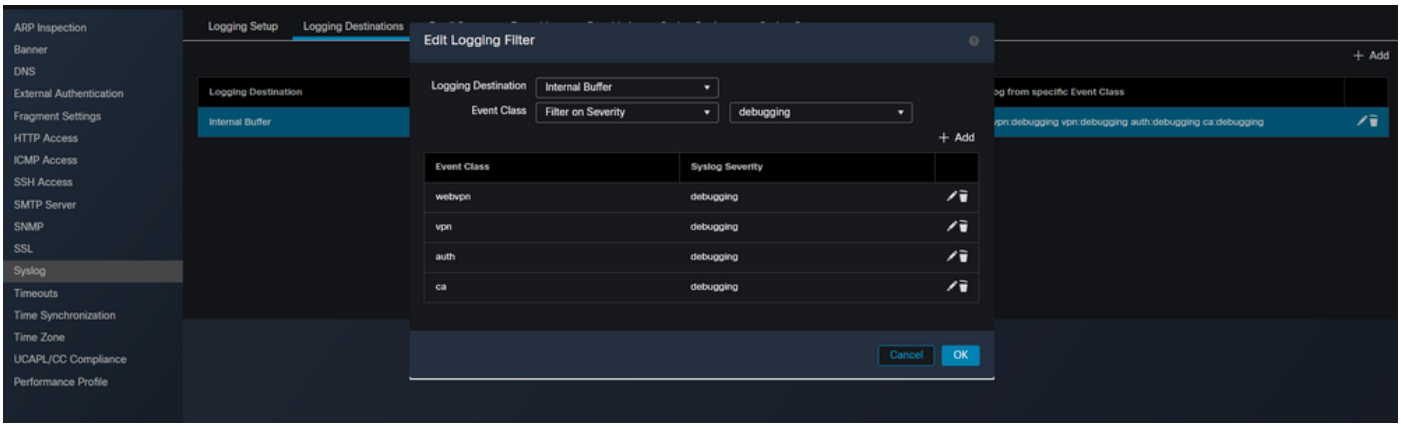


Clique **Logging Destinations** em e em **+Add**.



Nesta seção, o destino de registro é uma preferência do administrador e **Internal Buffer** é usado.

Altere **Event Class** para **Filter on Severity and debugging**. Quando isso estiver concluído, clique em +Add e escolha webvpn, vpn, authe ca debuggingtodos com a severidade Syslog de. Esta etapa permite que o administrador filtre essas saídas de depuração para uma mensagem de syslog de 711001 específica. Elas podem ser modificadas dependendo do tipo de solução de problemas. No entanto, os escolhidos neste exemplo abrangem os problemas mais comumente encontrados relacionados a VPN de site para site, acesso remoto e AAA.

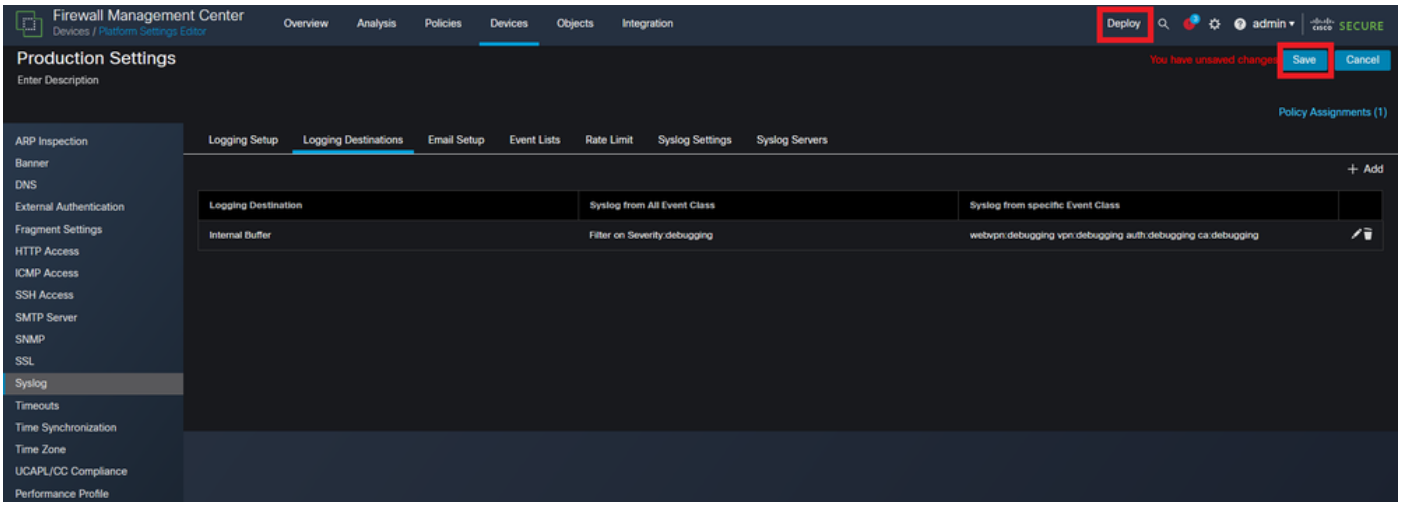


Crie classes de eventos e filtros para as depurações.

---

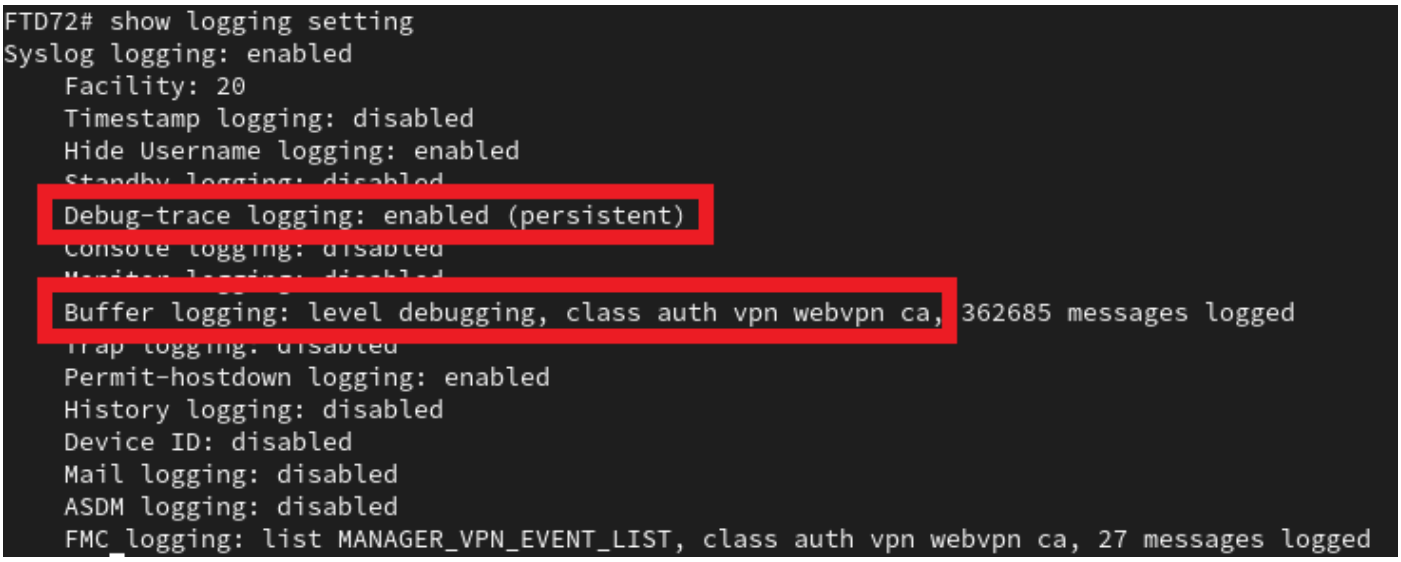
aviso: Isso altera o Nível de Log do Buffer para depuração e registra eventos de depuração para as classes especificadas para o buffer interno. É recomendável usar esse método de registro para fins de solução de problemas, e não para uso a longo prazo.

Choose Save na parte superior direita e, em seguida, Deploya configuração é alterada.



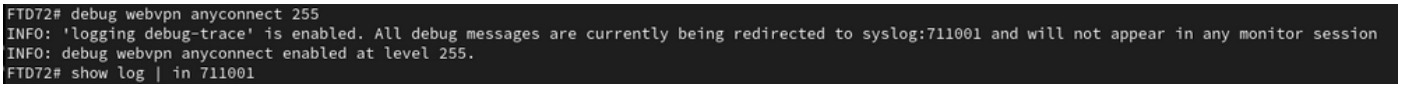
Defesa contra ameaças de firewall

Navegue até a CLI do FTD e emita o comandoshow logging setting. As configurações aqui refletem as alterações feitas no FMC. Certifique-se de que o log debug-trace esteja habilitado e que o log de buffer corresponda às classes e ao nível de log especificado.



Exiba as configurações de registro na CLI do FTD.

Por fim, aplique uma depuração para garantir que os logs estejam sendo redirecionados para syslog:711001. Neste exemplo, `debug webvpn anyconnect 255` é aplicada. Isso aciona um aviso de registro debug-trace, permitindo que o administrador saiba que essas depurações são redirecionadas. Para visualizar essas depurações, execute o comando `show log | in 711001`. Esse ID de syslog agora contém apenas depurações de VPN relevantes conforme aplicadas pelo administrador. Os logs existentes podem ser limpos com um buffer de registro limpo.



Mostra todas as depurações de VPN que estão sendo redirecionadas para o 711001 syslog.

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.