VPNトラブルシューティングのためのプラットフォーム設定の実装

内容

[はじめに](#)

[前提条件](#)

- [要件](#)
- [使用するコンポーネント](#)

[ファイアウォール管理センター](#)

[ファイアウォール脅威対策](#)

はじめに

このドキュメントでは、Secure Firewall Management Center(FMC)およびSecure Firewall Threat Defenseを使用して、VPNデバッグログを簡単に整理および識別する方法について説明します。

前提条件

要件

次の項目に関する知識があることが推奨されます。

- セキュアファイアウォール脅威対策(FTD)
- セキュアファイアウォール管理センター(FMC)

- FMC GUIおよびFTD CLIのナビゲーションに関する基本的な知識
- プラットフォーム設定の既存のポリシー割り当て

使用するコンポーネント

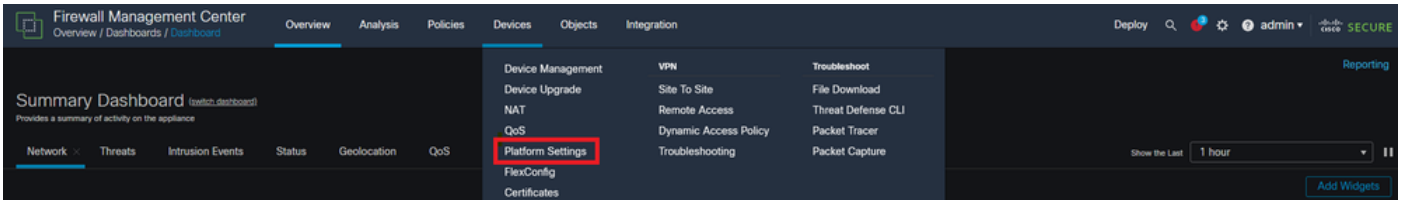
このドキュメントの情報は、次のソフトウェアとハードウェアのバージョンに基づくものです。

- Firewall Management Centerバージョン7.3
- Firewall Threat Defenseバージョン7.3

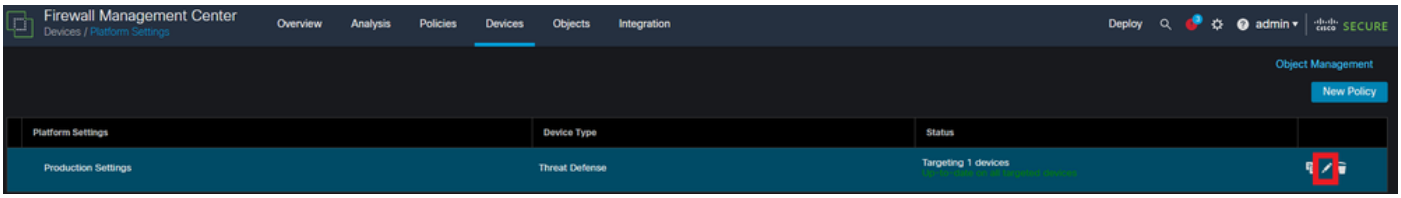
このドキュメントの情報は、特定のラボ環境にあるデバイスに基づいて作成されたものです。このドキュメントで使用するすべてのデバイスは、クリアな（デフォルト）設定で作業を開始しています。本稼働中のネットワークでは、各コマンドによって起こる可能性がある影響を十分確認してください。

ファイアウォール管理センター

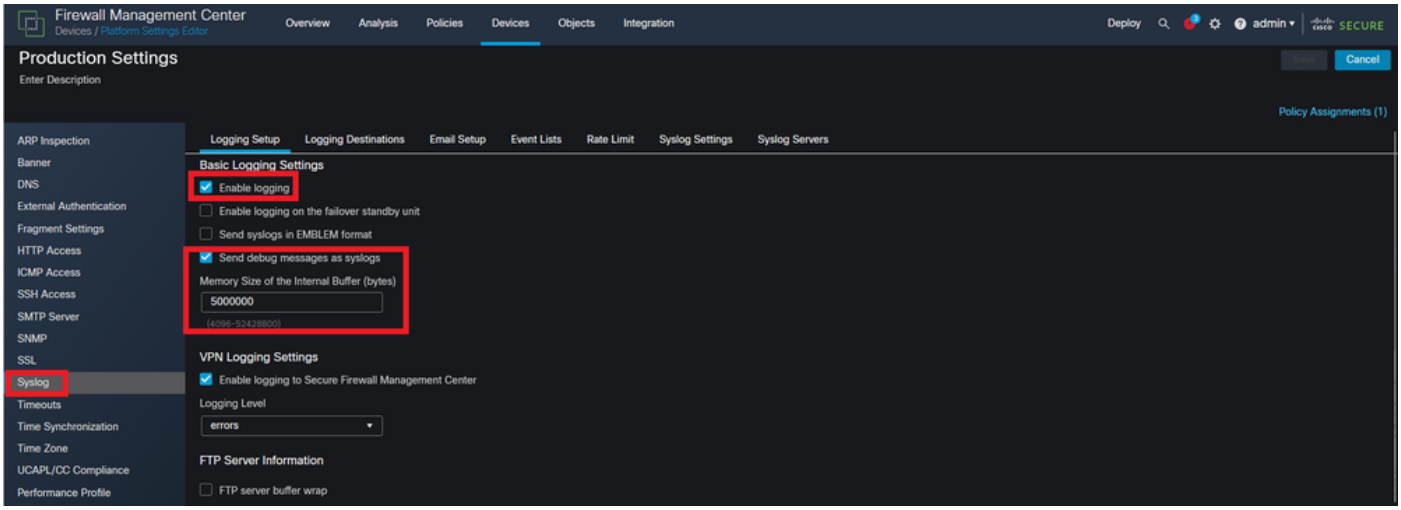
Devices > Platform Settingsの順に移動します。



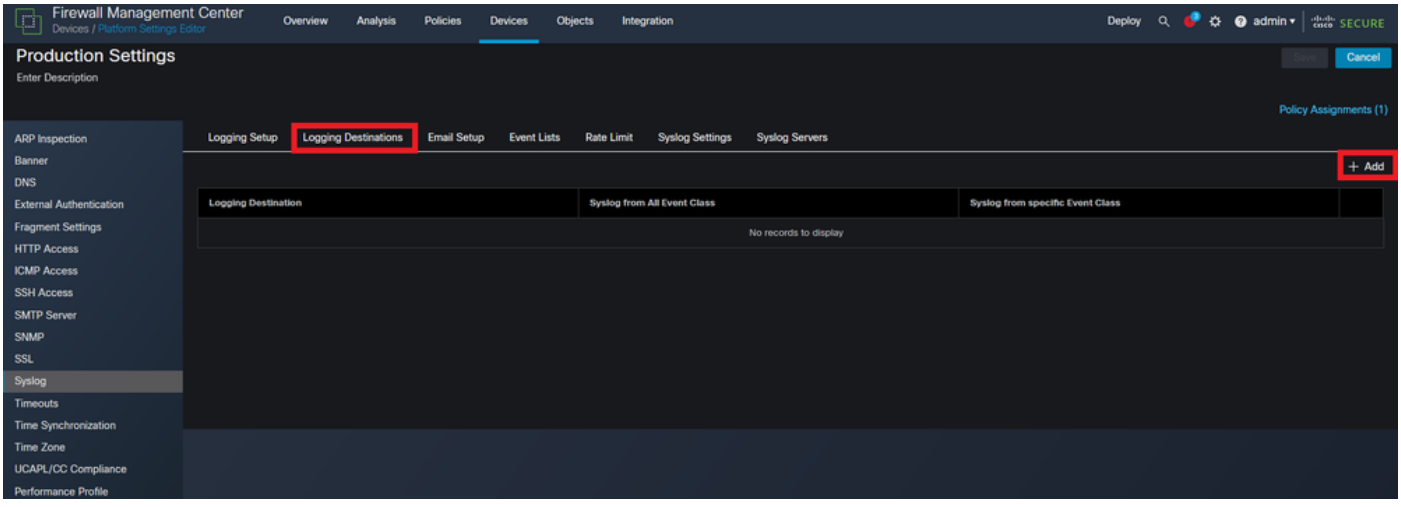
copyアイコンと**delete**アイコンの間にある鉛筆をクリックします。



オプションの左側の列でSysloginに移動し、Enable LoggingとSend debug messages as syslogがイネーブルになっていることを確認します。さらに、内部バッファのメモリサイズが、トラブルシューティングに適した値に設定されていることを確認します。

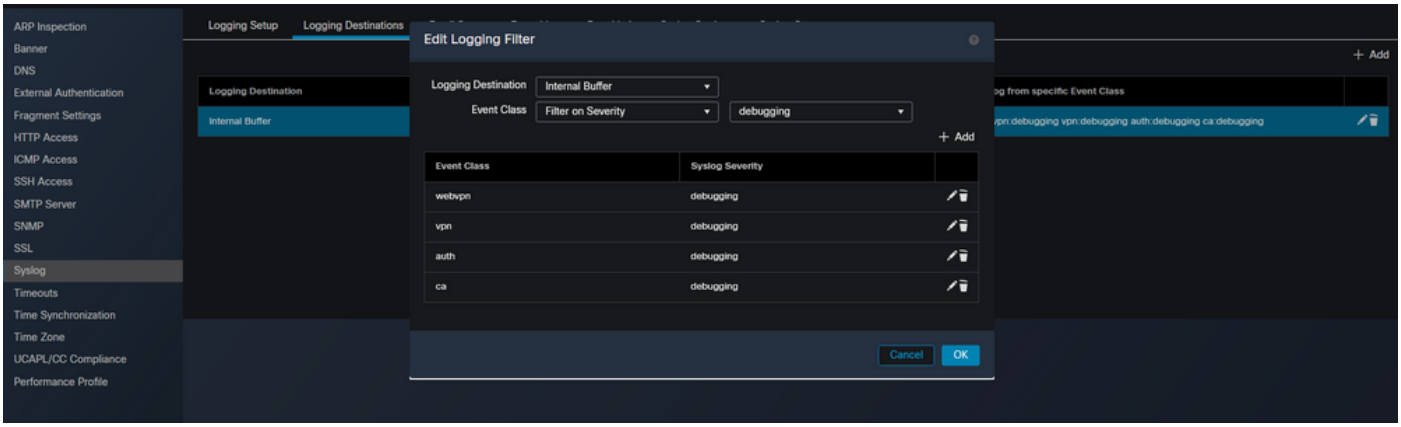


Logging Destinationsをクリックし、次に**+Add**をクリックする。



このセクションでは、ロギングの宛先は管理者のプリファレンスで、内部バッファが使用されます。

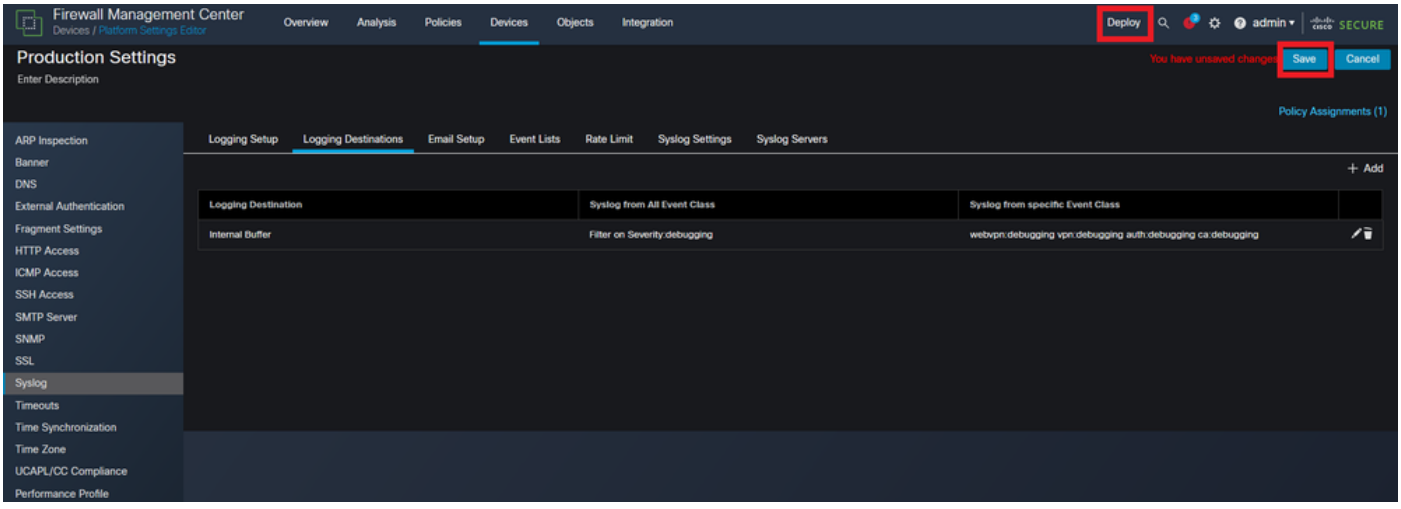
Event Classを**Filter on Severity and debugging**に変更します。 これが完了したら、+Addをクリックして、webvpn、vpn、auth、およびcallを選択し、syslogの重大度にはdebuggingを指定します。この手順により、管理者はこれらのデバッグ出力をフィルタリングして、711001という特定のsyslogメッセージを表示できます。これらは、トラブルシューティングのタイプに応じて変更できます。ただし、この例で選択した問題は、最も一般的に発生するサイト間、リモートアクセス、およびAAA VPN関連の問題をカバーしています。



デバッグ用のイベントクラスとフィルタを作成します。

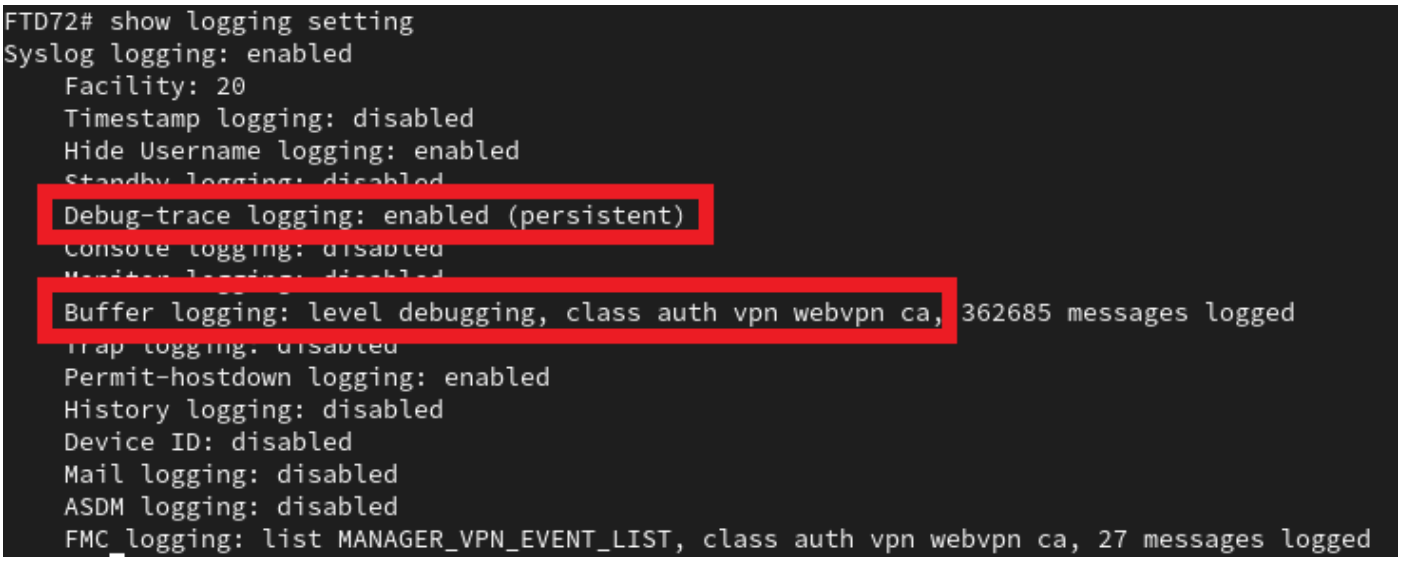
警告：これにより、バッファログレベルがdebuggingに変更され、内部バッファに指定されたクラスのデバッグイベントがログに記録されます。このロギング方法は、トラブルシューティングの目的で使用し、長期間の使用には使用しないことを推奨します。

右上のSaveを選択し、次に**Deploythe configuration changes**を選択します。



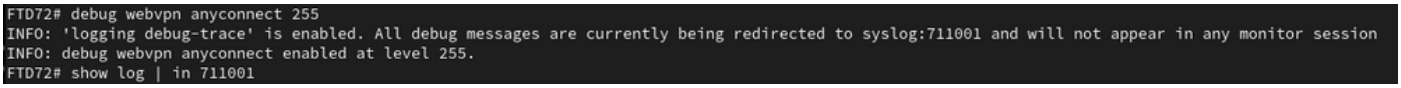
ファイアウォール脅威対策

FTD CLIに移動し、コマンドshow logging settingを発行します。ここでの設定には、FMCで行った変更が反映されます。debug-traceロギングが有効で、バッファロギングが指定されたクラスとロギングレベルに一致することを確認します。



FTD CLIでロギング設定を表示します。

最後に、ログがsyslog:711001に確実にリダイレクトされるようにデバッグを適用します。この例では、debug webvpn anyconnect 255が適用されます。これにより、ロギングdebug-trace通知がトリガーされ、これらのデバッグがリダイレクトされることを管理者に知らせます。これらのデバッグを表示するには、show log | in 711001コマンドを発行します。このsyslog IDには、管理者が適用した関連するVPNデバッグだけが含まれるようになりました。既存のログは、clear logging bufferを使用してクリアできます。



すべてのVPNデバッグがsyslog 711001にリダイレクトされていることを示します。

翻訳について
シスコは世界中のユーザにそれぞれの言語でサポート コンテンツを提供するために、機械と人による翻訳を組み合わせて、本ドキュメントを翻訳しています。ただし、最高度の機械翻訳であっても、専門家による翻訳のような正確性は確保されません。シスコは、これら翻訳の正確性について法的責任を負いません。原典である英語版（リンクからアクセス可能）もあわせて参照することを推奨します。