Implementa impostazioni della piattaforma per la risoluzione dei problemi VPN

Sommario

Introduzione

In questo documento viene descritto come organizzare e identificare facilmente i log di debug VPN utilizzando Secure Firewall Management Center e Secure Firewall Threat Defense.

Prerequisiti

Requisiti

Cisco raccomanda la conoscenza dei seguenti argomenti:

- Secure Firewall Threat Defense (FTD)
- Centro gestione firewall protetto (FMC)

- Conoscenze di base della navigazione nella GUI FMC e nella CLI FTD
- Assegnazione di criteri esistente per le impostazioni della piattaforma

Componenti usati

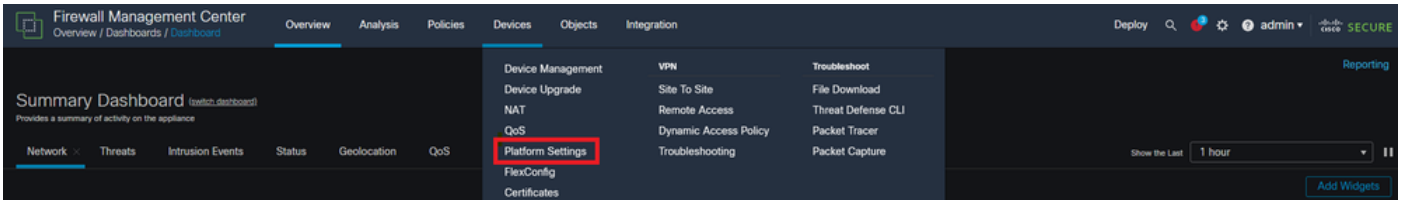
Le informazioni di questo documento si basano sulle seguenti versioni software e hardware:

- Firewall Management Center versione 7.3
- Firewall Threat Defense versione 7.3

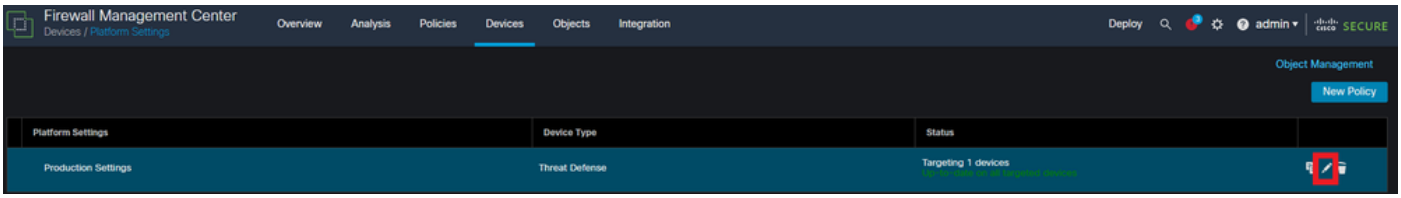
Le informazioni discusse in questo documento fanno riferimento a dispositivi usati in uno specifico ambiente di emulazione. Su tutti i dispositivi menzionati nel documento la configurazione è stata ripristinata ai valori predefiniti. Se la rete è operativa, valutare attentamente eventuali conseguenze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

Centro gestione firewall

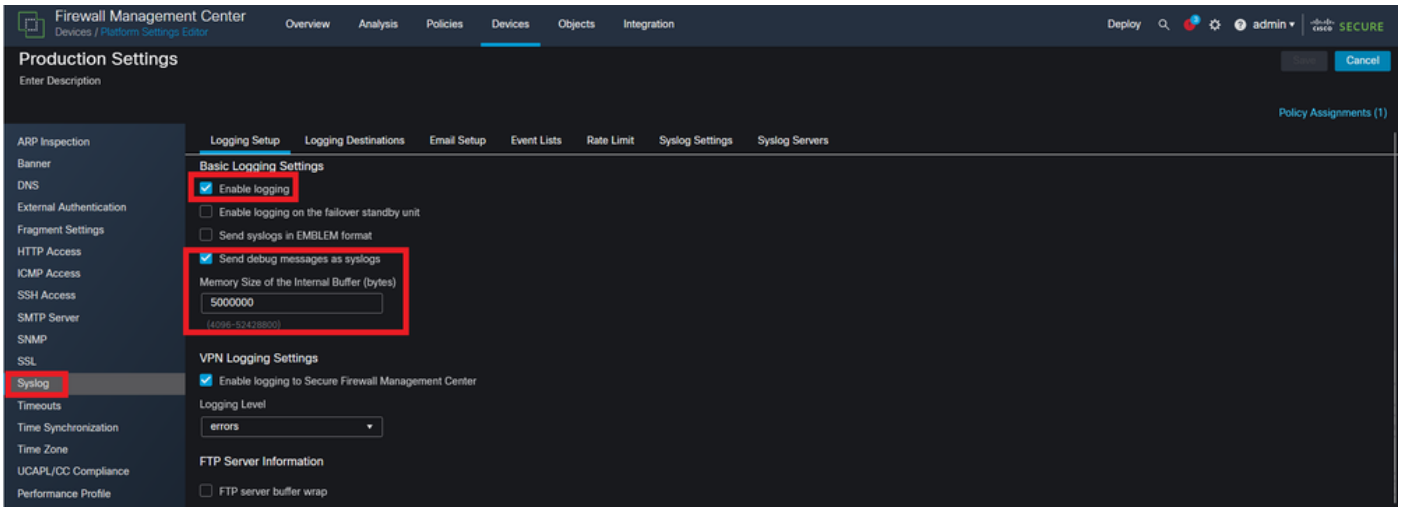
Passare a Devices > Platform Settings.



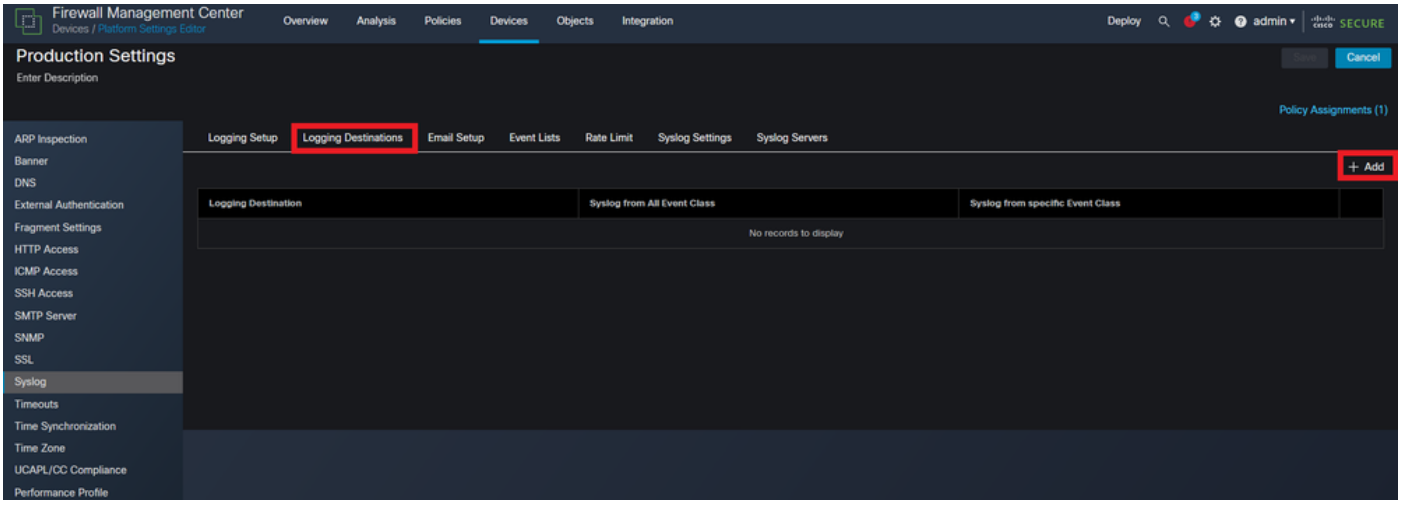
Fare clic sulla barra **pencil** tra copy e iconElimina.



Spostarsi Syslognella colonna di sinistra delle opzioni e assicurarsi che **Enable Logging**, e **Send debug messages as syslog** siano abilitati. Inoltre, accertarsi che sia Memory Size of the Internal Buffer impostato su un valore adeguato per la risoluzione dei problemi.

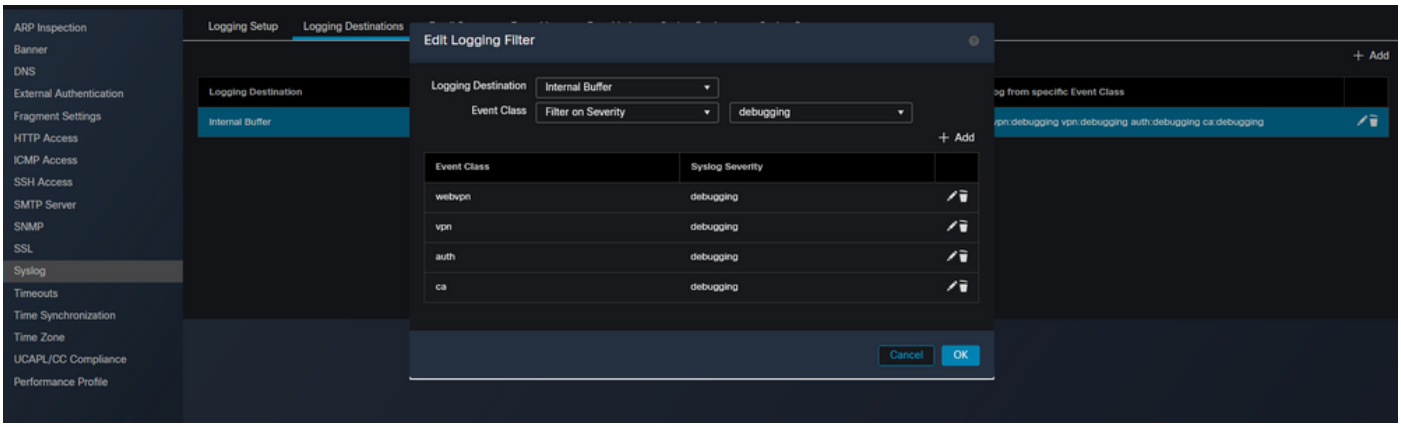


Fare **Logging Destinations** clic su, quindi su **+Add**.



In questa sezione, la destinazione di registrazione è una preferenza dell'amministratore e **Internal**

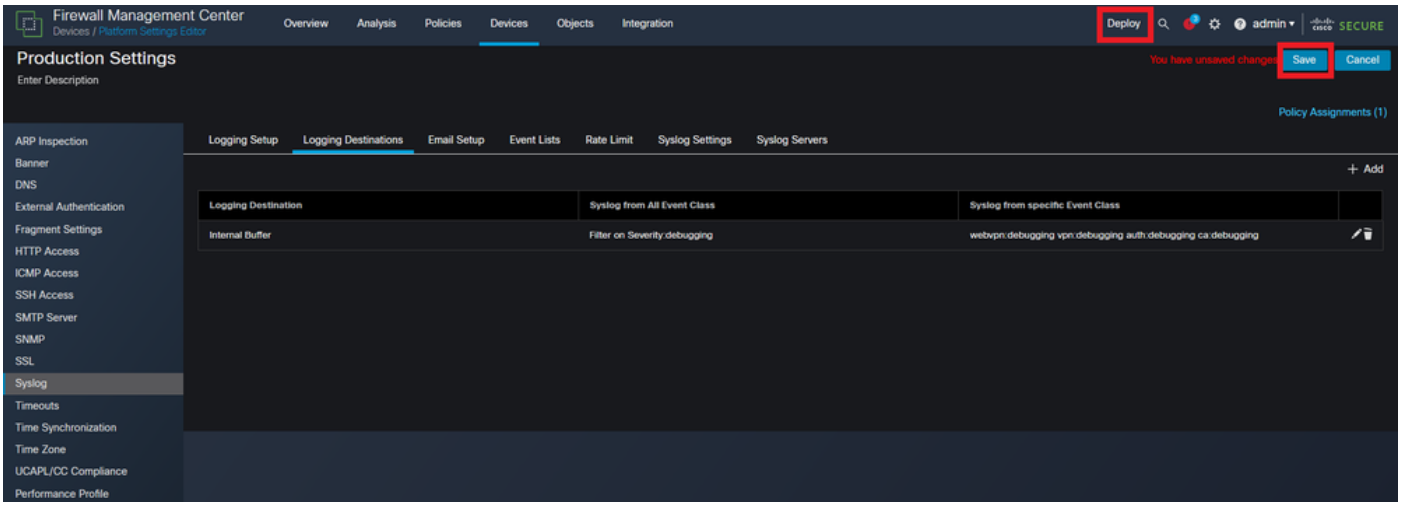
Buffer viene utilizzata. Cambiare **Event Class** in **Filter on Severity and debugging**. Al termine, fare clic su +Add e scegliere webvpn, vpn authe catutti con gravità Syslog pari a debugging. Questo passaggio consente all'amministratore di filtrare gli output di debug in base a uno specifico messaggio syslog di 711001. Tali output possono essere modificati a seconda del tipo di risoluzione dei problemi. Tuttavia, quelli scelti in questo esempio coprono i problemi più comuni che si verificano nelle connessioni da sito a sito, nell'accesso remoto e nelle VPN AAA.



Creare classi di eventi e filtri per i debug.

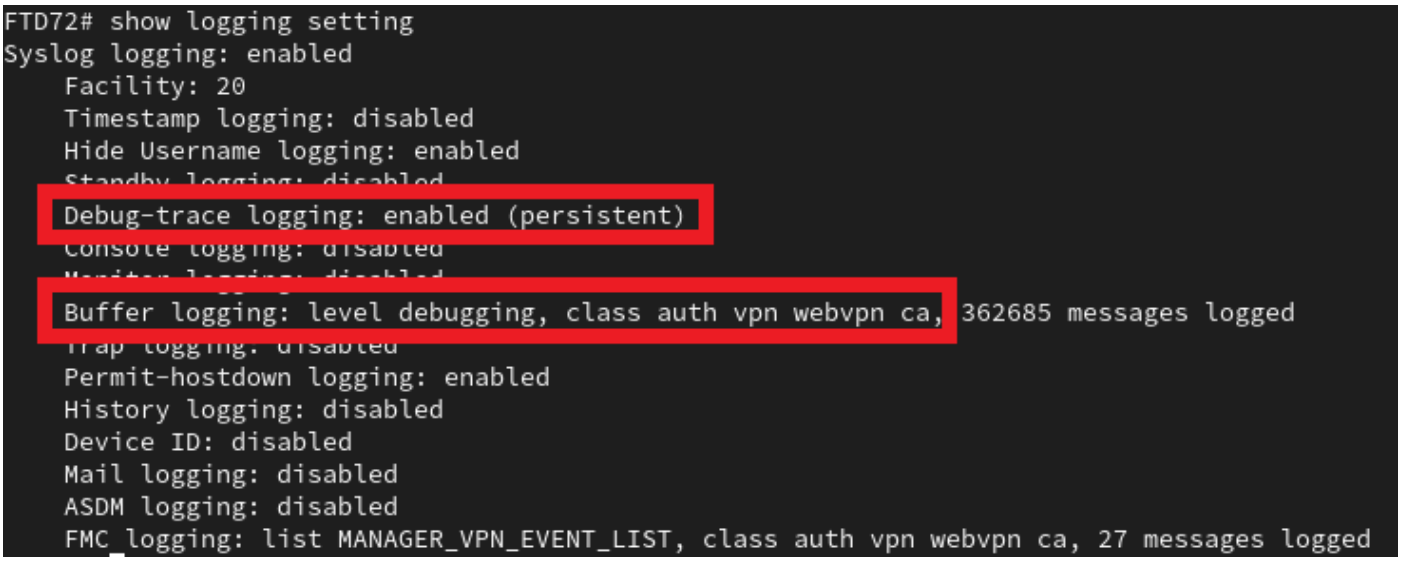
Avviso: In questo modo il livello di registrazione del buffer viene modificato in debug e vengono registrati gli eventi di debug per le classi specificate nel buffer interno. Si consiglia di utilizzare questo metodo di registrazione a scopo di risoluzione dei problemi e non per un utilizzo a lungo termine.

Choose Save in alto a destra, quindi Deployla configurazione cambia.



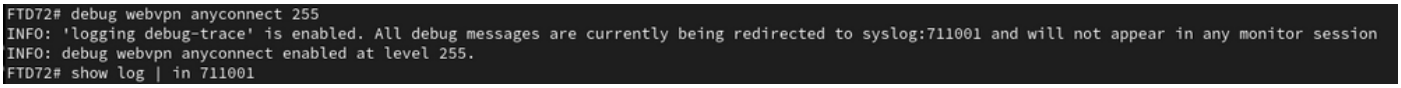
Firewall Threat Defense

Passare alla CLI FTD e usare il comandoshow logging setting. Le impostazioni qui riportate riflettono le modifiche apportate al CCP. Verificare che la registrazione della traccia di debug sia abilitata e che la registrazione del buffer corrisponda alle classi e al livello di registrazione specificati.



Visualizzare le impostazioni di registrazione nella CLI FTD.

Infine, applicare un comando di debug per assicurarsi che i log vengano reindirizzati a syslog:711001. Nell'esempio `debug webvpn anyconnect 255` riportato viene applicato. In questo modo viene attivato un avviso di registrazione di debug-trace che informa l'amministratore che i debug sono reindirizzati. Per visualizzare i debug, usare il comando `show log | in 711001`. Questo ID syslog ora contiene solo i debug VPN rilevanti applicati dall'amministratore. I registri esistenti possono essere cancellati con un buffer di registrazione non impostato.



Mostra tutti i debug VPN reindirizzati a syslog 711001.

Informazioni su questa traduzione

Cisco ha tradotto questo documento utilizzando una combinazione di tecnologie automatiche e umane per offrire ai nostri utenti in tutto il mondo contenuti di supporto nella propria lingua. Si noti che anche la migliore traduzione automatica non sarà mai accurata come quella fornita da un traduttore professionista. Cisco Systems, Inc. non si assume alcuna responsabilità per l’accuratezza di queste traduzioni e consiglia di consultare sempre il documento originale in inglese (disponibile al link fornito).