Implementeer platforminstellingen voor VPN-probleemoplossing

Inhoud

Inleiding

In dit document wordt beschreven hoe u eenvoudig VPN-foutopsporingslogboeken kunt organiseren en identificeren met behulp van Secure Firewall Management Center en Secure Firewall Threat Defense.

Voorwaarden

Vereisten

Cisco raadt kennis van de volgende onderwerpen aan:

- Secure Firewall Threat Defense (FTD)
- Secure Firewall Management Center (FMC)

- Basiskennis van navigeren door de FMC GUI en FTD CLI
- Bestaande beleidstoewijzing voor platforminstellingen

Gebruikte componenten

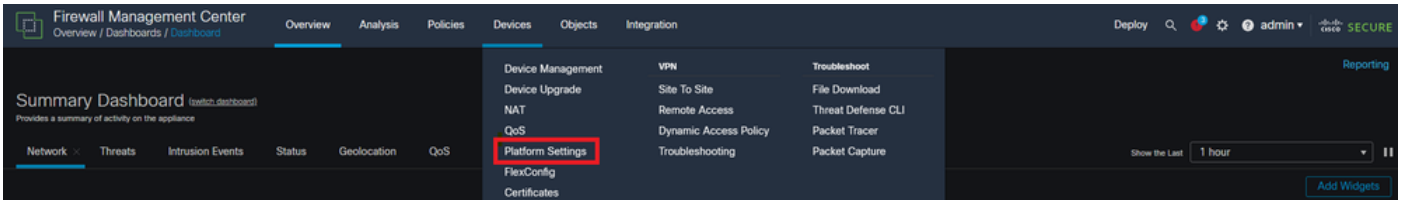
De informatie in dit document is gebaseerd op de volgende softwareversies en hardwareversies:

- Firewall Management Center versie 7.3
- Firewall Threat Defense versie 7.3

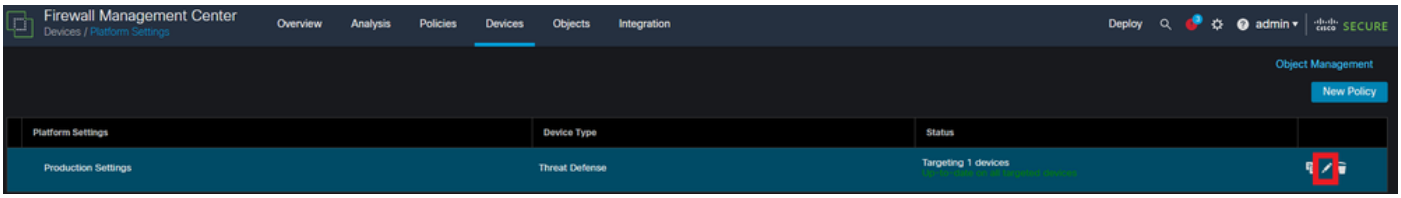
De informatie in dit document is gebaseerd op de apparaten in een specifieke laboratoriumomgeving. Alle apparaten die in dit document worden beschreven, hadden een opgeschoonde (standaard)configuratie. Als uw netwerk live is, moet u zorgen dat u de potentiële impact van elke opdracht begrijpt.

Firewall Management Center

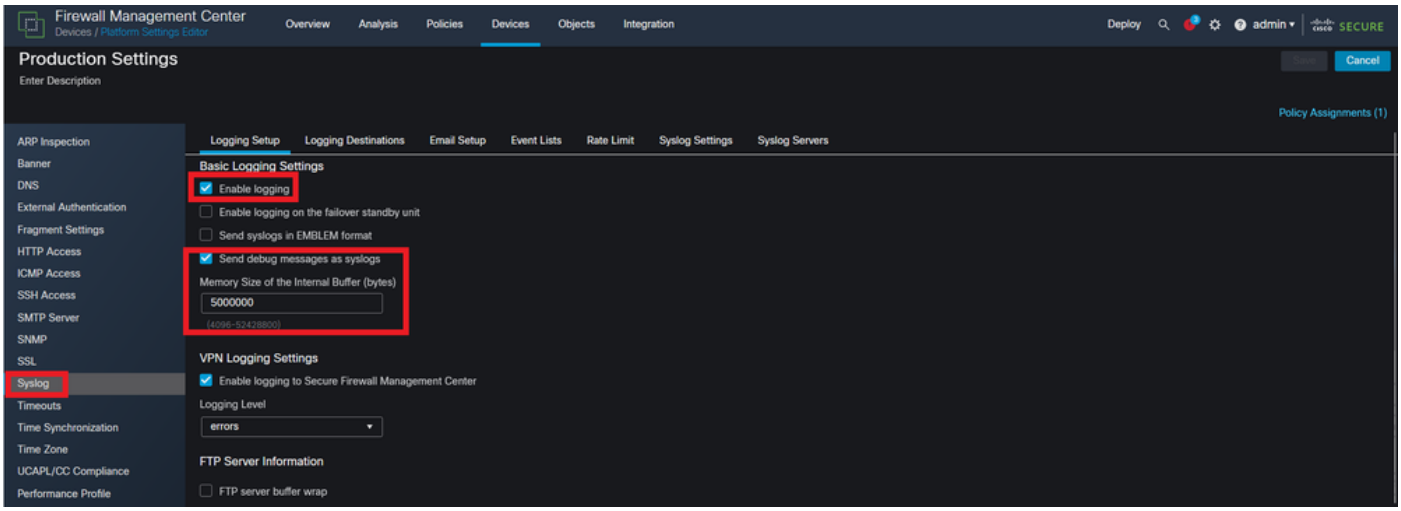
Navigeer naar Devices > Platform Settings.



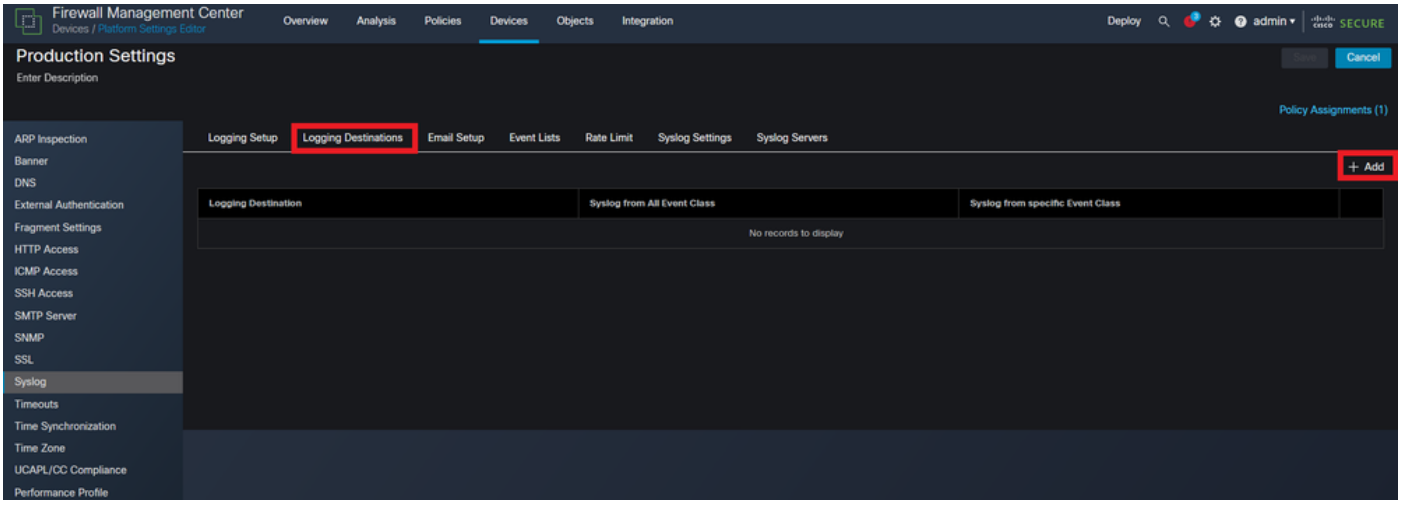
Klik op de **pencil** tussen de copy en verwijder icon.



Blader naar Syslogin de linkerkolom met opties en zorg ervoor dat **Enable Logging**en **Send debug messages as syslog** zijn ingeschakeld. Zorg er bovendien voor dat de Memory Size of the Internal Buffer is ingesteld met een waarde die geschikt is voor het oplossen van problemen.

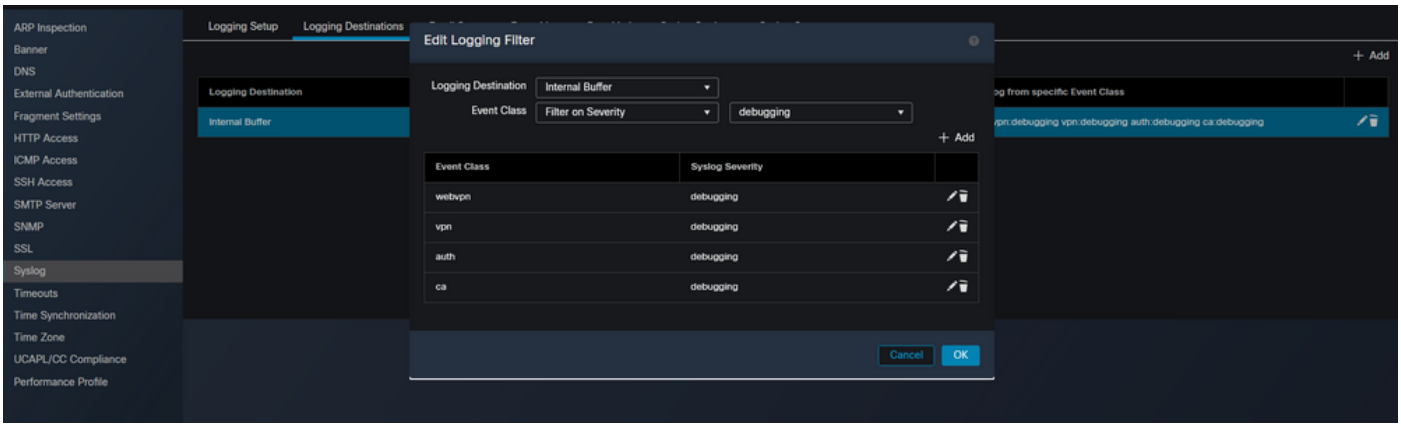


Klik **Logging Destinations** en klik vervolgens op **+Add**.



In deze sectie is de logboekbestemming een voorkeur van de beheerder en wordt **Internal Buffer**

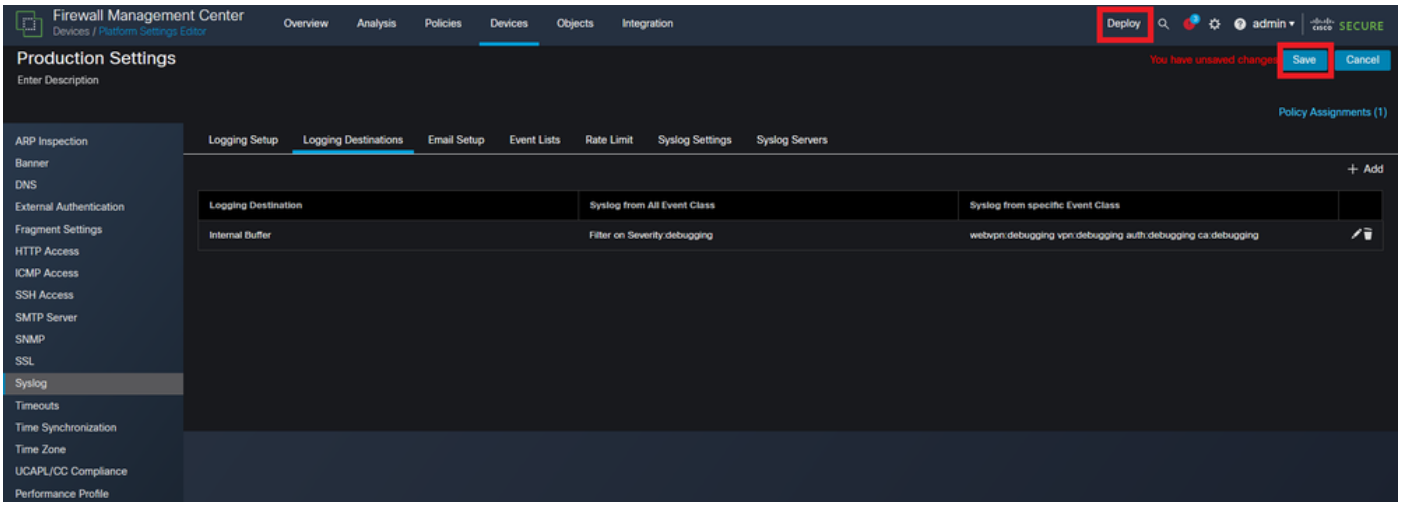
gebruikt. Wijzig **Event Class** in **Filter on Severity and debugging**. Als dit is voltooid, klikt u op +Add en kiest u webvpn, vpn, authen caallemaal met de ernst van de debuggingvan Syslog. Met deze stap kan de beheerder deze debug-uitgangen filteren naar een specifiek syslog-bericht van 711001. Deze kunnen worden aangepast afhankelijk van het type probleemoplossing. De gekozen in dit voorbeeld hebben echter betrekking op de meest voorkomende Site-to-Site-, Remote Access- en AAA VPN-gerelateerde problemen.



Maak gebeurtenisklassen en filters voor de foutopsporing.

Waarschuwing: hiermee wordt het bufferlogniveau gewijzigd in foutopsporing en worden foutopsporingsgebeurtenissen vastgelegd voor de klassen die zijn opgegeven voor de interne buffer. Het wordt aanbevolen om deze logmethode te gebruiken voor het oplossen van problemen en niet voor langdurig gebruik.

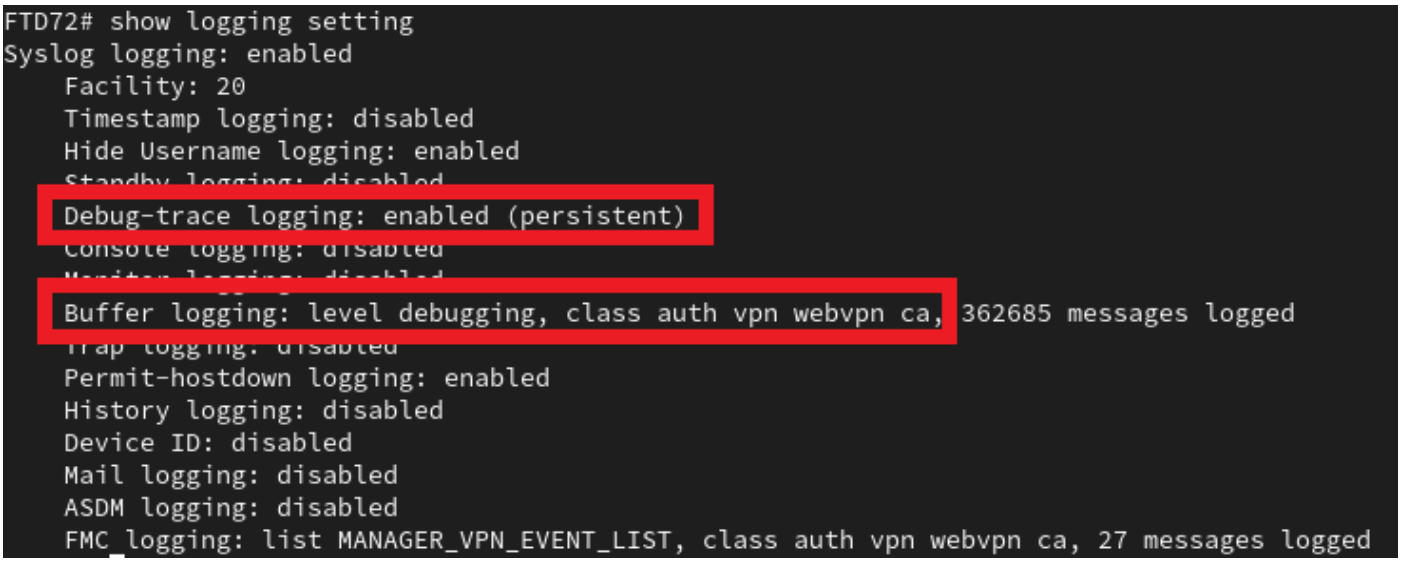
Choose Save rechtsboven en dan verandert Deploydе configuratie.



Firewall-dreigingsverdediging

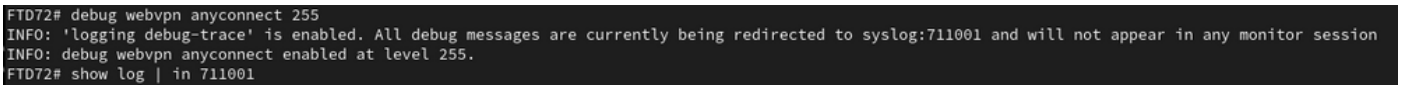
Navigeer naar de FTD CLI en geef de opdrachtshow logging setting. De instellingen hier weerspiegelen de wijzigingen die zijn aangebracht in het VCC. Zorg ervoor dat de logboekregistratie voor foutopsporing is ingeschakeld en dat de bufferlogboekregistratie overeenkomt met de opgegeven

klassen en logniveaus.



Geef de instellingen voor logboekregistratie weer in de FTD CLI.

Pas ten slotte een foutopsporing toe om ervoor te zorgen dat de logs worden omgeleid naar syslog: 711001. In dit voorbeeld wordt `debug webvpn anyconnect 255` toegepast. Dit activeert een melding voor het opsporen van foutmeldingen, waardoor de beheerder weet dat deze foutmeldingen worden omgeleid. Om deze debugs te bekijken, geeft u de opdracht `show log | in 711001`. Deze syslog-ID bevat nu alleen relevante VPN-foutmeldingen zoals toegepast door de beheerder. Bestaande logs kunnen worden gewist met een duidelijke logbuffer.



Geeft aan dat alle VPN-foutmeldingen worden omgeleid naar syslog 711001.

Over deze vertaling

Cisco heeft dit document vertaald via een combinatie van machine- en menselijke technologie om onze gebruikers wereldwijd ondersteuningscontent te bieden in hun eigen taal. Houd er rekening mee dat zelfs de beste machinevertaling niet net zo nauwkeurig is als die van een professionele vertaler. Cisco Systems, Inc. is niet aansprakelijk voor de nauwkeurigheid van deze vertalingen en raadt aan altijd het oorspronkelijke Engelstalige document (link) te raadplegen.