Implementierung von Plattformeinstellungen für die VPN-Fehlerbehebung

Inhalt

Einleitung

In diesem Dokument wird beschrieben, wie VPN-Debug-Protokolle mithilfe von Secure Firewall Management Center und Secure Firewall Threat Defense leicht organisiert und identifiziert werden können.

Voraussetzungen

Anforderungen

Cisco empfiehlt, dass Sie über Kenntnisse in folgenden Bereichen verfügen:

- Sichere Firewall-Bedrohungsabwehr (FTD)
- Secure Firewall Management Center (FMC)

- Grundlegendes Verständnis der Navigation in der FMC-GUI und FTD-CLI
- Vorhandene Richtlinienzuweisung für Plattformeinstellungen

Verwendete Komponenten

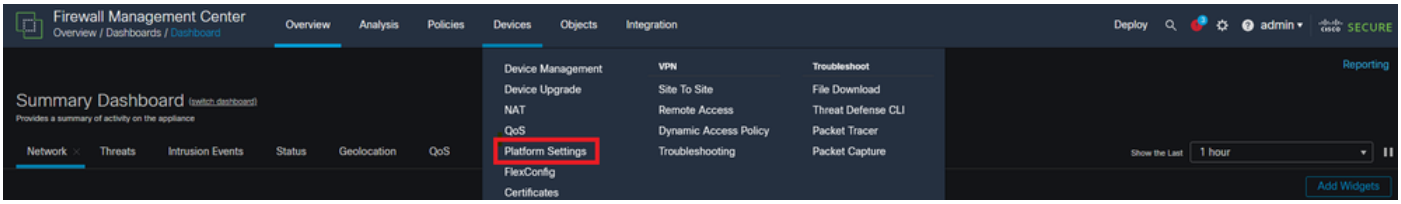
Die Informationen in diesem Dokument basieren auf den folgenden Software- und Hardwareversionen:

- Firewall Management Center Version 7.3
- Firewall Threat Defense Version 7.3

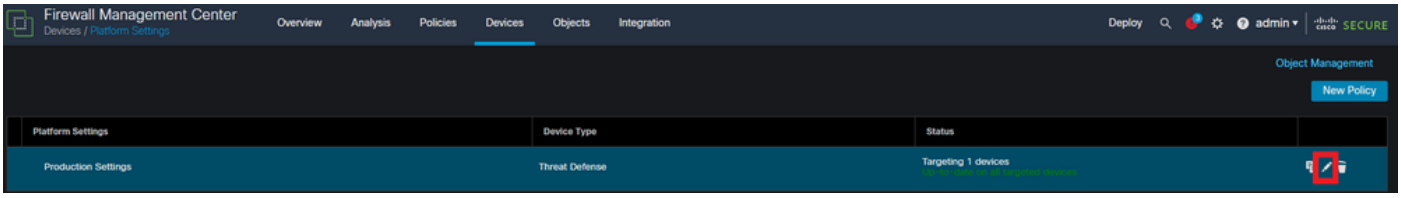
Die Informationen in diesem Dokument beziehen sich auf Geräte in einer speziell eingerichteten Testumgebung. Alle Geräte, die in diesem Dokument benutzt wurden, begannen mit einer gelöschten (Nichterfüllungs) Konfiguration. Wenn Ihr Netzwerk in Betrieb ist, stellen Sie sicher, dass Sie die möglichen Auswirkungen aller Befehle kennen.

Firewall-Verwaltungscenter

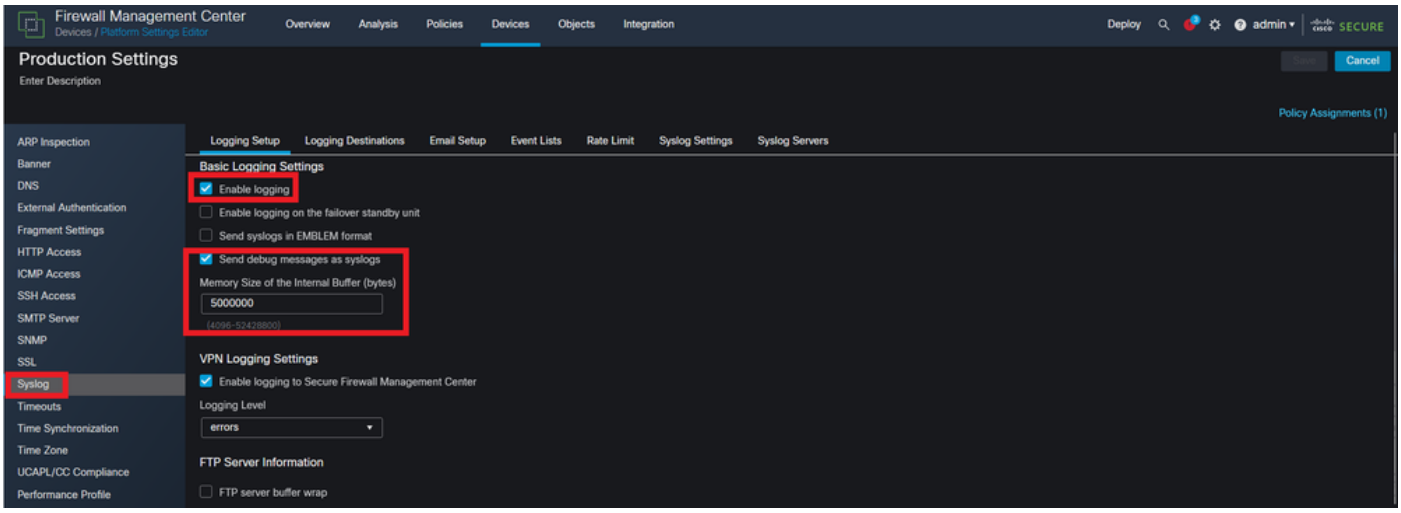
Navigieren Sie zu . Devices > Platform Settings



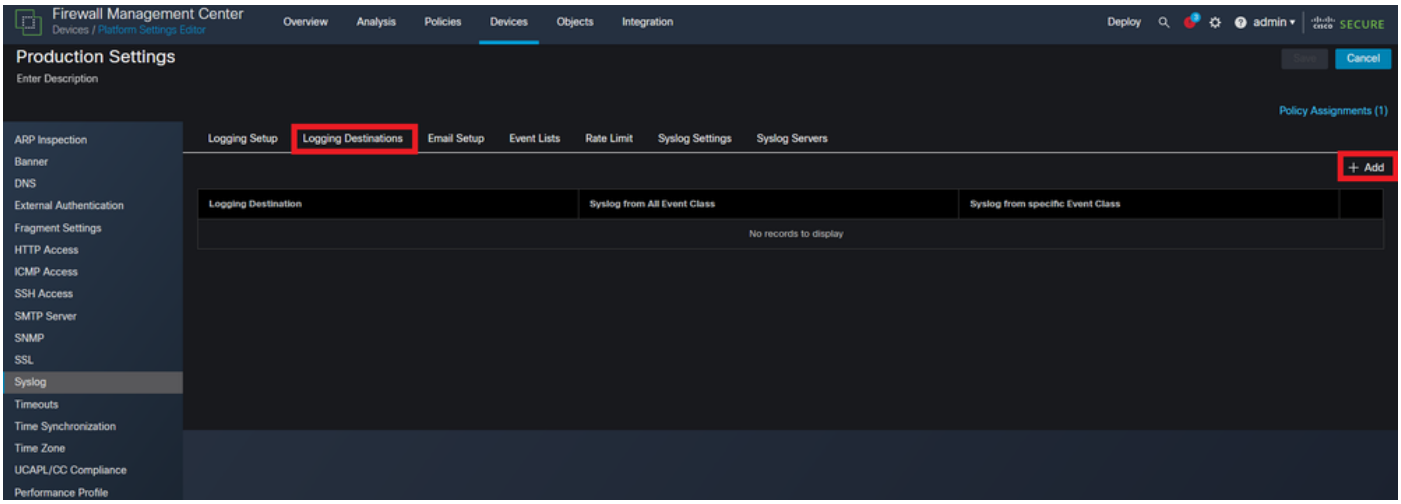
Klicken Sie auf **pencil** zwischen dem copy und dem Löschen icon.



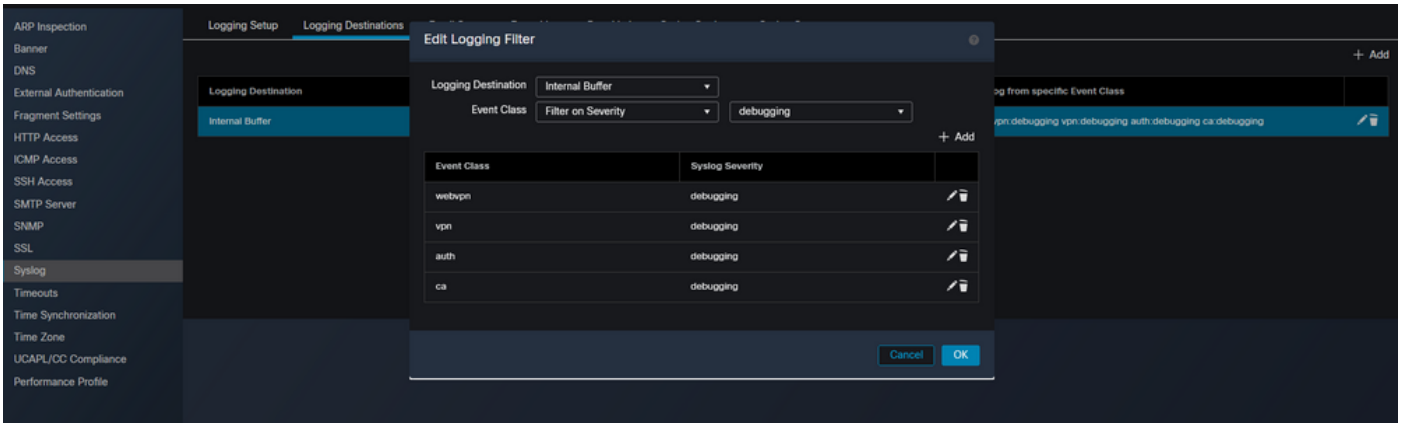
Navigieren Sie zu Syslogin der linken Spalte mit Optionen, und stellen Sie sicher, **Enable Logging**und **Send debug messages as syslog** sind aktiviert. Stellen Sie außerdem sicher, dass der Memory Size of the Internal Buffer Wert so eingestellt ist, dass er für die Fehlerbehebung geeignet ist.



Klicken **Logging Destinations** Sie auf und dann auf **+Add**.



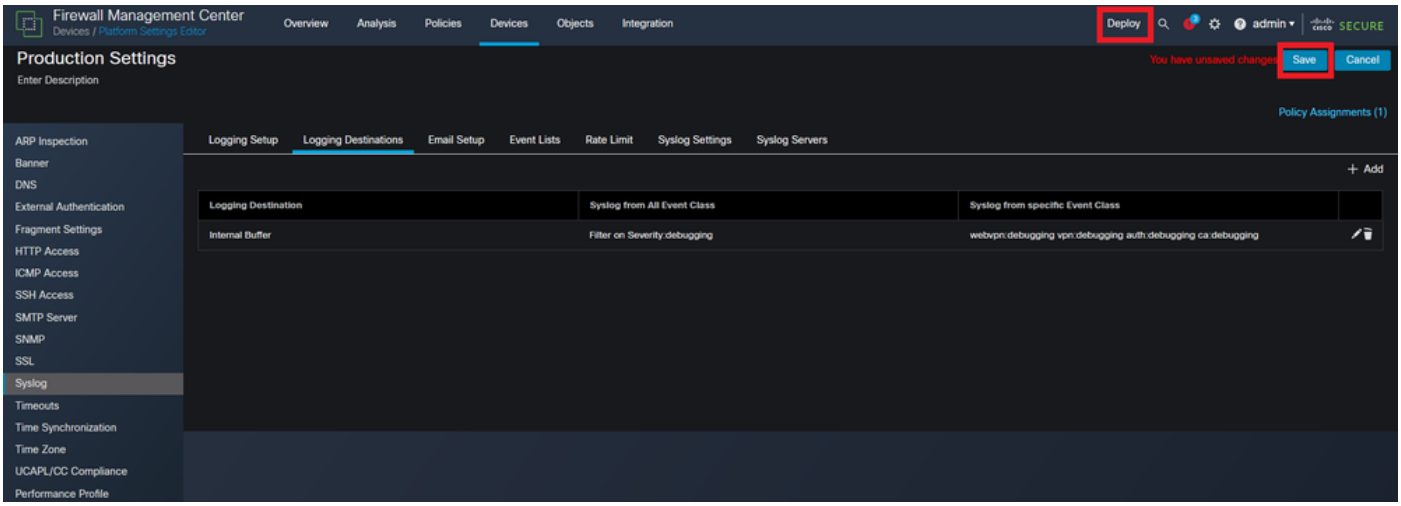
In diesem Abschnitt ist das Ziel der Protokollierung eine Präferenz des Administrators und **Internal Buffer** wird verwendet. Ändern Sie **Event Class Filter on Severity and debugging**. den Wert in After this is complete, click +Add and select webvpn, vpn, auth, and caall with Syslog Severity of debugging. Mit diesem Schritt kann der Administrator diese Debug-Ausgaben nach einer bestimmten Syslog-Meldung von 711001 filtern. Diese können je nach Art der Fehlerbehebung geändert werden. Die in diesem Beispiel ausgewählten beziehen sich jedoch auf die am häufigsten auftretenden standortübergreifenden, Remote-Zugriffs- und AAA-VPN-Probleme.



Erstellen Sie Ereignisklassen und Filter für die Debugs.

Warnung: Dadurch wird die Pufferprotokollierungsebene auf Debugging geändert, und Debug-Ereignisse für die im internen Puffer angegebenen Klassen werden protokolliert. Es wird empfohlen, diese Protokollierungsmethode zur Fehlerbehebung und nicht zur langfristigen Verwendung zu verwenden.

Choose Save oben rechts ein, und Deploydie Konfiguration ändert sich.



Abwehr von Firewall-Bedrohungen

Navigieren Sie zur FTD-CLI, und geben Sie den Befehl`show logging setting`ein. Die Einstellungen hier spiegeln die Änderungen wider, die am FMC vorgenommen wurden. Stellen Sie sicher, dass die Protokollierung von debug-trace aktiviert ist und die Protokollierung des Puffers mit den angegebenen Klassen und der angegebenen Protokollierungsebene übereinstimmt.

```
FTD72# show logging setting
Syslog logging: enabled
    Facility: 20
    Timestamp logging: disabled
    Hide Username logging: enabled
    Debug-trace logging: enabled (persistent)
    Buffer logging: level debugging, class auth vpn webvpn ca, 362685 messages logged
    Permit-hostdown logging: enabled
    History logging: disabled
    Device ID: disabled
    Mail logging: disabled
    ASDM logging: disabled
    FMC logging: list MANAGER_VPN_EVENT_LIST, class auth vpn webvpn ca, 27 messages logged
```

Anzeigen der Protokolleinstellungen in der FTD-CLI

Wenden Sie zuletzt ein Debugging an, um sicherzustellen, dass die Protokolle an syslog:711001 umgeleitet werden. In diesem Beispiel wird dieses `debug webvpn anyconnect 255` Debugging angewendet. Dadurch wird eine Meldung zur Fehlersuche ausgelöst, die den Administrator darüber informiert, dass die Fehlersuche umgeleitet wird. Um diese Debugs anzuzeigen, geben Sie den Befehl `show log | in 711001`ein. Diese Syslog-ID enthält jetzt nur noch relevante VPN-Debugging-Protokolle, die vom Administrator angewendet wurden. Bestehende Protokolle können mit einem leeren Protokollierungspuffer gelöscht werden.

```
FTD72# debug webvpn anyconnect 255
INFO: 'logging debug-trace' is enabled. All debug messages are currently being redirected to syslog:711001 and will not appear in any monitor session
INFO: debug webvpn anyconnect enabled at level 255.
FTD72# show log | in 711001
```

Zeigt an, dass alle VPN-Debugging-Vorgänge auf Syslog 711001 umgeleitet werden.

Informationen zu dieser Übersetzung

Cisco hat dieses Dokument maschinell übersetzen und von einem menschlichen Übersetzer editieren und korrigieren lassen, um unseren Benutzern auf der ganzen Welt Support-Inhalte in ihrer eigenen Sprache zu bieten. Bitte beachten Sie, dass selbst die beste maschinelle Übersetzung nicht so genau ist wie eine von einem professionellen Übersetzer angefertigte. Cisco Systems, Inc. übernimmt keine Haftung für die Richtigkeit dieser Übersetzungen und empfiehlt, immer das englische Originaldokument (siehe bereitgestellter Link) heranzuziehen.