Benutzerdefinierten Port für RAVPN auf FTD konfigurieren, von FMC verwaltet

Inhalt

Einleitung

In diesem Dokument wird das Verfahren zur Konfiguration eines benutzerdefinierten Ports für SSL und IKEv2 AnyConnect auf Firepower Threat Defense (FTD) beschrieben, die von FMC verwaltet werden.

Voraussetzungen

Anforderungen

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

- Grundlegendes zum Remote Access VPN (RAVPN)
- Erfahrung mit FirePOWER Management Center (FMC)

Verwendete Komponenten

Die Informationen in diesem Dokument basierend auf folgenden Software- und Hardware-Versionen:

- Cisco FTD - 7.6
- Cisco FMC - 7.6
- Windows 10

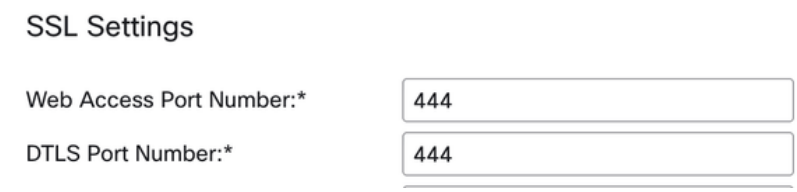
Die Informationen in diesem Dokument beziehen sich auf Geräte in einer speziell eingerichteten Testumgebung. Alle Geräte, die in diesem Dokument benutzt wurden, begannen mit einer gelöschten (Nichterfüllungs) Konfiguration. Wenn Ihr Netzwerk in Betrieb ist, stellen Sie sicher, dass Sie die möglichen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

Konfigurationen

Änderung der SSL-/DTLS-Ports für AnyConnect

1. Navigieren Sie zu Devices > VPN > Remote Access, und bearbeiten Sie die vorhandene RAS-Richtlinie.

2. Navigieren Sie zum Abschnitt "Access Interfaces" (Zugriffsschnittstellen), und ändern Sie die Web Access-Portnummer und die DTLS-Portnummer unter den SSL-Einstellungen in einen Port Ihrer Wahl.



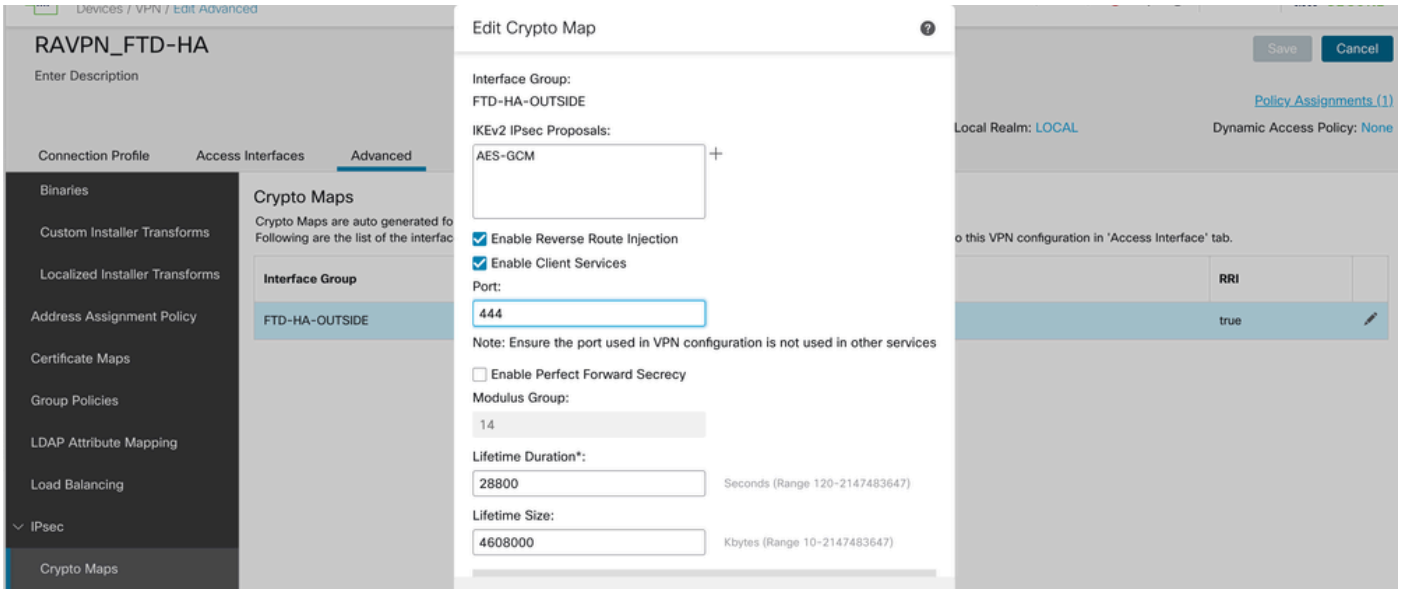
Änderung der SSL- und DTLS-Ports für AnyConnect

3. Speichern der Konfiguration

IKEv2-Portänderung für AnyConnect

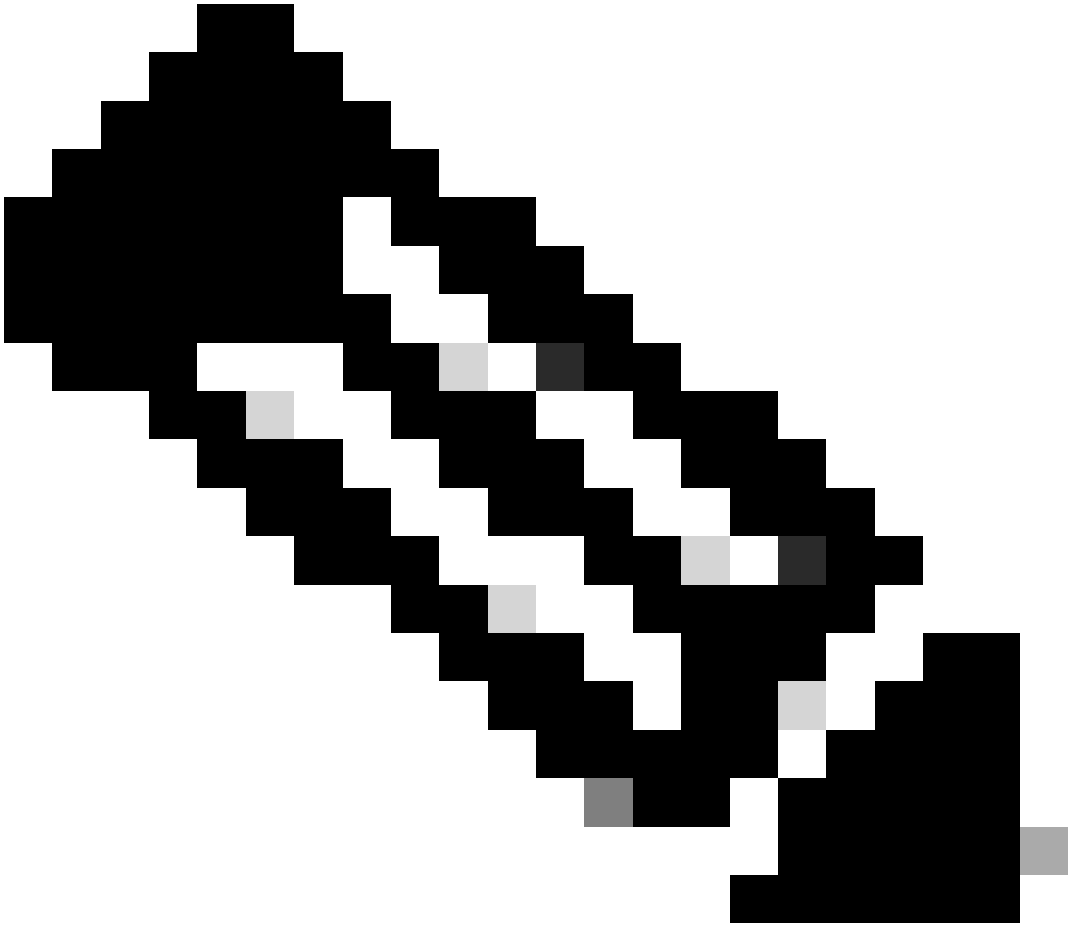
1. Navigieren Sie zu Devices > VPN > Remote Access, und bearbeiten Sie die vorhandene RAS-Richtlinie.

2. Navigieren Sie zum Abschnitt Erweitert, und navigieren Sie dann zu IPsec > Crypto Maps. Bearbeiten Sie die Richtlinie, und ändern Sie den Port zu Ihrem gewünschten Port.



IKEv2-Portänderung für AnyConnect

3. Speichern der Konfiguration und Bereitstellung.



Anmerkung: Beachten Sie bei der Verwendung von Custom Port zusammen mit AnyConnect Client Profiles, dass das Host-Adressfeld in der Serverliste für die Verbindung X.X.X.X:port (192.168.50.5:444) aufweisen muss.

Überprüfung

1. Nach der Bereitstellung kann die Konfiguration mit den Befehlen show run webvpn und show run crypto ikev2 überprüft werden:

```
<#root>

>

show run webvpn

webvpn

port 444  <----- Custom Port that has been configured for SSL
```

```
enable outside
```

dtls port 444 <----- Custom Port that has been configured for DTLS

```
http-headers
  hsts-server
   enable
   max-age 31536000
   include-sub-domains
   no preload
  hsts-client
   enable
  x-content-type-options
  x-xss-protection
  content-security-policy
anyconnect image disk0:/csm/cisco-secure-client-win-X.X.X.X-webdeploy-k9.pkg 1 regex "Windows"
anyconnect enable
tunnel-group-list enable
cache
  disable
error-recovery disable
```

<#root>

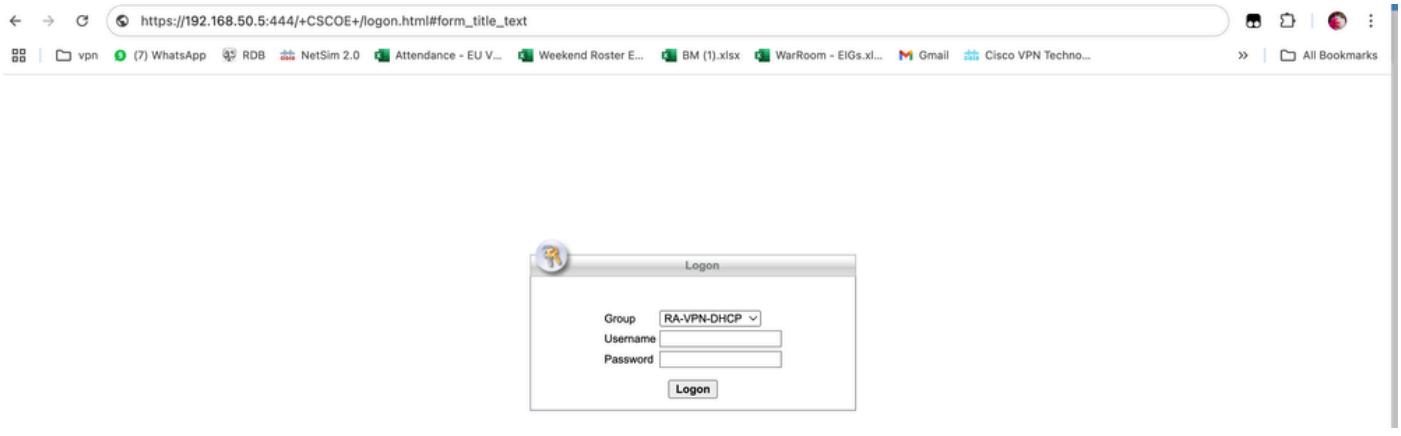
>

show run crypto ikev2

```
crypto ikev2 policy 10
 encryption aes-gcm-256 aes-gcm-192 aes-gcm
 integrity null
 group 21 20 19 16 15 14
 prf sha512 sha384 sha256 sha
 lifetime seconds 86400
```

crypto ikev2 enable outside client-services port 444 <----- Custom Port configured for IKEv2 Client Serv

2. Überprüfen Sie dies, indem Sie über den Browser/eine AnyConnect-Anwendung mit einem benutzerdefinierten Port auf den Remote-Zugriff zugreifen:



Überprüfung durch Zugriff auf AnyConnect mit benutzerdefiniertem Port

Fehlerbehebung

- Stellen Sie sicher, dass der in der RAS-Konfiguration verwendete Port nicht für andere Dienste verwendet wird.
- Stellen Sie sicher, dass der Port nicht vom ISP oder von zwischengeschalteten Geräten blockiert wird.
- Mithilfe von Aufzeichnungen auf FTD kann überprüft werden, ob Pakete die Firewall erreichen und ob die Antwort gesendet wird oder nicht.

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.