Configura porta personalizzata per RAVPN su FTD Gestito da FMC

Sommario

Introduzione

In questo documento viene descritta la procedura per configurare una porta personalizzata per SSL e IKEv2 AnyConnect su Firepower Threat Defense (FTD) gestito da FMC.

Prerequisiti

Requisiti

Cisco raccomanda la conoscenza dei seguenti argomenti:

- Conoscenze base di RAVPN (Remote Access VPN)
- Esperienza con Firepower Management Center (FMC)

Componenti usati

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

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

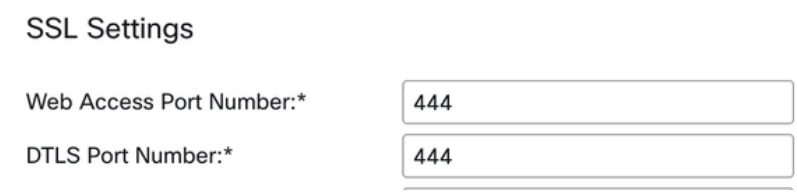
Le informazioni discusse in questo documento fanno riferimento a dispositivi usati in uno specifico ambiente di emulazione. Su tutti i dispositivi menzionati nel documento la configurazione è stata ripristinata ai valori predefiniti. Se la rete è operativa, valutare attentamente eventuali conseguenze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

Configurazioni

Modifica porta SSL/DTLS per AnyConnect

1. Passare a Dispositivi > VPN > Accesso remoto e modificare i criteri di Accesso remoto esistenti.

2. Passare alla sezione Interfacce di accesso e modificare il numero di porta di accesso Web e il numero di porta DTLS in Impostazioni SSL in una porta a scelta.



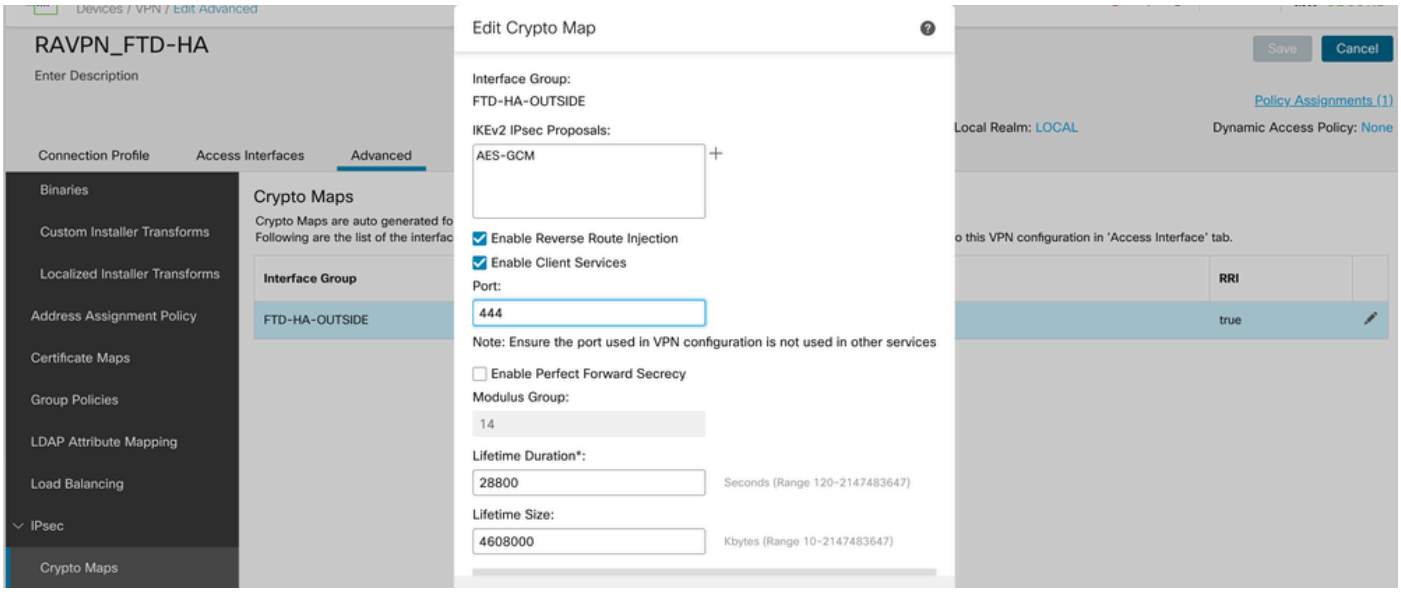
Modifica della porta SSL e DTLS per AnyConnect

3. Salvare la configurazione.

Modifica porta IKEv2 per AnyConnect

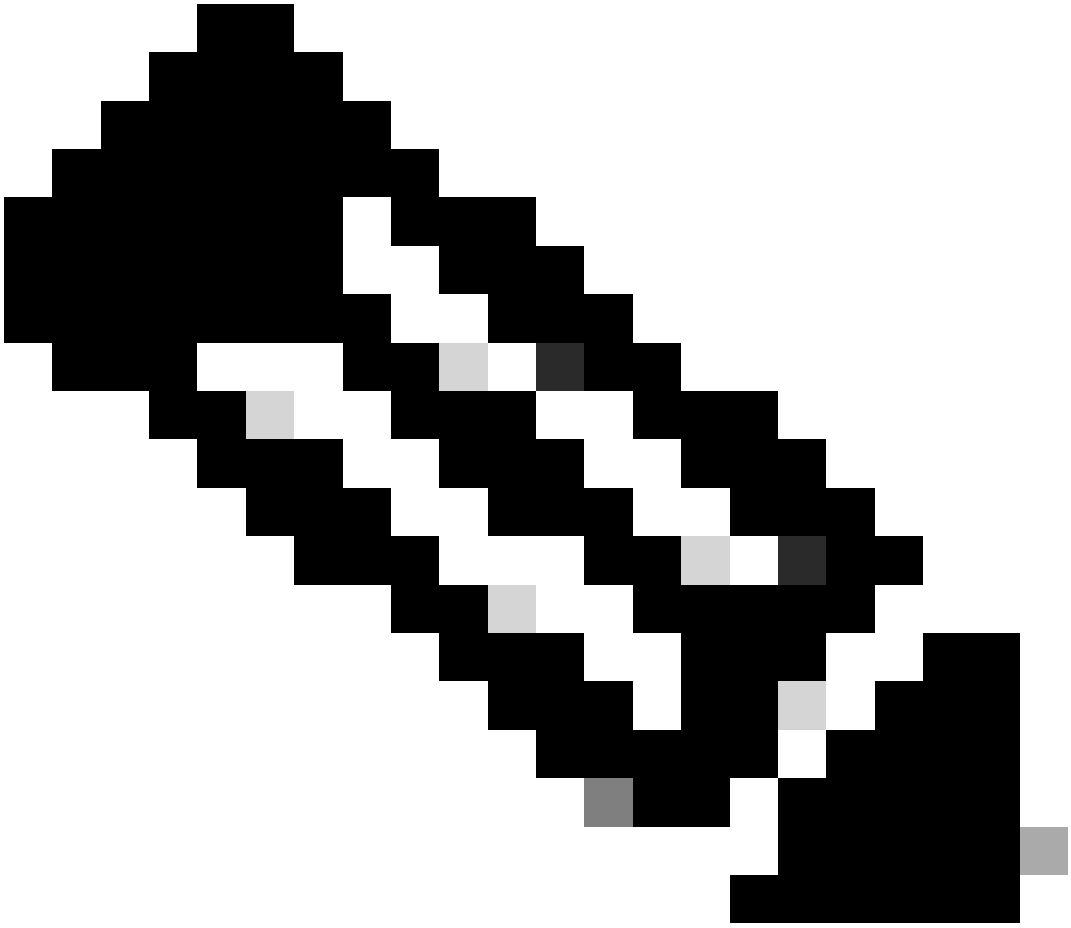
1. Passare a Dispositivi > VPN > Accesso remoto e modificare i criteri di Accesso remoto esistenti.

2. Passare alla sezione Advanced (Avanzate), quindi selezionare IPsec > Crypto Maps (Mappe crittografiche). Modificare il criterio e impostare la porta desiderata.



Modifica porta IKEv2 per AnyConnect

3. Salvare la configurazione e distribuirla.



Nota: Quando si utilizza Custom Port con AnyConnect Client Profiles, tenere presente che per la connettività il campo dell'indirizzo host nell'elenco dei server deve avere X.X.X.X:port (192.168.50.5:44).

Verifica

1. Dopo la distribuzione, la configurazione può essere verificata con i comandi show run webvpn e show run crypto ikev2:

```
<#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>

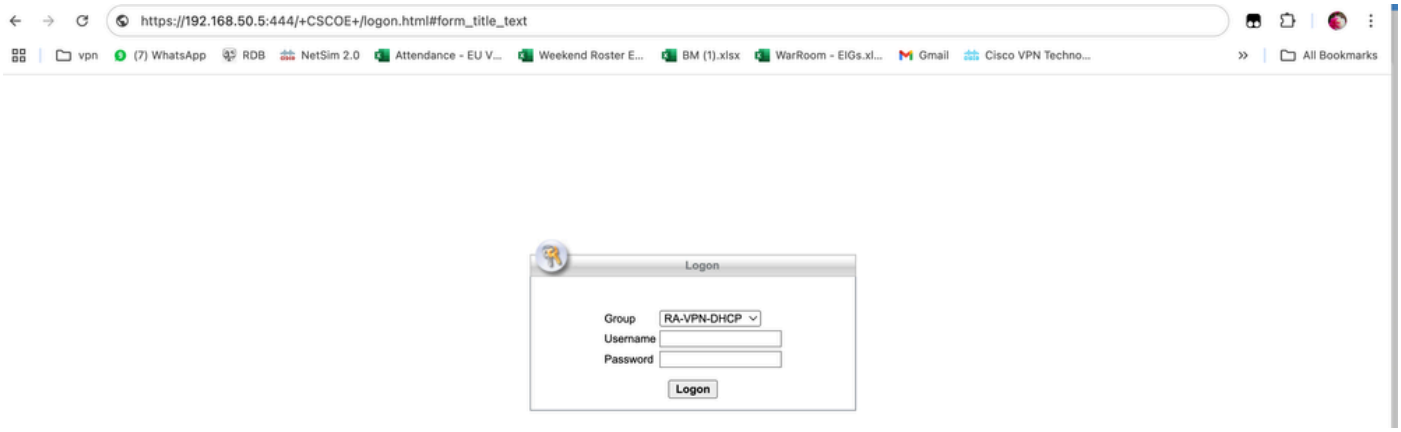
>

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. Verificare accedendo ad Accesso remoto dal browser/dall'applicazione AnyConnect con porta personalizzata:



Verifica accedendo a AnyConnect con la porta personalizzata

Risoluzione dei problemi

- Verificare che la porta utilizzata nella configurazione di Accesso remoto non sia utilizzata in altri servizi.
- Verificare che la porta non sia bloccata dall'ISP o da dispositivi intermedi.
- È possibile acquisire le immagini su FTD per verificare se i pacchetti stanno raggiungendo il firewall e se la risposta è stata inviata o meno.

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).