Configurazione del tunneling ripartito dinamico ASA/AnyConnect

Sommario

Introduzione

Questo documento descrive come configurare AnyConnect Secure Mobility Client per il tunneling a esclusione di split dinamico tramite ASDM.

Prerequisiti

Requisiti

Cisco raccomanda la conoscenza dei seguenti argomenti:

- Conoscenze base di ASA.
- Conoscenze base di Cisco Anyconnect Security Mobility Client.

Componenti usati

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

- ASA 9.12(3)9
- Adaptive Security Device Manager (ASDM) 7.13(1)
- AnyConnect 4.7.0

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.

Premesse

Il tunneling AnyConnect Split consente a Cisco AnyConnect Secure Mobility Client di accedere in modo sicuro alle risorse aziendali tramite IKEV2 o SSL (Secure Sockets Layer).

Nelle versioni precedenti a AnyConnect 4.5, in base ai criteri configurati su ASA (Adaptive Security Appliance), il comportamento del tunnel suddiviso può essere Specificato per il tunnel, Specificato per il tunnel Tutti i tunnel o Escluso.

Con l'avvento delle risorse del computer ospitato nel cloud, i servizi a volte si risolvono in un indirizzo IP diverso in base alla posizione dell'utente o al carico delle risorse ospitate nel cloud.

Poiché Anyconnect Secure Mobility Client fornisce il tunneling suddiviso a intervalli di subnet statiche, host o pool di IPV4 o IPV6, per gli amministratori di rete diventa difficile escludere domini/FQDN durante la configurazione di AnyConnect.

Ad esempio, un amministratore di rete desidera escludere il dominio Cisco.com dalla configurazione del tunnel di divisione, ma il mapping DNS per Cisco.com cambia poiché è ospitato nel cloud.

Utilizzando il tunneling con esclusione della divisione dinamica, Anyconnect risolve in modo dinamico l'indirizzo IPv4/IPv6 dell'applicazione ospitata e apporta le modifiche necessarie alla tabella di routing e ai filtri per consentire la connessione all'esterno del tunnel.

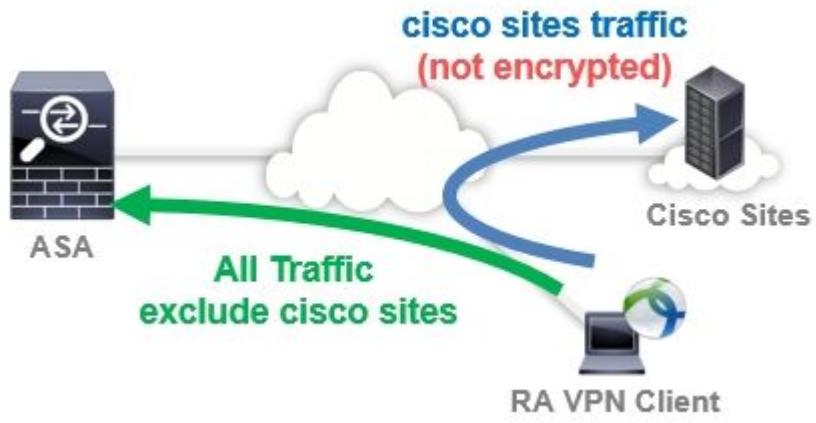
A partire da AnyConnect 4.5, il tunneling dello split dinamico può essere usato quando Anyconnect risolve in modo dinamico l'indirizzo IPv4/IPv6 dell'applicazione ospitata e apporta le modifiche necessarie alla tabella di routing e ai filtri per consentire la connessione all'esterno del tunnel

Configurazione

In questa sezione viene descritto come configurare Cisco AnyConnect Secure Mobility Client sull'appliance ASA.

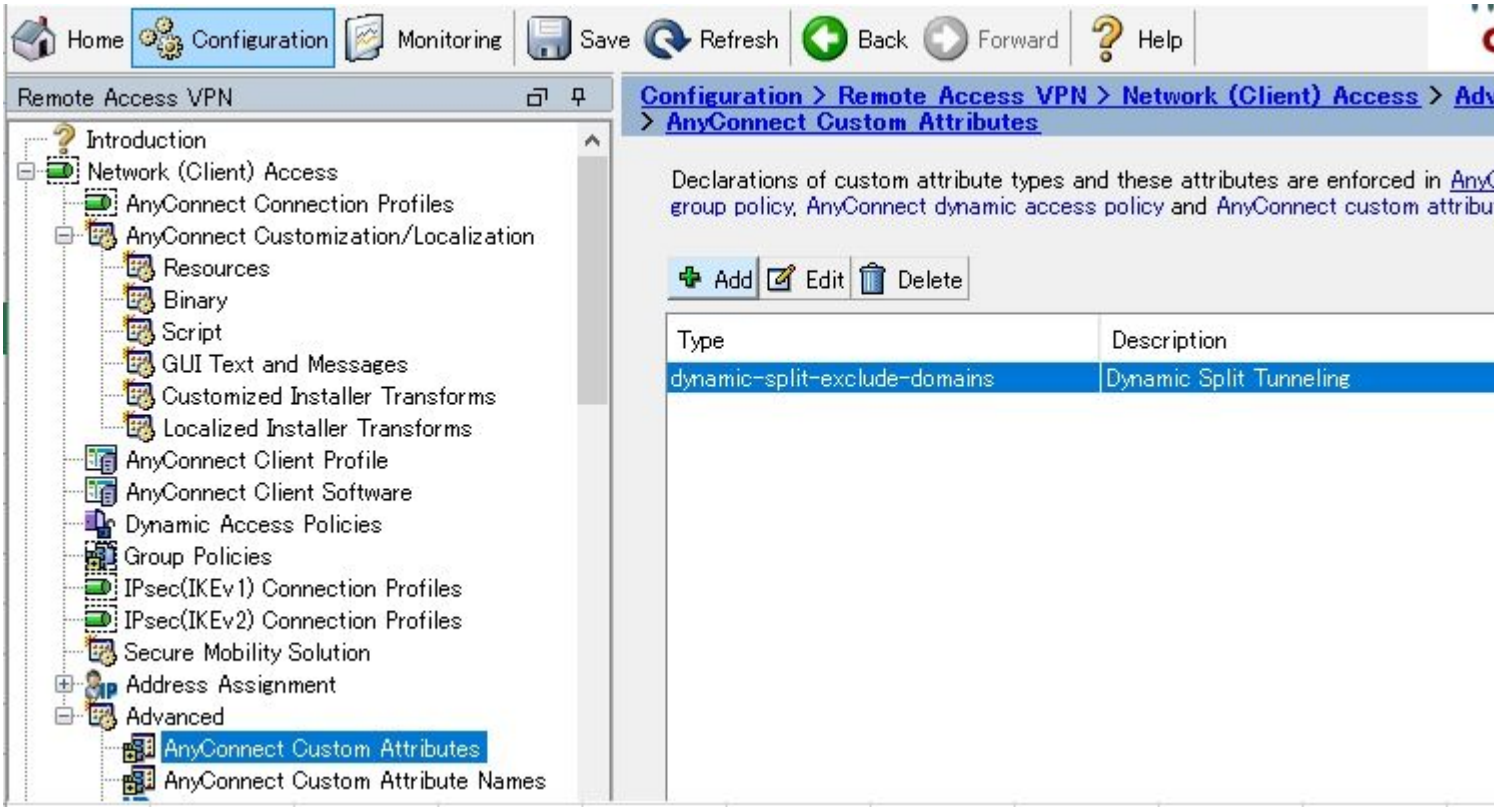
Esempio di rete

Nell'immagine è illustrata la topologia utilizzata per gli esempi di questo documento.



Passaggio 1. Creare attributi personalizzati AnyConnect.

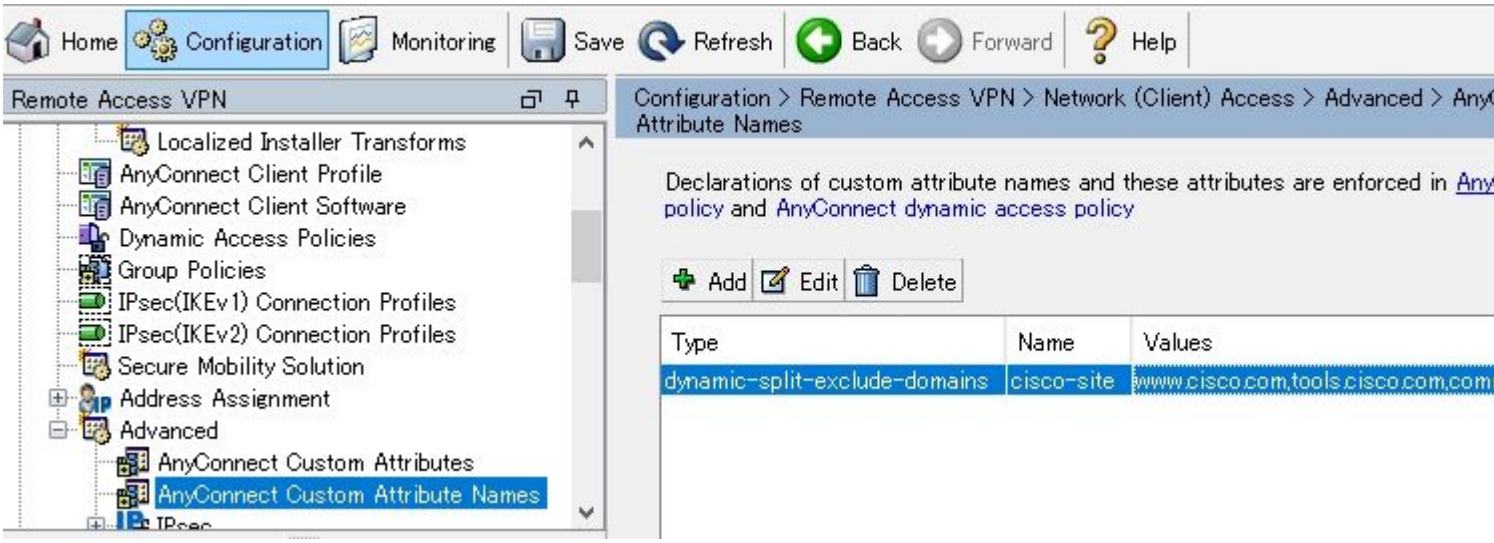
Passa a **Configuration > Remote Access VPN > Network (Client) Access > Advanced > AnyConnect Custom Attributes.**fare clic su **Add** e impostare **dynamic-split-exclude-domains** e una descrizione facoltativa, come illustrato nell'immagine:



Passaggio 2. Creare il nome personalizzato e configurare i valori di AnyConnect.

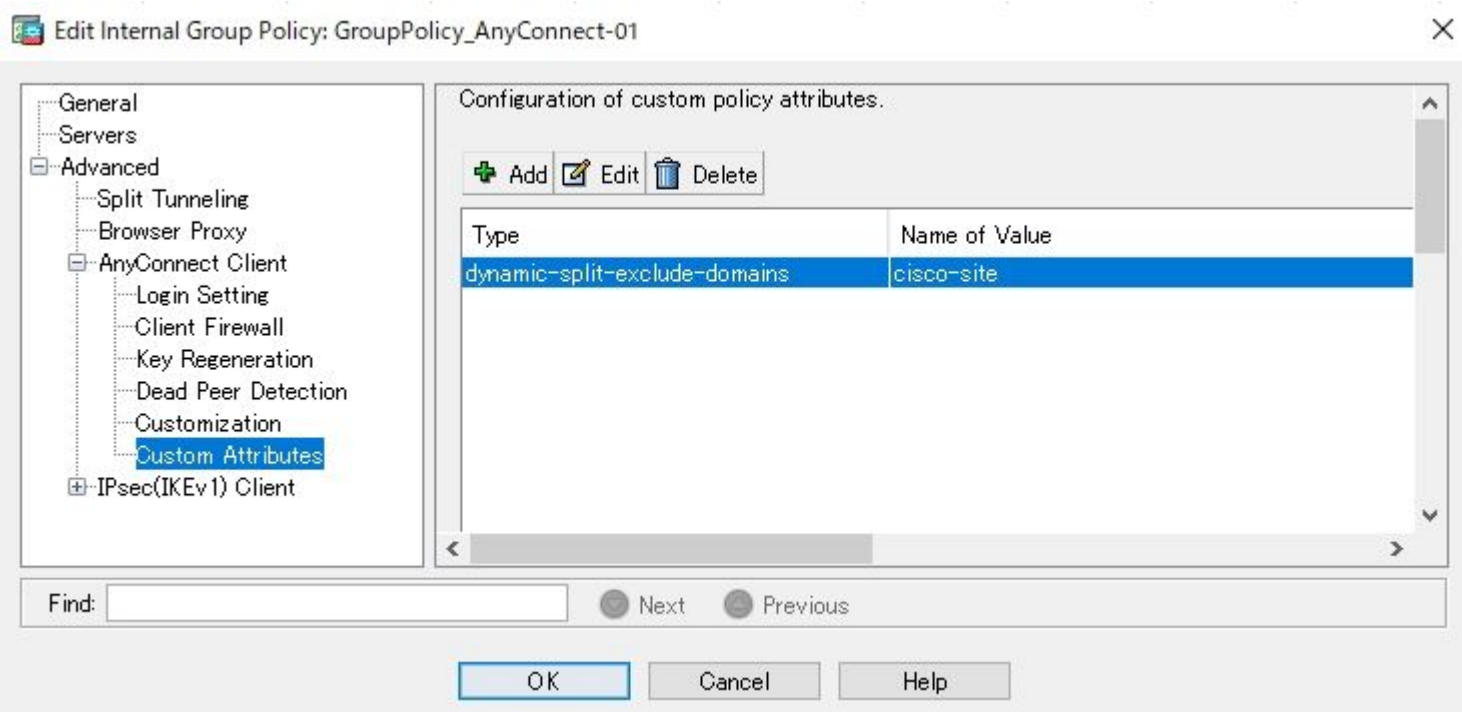
Passa a **Configuration > Remote Access VPN > Network (Client) Access > Advanced > AnyConnect Custom Attribute Names.**fare clic su **Add** e impostare il **dynamic-split-exclude-domains** creato in precedenza da Type, un nome arbitrario e Values, come mostrato nell'immagine:

Fare attenzione a non inserire uno spazio in Nome. (Esempio: Possibile "cisco-site" Impossibile "cisco site") Quando sono registrati più domini o FQDN in Valori, separarli con una virgola (,).



Passaggio 3. Aggiungere tipo e nome ai Criteri di gruppo.

Passa a **Configuration> Remote Access VPN> Network (Client) Access> Group Policies** e selezionare un oggetto Criteri di gruppo. Da quel momento in poi, passare a **Advanced> AnyConnect Client> Custom Attributes** e aggiungere il file **Type** e **Name,** come mostrato nell'immagine:



Esempio di configurazione CLI

Questa sezione fornisce la configurazione CLI del tunneling con split dinamico a scopo di riferimento.

<#root>

```
ASAv10# show run
  --- snip ---
webvpn


 enable outside

 anyconnect-custom-attr dynamic-split-exclude-domains description Dynamic Split Tunneling


 hsts
  enable
  max-age 31536000
  include-sub-domains
  no preload
 anyconnect image disk0:/anyconnect-win-4.7.04056-webdeploy-k9.pkg 1
 anyconnect enable
 tunnel-group-list enable
 cache
  disable
 error-recovery disable

anyconnect-custom-data dynamic-split-exclude-domains cisco-site www.cisco.com,tools.cisco.com,community.


group-policy GroupPolicy_AnyConnect-01 internal
```

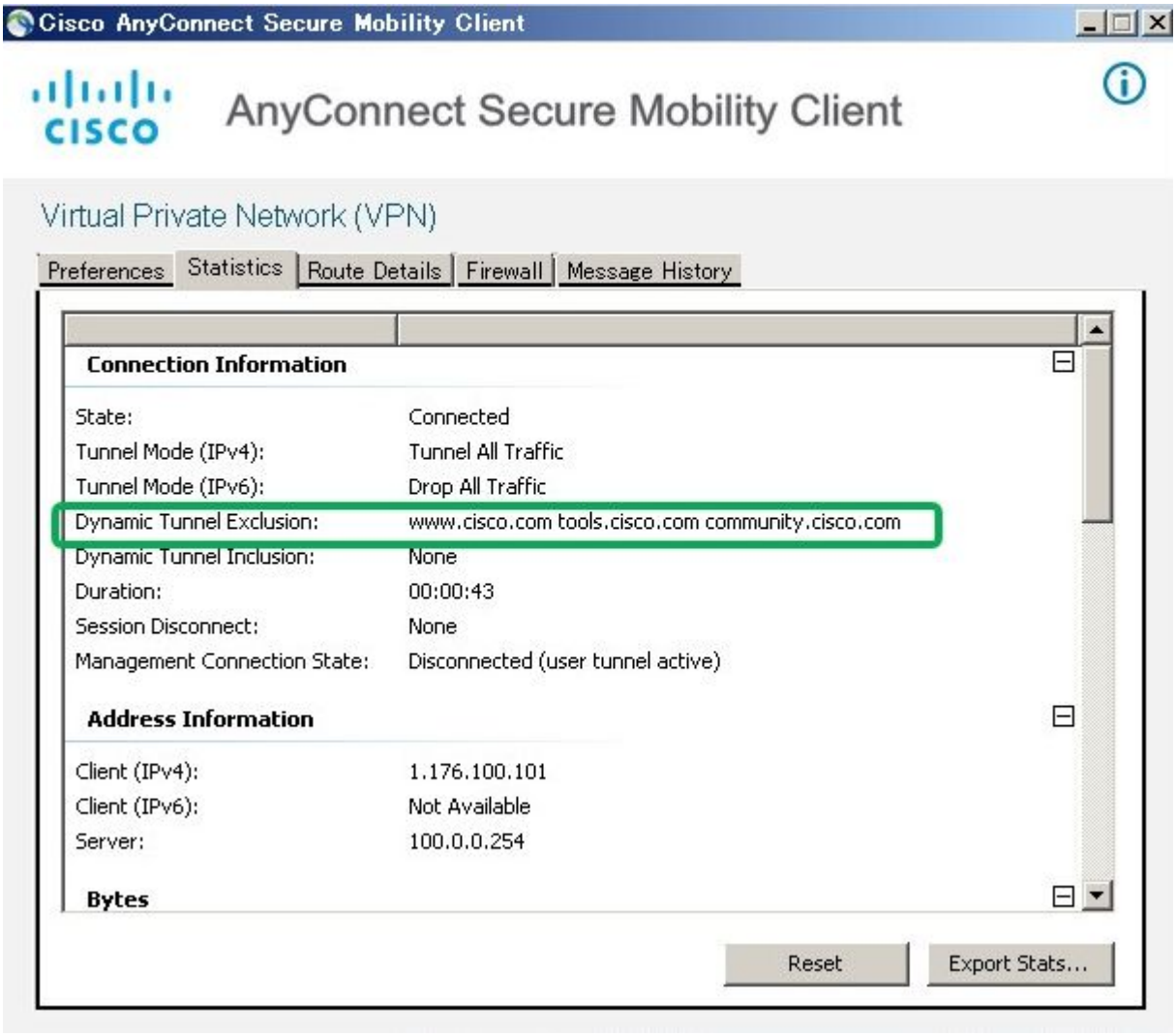
```
group-policy GroupPolicy_AnyConnect-01 attributes


 wins-server none
 dns-server value 10.0.0.0
 vpn-tunnel-protocol ssl-client
 split-tunnel-policy tunnelall
 split-tunnel-network-list value SplitACL
 default-domain value cisco.com

 anyconnect-custom dynamic-split-exclude-domains value cisco-site
```

Limitazioni

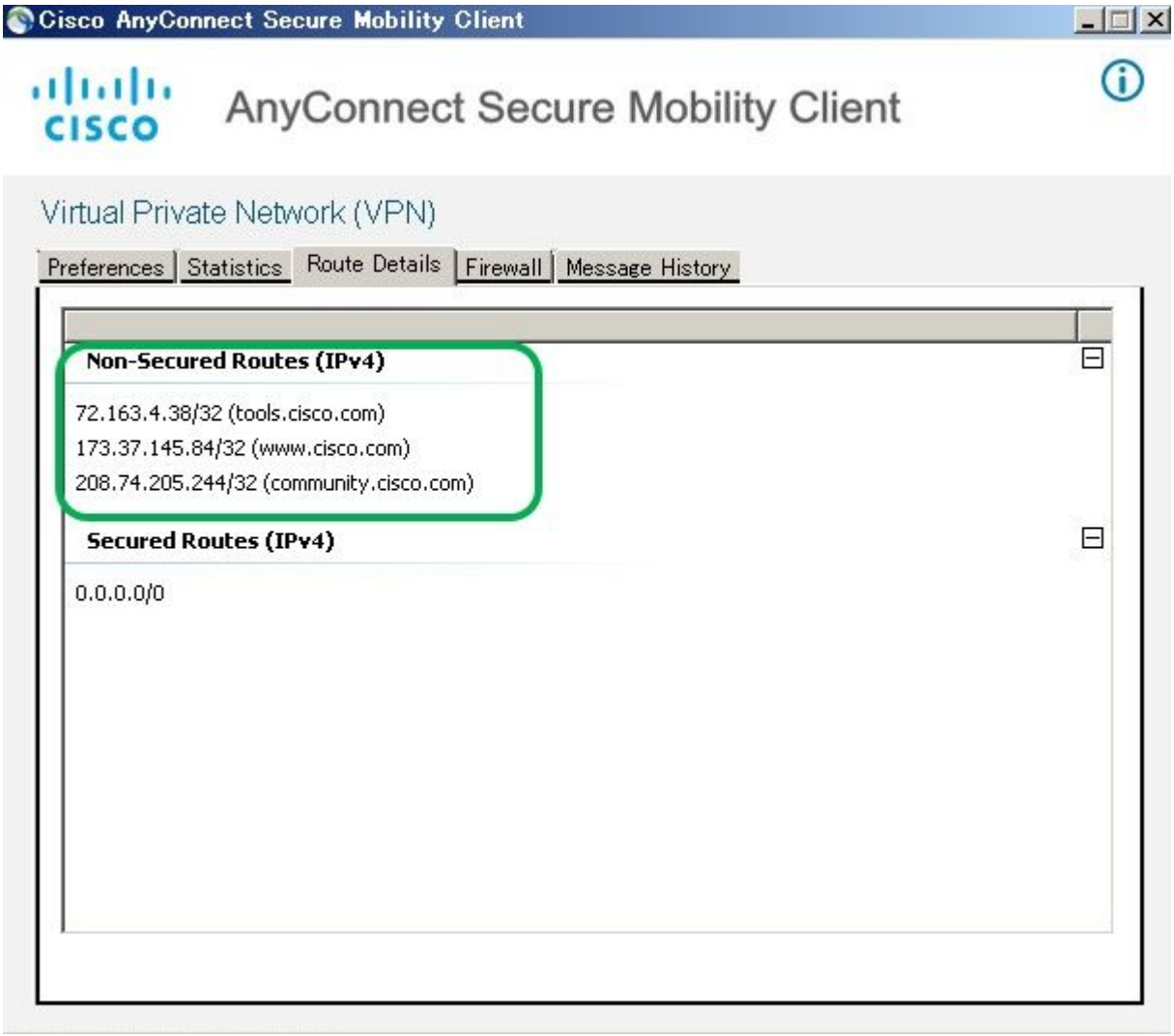
- Per utilizzare gli attributi personalizzati del tunneling dinamico suddiviso, è necessario disporre di ASA versione 9.0 o successive.
- Il carattere jolly nel campo Valori non è supportato.
- Il tunneling con split dinamico non è supportato sui dispositivi iOS (Apple) (richiesta miglioramento: 'Cisco bug ID CSCvr54798').

Verifica

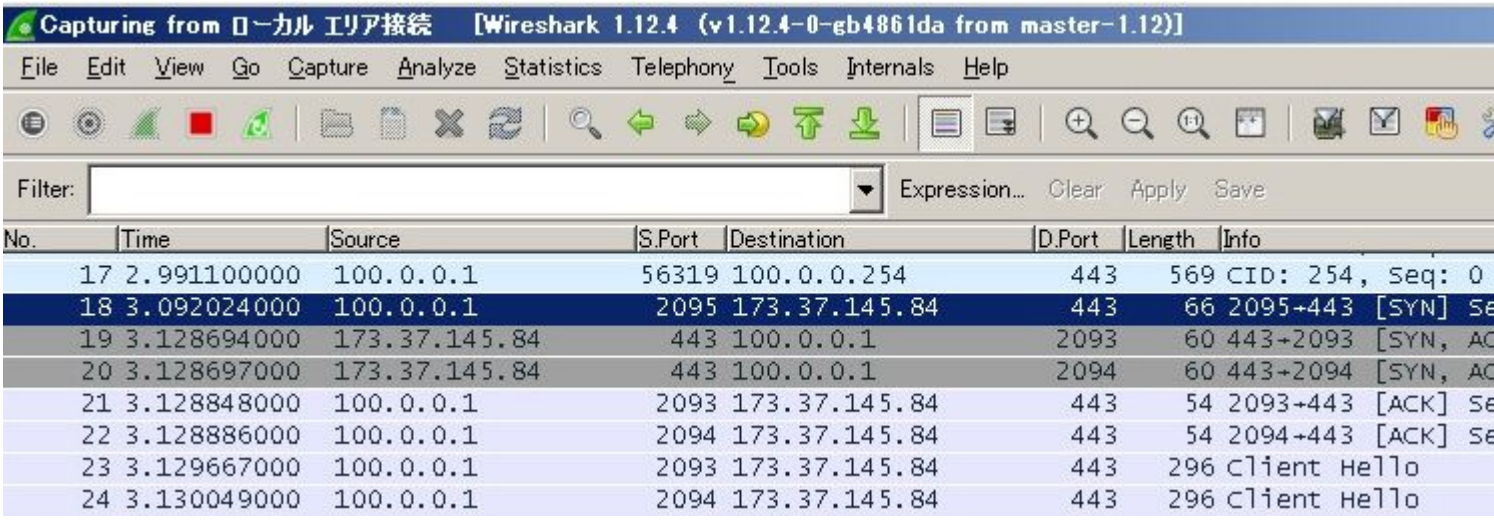
Per verificare la configurazione **Dynamic Tunnel Exclusions,** Avvia **AnyConnect** sul client, fare clic su **Advanced Window** > **Statistics,** come mostrato nell'immagine:



È inoltre possibile passare a **Advanced Window** > **Route Details** scheda in cui è possibile verificare **Dynamic Tunnel Exclusions** sono elencati in **Non-Secured Routes,** come mostrato nell'immagine.



In questo esempio, è stato configurato www.cisco.com in **Dynamic Tunnel Exclusion list** e l'acquisizione di Wireshark raccolta sull'interfaccia fisica del client AnyConnect conferma che il traffico diretto a www.cisco.com (198.51.100.0) non è crittografato da DTLS.



Risoluzione dei problemi

Se il carattere jolly è utilizzato nel campo Valori

Se nel campo Valori è configurato un carattere jolly, ad esempio ***.cisco.com** è configurato in Valori, la sessione AnyConnect viene disconnessa, come mostrato nei log:

```
Apr 02 2020 10:01:09: %ASA-4-722041: TunnelGroup <AnyConnect-01> GroupPolicy <GroupPolicy_AnyConnect-01>
Apr 02 2020 10:01:09: %ASA-5-722033: Group <GroupPolicy_AnyConnect-01> User <cisco> IP <172.16.0.0> Firs
Apr 02 2020 10:01:09: %ASA-6-722022: Group <GroupPolicy_AnyConnect-01> User <cisco> IP <172.16.0.0> TCP
Apr 02 2020 10:01:09: %ASA-6-722055: Group <GroupPolicy_AnyConnect-01> User <cisco> IP <172.16.0.0> Clie
Apr 02 2020 10:01:09: %ASA-4-722051: Group <GroupPolicy_AnyConnect-01> User <cisco> IP <172.16.0.0> IPv4
Apr 02 2020 10:01:09: %ASA-6-302013: Built inbound TCP connection 8570 for outside:172.16.0.0/44868 (172
Apr 02 2020 10:01:09: %ASA-4-722037: Group <GroupPolicy_AnyConnect-01> User <cisco> IP <172.16.0.0> SVC
Apr 02 2020 10:01:09: %ASA-5-722010: Group <GroupPolicy_AnyConnect-01> User <cisco> IP <172.16.0.0> SVC
Apr 02 2020 10:01:09: %ASA-6-716002: Group <GroupPolicy_AnyConnect-01> User <cisco> IP <172.16.0.0> WebV
Apr 02 2020 10:01:09: %ASA-4-113019: Group = AnyConnect-01, Username = cisco, IP = 172.16.0.0, Session d
```

> **Nota**: in alternativa, è possibile usare il dominio **cisco.com** in Valori per consentire FQDN come www.cisco.com e tools.cisco.com.

Nel caso in cui i percorsi non protetti non vengano visualizzati nella scheda Dettagli percorso

Il client AnyConnect apprende e aggiunge automaticamente l'indirizzo IP e il nome FQDN nella scheda Dettagli route, quando il client avvia il traffico per le destinazioni escluse.

Per verificare che gli utenti AnyConnect siano assegnati ai criteri di gruppo Anyconnect corretti, è possibile eseguire il comando '**show vpn-sessiondb anyconnect filter name**
'

<#root>

```
ASAv10# show vpn-sessiondb anyconnect filter name cisco

Session Type: AnyConnect

Username     : cisco                  Index : 7
Assigned IP  : 172.16.0.0          Public IP : 10.0.0.0
Protocol     : AnyConnect-Parent SSL-Tunnel DTLS-Tunnel
License      : AnyConnect Premium
Encryption   : AnyConnect-Parent: (1)none SSL-Tunnel: (1)AES-GCM-256 DTLS-Tunnel: (1)AES-GCM-256
Hashing      : AnyConnect-Parent: (1)none SSL-Tunnel: (1)SHA384 DTLS-Tunnel: (1)SHA384
Bytes Tx     : 7795373                Bytes Rx : 390956
```

Group Policy : GroupPolicy_AnyConnect-01

```
Tunnel Group : AnyConnect-01
Login Time   : 13:20:48 UTC Tue Mar 31 2020
Duration     : 20h:19m:47s
Inactivity   : 0h:00m:00s
VLAN Mapping : N/A                    VLAN : none
Audt Sess ID : 019600a9000070005e8343b0
Security Grp : none
```

Risoluzione dei problemi generali

È possibile usare lo strumento di diagnostica e segnalazione di AnyConnect (DART) per raccogliere i dati utili per risolvere i problemi di installazione e connessione di AnyConnect. La procedura guidata DART viene utilizzata sul computer su cui è in esecuzione AnyConnect. DART raggruppa i registri, lo stato e le informazioni di diagnostica per l'analisi di Cisco Technical Assistance Center (TAC) e non richiede privilegi di amministratore per l'esecuzione sul computer client.

Informazioni correlate

- **Guida dell'amministratore di Cisco AnyConnect Secure Mobility Client, versione 4.7 - Informazioni sul tunneling con split dinamico**
- **ASDM Book 3: Cisco ASA Series VPN ASDM Configuration Guide, 7.13 - Configure Dynamic Split Tunneling**

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).