Rilevamento e risoluzione dei problemi di AnyConnect Captive Portal

Sommario

Introduzione

Questo documento descrive la funzionalità di rilevamento di un portale captive di Cisco AnyConnect Mobility Client e i requisiti per il suo corretto funzionamento. Molti hotspot wireless in hotel, ristoranti, aeroporti e altri luoghi pubblici utilizzano portali vincolati per bloccare l'accesso degli utenti a Internet. Reindirizzano le richieste HTTP ai propri siti Web che richiedono agli utenti di immettere le proprie credenziali o di confermare i termini e le condizioni dell'host hotspot.

Prerequisiti

Requisiti

Cisco raccomanda la conoscenza di Cisco AnyConnect Secure Mobility Client.

Componenti usati

Le informazioni di questo documento si basano sulle seguenti versioni software:

- AnyConnect versione 3.1.04072
- Cisco Adaptive Security Appliance (ASA) versione 9.1.2

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

Molte strutture che offrono la connessione Wi-Fi e l'accesso cablato, come aeroporti, Internet café e hotel, richiedono agli utenti di pagare prima di ottenere l'accesso, accettano di attenersi a una politica di utilizzo accettabile, o entrambe. Queste strutture utilizzano una tecnica denominata portale captive per impedire la connessione delle applicazioni finché gli utenti non aprono un browser e accettano le condizioni di accesso.

Requisiti per la risoluzione del portale vincolato

Il supporto per il rilevamento e il monitoraggio e l'aggiornamento dei portali vincolati richiede una delle seguenti licenze:

- AnyConnect Premium (SSL (Secure Sockets Layer) VPN Edition)
- Cisco AnyConnect Secure Mobility

Èpossibile usare una licenza Cisco AnyConnect Secure Mobility per fornire supporto per il rilevamento e il ripristino di portali vincolati in combinazione con una licenza AnyConnect Essentials o AnyConnect Premium.

> **Nota**: il rilevamento e l'aggiornamento dei portali vincolati sono supportati dai sistemi operativi Microsoft Windows e Macintosh OS X supportati dalla versione di AnyConnect in uso.

Rilevamento hotspot portale vincolato

AnyConnect visualizza il messaggio **Unable to contact VPN server (Impossibile contattare il server VPN)** sull'interfaccia utente se non è possibile connettersi, indipendentemente dalla causa. Il server VPN specifica il gateway sicuro. Se Always-on è abilitato e non è presente un portale vincolato, il client continua a tentare di connettersi alla VPN e aggiorna di conseguenza il messaggio di stato.

Se la VPN sempre attiva è abilitata, il criterio dell'errore di connessione è chiuso, il monitoraggio e aggiornamento del portale captive è disabilitato e AnyConnect rileva la presenza di un portale captive, l'interfaccia utente di AnyConnect visualizza questo messaggio una volta per ciascuna connessione e una volta per ciascuna riconnessione:

```
The service provider in your current location is restricting access to the Internet.
The AnyConnect protection settings must be lowered for you to log on with the service
provider. Your current enterprise security policy does not allow this.
```

Se AnyConnect rileva la presenza di un portale captive e la configurazione di AnyConnect è diversa da quella descritta precedentemente, l'interfaccia utente di AnyConnect visualizza questo messaggio una volta per ciascuna connessione e una volta per ciascuna riconnessione:

```
The service provider in your current location is restricting access to the Internet.
You need to log on with the service provider before you can establish a VPN session.
You can try this by visiting any website with your browser.
```

> **Attenzione:** Il rilevamento del portale vincolato è abilitato per impostazione predefinita e non è configurabile. AnyConnect non modifica alcuna impostazione di configurazione del

browser durante il rilevamento del portale vincolato.

Correzione hotspot Captive Portal

La risoluzione dei problemi del portale vincolato è il processo in cui si soddisfano i requisiti di un hotspot del portale vincolato per ottenere l'accesso alla rete.

AnyConnect non corregge il portale vincolato; per l'esecuzione della correzione, l'utente finale deve affidarsi a.

Per eseguire la correzione del portale vincolato, l'utente finale soddisfa i requisiti del provider di hotspot. Questi requisiti possono includere il pagamento di una tariffa di accesso alla rete, una firma su una politica di utilizzo accettabile, entrambi, o altri requisiti definiti dal provider.

Se AnyConnect Always-on è abilitato e il criterio di errore della connessione è impostato su Closed, la risoluzione dei problemi del portale vincolato deve essere consentita esplicitamente in un profilo del client VPN AnyConnect. Se l'opzione Always-on è abilitata e il criterio Connessione non riuscita è impostato su Open, non è necessario consentire esplicitamente il monitoraggio e l'aggiornamento dei portali in un profilo AnyConnect VPN Client perché all'utente non è limitato l'accesso alla rete.

Rilevamento Portale Captive Falso

AnyConnect può presupporre erroneamente che si trovi in un portale riservato in queste situazioni.

- Se AnyConnect tenta di contattare un'ASA con un certificato contenente un nome di server (CN) non corretto, il client AnyConnect troverà tale certificato in un ambiente di portale vincolato.

  Per evitare questo problema, verificare che il certificato ASA sia configurato correttamente. Il valore CN nel certificato deve corrispondere al nome del server ASA nel profilo del client VPN.

- Se prima dell'appliance ASA vi è un altro dispositivo in rete che risponde al tentativo del client di contattare un'ASA bloccando l'accesso HTTPS all'ASA, il client AnyConnect interpreterà il dispositivo come un ambiente portale vincolato. Questa situazione può verificarsi quando un utente si trova su una rete interna e si connette tramite un firewall per connettersi all'appliance ASA.

  Se è necessario limitare l'accesso all'appliance ASA dall'interno dell'azienda, configurare il firewall in modo che il traffico HTTP e HTTPS verso l'indirizzo dell'appliance ASA non restituisca uno stato HTTP. L'accesso HTTP/HTTPS all'appliance ASA deve essere consentito o completamente bloccato (noto anche come black-holed) per evitare che le richieste HTTP/HTTPS inviate all'appliance ASA restituiscano una risposta imprevista.

Comportamento di AnyConnect

In questa sezione viene descritto il comportamento di AnyConnect.

1. AnyConnect prova una sonda HTTPS per il nome di dominio completo (FQDN) definito nel profilo XML.

2. Se si verifica un errore di certificato (FQDN non attendibile/errato), AnyConnect tenta di eseguire una sonda HTTP all'FQDN definito nel profilo XML. Se esiste una risposta diversa da HTTP 302, si considera dietro un portale vincolato.

Portale vincolato rilevato in modo non corretto con IKEV2

Quando si tenta di stabilire una connessione Internet Key Exchange versione 2 (IKEv2) a un'ASA con l'autenticazione SSL disabilitata e che esegue il portale ASDM (Adaptive Security Device Manager) sulla porta 443, la sonda HTTPS eseguita per il rilevamento dei portali vincolati determina il reindirizzamento al portale ASDM (**/admin/public/index.html**). Poiché questo comportamento non è previsto dal client, sembra un reindirizzamento del portale vincolato e il tentativo di connessione viene impedito in quanto sembra sia necessaria la risoluzione del portale vincolato.

Soluzioni

Se si verifica questo problema, di seguito sono elencate alcune soluzioni:

- Rimuovere i comandi HTTP dall'interfaccia in modo che l'ASA non sia in grado di ascoltare le connessioni HTTP sull'interfaccia.

- Rimuovere il trust point SSL sull'interfaccia.

- Abilitare i servizi client IKEV2.

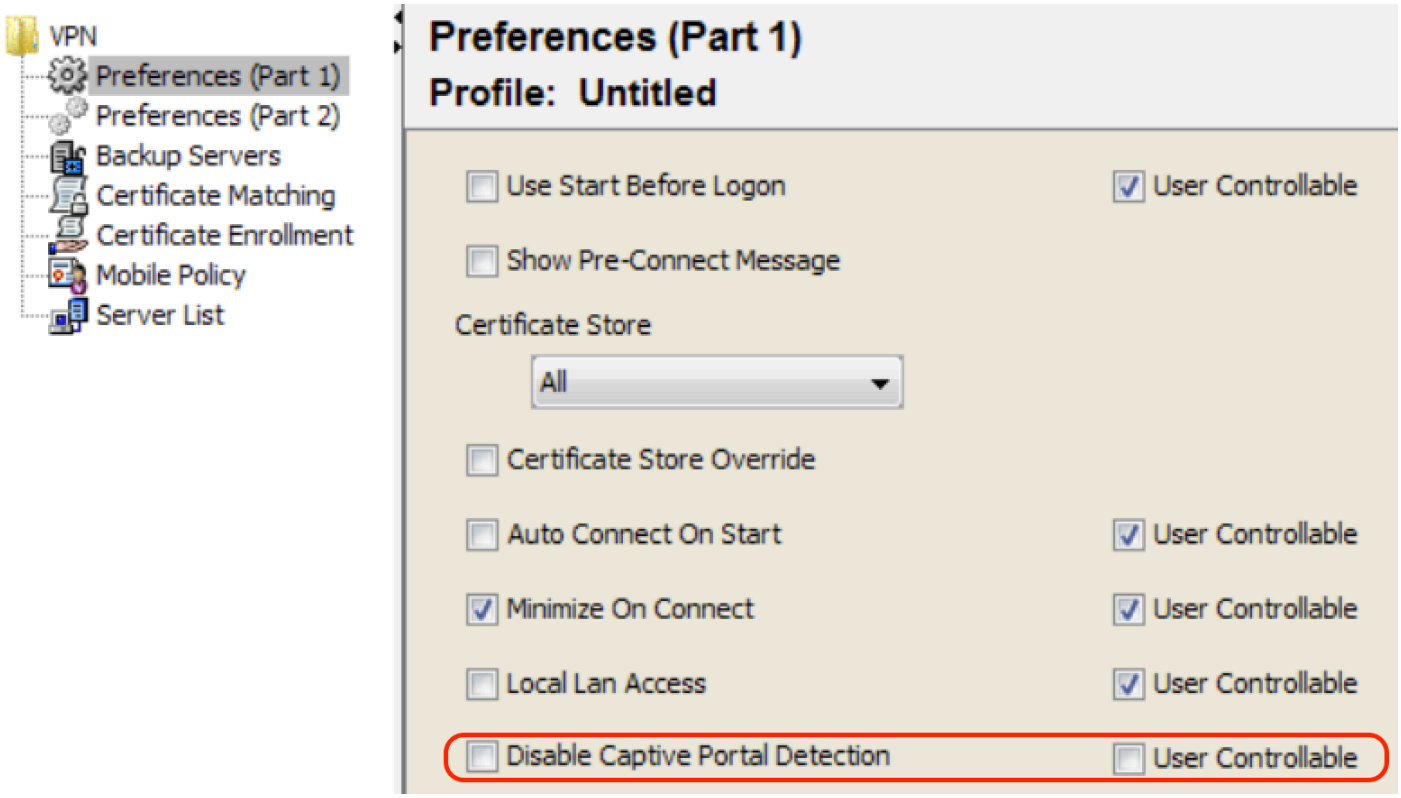
- Abilitare WebVPN sull'interfaccia.

Il problema è stato risolto dall'ID bug Cisco CSCud17825 nella versione 3.1(3103).

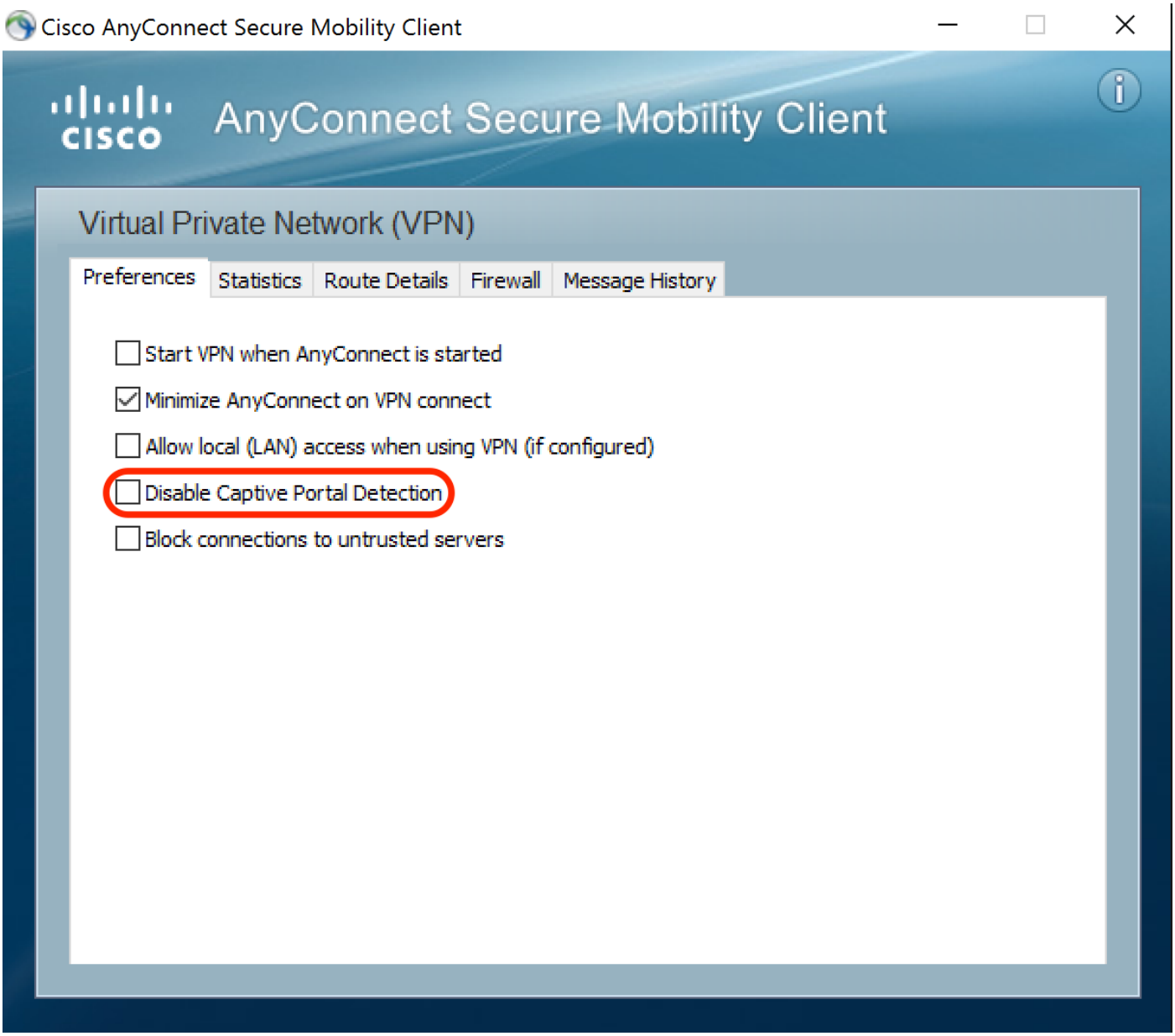
> **Attenzione:** Lo stesso problema si verifica per i router Cisco IOS®. Se il **server http ip** è abilitato su Cisco IOS, condizione necessaria se si utilizza la stessa casella del server PKI, AnyConnect rileva erroneamente il portale vincolato. Per risolvere il problema, usare **ip http access-class** per interrompere le risposte alle richieste HTTP AnyConnect, anziché richiedere l'autenticazione.

Disattiva la funzionalità Portale vincolato

Èpossibile disabilitare la funzione Captive Portal nel client AnyConnect versione 4.2.00096 e successive (vedere l'ID bug Cisco CSCud97386). L'amministratore può determinare se l'opzione deve essere configurabile dall'utente o disabilitata. Questa opzione è disponibile nella sezione Preferenze (Parte 1) dell'editor dei profili. L'amministratore può scegliere **Disabilita rilevamento portale vincolato** o **Controllabile dall'utente**, come mostrato nello snapshot dell'editor di profili:



Se è selezionata l'opzione Controllabile dall'utente, la casella di controllo viene visualizzata nella scheda Preferenze dell'interfaccia utente di AnyConnect Secure Mobility Client, come mostrato di seguito:


Cisco AnyConnect Secure Mobility Client
AnyConnect Secure Mobility Client
Virtual Private Network (VPN)
Preferences
Statistics
Route Details
Firewall
Message History
Start VPN when AnyConnect is started
Minimize AnyConnect on VPN connect
Allow local (LAN) access when using VPN (if configured)
Disable Captive Portal Detection
Block connections to untrusted servers