AnyConnect Captive Portal Detectie en verbetering

Inhoud

Inleiding

Dit document beschrijft de Cisco AnyConnect Mobility Client-detectiefunctie en de vereisten voor een correct functioneren. Veel draadloze hotspots op hotels, restaurants, luchthavens en andere openbare plekken gebruiken portals om de toegang van gebruikers tot internet te blokkeren. Ze sturen HTTP-aanvragen door naar hun eigen websites die van gebruikers vereisen dat ze hun aanmeldingsgegevens invoeren of de voorwaarden van de hotspot-host erkennen.

Voorwaarden

Vereisten

Cisco raadt u aan kennis te hebben van de Cisco AnyConnect Secure Mobility Client.

Gebruikte componenten

De informatie in dit document is gebaseerd op deze softwareversies:

- AnyConnect versie 3.1.040/72
- Cisco adaptieve security applicatie (ASA) versie 9.1.2

De informatie in dit document is gebaseerd op de apparaten in een specifieke laboratoriumomgeving. Alle apparaten die in dit document worden beschreven, hadden een opgeschoonde (standaard)configuratie. Als uw netwerk live is, moet u de potentiële impact van elke opdracht begrijpen.

Achtergrondinformatie

Veel faciliteiten die Wi-Fi en bekabelde toegang bieden, zoals luchthavens, koffiehuizen en hotels, eisen dat gebruikers betalen voordat ze toegang krijgen, stemmen ermee in een acceptabel gebruiksbeleid te volgen, of allebei. Deze faciliteiten maken gebruik van een techniek die een in gevangenschap genoemd portaal wordt genoemd om te voorkomen dat toepassingen zich aansluiten tot gebruikers een browser openen en de voorwaarden voor toegang accepteren.

Vereisten voor reparatie van interne portal

Voor ondersteuning van zowel detectie als herstel van een gevangen portal is een van deze licenties vereist:

- AnyConnect Premium (Secure Socket Layer (SSL) VPN-Edition)
- Cisco AnyConnect beveiligde mobiliteit

U kunt een Cisco AnyConnect Secure Mobility-licentie gebruiken om ondersteuning te bieden voor detectie en herstel van een portal in combinatie met een AnyConnect-essentiële of een AnyConnect Premium-licentie.

> **Opmerking**: De detectie en herstel van een portal wordt ondersteund op de besturingssysteem van Microsoft Windows en Macintosh OS X en wordt ondersteund door de release van AnyConnect die in gebruik is.

Detectie van hotspotsites

AnyConnect geeft het bericht **Kan geen VPN-server** op de GUI **benaderen** als het niet kan worden aangesloten, ongeacht de oorzaak. De VPN-server specificeert de beveiligde gateway. Als Always-on is ingeschakeld en er geen sprake is van een portal, blijft de client proberen verbinding te maken met VPN en wordt het statusbericht dienovereenkomstig bijgewerkt.

Als het altijd-on VPN ingeschakeld is, wordt het beleid voor aansluitingsfouten gesloten, wordt het beheer van een portal uitgeschakeld en wordt AnyConnect de aanwezigheid van een portal gedetecteerd, dan geeft de AnyConnect GUI dit bericht één keer per verbinding weer en één keer per opnieuw verbinding:

```
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.
```

Als AnyConnect de aanwezigheid van een portal detecteert en de AnyConnect-configuratie afwijkt van de eerder beschreven configuratie, dan geeft de AnyConnect GUI dit bericht één keer per verbinding en één keer per opnieuw aan:

```
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.
```

> **Voorzichtig:** De detectie van een portal is standaard ingeschakeld en is niet-configureerbaar. AnyConnect wijzigt geen instellingen voor het configureren van een browser tijdens de detectie van een portal.

POPULAIRE HULPVERANDERING

Het repareren van een portal is het proces waarbij u voldoet aan de vereisten van een hotspot die een portal ondersteunt, om toegang tot het netwerk te krijgen.

AnyConnect verbetert het gevangen portaal niet; het is afhankelijk van de eindgebruiker om het herstel uit te voeren.

De eindgebruiker voldoet aan de eisen van de hotspot-provider om het in gevangenschap opgenomen portaal te saneren. Deze vereisten kunnen onder meer bestaan uit betaling van een vergoeding voor toegang tot het net, ondertekening van een aanvaardbaar gebruiksbeleid, zowel als een andere door de aanbieder vastgestelde eis.

Het aanpassen van de portal moet expliciet worden toegestaan in een AnyConnect VPN-clientprofiel als AnyConnect Always-on is ingeschakeld en het beleid voor Connect-falen is ingesteld op Closed. Als Always-on is ingeschakeld en het beleid voor Connect-fouten is ingesteld op Open, hoeft u geen poortsanering in een AnyConnect VPN-clientprofiel expliciet toe te staan omdat de gebruiker niet beperkt is door netwerktoegang.

Detectie van storingsportal

AnyConnect kan in deze situaties vals veronderstellen dat hij zich in een portal bevindt.

- Als AnyConnect probeert contact op te nemen met een ASA met een certificaat dat een onjuiste servernaam (GN) bevat, dan denkt de AnyConnect-client dat dit zich in een portal-omgeving bevindt.

  Zorg ervoor dat het ASA-certificaat correct is geconfigureerd om dit probleem te voorkomen. De GN-waarde in het certificaat moet overeenkomen met de naam van de ASA-server in het VPN-clientprofiel.

- Als er een ander apparaat op het netwerk staat voor de ASA dat reageert op de poging van de klant om contact op te nemen met een ASA door HTTPS-toegang tot de ASA te blokkeren, dan denkt de AnyConnect-client dat het in een gevangen portal-omgeving is. Deze situatie kan voorkomen wanneer een gebruiker op een intern netwerk is en door een firewall verbindt om met de ASA te verbinden.

  Als u de toegang tot ASA van binnen het bedrijf moet beperken, moet u uw firewall zo configureren dat HTTP en HTTPS-verkeer naar het ASA-adres geen HTTP-status teruggeeft. HTTP/HTTPS-toegang tot de ASA moet hetzij worden toegestaan of volledig geblokkeerd (ook bekend als "zwart-heilig") om ervoor te zorgen dat HTTP/HTTPS-verzoeken die naar de ASA worden gestuurd geen onverwachte respons teruggeven.

AnyConnect-gedrag

In dit gedeelte wordt beschreven hoe de AnyConnect zich gedraagt.

1. AnyConnect probeert een HTTPS-toets naar de Fully Qualified Domain Name (FQDN), die in

het XML-profiel is gedefinieerd.

2. Als er een certificaatfout is (niet vertrouwd/fout FQDN), dan probeert AnyConnect een HTTP-sonde naar de FQDN die in het XML-profiel is gedefinieerd. Als er een andere reactie is dan een HTTP 302, dan acht het zichzelf achter een portaal dat in gevangenschap ligt.

Portal niet goed herkend met IKEV2

Wanneer u een verbinding van Internet Key Exchange Versie 2 (IKEv2) naar een ASA met SSL-verificatie probeert die de Adaptieve Security Devices Manager (ASDM)-poort op poort 443 exploiteert, wordt de HTTPS-test uitgevoerd voor de detectie van een portal in een redirect naar het ASDM-portaal (**/admin/public/index.html**). Aangezien de klant dit niet verwacht, lijkt het op een herleiding van een portal en wordt de verbindingspoging vermeden, omdat het lijkt dat het nodig is om een portaal te repareren.

zorgwekkende

Als u dit probleem tegenkomt, zijn hier een aantal werkronden:

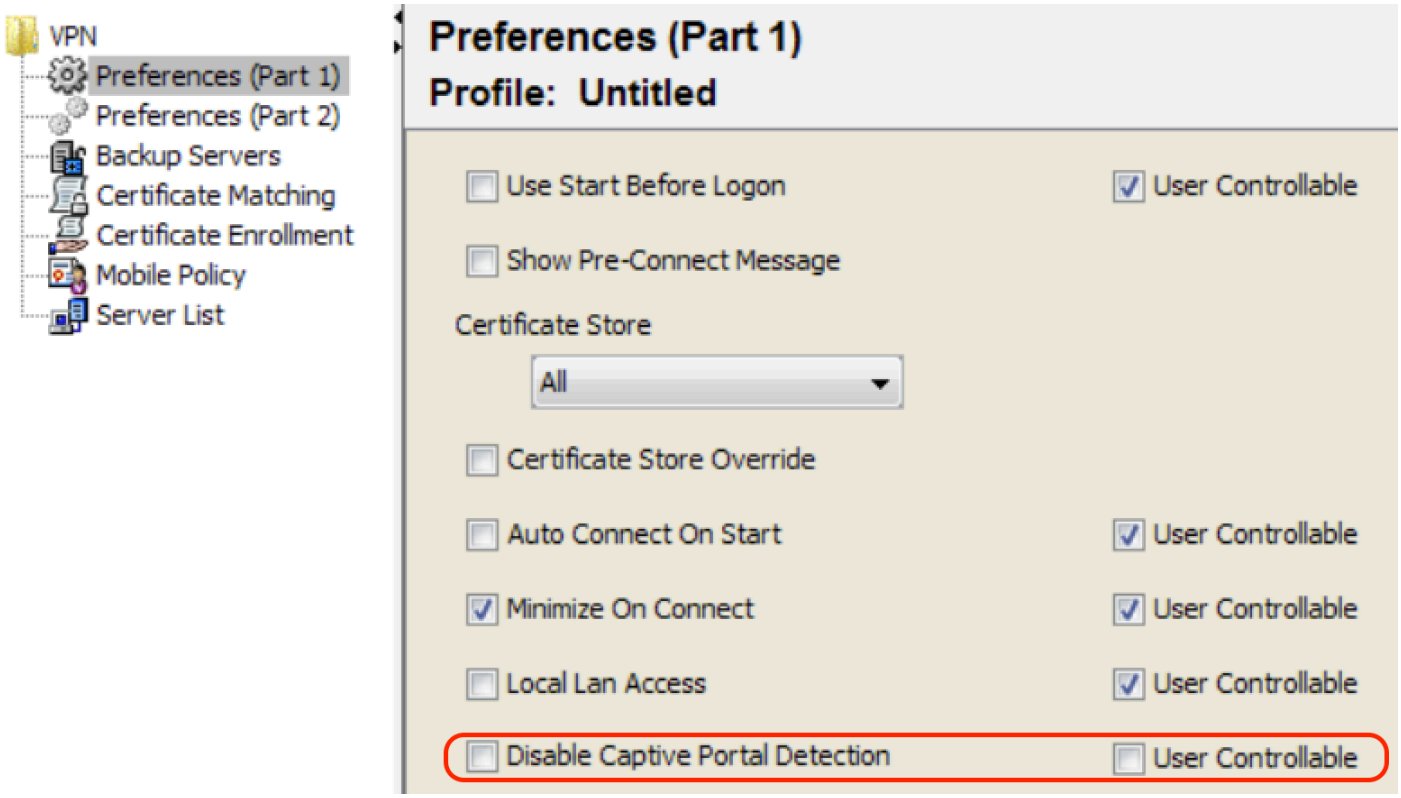
- Verwijder HTTP-opdrachten op die interface zodat de ASA niet naar HTTP-verbindingen op de interface zal luisteren.
- Verwijder het SSL-trustpunt op de interface.
- IKEV2-clientservices inschakelen.
- Schakel WebVPN in op de interface.

Dit probleem wordt opgelost door Cisco bug-ID CSCud17825 in versie 3.1(3103).

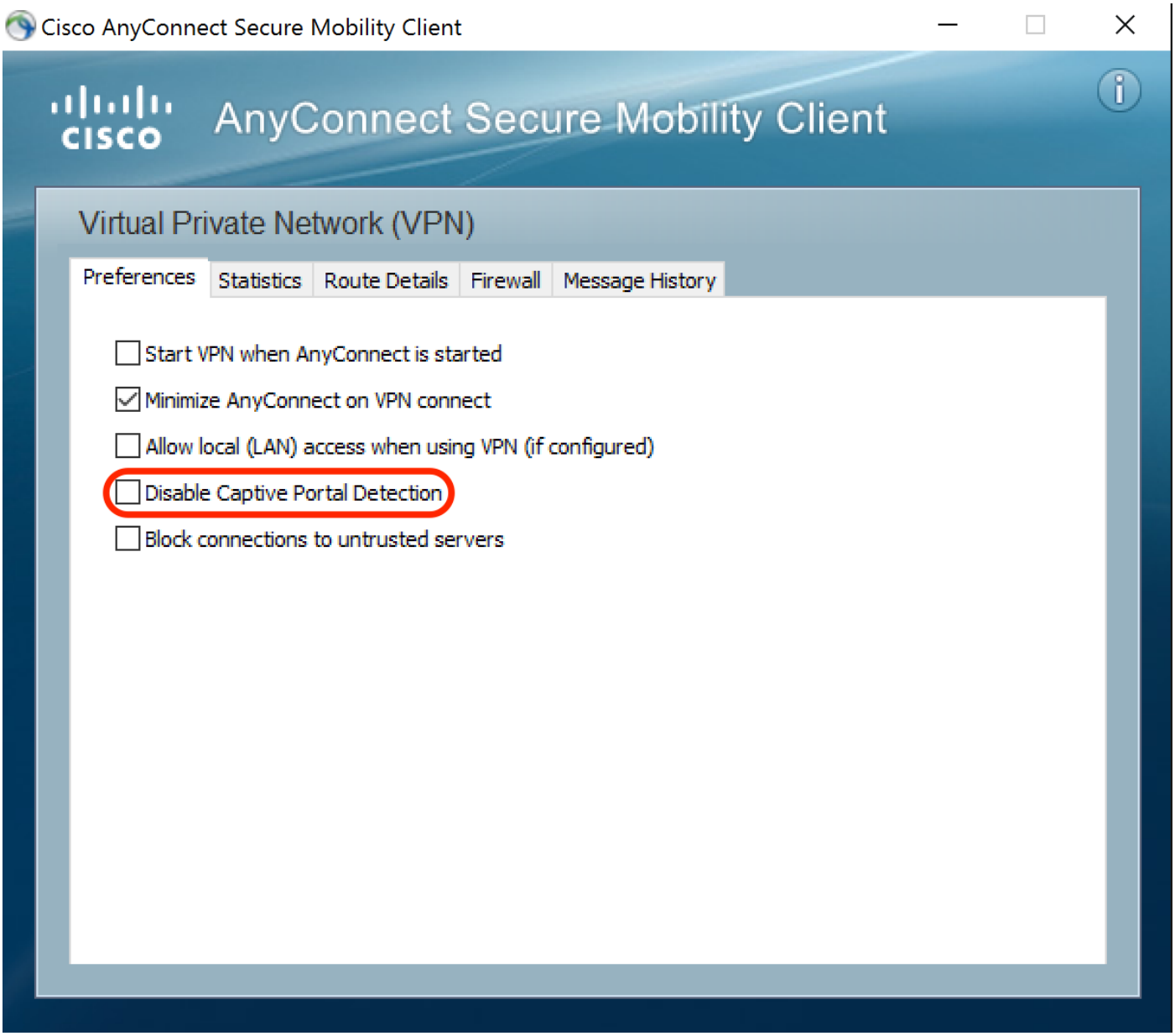
> **Voorzichtig:** Het zelfde probleem bestaat voor Cisco IOS® routers. Als **ip http server** is ingeschakeld op Cisco IOS, wat vereist is als hetzelfde vak wordt gebruikt als de PKI Server, detecteert AnyConnect vals een portal. De tijdelijke oplossing is om **ip http access-class** te gebruiken om reacties op AnyConnect HTTP-verzoeken te stoppen in plaats van om verificatie te vragen.

De functie Captive Portal uitschakelen

Het is mogelijk de optie voor het portal uit te schakelen in AnyConnect-clientversie 4.2.0096 en later (zie Cisco bug-ID CSCud97386). De beheerder kan bepalen of de optie configureerbaar of uitgeschakeld is. Deze optie is beschikbaar onder het gedeelte Voorkeuren (Deel 1) in de profieleditor. De beheerder kan kiezen **om Captive Portal Detectie** of **User Controllable** uit te schakelen zoals in deze snapshot van de profieleditor wordt getoond:



Als door de gebruiker kan worden bediend, verschijnt het selectieteken op het tabblad Voorkeuren van de AnyConnect Secure Mobility Client UI zoals hier wordt getoond:


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