Interop zwischen AnyConnect und dem OpenDNS Roaming Client

Inhalt

Einführung
Voraussetzungen
Anforderungen
Verwendete Komponenten
Hintergrundinformationen
Funktionalität
AnyConnect DNS-Verarbeitung
Windows 7+
Split-Include-Konfiguration (Tunnel-all DNS deaktiviert und kein Split-DNS)
Konfiguration nach Untergliederung (Tunnel-all DNS deaktiviert und kein Split-DNS)
Split-DNS (Tunnel-all DNS deaktiviert, Split-Include konfiguriert)
Mac OS X
Konfiguration des gesamten Tunnels (und Split-Tunneling mit aktiviertem Tunnel-All-DNS)
Split-Include-Konfiguration (Tunnel-all DNS deaktiviert und kein Split-DNS)
Konfiguration nach Untergliederung (Tunnel-all DNS deaktiviert und kein Split-DNS)
Split-DNS (Tunnel-all DNS deaktiviert, Split-Include konfiguriert)
Linux
Konfiguration des gesamten Tunnels (und Split-Tunneling mit aktiviertem Tunnel-All-DNS)
Split-Include-Konfiguration (Tunnel-all DNS deaktiviert und kein Split-DNS)
Konfiguration nach Untergliederung (Tunnel-all DNS deaktiviert und kein Split-DNS)
Split-DNS (Tunnel-all DNS deaktiviert, Split-Include konfiguriert)
OpenDNS Roaming-Client
Einschränkungen
Problemumgehung
Konfigurationen
Tunnel-OpenDNS-Datenverkehr
OpenDNS-Datenverkehr vom VPN-Tunnel ausschließen
Überprüfen

Einführung

In diesem Dokument werden einige der aktuellen Einschränkungen und die verfügbaren Problemumgehungen beschrieben, die die Zusammenarbeit von AnyConnect und dem OpenDNS-Roaming-Client ermöglichen. Cisco Kunden verlassen sich bei der sicheren und verschlüsselten Kommunikation mit ihren Unternehmensnetzwerken auf den AnyConnect VPN-Client. Der OpenDNS-Roaming-Client ermöglicht Benutzern die sichere Nutzung von DNS-Diensten mithilfe von öffentlichen OpenDNS-Servern. Beide Clients fügen eine Vielzahl von Sicherheitsfunktionen auf dem Endgerät hinzu. Daher ist es wichtig, dass diese miteinander interagieren.

Voraussetzungen

Praktische Erfahrung mit dem AnyConnect- und OpenDNS-Roaming-Client.

Vertrautheit mit der ASA- oder IOS/IOS-XE-Headend-Konfiguration (Tunnelgruppe/Gruppenrichtlinie) für AnyConnect VPN.

Anforderungen

Cisco empfiehlt, über Kenntnisse in folgenden Bereichen zu verfügen:

- ASA- oder IOS/IOS-XE-Headend
- Endpunkt, auf dem der AnyConnect VPN-Client und der OpenDNS-Roaming-Client ausgeführt werden

Verwendete Komponenten

Die Informationen in diesem Dokument basieren auf den folgenden Software- und Hardwareversionen:

- ASA Headend aktuelle Version 9.4
- Windows 7
- AnyConnect-Client 4.2.00096
- OpenDNS Roaming-Client 2.0.154

Die Informationen in diesem Dokument wurden von den Geräten in einer bestimmten Laborumgebung erstellt. Alle in diesem Dokument verwendeten Geräte haben mit einer leeren (Standard-)Konfiguration begonnen. Wenn Ihr Netzwerk in Betrieb ist, stellen Sie sicher, dass Sie die potenziellen Auswirkungen eines Befehls verstehen.

Hintergrundinformationen

OpenDNS entwickelt derzeit ein AnyConnect-Plugin für das Cisco AnyConnect-Team, das in Zukunft verfügbar sein wird. Zwar wurden keine Daten festgelegt, diese Integration ermöglicht es dem Roaming-Client jedoch, mit dem AnyConnect-Client zusammenzuarbeiten, ohne dass die Problemumgehungen bearbeitet werden müssen. Dadurch kann AnyConnect auch als Bereitstellungsmechanismus für den Roaming-Client fungieren.

Funktionalität

AnyConnect DNS-Verarbeitung

Das VPN-Headend kann auf verschiedene Weise konfiguriert werden, um den Datenverkehr vom AnyConnect-Client zu verarbeiten.

1. Vollständige Tunnelkonfiguration (Tunnel-all): Dadurch wird der gesamte Datenverkehr vom Endpunkt verschlüsselt über den VPN-Tunnel gesendet, sodass der Datenverkehr den

Adapter für die öffentliche Schnittstelle nie im Klartext verlässt.

2. Tunnelkonfiguration aufteilen:

   a) Split-Include-Tunneling: Datenverkehr, der nur an bestimmte Subnetze oder Hosts gerichtet ist, die am VPN-Headend definiert sind, wird über den Tunnel gesendet, der restliche Datenverkehr wird im Klartext außerhalb des Tunnels gesendet.

   b) Split-exclude-Tunneling: Datenverkehr, der nur an bestimmte Subnetze oder Hosts gerichtet ist, die am VPN-Headend definiert sind, wird von der Verschlüsselung ausgeschlossen und lässt die öffentliche Schnittstelle in Klartext, der gesamte andere Datenverkehr wird verschlüsselt und nur über den Tunnel gesendet

Jede dieser Konfigurationen legt fest, wie die DNS-Auflösung vom AnyConnect-Client in Abhängigkeit vom Betriebssystem des Endgeräts behandelt wird. In Version 4.2 nach dem Fix für CSCuf07885 wurde das Verhalten des DNS-Verarbeitungsmechanismus auf AnyConnect für Windows geändert.

Windows 7+

Konfiguration des gesamten Tunnels (und Split-Tunneling mit aktiviertem Tunnel-All-DNS)

Pre-AnyConnect 4.2:

Nur DNS-Anfragen an DNS-Server, die unter der Gruppenrichtlinie konfiguriert wurden (Tunnel-DNS-Server), sind zulässig. Der AnyConnect-Treiber antwortet auf alle anderen Anfragen mit der Antwort "Kein solcher Name". Daher kann die DNS-Auflösung nur mithilfe der Tunnel-DNS-Server erfolgen.

AnyConnect 4.2 +

DNS-Anfragen an DNS-Server sind zulässig, sofern sie vom VPN-Adapter stammen und über den Tunnel gesendet werden. Alle anderen Anfragen werden mit "no such name"-Antwort beantwortet, und die DNS-Auflösung kann nur über den VPN-Tunnel erfolgen.

Vor dem CSCuf07885-Fix schränkt AC die Ziel-DNS-Server ein. Mit dem Fix für CSCuf07885 schränkt es jedoch ein, welche Netzwerkadapter DNS-Anfragen initiieren können.

Split-Include-Konfiguration (Tunnel-all DNS deaktiviert und kein Split-DNS)

Der AnyConnect-Treiber stört den nativen DNS-Resolver nicht. Daher wird die DNS-Auflösung basierend auf der Reihenfolge der Netzwerkadapter vorgenommen, und AnyConnect ist immer der bevorzugte Adapter, wenn VPN verbunden wird. So wird zunächst eine DNS-Abfrage über den Tunnel gesendet, und wenn sie nicht aufgelöst wird, versucht der Resolver, sie über die öffentliche Schnittstelle aufzulösen. Die Split-Include-Zugriffsliste muss das Subnetz für die Tunnel-DNS-Server enthalten. Ab AnyConnect 4.2 werden Host-Routen für die Tunnel-DNS-Server vom AnyConnect-Client automatisch als Split-Include-Netzwerke (sichere Routen) hinzugefügt, sodass die Split-Include-Zugriffsliste keine explizite Hinzufügung des Tunnel-DNS-

Server-Subnetzes mehr erfordert.

Konfiguration nach Untergliederung (Tunnel-all DNS deaktiviert und kein Split-DNS)

Der AnyConnect-Treiber stört den nativen DNS-Resolver nicht. Daher wird die DNS-Auflösung basierend auf der Reihenfolge der Netzwerkadapter vorgenommen, und AnyConnect ist immer der bevorzugte Adapter, wenn VPN verbunden wird. So wird zunächst eine DNS-Abfrage über den Tunnel gesendet, und wenn sie nicht aufgelöst wird, versucht der Resolver, sie über die öffentliche Schnittstelle aufzulösen. Die Zugriffsliste "split-exclude" sollte nicht das Subnetz enthalten, das die Tunnel-DNS-Server(s) abdeckt. Ab AnyConnect 4.2 werden Host-Routen für die Tunnel-DNS-Server vom AnyConnect-Client automatisch als Split-Include-Netzwerke (sichere Routen) hinzugefügt, um Fehlkonfigurationen in der Split-Exclusion-Zugriffsliste zu vermeiden.

Split-DNS (Tunnel-all DNS deaktiviert, Split-Include konfiguriert)

Pre-AnyConnect 4.2

DNS-Anfragen, die mit den Split-DNS-Domänen übereinstimmen, dürfen DNS-Server tunneln, sind jedoch nicht für andere DNS-Server zulässig. Um zu verhindern, dass solche internen DNS-Abfragen den Tunnel verlassen, antwortet der AnyConnect-Treiber mit 'no such name', wenn die Abfrage an andere DNS-Server gesendet wird. Split-DNS-Domänen können also nur über die Tunnel-DNS-Server aufgelöst werden.

DNS-Anfragen, die nicht mit den Split-DNS-Domänen übereinstimmen, sind an andere DNS-Server zulässig, jedoch nicht zum Tunnel von DNS-Servern zulässig. Selbst in diesem Fall antwortet der AnyConnect-Treiber mit "no such name" (Kein solcher Name), wenn eine Abfrage für Nicht-Split-DNS-Domänen über den Tunnel versucht wird. Nicht-Split-DNS-Domänen können daher nur über öffentliche DNS-Server außerhalb des Tunnels aufgelöst werden.

AnyConnect 4.2 +

DNS-Anfragen, die den Split-DNS-Domänen entsprechen, sind für alle DNS-Server zulässig, sofern sie vom VPN-Adapter stammen. Wenn die Abfrage von der öffentlichen Schnittstelle generiert wird, antwortet der AnyConnect-Treiber mit einem 'no solch name', um den Resolver zu zwingen, den Tunnel immer für die Namensauflösung zu verwenden. So können Split-DNS-Domänen nur über den Tunnel aufgelöst werden.

DNS-Anfragen, die nicht mit den Split-DNS-Domänen übereinstimmen, sind für alle DNS-Server zulässig, solange sie vom physischen Adapter stammen. Wenn die Abfrage vom VPN-Adapter generiert wird, antwortet AnyConnect mit "no such name" (Kein solcher Name), um den Resolver zu zwingen, stets eine Namensauflösung über die öffentliche Schnittstelle zu versuchen. Nicht-Split-DNS-Domänen können also nur über die öffentliche Schnittstelle aufgelöst werden.

Mac OS X

Konfiguration des gesamten Tunnels (und Split-Tunneling mit aktiviertem Tunnel-All-DNS)

Wenn AnyConnect verbunden ist, werden in der DNS-Konfiguration des Systems nur DNS-Tunnel-Server verwaltet, sodass DNS-Anfragen nur an den/die Tunnel-DNS-Server(s) gesendet werden können.

Split-Include-Konfiguration (Tunnel-all DNS deaktiviert und kein Split-DNS)

AnyConnect stört den nativen DNS-Resolver nicht. Die Tunnel-DNS-Server werden als bevorzugte Resolver konfiguriert, wobei die Priorität gegenüber öffentlichen DNS-Servern liegt. Dadurch wird sichergestellt, dass die erste DNS-Anforderung für eine Namensauflösung über den Tunnel gesendet wird. Da die DNS-Einstellungen unter Mac OS X global sind, ist es nicht möglich, dass DNS-Abfragen öffentliche DNS-Server außerhalb des Tunnels verwenden, wie in CSCtf20226 dokumentiert. Ab AnyConnect 4.2 werden Host-Routen für die Tunnel-DNS-Server vom AnyConnect-Client automatisch als Split-Include-Netzwerke (sichere Routen) hinzugefügt, sodass die Split-Include-Zugriffsliste keine explizite Hinzufügung des Tunnel-DNS-Server-Subnetzes mehr erfordert.

Konfiguration nach Untergliederung (Tunnel-all DNS deaktiviert und kein Split-DNS)

AnyConnect stört den nativen DNS-Resolver nicht. Die Tunnel-DNS-Server werden als bevorzugte Resolver konfiguriert, wobei die Priorität gegenüber öffentlichen DNS-Servern liegt. Dadurch wird sichergestellt, dass die erste DNS-Anforderung für eine Namensauflösung über den Tunnel gesendet wird. Da die DNS-Einstellungen unter Mac OS X global sind, ist es nicht möglich, dass DNS-Abfragen öffentliche DNS-Server außerhalb des Tunnels verwenden, wie in CSCtf20226 dokumentiert. Ab AnyConnect 4.2 werden Host-Routen für die Tunnel-DNS-Server vom AnyConnect-Client automatisch als Split-Include-Netzwerke (sichere Routen) hinzugefügt, sodass die Split-Include-Zugriffsliste keine explizite Hinzufügung des Tunnel-DNS-Server-Subnetzes mehr erfordert.

Split-DNS (Tunnel-all DNS deaktiviert, Split-Include konfiguriert)

Wenn Split-DNS für beide IP-Protokolle (IPv4 und IPv6) aktiviert ist oder nur für ein Protokoll aktiviert ist und kein Adresspool für das andere Protokoll konfiguriert ist:
True Split-DNS, ähnlich Windows, wird erzwungen. True Split-DNS bedeutet, dass Anfragen, die mit den Split-DNS-Domänen übereinstimmen, nur über den Tunnel gelöst werden. Sie werden nicht an DNS-Server außerhalb des Tunnels übertragen.

Wenn Split-DNS nur für ein Protokoll aktiviert ist und dem anderen Protokoll eine Client-Adresse zugewiesen ist, wird nur "DNS Fallback for Split-Tunneling" erzwungen. Das bedeutet, dass der AC nur DNS-Anfragen zulässt, die die Split-DNS-Domänen über Tunnel abgleichen (andere Anfragen werden vom AC mit der "abgelehnten" Antwort beantwortet, um Failover auf öffentliche DNS-Server zu erzwingen), aber nicht durchsetzen kann, dass Anfragen, die Split-DNS-Domänen zuordnen, nicht über den öffentlichen Adapter in die Clear-Route gesendet werden.

Linux

Konfiguration des gesamten Tunnels (und Split-Tunneling mit aktiviertem Tunnel-All-DNS)

Wenn AnyConnect verbunden ist, werden in der DNS-Konfiguration des Systems nur DNS-Tunnel-Server verwaltet, sodass DNS-Anfragen nur an den/die Tunnel-DNS-Server(s) gesendet werden können.

Split-Include-Konfiguration (Tunnel-all DNS deaktiviert und kein Split-DNS)

AnyConnect stört den nativen DNS-Resolver nicht. Die Tunnel-DNS-Server werden als bevorzugte Resolver konfiguriert, wobei die Priorität gegenüber öffentlichen DNS-Servern liegt. Dadurch wird sichergestellt, dass die erste DNS-Anforderung für eine Namensauflösung über den Tunnel gesendet wird.

Konfiguration nach Untergliederung (Tunnel-all DNS deaktiviert und kein Split-DNS)

AnyConnect stört den nativen DNS-Resolver nicht. Die Tunnel-DNS-Server werden als bevorzugte Resolver konfiguriert, wobei die Priorität gegenüber öffentlichen DNS-Servern liegt. Dadurch wird sichergestellt, dass die erste DNS-Anforderung für eine Namensauflösung über den Tunnel gesendet wird.

Split-DNS (Tunnel-all DNS deaktiviert, Split-Include konfiguriert)

Wenn Split-DNS aktiviert ist, wird nur "DNS-Fallback für Split-Tunneling" erzwungen. Das bedeutet, dass der AC nur DNS-Anfragen zulässt, die die Split-DNS-Domänen über Tunnel abgleichen (andere Anfragen werden vom AC mit der "abgelehnten" Antwort beantwortet, um Failover auf öffentliche DNS-Server zu erzwingen), aber nicht durchsetzen kann, dass Anfragen, die Split-DNS-Domänen zuordnen, nicht über den öffentlichen Adapter in die Clear-Route gesendet werden.

OpenDNS Roaming-Client

Der Roaming-Client ist eine Software, die DNS-Dienste auf dem Endpunkt verwaltet und die öffentlichen OpenDNS-Server zur Sicherung und Verschlüsselung des DNS-Datenverkehrs verwendet.

Im Idealfall sollte sich der Client in einem geschützten und verschlüsselten Zustand befinden. Kann der Client jedoch keine TLS-Sitzung mit dem öffentlichen OpenDNS-Resolver-Server (208.67.222.222) einrichten, versucht er, auf dem UDP-Port 53 unverschlüsselten DNS-Datenverkehr an 208.67.222.222 zu senden. Der Roaming-Client verwendet ausschließlich die öffentliche Resolver-IP-Adresse 208.67.222.222 von OpenDNS (es gibt einige weitere, z. B. 208.67.220.220, 208.67.222.220 und 208.67.7.722202022222222222222222222220. 220,222). Sobald der Roaming-Client installiert ist, legt er 127.0.0.1 (localhost) als lokalen DNS-Server fest und überschreibt die aktuellen DNS-Einstellungen für die einzelnen Schnittstellen. Aktuelle DNS-Einstellungen werden in lokalen resolv.conf-Dateien (auch unter Windows) im

Roaming Client-Konfigurationsordner gespeichert. OpenDNS sichert selbst die DNS-Server, die über den AnyConnect-Adapter abgerufen werden. Wenn beispielsweise 192.168.92.2 der DNS-Server auf dem öffentlichen Adapter ist, erstellt OpenDNS die resolv.conf an folgendem Speicherort:

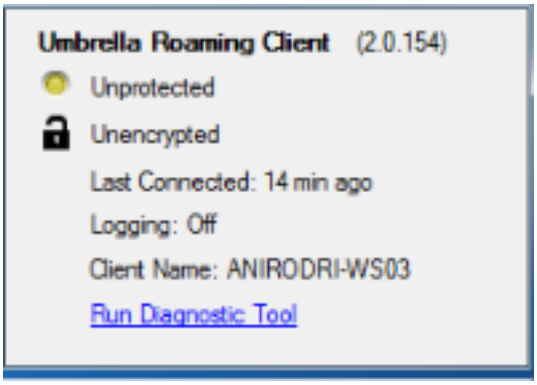
C:\ProgramData\OpenDNS\ERC\Resolver1-LocalAreaConnection-resolv.conf
nameserver 192.168.92.2

Der Roaming-Client verschlüsselt jedes Paket, das auf OpenDNS gesetzt ist. Es wird jedoch kein Verschlüsselungstunnel zu 208.67.222.222 gestartet oder verwendet. Der Roaming-Client verfügt über eine optionale Funktion zur Durchsetzung der IP-Schicht, mit der eine IPSec-Verbindung für Nicht-DNS-Zwecke geöffnet wird, um IP-Adressen zu blockieren. Dies wird automatisch deaktiviert, wenn eine aktive AnyConnect-Verbindung besteht. Außerdem wird an 127.0.0.1:53 gebunden, um lokal auf dem Computer generierte Abfragen zu empfangen. Wenn der Endpunkt einen Namen auflösen muss, werden die lokalen Abfragen aufgrund des Überschreibens an 127.0.0.1 weitergeleitet, und der zugrunde liegende dnscrypt-Proxy-Prozess des Roaming-Clients leitet sie über den verschlüsselten Kanal an die öffentlichen OpenDNS-Server weiter.

Wenn der DNS-Datenfluss nicht auf 127.0.0.1:53 beschränkt ist, kann der Roaming-Client nicht funktionieren, und es wird Folgendes ausgeführt. Wenn der Client die öffentlichen DNS-Server oder die gebundene Adresse 127.0.0.1:53 nicht erreichen kann, wechselt er in den Zustand "Fail-Open" und stellt die DNS-Einstellungen auf den lokalen Adaptern wieder her. Im Hintergrund werden weiterhin Tests an 208.67.222.222 gesendet. Wenn die sichere Verbindung wiederhergestellt wird, kann sie in den aktiven Modus wechseln.

Einschränkungen

Nach der Betrachtung der High-Level-Funktionalität beider Clients ist es offensichtlich, dass der Roaming-Client die Möglichkeit haben muss, die lokalen DNS-Einstellungen zu ändern und an 127.0.0.1:53 zu binden, um Abfragen über den sicheren Kanal weiterzuleiten. Wenn VPN verbunden ist, sind die einzigen Konfigurationen, bei denen AnyConnect die native DNS-Auflösung nicht beeinträchtigt, die Split-Include- und Split-Exclusion-Konfiguration (wobei Split-Tunnel-All DNS deaktiviert ist). Daher wird derzeit empfohlen, eine dieser Konfigurationen zu verwenden, wenn der Roaming-Client ebenfalls verwendet wird. Der Roaming-Client verbleibt im ungeschützten/unverschlüsselten Zustand, wenn die Konfiguration des gesamten Tunnels verwendet oder Split-Tunnel-All DNS aktiviert ist, wie im Bild gezeigt.



Problemumgehung

Wenn die Kommunikation zwischen dem Roaming-Client und den OpenDNS-Servern mithilfe des VPN-Tunnels geschützt werden soll, kann eine Dummy Split-Exclusion-Zugriffsliste am VPN-Headend verwendet werden. Dies ist der nächste Schritt zu einer vollständigen Tunnelkonfiguration. Wenn dies nicht der Fall ist, kann "split-include" verwendet werden, wenn die Zugriffsliste die öffentlichen OpenDNS-Server nicht enthält, oder "split-exclude" verwendet werden, wenn die Zugriffsliste die öffentlichen OpenDNS-Server enthält.

Darüber hinaus kann bei Verwendung des Roaming-Clients der Split-DNS-Modus nicht verwendet werden, da dies zu einem Verlust der lokalen DNS-Auflösung führt. Split-Tunnel-all DNS sollte ebenfalls deaktiviert bleiben. Sie wird jedoch teilweise unterstützt und sollte es dem Roaming-Client ermöglichen, nach dem Failover verschlüsselt zu werden.

Konfigurationen

Tunnel-OpenDNS-Datenverkehr

In diesem Beispiel wird eine Dummy-IP-Adresse in der Zugriffsliste "split-exclude" verwendet. Bei dieser Konfiguration erfolgt die gesamte Kommunikation mit 208.67.222.222 über den VPN-Tunnel, und der Roaming-Client arbeitet in einem verschlüsselten und geschützten Zustand.

```
ciscoasa# sh run access-li split
access-list split standard permit host 2.2.2.2

ciscoasa# sh run group-policy
group-policy GroupPolicy-OpenDNS internal
group-policy GroupPolicy-OpenDNS attributes
 wins-server none
 dns-server value 1.1.1.1
 vpn-tunnel-protocol ssl-client
 split-tunnel-policy excludespecified
 split-tunnel-network-list value split
 default-domain value cisco.com
 address-pools value acpool
 webvpn
 anyconnect profiles value AnyConnect type user
ciscoasa#
```

OpenDNS-Datenverkehr vom VPN-Tunnel ausschließen

In diesem Beispiel wird die OpenDNS-Resolver-Adresse in der Zugriffsliste für "split-exclude" verwendet. Bei dieser Konfiguration erfolgt die gesamte Kommunikation mit 208.67.222.222 außerhalb des VPN-Tunnels, und der Roaming-Client arbeitet in einem verschlüsselten und geschützten Zustand.

```
ciscoasa# sh run access-li split
access-list split standard permit host 208.67.222.222

ciscoasa# sh run group-policy
group-policy GroupPolicy-OpenDNS internal
group-policy GroupPolicy-OpenDNS attributes
```

```
 wins-server none
 dns-server value 1.1.1.1
 vpn-tunnel-protocol ssl-client
 split-tunnel-policy excludespecified
 split-tunnel-network-list value split
 default-domain value cisco.com
 address-pools value acpool
 webvpn
 anyconnect profiles value AnyConnect type user
ciscoasa#
```

Dieses Beispiel zeigt eine Split-Include-Konfiguration für ein internes 192.168.1.0/24 Subnetz. Bei dieser Konfiguration wird der Roaming-Client weiterhin verschlüsselt und geschützt betrieben, da der Datenverkehr zum 208.67.222.222.22-Standard nicht über den Tunnel gesendet wird.

```
ciscoasa# sh run access-li split
access-list split standard permit 192.168.1.0 255.255.255.0

ciscoasa# sh run group-policy
group-policy GroupPolicy-OpenDNS internal
group-policy GroupPolicy-OpenDNS attributes
 wins-server none
 dns-server value 1.1.1.1
 vpn-tunnel-protocol ssl-client
 split-tunnel-policy tunnelspecified
 split-tunnel-network-list value split
 default-domain value cisco.com
 address-pools value acpool
 webvpn
 anyconnect profiles value AnyConnect type user
ciscoasa#
```

Note: Split-tunnel-all-dns must be disabled in all of the scenarios

Überprüfen

Wenn VPN verbunden ist, sollte der Roaming-Client wie in diesem Bild gezeigt geschützt und verschlüsselt angezeigt werden: