ASA: Acceso remoto del modo del Multi-contexto (AnyConnect) VPN

Contenido

Introducción

Este documento describe cómo configurar el Red privada virtual (VPN) del Acceso Remoto (RA) en el Firewall adaptante del dispositivo de seguridad de Cisco (ASA) en el modo del contexto múltiple (MC). Muestra Cisco ASA en el modo de contexto múltiple soportado/las características no admitidas y requisito para obtener la licencia en cuanto a RA VPN.

Prerrequisitos

Requisitos

Cisco recomienda que tenga conocimiento sobre estos temas:

- Configuración de SSL ASA AnyConnect
- Configuración del contexto múltiple ASA

Componentes Utilizados

La información que contiene este documento se basa en las siguientes versiones de software y hardware.

- Dos código que se ejecuta ASA 5585 9.5(2)
- Cliente 3.1.10010 de AnyConnect

La información que contiene este documento se creó a partir de los dispositivos en un ambiente de laboratorio específico. Todos los dispositivos que se utilizan en este documento se pusieron en funcionamiento con una configuración verificada (predeterminada). Si la red está funcionando, debe asegurarse de comprender el posible impacto que puede tener un comando.

Antecedentes

el Multi-contexto es una forma de virtualización que permita que las copias independientes múltiples de una aplicación se ejecuten simultáneamente en el mismo hardware, con cada copia (o el dispositivo virtual) apareciendo que un dispositivo físico separado al usuario. Esto permite que un solo ASA aparezca como ASA múltiples a los usuarios independientes múltiples. La familia ASA ha soportado los Firewall virtuales desde su versión inicial; sin embargo, no había soporte de la virtualización para el Acceso Remoto en el ASA. El soporte VPN LAN2LAN (L2L) para el multi-contexto fue agregado para la versión 9.0. A partir del multi-contexto el **9.5.2** basado soporte de la virtualización para las conexiones del Acceso Remoto VPN (RA) al ASA.

Características admitidas

- Conectividad de AnyConnect 3.X+ SSL (IPv4, IPv6)
- Configuración centralizada de la imagen de AnyConnect
- Actualización de la imagen de AnyConnect

Características no admitidas

- IKEv2, IKEv1
- Stateful Failover
- Virtualización de destello
- Configuración de la imagen de AnyConnect por el contexto
- WebLaunch
- Descarga del perfil del cliente
- DAP y CoA
- CSD/Hostscan
- Balanceo de carga VPN
- Nombre de usuario-de-certificado y prefill-nombre de usuario
- Arreglo para requisitos particulares/localización

Autorización

- Licencia de AnyConnect Apex requerida
- El esencial autoriza ignorado/no permitido
- Flexibilidad de configuración para controlar el uso máximo de la licencia por el contexto

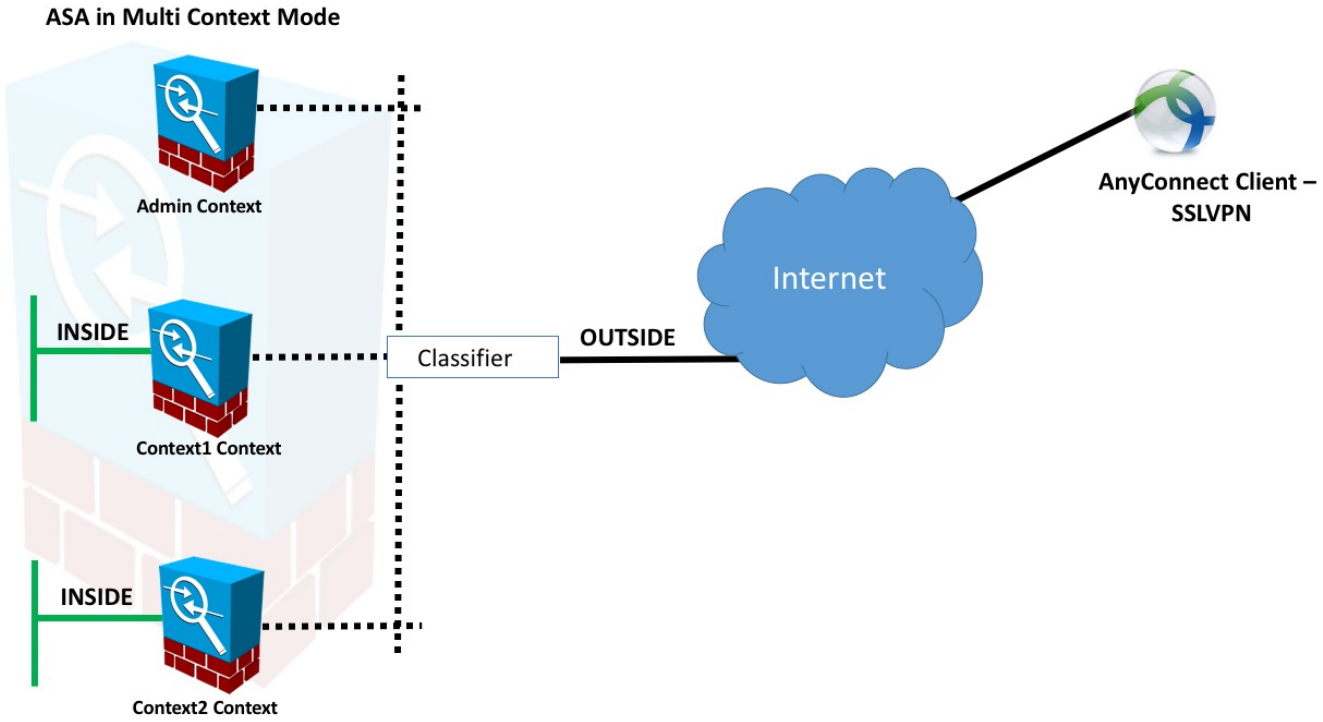
- Flexibilidad de configuración para permitir la licencia que reparte por el contexto

Configurar

Esta sección describe cómo configurar Cisco ASA como servidor local de CA.

> Nota: Use la Command Lookup Tool (clientes registrados solamente) para obtener más información sobre los comandos usados en esta sección.

Diagrama de la red



> **Nota:** Los contextos múltiples en este ejemplo comparten una interfaz (AFUERA), después el clasificador utiliza las direcciones MAC (autos o manuales) únicas de la interfaz para remitir los paquetes. Para más detalles en cómo el dispositivo de seguridad clasifica los paquetes en el contexto múltiple refiérase cómo el ASA clasifica los paquetes

Configuraciones

Contexto del sistema

Paso 1. Configuración de failover.

```
 !! Active Firewall

failover
failover lan unit primary
failover lan interface LAN_FAIL GigabitEthernet0/3
failover link LAN_FAIL GigabitEthernet0/3
```

```
failover interface ip LAN_FAIL 10.1.1.1 255.255.255.252 standby 10.1.1.2
failover group 1
failover group 2

 !! Secondary Firewall

failover
failover lan unit secondary
failover lan interface LAN_FAIL GigabitEthernet0/3
failover link LAN_FAIL GigabitEthernet0/3
failover interface ip LAN_FAIL 10.1.1.1 255.255.255.252 standby 10.1.1.2
failover group 1
failover group 2
```

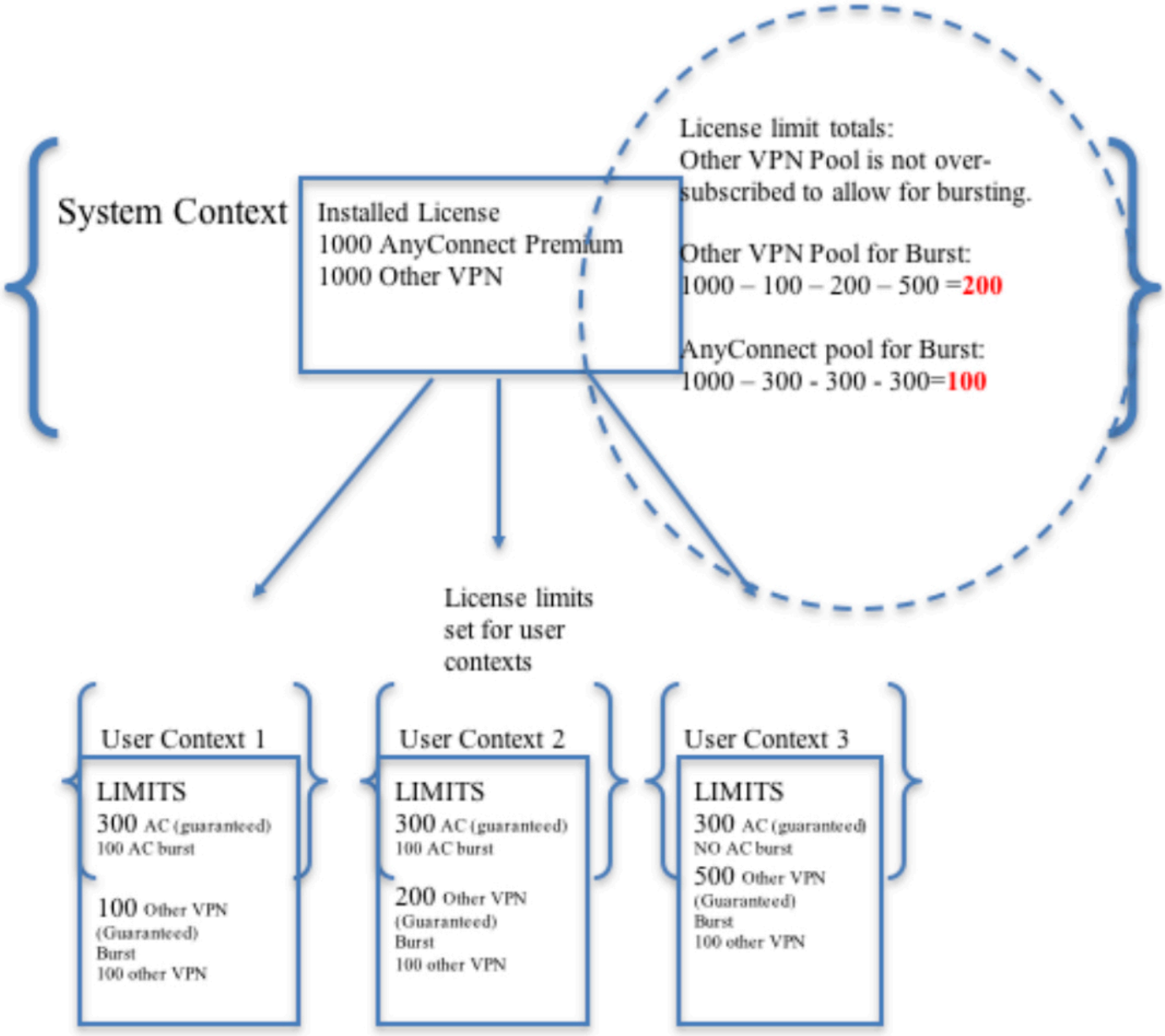
Paso 2. Afecte un aparato VPN Resouce.

Configurado vía la configuración existente de la clase…. Las licencias son permitidas por el número de licencias o % del total por el contexto

Nuevos tipos de recurso presentados para MC RAVPN:

- VPN AnyConnect: Garantizado a un contexto y no puede ser oversubscribed
- Explosión AnyConnect VPN: No prohiba a contexto las licencias adicionales más allá del límite garantizado. El pool de la explosión consiste en cualquier licencia no garantizada a un contexto y se permite a un contexto repartido sobre una base del primero-venir-primero-servicio

Modelo del aprovisionamiento de la licencia VPN:



Nota: ASA5585 ofrece a 10,000 sesiones del usuario máximas de Cisco AnyConnect y en este Cisco AnyConnect del ejemplo 4000 afectan un aparato la sesión del usuario por el contexto.

```
class resource02
 limit-resource VPN AnyConnect  4000
 limit-resource VPN Burst AnyConnect  2000

class resource01
 limit-resource VPN AnyConnect 4 000
 limit-resource VPN Burst AnyConnect  2000
```

Paso 3. Configure los contextos y asigne los recursos.

Nota: En este ejemplo GigabitEthernet0/0 se comparte entre todo el contexto.

```
admin-context admin
context admin
  allocate-interface GigabitEthernet0/0
  config-url disk0:/admin
```

```
context context1
  member resource01
  allocate-interfaceGigabitEthernet0/0
  allocate-interface GigabitEthernet0/1
  config-url disk0:/context1
  join-failover-group 1

context context2
  member resource02
  allocate-interface GigabitEthernet0/0
  allocate-interface GigabitEthernet0/2
  config-url disk0:/context2
  join-failover-group 2
```

Paso 4. Instale la licencia de Apex en el Firewall.

Activando o desactivando las claves de activación

Contexto Admin

Paso 1. Instale el paquete del cliente de AnyConnect.

> **Nota:** 1. El almacenamiento de destello no se virtualiza y es solamente accesible del contexto del sistema.
> 2. Copie los archivos al flash en la imagen de AnyConnect del contexto del sistema es decir.
> 3. La imagen de AnyConnect es una configuración compartida.
> 4. Configurado en el contexto admin solamente. No disponible en otros contextos.
> 5. Todos los contextos refieren automáticamente a esta configuración global de la imagen de AnyConnect.

```
webvpn
 anyconnect image disk0:/anyconnect-win-3.1.10010-k9.pkg 1
 anyconnect enable
```

Contexto de encargo 1

```
 !! Shared interface configuration - OUTSIDE (GigabitEthernet0/0)

interface GigabitEthernet0/0
 nameif OUTSIDE
 security-level 0
 ip address 10.106.44.38  255.255.255.0 standby 10.106.44.39

!! Enable WebVPN on respective interfaces

webvpn
 enable OUTSIDE
 anyconnect enable

!! IP pool and username configuration

ip local pool mypool 192.168.1.1-192.168.50.1 mask 255.255.0.0

username cisco password cisco

!! Configure the require connection profile for SSL VPN

group-policy GroupPolicy_MC_RAVPN_1 internal
group-policy GroupPolicy_MC_RAVPN_1 attributes
```

```
 banner value "Welcome to Context1 SSLVPN"
 wins-server none
 dns-server value 192.168.20.10
 vpn-tunnel-protocol ssl-client
 split-tunnel-policy tunnelspecified
 split-tunnel-network-list value split
 default-domain value cisco.com

tunnel-group MC_RAVPN_1 type remote-access
tunnel-group MC_RAVPN_1 general-attributes
 address-pool mypool
 default-group-policy GroupPolicy_MC_RAVPN_1
tunnel-group MC_RAVPN_1 webvpn-attributes
 group-alias MC_RAVPN_1 enable
 group-url https://10.106.44.38/context1  enable
```

Contexto de encargo 2

```
 !! Shared interface configuration - OUTSIDE (GigabitEthernet0/0)

interface GigabitEthernet0/0
 nameif OUTSIDE
 security-level 0
 ip address 10.106.44.36  255.255.255.0 standby 10.106.44.37

!! Enable WebVPN on respective interface

webvpn
 enable OUTSIDE
 anyconnect enable

!! IP pool and username configuration

ip local pool mypool 192.168.51.1-192.168.101.1 mask 255.255.0.0

username cisco password cisco

!! Configure the require connection profile for SSL VPN

group-policy GroupPolicy_MC_RAVPN_2 internal
group-policy GroupPolicy_MC_RAVPN_2 attributes
 banner value "Welcome to Context2 SSLVPN"
 wins-server none
 dns-server value 192.168.60.10
 vpn-tunnel-protocol ssl-client
 split-tunnel-policy tunnelspecified
 split-tunnel-network-list value split
 default-domain value cisco.com

tunnel-group MC_RAVPN_2 type remote-access
tunnel-group MC_RAVPN_2 general-attributes
 address-pool mypool
 default-group-policy GroupPolicy_MC_RAVPN_2
tunnel-group MC_RAVPN_2 webvpn-attributes
 group-alias MC_RAVPN_2 enable
 group-url https://10.106.44.36/context2 enable
```

Verificación

Utilize esta sección para confirmar que su configuración funcione correctamente.

Nota: La herramienta del Output Interpreter (clientes registrados solamente) apoya los

ciertos comandos show. Utilice la herramienta del Output Interpreter para ver una análisis de la salida del comando show.

Verifique si la licencia de Apex está instalada

El ASA no reconoce específicamente una licencia de AnyConnect Apex sino que aplica las características de la licencia de una licencia de Apex que incluyen:

- Premio de AnyConnect autorizado al límite de la plataforma
- AnyConnect para el móvil
- AnyConnect para el teléfono del Cisco VPN
- Evaluación avanzada del punto final

Verifique si el paquete de AnyConnect está instalado en el contexto Admin y está disponible en los contextos de encargo

```
 !! AnyConnect package is installed in Admin Context

ciscoasa/pri/ admin/act# show run webvpn
webvpn
 anyconnect image disk0:/anyconnect-win-3.1.10010-k9.pkg 1
 anyconnect enable

ciscoasa/pri/admin/act# show webvpn anyconnect
1. disk0:/anyconnect-win-3.1.10010-k9.pkg 1 dyn-regex=/Windows NT/
  CISCO STC win2k+
  3,1,10010
  Hostscan Version 3.1.10010
  Wed 07/22/2015 12:06:07.65

1 AnyConnect Client(s) installed

!! AnyConnect package is available in context1
ciscoasa/pri/admin/act# changeto context context1

ciscoasa/pri/context1/act# show run webvpn
webvpn
 enable OUTSIDE
 anyconnect enable
 tunnel-group-list enable

ciscoasa/pri/context1/act# show webvpn anyconnect
1. disk0:/anyconnect-win-3.1.10010-k9.pkg 1 dyn-regex=/Windows NT/
  CISCO STC win2k+
  3,1,10010
  Hostscan Version 3.1.10010
  Wed 07/22/2015 12:06:07.65

1 AnyConnect Client(s) installed
```

Verifique si los usuarios pueden conectar vía AnyConnect en los contextos de encargo

Consejo: Para un mejor reloj de la visualización debajo de los vídeos en la pantalla completa.

```
 !! One Active Connection on Context1

ciscoasa/pri/context1/act# show vpn-sessiondb anyconnect

Session Type: AnyConnect

Username     : cisco                  Index        : 5
Assigned IP  : 192.168.1.1            Public IP    : 10.142.168.102
Protocol     : AnyConnect-Parent SSL-Tunnel DTLS-Tunnel
License      : AnyConnect Premium, AnyConnect for Mobile
Encryption   : AnyConnect-Parent: (1)none  SSL-Tunnel: (1)AES-GCM-256  DTLS-Tunnel: (1)AES256
Hashing      : AnyConnect-Parent: (1)none  SSL-Tunnel: (1)SHA384  DTLS-Tunnel: (1)SHA1
Bytes Tx     : 3186                   Bytes Rx     : 426
Group Policy : GroupPolicy_MC_RAVPN_1 Tunnel Group : MC_RAVPN_1
Login Time   : 15:33:25 UTC Thu Dec 3 2015
Duration     : 0h:00m:05s
Inactivity   : 0h:00m:00s
VLAN Mapping : N/A                    VLAN         : none
Audt Sess ID : 0a6a2c2600005000566060c5
Security Grp : none

!! Changing Context to Context2

ciscoasa/pri/context1/act# changeto context context2

!! One Active Connection on Context2

ciscoasa/pri/context2/act# show vpn-sessiondb anyconnect

Session Type: AnyConnect

Username     : cisco                  Index        : 1
Assigned IP  : 192.168.51.1           Public IP    : 10.142.168.94
Protocol     : AnyConnect-Parent SSL-Tunnel DTLS-Tunnel
License      : AnyConnect Premium
Encryption   : AnyConnect-Parent: (1)none  SSL-Tunnel: (1)AES256  DTLS-Tunnel: (1)AES256
Hashing      : AnyConnect-Parent: (1)none  SSL-Tunnel: (1)SHA1  DTLS-Tunnel: (1)SHA1
Bytes Tx     : 10550                  Bytes Rx     : 1836
Group Policy : GroupPolicy_MC_RAVPN_2 Tunnel Group : MC_RAVPN_2
Login Time   : 15:34:16 UTC Thu Dec 3 2015
Duration     : 0h:00m:17s
Inactivity   : 0h:00m:00s
VLAN Mapping : N/A                    VLAN         : none
Audt Sess ID : 0a6a2c2400001000566060f8
Security Grp : none

!! Changing Context to System

ciscoasa/pri/context2/act# changeto system

!! Notice total number of connections are two (for the device)

ciscoasa/pri/act# show vpn-sessiondb license-summary
----------------------------------------------------------------------------
VPN Licenses and Configured Limits Summary
----------------------------------------------------------------------------
                                   Status : Capacity : Installed :  Limit
                                 ----------------------------------------
AnyConnect Premium               :  ENABLED :    10000 :     10000 :   NONE
Other VPN (Available by Default) :  ENABLED :    10000 :     10000 :   NONE
AnyConnect for Mobile            :  ENABLED(Requires Premium or Essentials)
Advanced Endpoint Assessment     :  ENABLED(Requires Premium)
AnyConnect for Cisco VPN Phone   :  ENABLED
VPN-3DES-AES                     :  ENABLED
```

```
VPN-DES                         :  ENABLED
----------------------------------------------------------------------------

----------------------------------------------------------------------------
VPN Licenses Usage Summary
----------------------------------------------------------------------------
                        Local : Shared :   All  :   Peak :  Eff.  :
                       In Use : In Use : In Use : In Use :  Limit : Usage
                      ------------------------------------------------
AnyConnect Premium     :      2 :      0 :       2 :      2 :  10000 :    0%
 AnyConnect Client     :                :       2 :      2          :    0%
   AnyConnect Mobile   :                :       2 :      2          :    0%
Other VPN              :                :       0 :      0 :  10000 :    0%
 Site-to-Site VPN      :                :       0 :      0          :    0%
----------------------------------------------------------------------------

!! Notice the resource usage per Context

ciscoasa/pri/act# show resource usage all resource VPN AnyConnect
Resource                 Current        Peak      Limit        Denied Context
AnyConnect                     1           1       4000             0 context1
AnyConnect                     1           1       4000             0 context2
```

Troubleshooting

Esta sección proporciona la información que usted puede utilizar para resolver problemas su configuración.

Resolver problemas AnyConnect

> **Consejo:** En caso de que el ASA no tenga licencia de Apex instalada, la sesión de AnyConnect sería terminada con el Syslog abajo:
>
> %ASA-6-725002: El dispositivo completó el contacto SSL con el cliente OUTSIDE:10.142.168.86/51577 a 10.106.44.38/443 para la sesión TLSv1
> %ASA-6-113012: Autenticación de usuario AAA acertada: base de datos local: user = Cisco
> %ASA-6-113009: El AAA extrajo la directiva del grupo predeterminado (GroupPolicy_MC_RAVPN_1) para el user = Cisco
> %ASA-6-113008: El estatus de transacción AAA VALIDA: user = Cisco
> %ASA-3-716057: Sesión IP <10.142.168.86> del usuario del grupo terminada, ninguna licencia de AnyConnect Apex disponible
> %ASA-4-113038: IP <10.142.168.86> del usuario del grupo incapaz de crear la sesión del padre de AnyConnect.

Referencias

Release Notes: 9.5(2)

Información Relacionada

- Cisco ASA 5500 Series Adaptive Security Appliances
- Guía de Troubleshooting del cliente VPN de AnyConnect - Problemas comunes
- Manejando, monitoreando, y resolver problemas las sesiones de AnyConnect

- Soporte Técnico y Documentación - Cisco Systems