

Contenido

[Introducción](#)

[prerrequisitos](#)

[Requisitos](#)

[Componentes Utilizados](#)

[Antecedentes](#)

[Características admitidas](#)

[Características no admitidas](#)

[Autorización](#)

[Configurar](#)

[Diagrama de la red](#)

[Configuraciones](#)

[Contexto del sistema](#)

[Contexto Admin](#)

[Contexto de encargo 1](#)

[Contexto de encargo 2](#)

[Verificación](#)

[Verifique si la licencia de Apex está instalada](#)

[Verifique si el paquete de AnyConnect está instalado en el contexto Admin y está disponible en los contextos de encargo](#)

[Verifique si los usuarios pueden conectar vía AnyConnect en los contextos de encargo](#)

[Troubleshooting](#)

[Referencias](#)

[Información Relacionada](#)

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

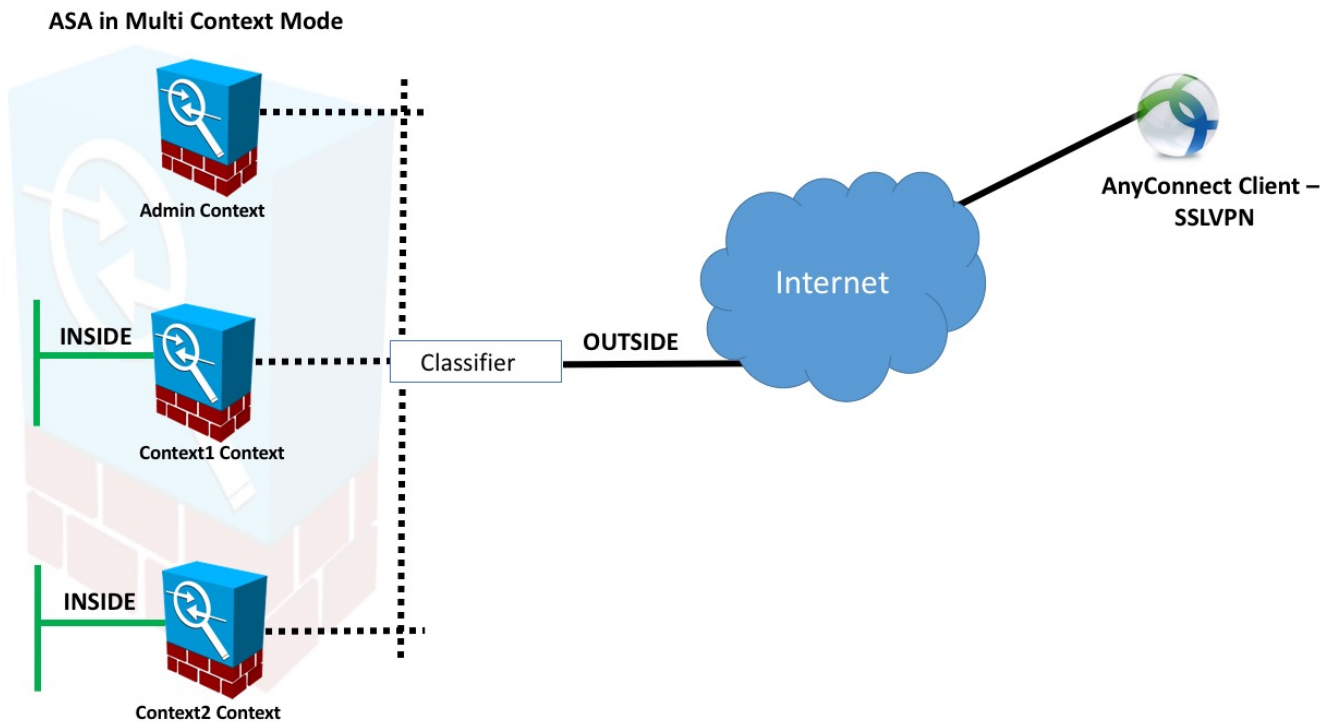
- Licencia de AnyConnect Apex requerida
- El esencial autoriza ignorado/no permitido
- Flexibilidad de configuración para controlar el uso máximo de la licencia por el contexto
- Flexibilidad de configuración para permitir la licencia que reparte por el contexto

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.

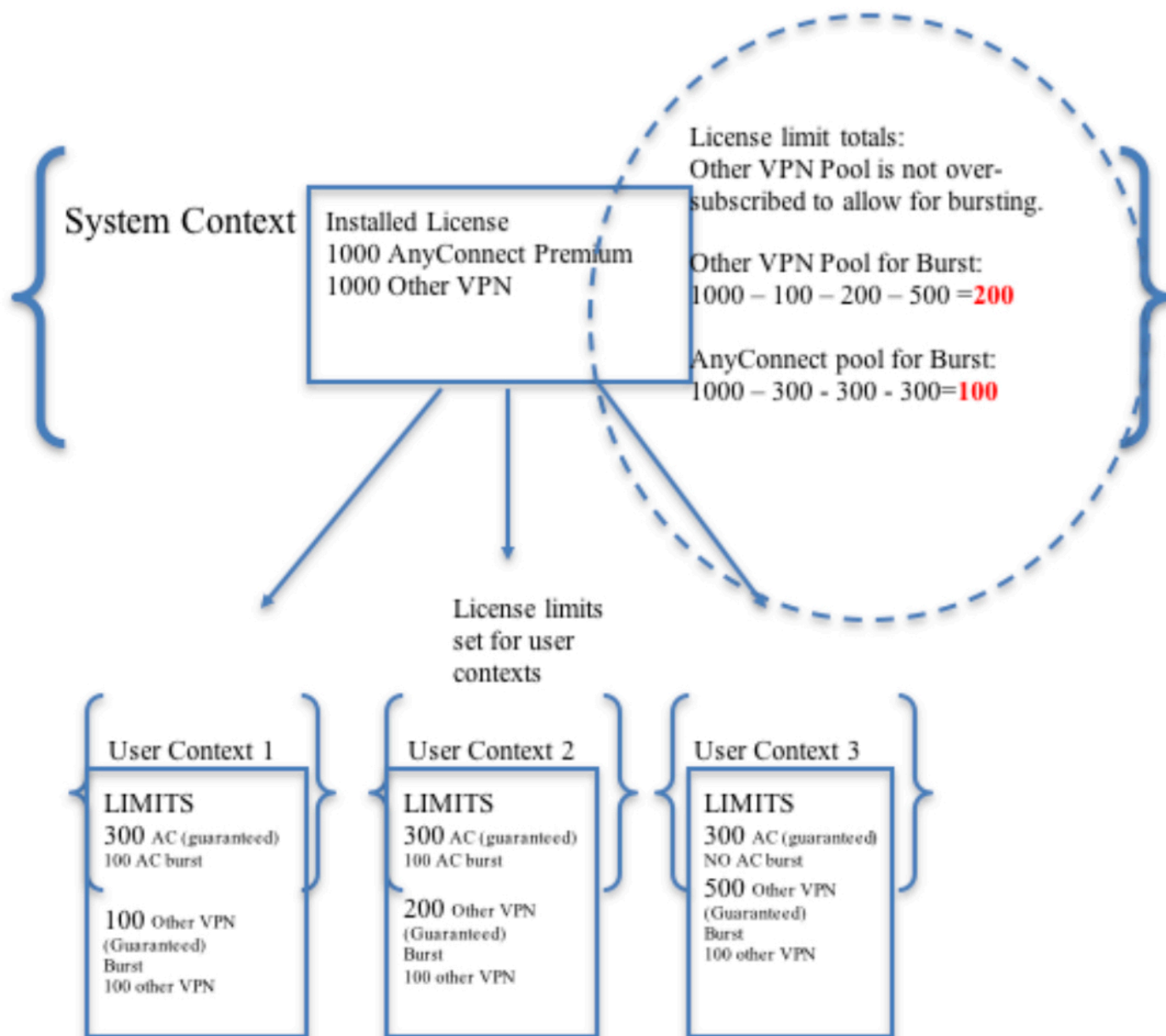
Paso 2. Afecte un aparato VPN Resource.

¿Configurado vía la clase existente? configuración. 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 pueda? t sea oversubscribed
- Explosión AnyConnect VPN: No prohíba 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.

Paso 3. Configure los contextos y asigne los recursos.

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

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.

Contexto de encargo 1

Contexto de encargo 2

Verificación

Utilice 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

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.

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](#)