Las conexiones inalámbricas de la movilidad fallan y no se recuperan cuando se reinicia el ASA

Contenido

Introducción

Este documento describe un problema donde una conexión de la trayectoria de la movilidad (usando el User Datagram Protocol (UDP) y protocolo IP 93) esa atraviesa un dispositivo de seguridad adaptante (ASA) pudo ir abajo y continuar fallando hasta que se recarguen los dispositivos de la movilidad, o se para y se deja inactivo por poco tiempo y después se recomienza el tráfico de la trayectoria de la movilidad.

Prerrequisitos

Requisitos

Cisco recomienda que tenga conocimiento sobre estos temas:

- Dispositivo de seguridad adaptante de Cisco (ASA)
- Regulador del Wireless LAN (WLC)

Componentes Utilizados

Este documento no tiene restricciones específicas en cuanto a versiones de software y de

hardware.

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, asegúrese de haber comprendido el impacto que puede tener cualquier comando.

Convenciones

Consulte Convenciones de Consejos Técnicos de Cisco para obtener información sobre las convenciones sobre documentos.

Problema

En esta situación un regulador del Wireless LAN (WLC) en 10.10.1.2 intenta comunicar con el WLC en 10.10.9.3, pero la comunicación falla.

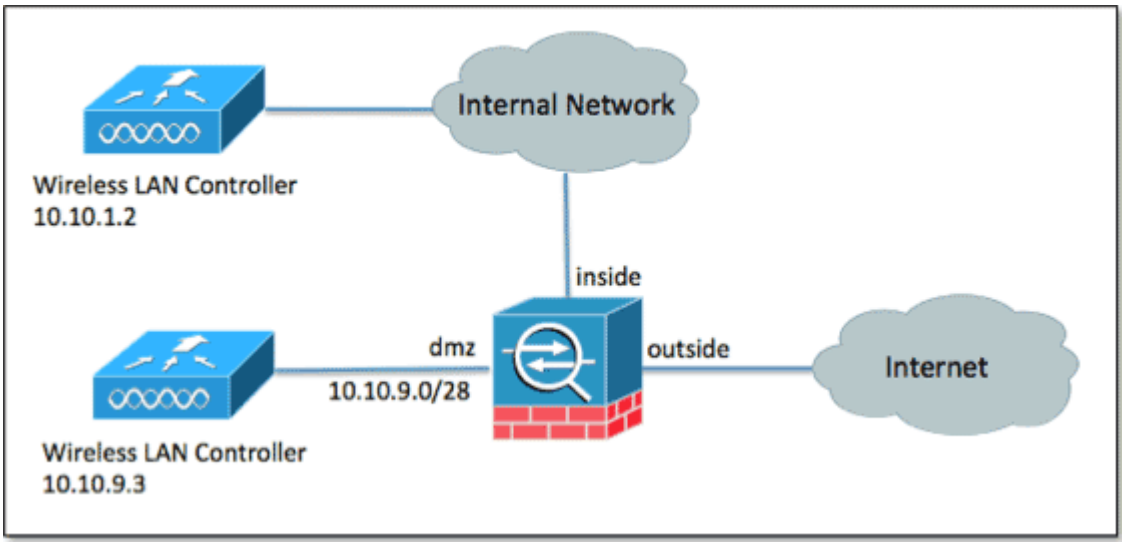
Este problema se puede accionar por ninguno de estos eventos:

- Se reinicia El ASA.
- La tabla de ruteo es modificada por un administrador o un Routing Protocol.
- Una interfaz es apagada, después traída la salvaguardia por el administrador.

Además del tráfico de la movilidad, este problema se pudo experimentar para cualquier protocolo IP UDP o del no TCP.

Este problema es un no bug sino una consecuencia de la topología de red y de la configuración ASA. Vea abajo para la causa y la solución a este problema.

Topología de red de muestra



Configuración de ruteo ASA:

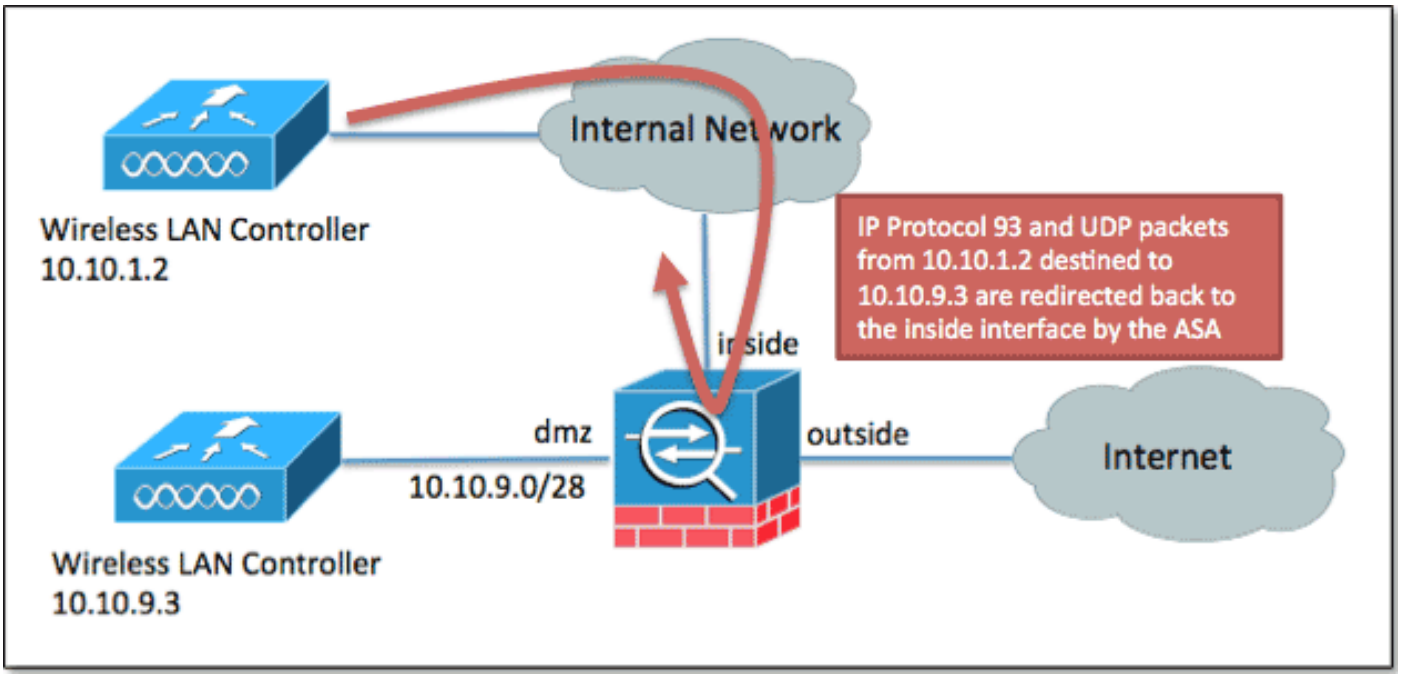
```
!
route outside 0.0.0.0 0.0.0.0 192.168.4.3 1
route inside 10.0.0.0 255.0.0.0 192.168.254.1 1
!
same-security-traffic permit intra-interface
!
```

Configuración de la interfaz del dmz ASA:

```
!
interface Gigabit-Ethernet0/1.10
vlan 10
nameif dmz
security-level 75
ip address 10.10.9.1 255.255.255.240 standby 10.10.9.2
!
```

Activador del problema

Se acciona el problema cuando el WLC en 10.10.1.2 envía el tráfico destinado al WLC en 10.10.9.3. Estos paquetes hacen el ASA construir una conexión en su tabla de conexiones que mande el tráfico de la movilidad la interfaz incorrecta ASA (dentro).



Este problema es causado por la interfaz de destino “dmz” del ASA que es en el plumón/el estado inactivo cuando la conexión fue construida, que da lugar a la conexión que es creada una interfaz diversa, no óptima. La interfaz del dmz pudo estar abajo de debido a un problema de cable, a un Ethernet o a la cuestión de la negociación del canal del puerto, o puede ser que administrativo sea apagada.

A la hora del problema, las conexiones de la trayectoria de la movilidad pueden ser consideradas como siendo creado como “intra-interfaz” del ASA, que está ruteando se retiran los paquetes la misma interfaz interior que llegaron encendido:

```
ASA# show conn address 10.10.1.2
15579 in use, 133142 most used
97 inside 10.10.9.3 inside 10.10.1.2, idle 0:00:00, bytes 32210
UDP inside 10.10.9.3:16666 inside 10.10.1.2:16666, idle 0:00:00, bytes 4338, flags -
97 inside 10.10.9.3 inside 10.10.1.2, idle 0:00:00, bytes 157240
```

```
ASA#
```

El punto final de la movilidad en 10.10.1.2 continúa enviando el tráfico destinado a 10.10.9.3, que hace juego estas conexiones existentes. Incluso si la interfaz del dmz era progresar al estado up-up, el tráfico de la movilidad originado de 10.10.1.2 correspondería con las conexiones existentes en la tabla (en vez de construir una nueva conexión a la interfaz del dmz) que reajusta el descanso de las conexiones en el ASA, que prolonga el problema.

En resumen, estos eventos pueden accionar el problema:

1. El dispositivo en 10.10.1.2 envía un protocolo 97 o el paquete UDP a 10.10.9.3.
2. El ASA recibe el paquete en la interfaz interior, pero la interfaz del dmz está abajo, que da lugar a la ruta más específica a la red de destino que falta de la tabla de ruteo. Puesto que habilitan al **comando intra-interface del permiso de la mismo-Seguridad** en el ASA, sigue una Static ruta configurada para la red 10.0.0.0/8 detrás a través de la interfaz interior, construye una conexión en la tabla de conexiones, y después envía el paquete se retira la interfaz interior hacia la red interna.
3. En algún momento la interfaz del dmz pudo venir salvaguardia y la ruta se agrega de nuevo a la tabla; sin embargo, puesto que la conexión para el tráfico del protocolo 97 fue construida ya en el paso #2, los paquetes subsiguientes harán juego la conexión y la tabla de ruteo está sobregrabada, y el tráfico no alcanza el servidor en el dmz.

Solución

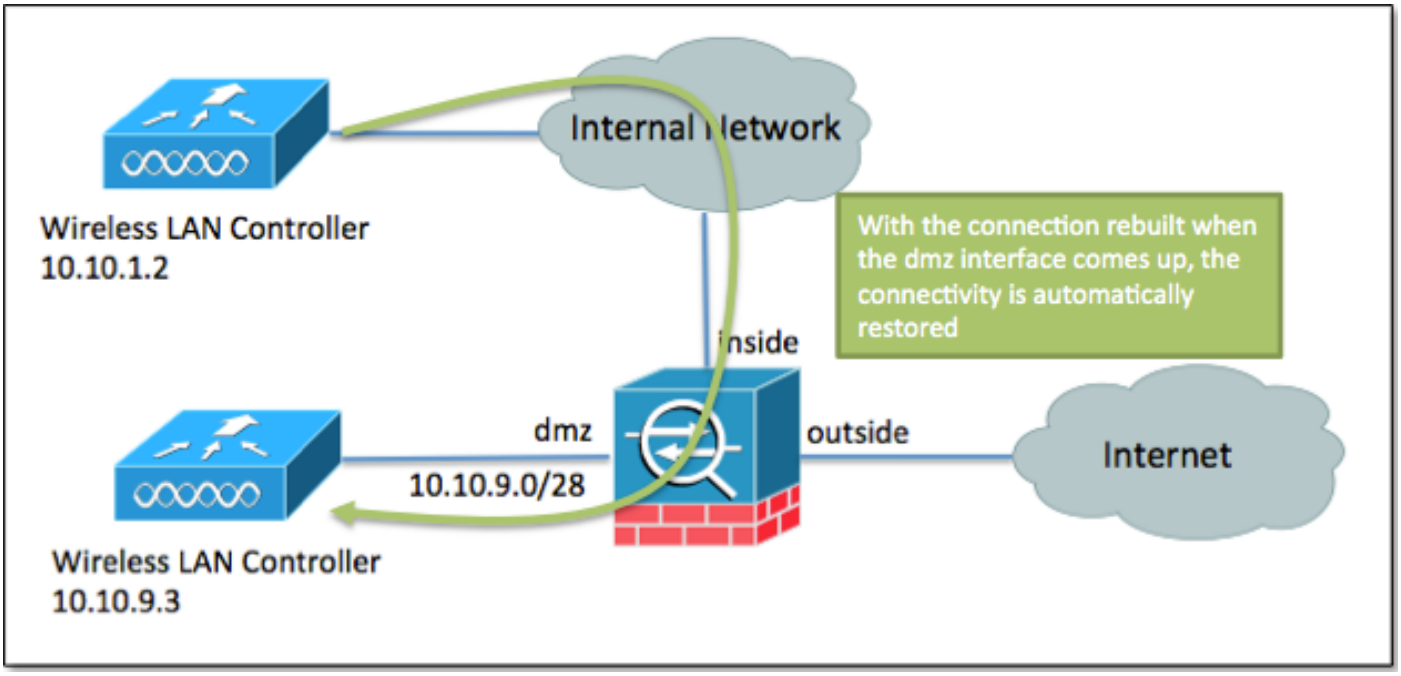
Solución 1

Una Solución posible para este problema es quitar el **comando intra-interface del permiso de la mismo-Seguridad** del ASA. Esta solución evita la conexión del giro de 180 grados sea construida se retira la misma interfaz en la cual el paquete original fue recibido, que permite que la conexión correcta sea construida cuando sube la interfaz. Sin embargo, dependiendo de la tabla de ruteo del ASA, esta solución no pudo trabajar (el tráfico se pudo rutear a otra interfaz con excepción del destino deseado basado en la tabla de ruteo), y el **comando intra-interface del permiso de la mismo-Seguridad** pudo ser necesario para otras conexiones en el ASA.

Solución 2

Para esta instancia específica, el problema fue atenuado con éxito habilitando la característica del **descanso flotar-CONN**. Esta característica, que no se habilita por abandono, hizo el ASA derribar estas conexiones un minuto después de que una más ruta preferida a uno de los puntos finales se agrega a la tabla de ruteo hacia fuera una nueva interfaz del ASA, que ocurre cuando sube la interfaz del dmz. Las conexiones entonces se reconstruyen inmediatamente cuando el próximo paquete llega el ASA, usando la interfaz preferida (dmz, en vez del interior para el host de 10.10.9.3).

```
ASA(config)# timeout floating-conn 0:01:00
```



Cuando se atenúa el problema, las conexiones correctas se construyen en la tabla de conexiones ASA y la Conectividad se restablece automáticamente:

```
ASA# show conn address 10.10.1.2
15329 in use, 133142 most used
97 dmz 10.10.9.3 inside10.10.1.2, idle 0:00:00, bytes 3175742510
UDP dmz 10.10.9.3:16666 inside 10.10.1.2:16666, idle 0:00:00, bytes 40651338, flags -
97 dmz 10.10.9.3 inside10.10.1.2, idle 0:00:00, bytes 1593457240
ASA#
```

Información Relacionada

- Referencia de comandos ASA 9.1 - comando del descanso flotar-CONN
- Soporte Técnico y Documentación - Cisco Systems