

# As conexões wireless da mobilidade falham e não recuperam quando o ASA é recarregado

## Índice

[Introdução](#)

[Pré-requisitos](#)

[Requisitos](#)

[Componentes Utilizados](#)

[Convenções](#)

[Problema](#)

[Exemplo de topologia de rede](#)

[Disparador do problema](#)

[Solução](#)

[Solução 1](#)

[Solução 2](#)

[Informações Relacionadas](#)

## Introdução

Este documento descreve um problema onde uma conexão do trajeto da mobilidade (usando o User Datagram Protocol (UDP) e o protocolo IP 93) essa atravesse uma ferramenta de segurança adaptável (ASA) possa ir para baixo e continuar a falhar até que os dispositivos da mobilidade estejam recarregados, ou o tráfego do trajeto da mobilidade está parado e deixado inativo por um curto período de tempo e reiniciado então.

## Pré-requisitos

### Requisitos

A Cisco recomenda que você tenha conhecimento destes tópicos:

- Ferramenta de segurança adaptável de Cisco (ASA)
- Controlador do Wireless LAN (WLC)

### [Componentes Utilizados](#)

Este documento não se restringe a versões de software e hardware específicas.

As informações neste documento foram criadas a partir de dispositivos em um ambiente de

laboratório específico. Todos os dispositivos utilizados neste documento foram iniciados com uma configuração (padrão) inicial. Se a sua rede estiver ativa, certifique-se de que entende o impacto potencial de qualquer comando.

## Convenções

Consulte as [Convenções de Dicas Técnicas da Cisco](#) para obter informações sobre convenções de documentos.

## Problema

Nesta situação um controlador do Wireless LAN (WLC) em 10.10.1.2 tenta comunicar-se com o WLC em 10.10.9.3, mas a comunicação falha.

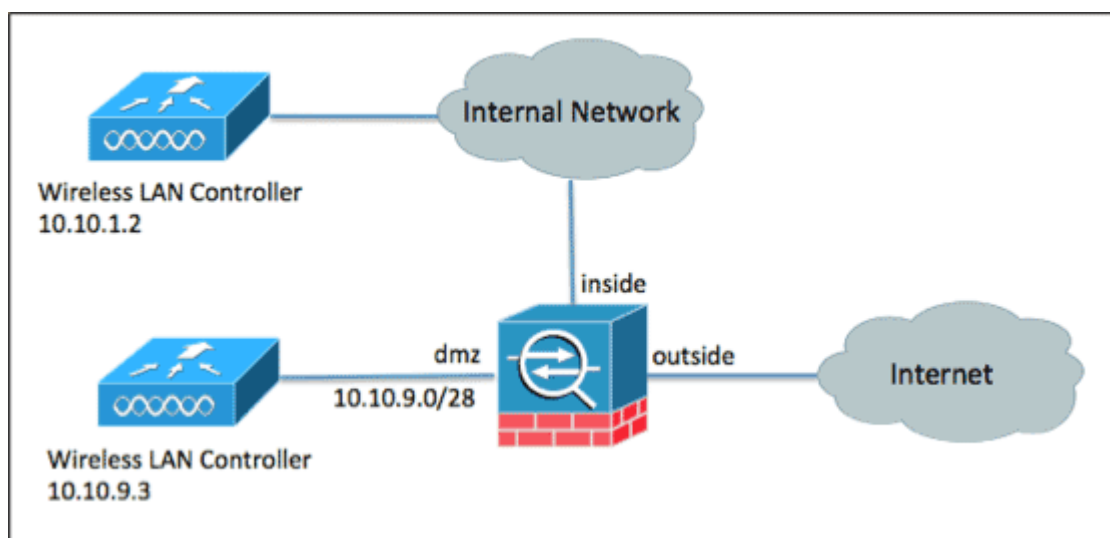
Este problema pode ser provocado por qualquens um eventos:

- O ASA é recarregado.
- A tabela de roteamento é alterada por um administrador ou por um protocolo de roteamento.
- Uma relação é fechada, a seguir trazida o apoio pelo administrador.

Além do tráfego da mobilidade, este problema pôde ser experiente para todo o UDP ou protocolos IP não-TCP.

Este problema é um não erro mas uma consequência da topologia de rede e da configuração ASA. Veja abaixo para a causa e a solução a este problema.

## Exemplo de topologia de rede



Configuração de roteamento 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  
!
```

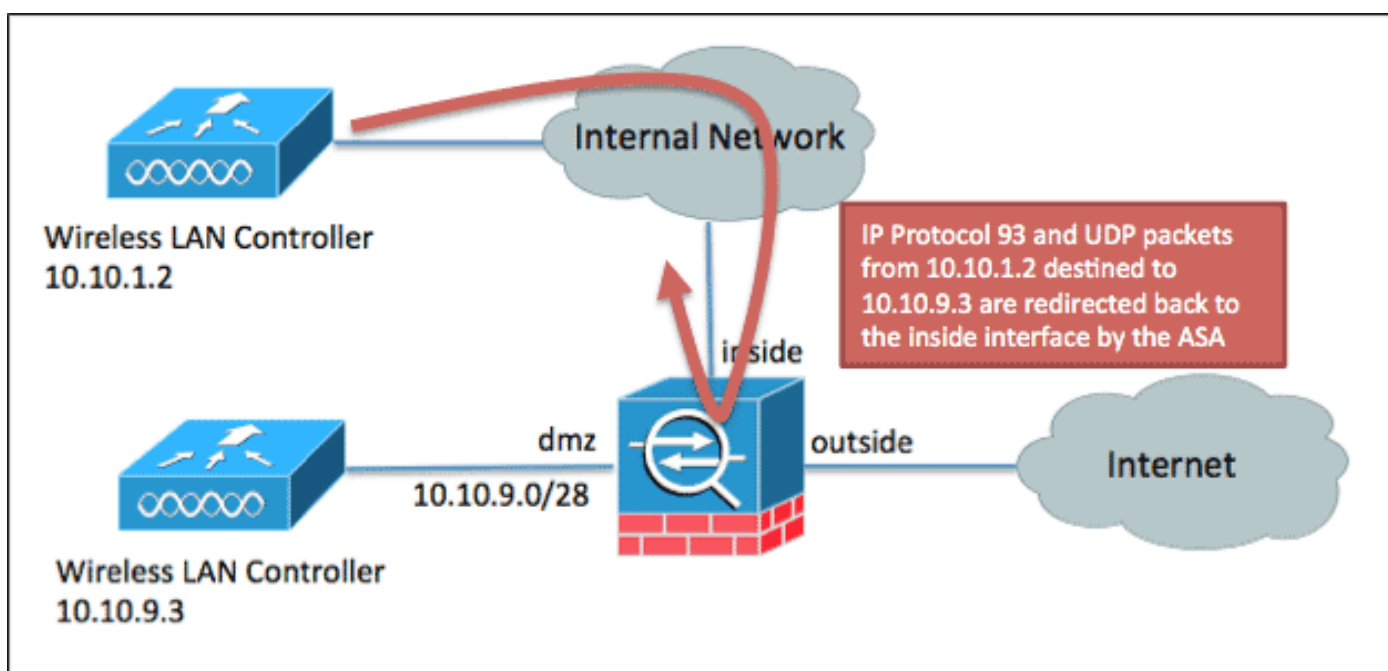
```
same-security-traffic permit intra-interface
!
```

## Configuração da interface do 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
!
```

## Disparador do problema

O problema é provocado quando o WLC em 10.10.1.2 envia o tráfego destinado ao WLC em 10.10.9.3. Estes pacotes fazem com que o ASA construa uma conexão em sua tabela de conexão que envia ao tráfego da mobilidade para fora a relação errada ASA (para dentro).



Esta edição é causada pela interface de destino “dmz” do ASA que é na pena/estado inativo então a conexão foi construída, que conduz à conexão que está sendo construída para fora uma relação diferente, não-otimizados. A relação do dmz pôde ser abaixo de devido a um problema de cabo, a um Ethernet ou à edição da negociação do canal de porta, ou pôde administrativamente ser fechada.

Na altura do problema, as conexões do trajeto da mobilidade podem ser consideradas como sendo criado como a “intra-relação” do ASA, que está distribuindo os pacotes para trás para fora a mesma interface interna que chegaram sobre:

```
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#
```

O valor-limite da mobilidade em 10.10.1.2 continua a enviar o tráfego destinado a 10.10.9.3, que combina estas conexões existentes. Mesmo se a relação do dmz era progredir ao estado up/up, o tráfego da mobilidade originado de 10.10.1.2 combinaria as conexões existentes na tabela (em

vez de construir uma nova conexão à relação do dmz) que restaura o intervalo das conexões no ASA, que prolonga o problema.

Em resumo, estes eventos podem provocar a edição:

1. O dispositivo em 10.10.1.2 envia um protocolo 97 ou o pacote de UDP a 10.10.9.3.
2. O ASA recebe o pacote na interface interna, mas a relação do dmz está para baixo, que conduz à rota mais específica à rede de destino que falta da tabela de roteamento. Desde que o **comando intra-interface da licença da mesmo-Segurança** é permitido no ASA, segue uma rota estática configurada para a rede 10.0.0.0/8 para trás através da interface interna, constrói uma conexão na tabela de conexão, e envia então ao pacote para trás para fora a interface interna para a rede interna.
3. Em algum momento a relação do dmz pôde vir apoio e a rota é adicionada de volta à tabela; contudo, desde que a conexão para o tráfego do protocolo 97 foi construída já na etapa #2, os pacotes subsequente combinarão a conexão e a tabela de roteamento overwritten, e o tráfego não alcança o server no dmz.

## Solução

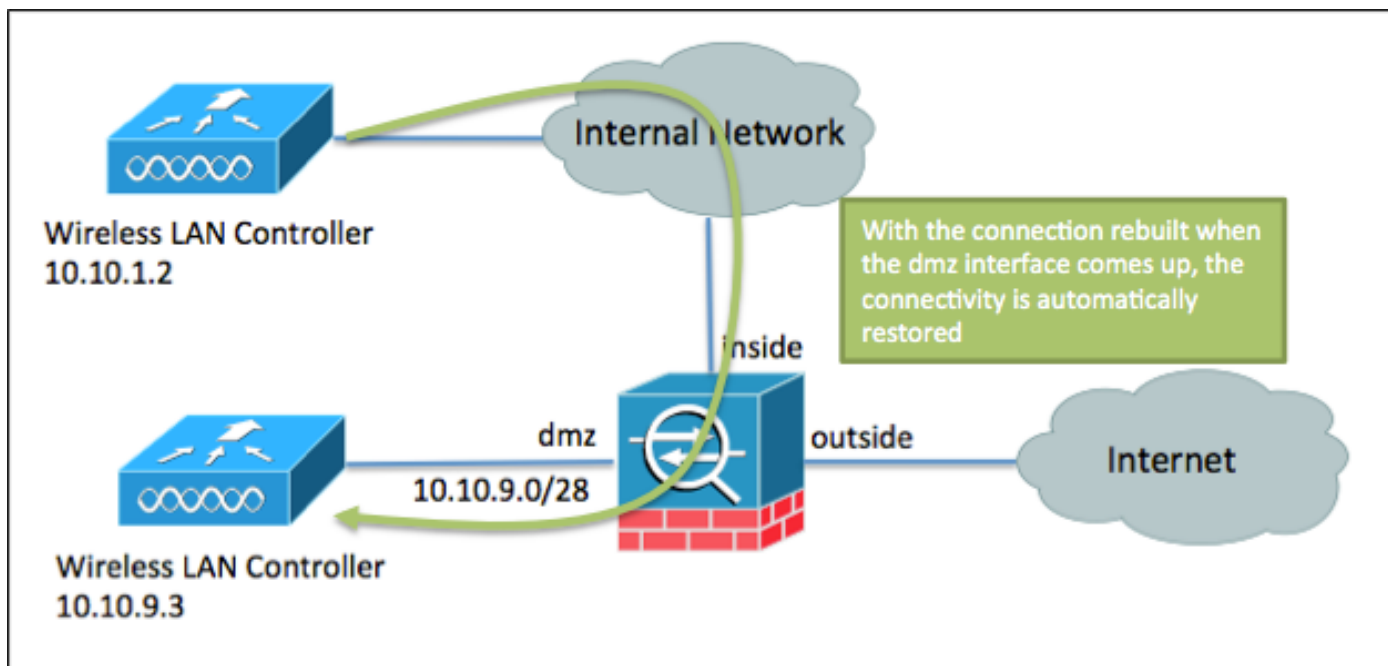
### Solução 1

Uma solução possível para esta edição é remover o **comando intra-interface da licença da mesmo-Segurança** do ASA. Esta solução impede a conexão da inversão de marcha esteja construída para trás para fora a mesma relação em que o pacote original foi recebido, que permite que a conexão correta seja construída quando a relação vem acima. Contudo, segundo a tabela de roteamento do ASA, esta solução não pôde trabalhar (o tráfego pôde ser distribuído a uma outra relação a não ser o destino pretendido baseado na tabela de roteamento), e o **comando intra-interface da licença da mesmo-Segurança** pôde ser necessário para outras conexões no ASA.

### Solução 2

Para este exemplo específico, o problema foi abrandado com sucesso permitindo a característica do **intervalo flutuar-CONN**. Esta característica, que não é permitida à revelia, fez com que o ASA rasgasse para baixo estas conexões um minuto depois que mais rota preferida a um dos valores-limite é adicionada à tabela de roteamento para fora uma relação nova do ASA, que ocorre quando a relação do dmz vem acima. As conexões são reconstruídas então imediatamente quando o próximo pacote chega no ASA, usando a relação mais preferida (dmz, em vez do interior para o host de 10.10.9.3).

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



Quando o problema é abrandado, as conexões corretas estão construídas na tabela de conexão ASA e a Conectividade é restaurada automaticamente:

```
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#
```

## Informações Relacionadas

- [Referência de comandos ASA 9.1 - comando do intervalo flutuar-CONN](#)
- [Suporte Técnico e Documentação - Cisco Systems](#)