

A customer had a hardware failure the other day and I went and replaced the router. It was an ISR4231 and was running Zone Based Firewall. I originally had set this router up so I know at one time everything was working. After the replacement, we were getting one-way audio (PSTN connection via FXO). We had this problem initially, but the fix was not well documented in the TAC case. However if I removed the ZBF then audio would work in both directions. I rebuilt the firewall from scratch allowing SIP, RTP, etc but audio was still being blocked. I had but all interfaces in the same zone (INSIDE) except for the internet connection. This is supposed to allow all communications between interfaces in the same zone, but no bueno. Added it to the self zone but that didn't make a difference either. In doing some research I found that you can also create a 'default' zone.

From the Security Configuration Guide: Traffic from a zone interface to a nonzone interface or from a nonzone interface to a zone interface is always dropped; unless default zones are enabled (default zone is a nonzone interface).

I think I'm starting to get it. What if I only have one zone (OUTSIDE) and all the others are in the default zone?? That works. I still don't know why/where the audio was being blocked, but not having the internal interfaces in a zone fixed the issue. You have to manually add the default zone in the firewall config!

```
ROUTER(config-if)#zone-member security ?  
  self  System defined Zone
```

```
ROUTER(config)#zone security ?  
  WORD  Name of security zone
```

```
ROUTER(config)#zone security default ?  
  <cr>
```

```
ROUTER(config)#zone security default
```

```
ROUTER(config-sec-zone)#?
```

Zone configuration commands:

```
  description  Zone description  
  exit         Exit from zone configuration mode  
  no          Negate or set default values of a command
```

```
ROUTER(config-sec-zone)#descr DEFAULT ZONE - NO POLICY
```

```
ROUTER(config-sec-zone)#exit
```

```
ROUTER(config)#interface gi0/0
```

```
ROUTER(config-if)#zone-member security ?
  default  DEFAULT ZONE - NO POLICY
  self     System defined Zone

ROUTER(config-if)#zone-member security default
ROUTER(config-if)#end
ROUTER#show zone security default
zone default
  Description: DEFAULT ZONE - NO POLICY
  Member Interfaces:
  GigabitEthernet0/0
```