pfSense - Bug #11338

WireGuard cannot connect to an IPv6 endpoint

01/29/2021 12:50 PM - Jim Pingle

Status:	Resolved	**Start date:**	01/29/2021
Priority:	Normal	**Due date:**	
Assignee:	Peter Grehan	**% Done:**	0%
Category:	WireGuard	**Estimated time:**	0.00 hour
Target version:	2.5.0		
Plus Target Version:		**Affected Version:**	2.5.x
Release Notes:	Default	**Affected Architecture:**	

Description

WireGuard won't connect if using an IPv6 endpoint address on either end.

The IPv6 address in the config file doesn't have brackets around it when it should.

Even with a properly formatted Endpoint line in the configuration file, however, the wg command doesn't show the endpoint as being configured.

I have a commit ready to fix the formatting issue, but the parsing issue still needs attention.

Associated revisions

Revision f32e1438 - 01/29/2021 12:54 PM - Jim Pingle

Add brackets around IPv6 endpoint address. Issue #11338

History

#1 - 01/29/2021 01:03 PM - Jim Pingle

- Subject changed from WireGuard doesn't parse an IPv6 endpoint address to WireGuard cannot connect to an IPv6 endpoint

Sample config, after my config file fix:

```
: cat /etc/wg/wg0.conf
# This WireGuard config file has been created automatically. Do not edit!
# Description: Tunnel to B

[Interface]
PrivateKey = <key>
ListenPort = 51820

# Peer: B
[Peer]
PublicKey = SKZza23ibQOb6iiUMQeXFKkzvzRnyftAKKru08BO2wM=
EndPoint = [2001:db8::21]:51820
AllowedIPs = 2001:db8:1:df25::2/128, 2001:db8:1:df10::/64
```

wg output which is lacking a peer endpoint:

```
: wg
interface: wg0
  public key: +jKgI1Y8DAWMEobY0n7PtBx9lm9oOv00FHAS5v7cRmQ=
  private key: (hidden)
  listening port: 51820

peer: SKZza23ibQOb6iiUMQeXFKkzvzRnyftAKKru08BO2wM=
  allowed ips: 2001:db8:1:df10::/64, 2001:db8:1:df25::2/128
```

If I switch it to an IPv4 endpoint it works OK. So either the wg utility is failing to parse it or it's getting lost somewhere deeper

#2 - 01/29/2021 03:30 PM - Scott Long

- Assignee set to Steve Beaver

#3 - 01/29/2021 03:39 PM - Scott Long

- Assignee changed from Steve Beaver to Peter Grehan

#4 - 01/29/2021 11:17 PM - Viktor Gurov

- Status changed from New to Feedback

#5 - 01/30/2021 01:08 AM - Viktor Gurov

- Status changed from Feedback to New

#6 - 01/30/2021 02:48 AM - Peter Grehan

Took a while to set this up, but I can get a repro with an OpenBSD client.

Tunnel traffic is being delivered to wg, but it is failing with "wg0: Invalid handshake initiation" which indicates an error returned from the noise_consume_initiation() routine.

(as an aside, I tested IPv6 over an IPv4 tunnel, which worked fine other than a minor error in tcpdump rx which I'll checkin).

#7 - 01/31/2021 12:43 AM - Peter Grehan

The above wasn't correct: just another misconfiguration :(

There are a number of issues, all boiling down to "struct sockaddr" being smaller than "struct sockaddr_in6", resulting in addresses being truncated or size checks failing.

The first issue was in kernel code in wg_input(), where the UDP source address was being copied to a struct sockaddr. In the v6 case, this was resulting in the address being truncated, and an incorrect address being used to reply to the sender. This would result in the initial handshake never succeeding, and no date being sent over the tunnel.

Once this was fixed, a wildcard endpoint (OpenBSD) was able to communicate with v4 traffic over a v6 tunnel.

The next issue was a combination of sockaddr vs sockaddr_in6 issues in both the kernel's handling of the WG_SET/GET ioctls, and also code in the wg utility. Once these were fixed, v6 endpoints could be configured and also displayed correctly.

```
[21.02-DEVELOPMENT][admin@pfSense.home.arpa]/root: wg
interface: wg0
  public key: 0XsS9biScR0S6/DLVYRv0yON3R53TplDQzgW9Y8ZNE4=
  private key: (hidden)
  listening port: 51820

peer: p4zVA9wYwWorvuYoQ96xqSK1/V4FtqxaH+InRaG8/0A=
  endpoint: [2001:f00:f00b::129]:51821
  allowed ips: 2001:f00:f00b::/64

peer: XJmG0uaQAs7DUVFxJDQhB36VdsH/zqJapPu3v4y9zig=
  endpoint: [fd87:afd:a3fd:181b::40]:51820
  allowed ips: 10.0.0.0/24

peer: pnYy/12d2WZGtPF/+usF8DgOl8DVvwHPk5kRra+MGhA=
  endpoint: 192.168.1.113:51820
  allowed ips: ::/0
```

#8 - 01/31/2021 01:00 AM - Peter Grehan

- File PR11338_if_wg.diff added

- File PR11338_wg_tools.diff added

if_wg.diff - kernel diff
wg_tools - wireguard_tools diff

#9 - 02/01/2021 06:39 AM - Renato Botelho

- Status changed from New to Feedback

Peter Grehan wrote:

> if_wg.diff - kernel diff
> wg_tools - wireguard_tools diff

I've imported both patches and they will be available on next round of snapshots

#10 - 02/02/2021 08:05 AM - Jim Pingle

- Status changed from Feedback to Resolved

Latest snapshot looks good!

```
: cat /etc/wg/wg0.conf
# This WireGuard config file has been created automatically. Do not edit!
# Description: Tunnel to B

[Interface]
PrivateKey = <key>
ListenPort = 51820

# Peer: B
[Peer]
PublicKey = SKZza23ibQOb6iiUMQeXFKkzvzRnyftAKKru08BO2wM=
EndPoint = [2001:db8::21]:51820
AllowedIPs = 10.8.210.2/32, 10.21.0.0/24, 2001:db8:1:df25::2/128, 2001:db8:1:df10::/64
```

```
: wg
interface: wg0
  public key: +jKgI1Y8DAWMEobY0n7PtBx9lm9oOv00FHAS5v7cRmQ=
  private key: (hidden)
  listening port: 51820

peer: SKZza23ibQOb6iiUMQeXFKkzvzRnyftAKKru08BO2wM=
  endpoint: [2001:db8::21]:51820
  allowed ips: 2001:db8:1:df10::/64, 2001:db8:1:df25::2/128, 10.21.0.0/24, 10.8.210.2/32
```

```
: ping -S 10.8.210.1 10.8.210.2
PING 10.8.210.2 (10.8.210.2) from 10.8.210.1: 56 data bytes
64 bytes from 10.8.210.2: icmp_seq=0 ttl=64 time=0.854 ms
```

```
64 bytes from 10.8.210.2: icmp_seq=1 ttl=64 time=0.532 ms
```

```
: pfctl -ss | grep 51820
mvneta2 udp 2001:db8::8[51820] -> 2001:db8::21[51820]       MULTIPLE:MULTIPLE
```

Thanks!

Files

PR11338_wg_tools.diff	1.61 KB	01/31/2021	Peter Grehan
PR11338_if_wg.diff	2.17 KB	01/31/2021	Peter Grehan