pfSense - Bug #6937

Inbound traffic on enc0 is not creating a state with mobile IPsec

11/16/2016 08:47 AM - Jim Pingle

Status:	Resolved	**Start date:**	11/16/2016
Priority:	Very High	**Due date:**	
Assignee:	Luiz Souza	**% Done:**	0%
Category:	IPsec	**Estimated time:**	0.00 hour
Target version:	2.4.0		
Affected Version:	2.4	**Affected Architecture:**	All

Description

Traffic entering enc0 on 2.4 is not creating a state, thus TCP traffic will not pass. ICMP works as the return traffic will create a state outbound.

History

#1 - 11/16/2016 08:47 AM - Jim Pingle

- Status changed from New to Confirmed

#2 - 11/18/2016 02:15 PM - Renato Botelho

- Assignee set to Luiz Souza

#3 - 12/01/2016 11:48 AM - Jim Pingle

- Subject changed from Inbound traffic on enc0 is not creating a state to Inbound traffic on enc0 is not creating a state with mobile IPsec

After some more testing this appears to be a problem only with mobile IPsec, specifically (at least) IKEv2 EAP-RADIUS.

A site-to-site IPsec connection using IKEv1 or IKEv2 does not have the same problem, states are created properly.

A ping from a mobile IPsec client (10.7.200.1) to the firewall LAN (10.7.0.1) produces only this in the firewall states table:

```
enc0 icmp 10.7.0.1:1 -> 10.7.200.1:1       0:0
   age 00:00:03, expires in 00:00:09, 3:0 pkts, 180:0 bytes, rule 88
   id: 00000000583e4bc5 creatorid: b95c5943
```

As you can see, that is in the "wrong" direction as it's the ICMP reply creating the state and not the original message from the client.

Attempting a TCP connection from the client to the server fails because TCP cannot create a state with a reply, instead, the dropped traffic shows in the firewall log:

```
Dec  1 12:46:32 block enc0 TCP:SA 10.7.0.1:443 10.7.200.1:50124
```

```
Dec  1 12:47:02 shona filterlog: 6,16777216,,1000000104,enc0,match,block,out,4,0x0,,64,0,0,DF,6,tcp,48,10.7.0.1,10.7.200.1,443,50132,0,SA,1687100934,2626059616,65228,,mss;sackOK;eol
```

#4 - 01/11/2017 10:42 PM - Jun Wang

Found the same problem on a 2 weeks old SG-1000. Kinda annoying since mobile ipsec is the reason I bought it.

#5 - 01/12/2017 10:11 AM - Vladimir Putin

Please read this https://forum.pfsense.org/index.php?topic=117827

#6 - 02/06/2017 02:07 PM - Luiz Souza

- Status changed from Confirmed to Feedback

Jimp, can you check the latest build ?

Relevant commit: https://github.com/pfsense/FreeBSD-src/commit/5d8a65f506d84b404e56a14febffd9c19e3967ac

#7 - 02/06/2017 03:27 PM - Jim Pingle

No change on the latest snap built after that commit.

#8 - 02/13/2017 09:20 AM - Jim Pingle

- Status changed from Feedback to Assigned

#9 - 03/03/2017 10:53 PM - Luiz Souza

- Status changed from Assigned to Feedback

New changes were made to handle this issue. Waiting on JimP comments.

#10 - 03/04/2017 05:11 PM - Jim Pingle

- Status changed from Feedback to Resolved

Works great on the latest snapshot, thanks!