pfSense - Bug #8765

Per-user firewall rules for IPsec do not work

08/07/2018 03:39 PM - Jim Pingle

Status:	Resolved	**Start date:**	08/07/2018
Priority:	Normal	**Due date:**	
Assignee:	Jim Pingle	**% Done:**	100%
Category:	IPsec	**Estimated time:**	0.00 hour
Target version:	2.4.4		
Affected Version:	All	**Affected Architecture:**	All

Description

The IPsec attribute code which processes firewall rules passed back through authentication is missing spaces, causing it to form invalid rules.

Fixed by PR https://github.com/pfsense/pfsense/pull/3942 which was merged a while ago

History

#1 - 09/21/2018 01:11 PM - Jim Pingle

- Status changed from Feedback to Resolved

- Assignee set to Jim Pingle

Looks good.

Added this to RADIUS user reply attributes:

```
Cisco-AVPair = "ip:inacl#1=permit tcp any any",
Cisco-AVPair += "ip:outacl#1=permit tcp any any"
```

Connected to an xauth mobile VPN (rules won't work with EAP, different auth mechanism in strongSwan).

Rules file looks OK:

```
: cat ipsec_86068river.rules
pass in quick on enc0 proto tcp from any to any no state
pass out quick on enc0 proto tcp from any to any no state
```

pf loaded the rules OK:

```
: pfSsh.php playback pfanchordrill
[...]
ipsec rules/nat contents:

ipsec/river rules/nat contents:
pass in quick on enc0 proto tcp all no state
pass out quick on enc0 proto tcp all no state
[...]
```