pfSense - Feature #7072

vpn_openvpn_server.php / vpn_openvpn_client.php : Add controls to OpenVPN for Negotiable Crypto Parameters

01/03/2017 09:56 AM - Jim Pingle

Status:	Resolved	**Start date:**	01/03/2017
Priority:	Normal	**Due date:**	
Assignee:	Jim Pingle	**% Done:**	90%
Category:	OpenVPN	**Estimated time:**	0.00 hour
Target version:	2.4.0		

Description

OpenVPN 2.4 automatically attempts to negotiate crypto between the client and server, due to this, the tunnel can end up using an unexpected algorithm. For example, if both sides are set to AES-256-CBC but both client and server support AES-256-GCM, they will use AES-256-GCM instead of what was chosen. In cases for older clients, it will accept any that match the chosen cipher or from the list of negotiable ciphers.

- Need to add a multi-select box (reorderable?) of ciphers for --ncp-ciphers
  - Possible choices are the same as the 'crypto' gui option, the list is provided by openvpn_get_cipherlist()
  - Order of the list is important, as it determines the preference for what the server/client will try
  - In the config, this ends up a colon-separated string
- Need to add a checkbox for --ncp-disable to disable NCP

Info from the man page:

```
              For servers, the first cipher from cipher_list will be pushed to
              clients that support cipher negotiation.

              Cipher negotiation is enabled in client-server mode only.  I.e.
              if --mode is set to 'server' (server-side, implied by setting
              --server ), or if --pull is specified (client-side, implied by
              setting --client).

              If both peers support and do not disable NCP, the negotiated
              cipher will override the cipher specified by --cipher.

              Additionally, to allow for more smooth transition, if NCP is
              enabled, OpenVPN will inherit the cipher of the peer if that
              cipher is different from the local --cipher setting, but the
              peer cipher is one of the ciphers specified in --ncp-ciphers.
              E.g. a non-NCP client (<=2.3, or with --ncp-disabled set)
              connecting to a NCP server (2.4+) with "--cipher BF-CBC" and
              "--ncp-ciphers AES-256-GCM:AES-256-CBC" set can either specify
              "--cipher BF-CBC" or "--cipher AES-256-CBC" and both will work.
```

If the multi-select part is not feasible, we at least need the checkbox to allow users to avoid unexpected surprises. The ncp-ciphers list could be handled via advanced options.

Talked to sbeaver, we don't yet have a control that would handle the ordered multi-select, but there are several potential areas where it could be used (auth server selection on OpenVPN could use it, too, and if we add a --tls-ciphers control)

Associated revisions

Revision c73367d2 - 01/04/2017 12:57 PM - Jim Pingle

Add backend support to OpenVPN for NCP. Ticket #7072

Revision d66cfa3d - 01/04/2017 01:10 PM - Jim Pingle

Validate the submitted Encryption Algorithm and NCP Algorithm list. Ticket #7072

Revision 9423ff32 - 01/04/2017 01:45 PM - Jim Pingle

Whitespace fixes. Ticket #7072

Revision fa351dd3 - 01/04/2017 01:45 PM - Jim Pingle

Add NCP options to OpenVPN client. Fixes #7072

Revision e2f0ad13 - 01/04/2017 02:28 PM - Jim Pingle

Some improvements to the NCP validation. Ticket #7072

Revision 625b688c - 01/04/2017 02:35 PM - Jim Pingle

Fix NCP breaking save on a new server/client. Ticket #7072

History

#1 - 01/04/2017 01:12 PM - Jim Pingle

See also:

- bd07fbdb4b81fc358b8fa55b06469dde7a3870df
- 6c00adf3316d2c5214f7e9cf2e5f138c32845d58
- 9d773c1792832948a119068434b76d1fd8e5bfb0

#2 - 01/04/2017 01:47 PM - Jim Pingle

- Assignee changed from Steve Beaver to Jim Pingle

#3 - 01/04/2017 01:50 PM - Jim Pingle

- Status changed from Assigned to Feedback

- % Done changed from 0 to 100

Applied in changeset fa351dd3c13e65dfabfb0f2ac2ed72b332276892.

#4 - 01/04/2017 03:38 PM - Jim Pingle

- Status changed from Feedback to Assigned

- Assignee changed from Jim Pingle to Steve Beaver

- % Done changed from 100 to 90

There's one little problem left with the NCP list control. Clicking in empty area on the right side adds a "null" entry when it shouldn't.

#5 - 01/04/2017 04:26 PM - Steve Beaver

- Status changed from Assigned to Feedback

- Assignee changed from Steve Beaver to Jim Pingle

Fixed

#6 - 01/04/2017 06:22 PM - Jim Pingle

- Status changed from Feedback to Resolved

Looks good