strongSwan - Issue #796

TNC EAP Config Failing to Authenticate with Android StrongSwan Client.

22.12.2014 02:22 - Jim Smith

Status:	Closed		
Priority:	Normal		
Assignee:	Andreas Steffen		
Category:	android		
Affected version:	5.2.1	**Resolution:**	No feedback

Description

We use your product currently but have only recently attempted to enable TNC Server. Was recompiled with modules and modules load. Subject Distinguished Name and Subject Alternative Names correct in Keys. We are getting this error: INFORMATIONAL request 13 [N(AUTH_FAILED)]. Any guidance would be greatly appreciated.

Logs and Configs Below:

Dec 21 19:50:41 Web1-001 charon: 10[ENC] parsed IKE_SA_INIT request 0 [SA KE No N(NATD_S_IP) N(NATD_D_IP) N((16430))]
Dec 21 19:50:41 Web1-001 charon: 10[IKE] 72.205.223.155 is initiating an IKE_SA
Dec 21 19:50:41 Web1-001 charon: 10[IKE] local host is behind NAT, sending keep alives
Dec 21 19:50:41 Web1-001 charon: 10[IKE] remote host is behind NAT
Dec 21 19:50:41 Web1-001 charon: 10[ENC] generating IKE_SA_INIT response 0 [SA KE No N(NATD_S_IP) N(NATD_D_IP)]
Dec 21 19:50:41 Web1-001 charon: 10[NET] sending packet: from 192.168.10.100[500] to 72.205.223.155[35493] (432 bytes)
Dec 21 19:50:41 Web1-001 charon: 12[NET] received packet: from 72.205.223.155[47396] to 192.168.10.100[4500] (540 bytes)
Dec 21 19:50:41 Web1-001 charon: 12[ENC] parsed IKE_AUTH request 1 [IDi N(INIT_CONTACT) CERTREQ CPRQ N(ESP_TFC_PAD_N) SA TSi TSr N(MOBIKE_SUP) N(NO_ADD_ADDR) N(EAP_ONLY)]
Dec 21 19:50:41 Web1-001 charon: 12[IKE] received cert request for "C=CH, O=strongSwan, CN=strongSwan Root CA"
Dec 21 19:50:41 Web1-001 charon: 12[CFG] looking for peer configs matching 192.168.10.100[%any]...72.205.223.155[alexander@mydomain.org]
Dec 21 19:50:41 Web1-001 charon: 12[CFG] selected peer config 'rw-allow'
Dec 21 19:50:41 Web1-001 charon: 12[IKE] initiating EAP_TTLS method (id 0x06)
Dec 21 19:50:41 Web1-001 charon: 12[IKE] received ESP_TFC_PADDING_NOT_SUPPORTED, not using ESPv3 TFC padding
Dec 21 19:50:41 Web1-001 charon: 12[IKE] peer supports MOBIKE
Dec 21 19:50:41 Web1-001 charon: 12[ENC] generating IKE_AUTH response 1 [IDr EAP/REQ/TTLS]
Dec 21 19:50:41 Web1-001 charon: 12[NET] sending packet: from 192.168.10.100[4500] to 72.205.223.155[47396] (108 bytes)
Dec 21 19:50:41 Web1-001 charon: 14[NET] received packet: from 72.205.223.155[47396] to 192.168.10.100[4500] (268 bytes)
Dec 21 19:50:41 Web1-001 charon: 14[ENC] parsed IKE_AUTH request 2 [EAP/RES/TTLS]
Dec 21 19:50:41 Web1-001 charon: 14[TLS] negotiated TLS 1.2 using suite TLS_DHE_RSA_WITH_AES_128_CBC_SHA
Dec 21 19:50:41 Web1-001 charon: 14[TLS] sending TLS server certificate 'C=CH, O=strongSwan, CN=mydomain.org'
Dec 21 19:50:41 Web1-001 charon: 14[TLS] sending TLS cert request for 'C=CH, O=strongSwan, CN=strongSwan Root CA'
Dec 21 19:50:41 Web1-001 charon: 14[ENC] generating IKE_AUTH response 2 [EAP/REQ/TTLS]
Dec 21 19:50:41 Web1-001 charon: 14[NET] sending packet: from 192.168.10.100[4500] to 72.205.223.155[47396] (1100 bytes)
Dec 21 19:50:41 Web1-001 charon: 16[NET] received packet: from 72.205.223.155[47396] to 192.168.10.100[4500] (76 bytes)
Dec 21 19:50:41 Web1-001 charon: 16[ENC] parsed IKE_AUTH request 3 [EAP/RES/TTLS]
Dec 21 19:50:41 Web1-001 charon: 16[ENC] generating IKE_AUTH response 3 [EAP/REQ/TTLS]
Dec 21 19:50:41 Web1-001 charon: 16[NET] sending packet: from 192.168.10.100[4500] to 72.205.223.155[47396] (1100 bytes)
Dec 21 19:50:41 Web1-001 charon: 06[NET] received packet: from 72.205.223.155[47396] to 192.168.10.100[4500] (76 bytes)
Dec 21 19:50:41 Web1-001 charon: 06[ENC] parsed IKE_AUTH request 4 [EAP/RES/TTLS]
Dec 21 19:50:41 Web1-001 charon: 06[ENC] generating IKE_AUTH response 4 [EAP/REQ/TTLS]
Dec 21 19:50:41 Web1-001 charon: 06[NET] sending packet: from 192.168.10.100[4500] to 72.205.223.155[47396] (140 bytes)
Dec 21 19:50:41 Web1-001 charon: 08[NET] received packet: from 72.205.223.155[47396] to 192.168.10.100[4500] (428 bytes)
Dec 21 19:50:41 Web1-001 charon: 08[ENC] parsed IKE_AUTH request 5 [EAP/RES/TTLS]
Dec 21 19:50:41 Web1-001 charon: 08[IKE] sending tunneled EAP-TTLS AVP [EAP/REQ/ID]
Dec 21 19:50:41 Web1-001 charon: 08[ENC] generating IKE_AUTH response 5 [EAP/REQ/TTLS]
Dec 21 19:50:41 Web1-001 charon: 08[NET] sending packet: from 192.168.10.100[4500] to 72.205.223.155[47396] (220 bytes)
Dec 21 19:50:42 Web1-001 charon: 04[NET] received packet: from 72.205.223.155[47396] to 192.168.10.100[4500] (188 bytes)
Dec 21 19:50:42 Web1-001 charon: 04[ENC] parsed IKE_AUTH request 6 [EAP/RES/TTLS]
Dec 21 19:50:42 Web1-001 charon: 04[IKE] received tunneled EAP-TTLS AVP [EAP/RES/ID]
Dec 21 19:50:42 Web1-001 charon: 04[IKE] received EAP identity 'alexander@mydomain.org'
Dec 21 19:50:42 Web1-001 charon: 04[IKE] phase2 method EAP_MD5 selected
Dec 21 19:50:42 Web1-001 charon: 04[IKE] sending tunneled EAP-TTLS AVP [EAP/REQ/MD5]
Dec 21 19:50:42 Web1-001 charon: 04[ENC] generating IKE_AUTH response 6 [EAP/REQ/TTLS]

Dec 21 19:50:42 Web1-001 charon: 04[NET] sending packet: from 192.168.10.100[4500] to 72.205.223.155[47396] (172 bytes)
Dec 21 19:50:42 Web1-001 charon: 02[NET] received packet: from 72.205.223.155[47396] to 192.168.10.100[4500] (172 bytes)
Dec 21 19:50:42 Web1-001 charon: 02[ENC] parsed IKE_AUTH request 7 [EAP/RES/TTLS]
Dec 21 19:50:42 Web1-001 charon: 02[IKE] received tunneled EAP-TTLS AVP [EAP/RES/MD5]
Dec 21 19:50:42 Web1-001 charon: 02[IKE] EAP_TTLS phase2 authentication of 'alexander@mydomain.org' with EAP_MD5 successful
Dec 21 19:50:42 Web1-001 charon: 02[IKE] phase2 method EAP_PT_EAP selected
Dec 21 19:50:42 Web1-001 charon: 02[IKE] sending tunneled EAP-TTLS AVP [EAP/REQ/PT]
Dec 21 19:50:42 Web1-001 charon: 02[ENC] generating IKE_AUTH response 7 [EAP/REQ/TTLS]
Dec 21 19:50:42 Web1-001 charon: 02[NET] sending packet: from 192.168.10.100[4500] to 72.205.223.155[47396] (156 bytes)
Dec 21 19:50:42 Web1-001 charon: 15[NET] received packet: from 72.205.223.155[47396] to 192.168.10.100[4500] (316 bytes)
Dec 21 19:50:42 Web1-001 charon: 15[ENC] parsed IKE_AUTH request 8 [EAP/RES/TTLS]
Dec 21 19:50:42 Web1-001 charon: 15[IKE] received tunneled EAP-TTLS AVP [EAP/RES/PT]
Dec 21 19:50:42 Web1-001 charon: 15[TNC] assigned TNCCS Connection ID 1
Dec 21 19:50:42 Web1-001 charon: 15[IMV] IMV 1 "Test" created a state for IF-TNCCS 2.0 Connection ID 1: +long +excl soh
Dec 21 19:50:42 Web1-001 charon: 15[IMV]   over IF-T for Tunneled EAP 2.0 with maximum PA-TNC message size of 65490 bytes
Dec 21 19:50:42 Web1-001 charon: 15[IMV]   user AR identity 'alexander@mydomain.org' authenticated by password
Dec 21 19:50:42 Web1-001 charon: 15[IMV] IMV 2 "Scanner" created a state for IF-TNCCS 2.0 Connection ID 1: +long +excl soh
Dec 21 19:50:42 Web1-001 charon: 15[IMV]   over IF-T for Tunneled EAP 2.0 with maximum PA-TNC message size of 65490 bytes
Dec 21 19:50:42 Web1-001 charon: 15[IMV]   user AR identity 'alexander@mydomain.org' authenticated by password
Dec 21 19:50:42 Web1-001 charon: 15[IMV] IMV 1 "Test" changed state of Connection ID 1 to 'Handshake'
Dec 21 19:50:42 Web1-001 charon: 15[IMV] IMV 2 "Scanner" changed state of Connection ID 1 to 'Handshake'
Dec 21 19:50:42 Web1-001 charon: 15[TNC] received TNCCS batch (160 bytes) for Connection ID 1
Dec 21 19:50:42 Web1-001 charon: 15[TNC] => 160 bytes @ 0x7f8df0000bf6
Dec 21 19:50:42 Web1-001 charon: 15[TNC]   0: 02 00 00 01 00 00 00 A0 00 00 00 00 00 00 00 06 ....
Dec 21 19:50:42 Web1-001 charon: 15[TNC]   16: 00 00 00 1F 41 63 63 65 70 74 2D 4C 61 6E 67 75 ....Accept-Langu
Dec 21 19:50:42 Web1-001 charon: 15[TNC]   32: 61 67 65 3A 20 65 6E 80 00 00 00 00 00 00 01 00 age: en.........
Dec 21 19:50:42 Web1-001 charon: 15[TNC]   48: 00 00 79 00 00 00 00 00 00 00 01 00 01 FF FF 01 ..y.............
Dec 21 19:50:42 Web1-001 charon: 15[TNC]   64: 00 00 00 1B 4A 8E 39 00 00 00 00 00 00 00 02 00 ....J.9.........
Dec 21 19:50:42 Web1-001 charon: 15[TNC]   80: 00 00 18 00 2B 79 00 00 41 6E 64 72 6F 69 64 00 ....+y..Android.
Dec 21 19:50:42 Web1-001 charon: 15[TNC]   96: 00 00 00 00 00 00 00 04 00 00 00 25 05 34 2E 31 2E ....%.4.1.
Dec 21 19:50:42 Web1-001 charon: 15[TNC] 112: 32 11 4A 5A 4F 35 34 4B 2E 49 37 30 35 56 52 42 2.JZO54K.I705VRB
Dec 21 19:50:42 Web1-001 charon: 15[TNC] 128: 4D 49 31 00 00 00 00 90 2A 00 00 00 08 00 00 00 1C MI1.....*........
Dec 21 19:50:42 Web1-001 charon: 15[TNC] 144: 33 38 63 64 35 39 38 61 37 62 30 37 33 36 37 35 38cd598a7b073675
Dec 21 19:50:42 Web1-001 charon: 15[TNC] PB-TNC state transition from 'Init' to 'Server Working'
Dec 21 19:50:42 Web1-001 charon: 15[TNC] processing PB-TNC CDATA batch
Dec 21 19:50:42 Web1-001 charon: 15[TNC] processing IETF/PB-Language-Preference message (31 bytes)
Dec 21 19:50:42 Web1-001 charon: 15[TNC] processing IETF/PB-PA message (121 bytes)
Dec 21 19:50:42 Web1-001 charon: 15[TNC] setting language preference to 'en'
Dec 21 19:50:42 Web1-001 charon: 15[TNC] handling PB-PA message type 'IETF/Operating System' 0x000000/0x00000001
Dec 21 19:50:42 Web1-001 charon: 15[TNC] message type 0x000000/0x00000001 not supported by any IMV
Dec 21 19:50:42 Web1-001 charon: 15[IMV] no workitems available - no evaluation possible
Dec 21 19:50:42 Web1-001 charon: 15[TNC] creating PA-TNC message with ID 0xfd26399d
Dec 21 19:50:42 Web1-001 charon: 15[TNC] creating PA-TNC attribute type 'IETF/Assessment Result' 0x000000/0x00000009
Dec 21 19:50:42 Web1-001 charon: 15[TNC] => 4 bytes @ 0x7f8df0004ac0
Dec 21 19:50:42 Web1-001 charon: 15[TNC]   0: 00 00 00 04   ....
Dec 21 19:50:42 Web1-001 charon: 15[IMV] created PA-TNC message: => 24 bytes @ 0x7f8df0004dc0
Dec 21 19:50:42 Web1-001 charon: 15[IMV]   0: 01 00 00 00 FD 26 39 9D 00 00 00 00 00 00 00 09 .....&9.........
Dec 21 19:50:42 Web1-001 charon: 15[IMV]   16: 00 00 00 10 00 00 00 04   ....
Dec 21 19:50:42 Web1-001 charon: 15[TNC] creating PB-PA message type 'IETF/VPN' 0x000000/0x00000007
Dec 21 19:50:42 Web1-001 charon: 15[TNC] IMV 2 provides recommendation 'allow' and evaluation 'don't know'
Dec 21 19:50:42 Web1-001 charon: 15[TNC] PB-TNC state transition from 'Server Working' to 'Client Working'
Dec 21 19:50:42 Web1-001 charon: 15[TNC] creating PB-TNC SDATA batch
Dec 21 19:50:42 Web1-001 charon: 15[TNC] adding IETF/PB-PA message
Dec 21 19:50:42 Web1-001 charon: 15[TNC] sending PB-TNC SDATA batch (56 bytes) for Connection ID 1
Dec 21 19:50:42 Web1-001 charon: 15[TNC] => 56 bytes @ 0x7f8df00047c0
Dec 21 19:50:42 Web1-001 charon: 15[TNC]   0: 02 80 00 02 00 00 00 38 80 00 00 00 00 00 00 01 ....8........
Dec 21 19:50:42 Web1-001 charon: 15[TNC]   16: 00 00 00 30 00 00 00 00 00 00 00 07 FF FF 00 02 ...0............
Dec 21 19:50:42 Web1-001 charon: 15[TNC]   32: 01 00 00 00 FD 26 39 9D 00 00 00 00 00 00 00 09 .....&9.........
Dec 21 19:50:42 Web1-001 charon: 15[TNC]   48: 00 00 00 10 00 00 00 04   ....
Dec 21 19:50:42 Web1-001 charon: 15[IKE] sending tunneled EAP-TTLS AVP [EAP/REQ/PT]
Dec 21 19:50:42 Web1-001 charon: 15[ENC] generating IKE_AUTH response 8 [EAP/REQ/TTLS]
Dec 21 19:50:42 Web1-001 charon: 15[NET] sending packet: from 192.168.10.100[4500] to 72.205.223.155[47396] (204 bytes)
Dec 21 19:50:42 Web1-001 charon: 05[NET] received packet: from 72.205.223.155[47396] to 192.168.10.100[4500] (156 bytes)
Dec 21 19:50:42 Web1-001 charon: 05[ENC] parsed IKE_AUTH request 9 [EAP/RES/TTLS]
Dec 21 19:50:42 Web1-001 charon: 05[IKE] received tunneled EAP-TTLS AVP [EAP/RES/PT]
Dec 21 19:50:42 Web1-001 charon: 05[TNC] received TNCCS batch (8 bytes) for Connection ID 1

Dec 21 19:50:42 Web1-001 charon: 05[TNC] => 8 bytes @0x7f8dc80009e6
Dec 21 19:50:42 Web1-001 charon: 05[TNC] 0: 02 00 00 01 00 00 00 08 ....
Dec 21 19:50:42 Web1-001 charon: 05[TNC] PB-TNC state transition from 'Client Working' to 'Server Working'
Dec 21 19:50:42 Web1-001 charon: 05[TNC] processing PB-TNC CDATA batch
Dec 21 19:50:42 Web1-001 charon: 05[TNC] received empty PB-TNC CDATA batch
Dec 21 19:50:42 Web1-001 charon: 05[TNC] IMV 1 is setting reason string to 'IMC Test was not configured with "command = allow"'
Dec 21 19:50:42 Web1-001 charon: 05[TNC] IMV 1 is setting reason language to 'en'
Dec 21 19:50:42 Web1-001 charon: 05[TNC] IMV 1 provides recommendation 'no recommendation' and evaluation 'don't know'
Dec 21 19:50:42 Web1-001 charon: 05[TNC] IMV 2 provides recommendation 'allow' and evaluation 'don't know'
Dec 21 19:50:42 Web1-001 charon: 05[IMV] IMV 1 "Test" changed state of Connection ID 1 to 'Allowed'
Dec 21 19:50:42 Web1-001 charon: 05[IMV] IMV 2 "Scanner" changed state of Connection ID 1 to 'Allowed'
Dec 21 19:50:42 Web1-001 charon: 05[TNC] PB-TNC state transition from 'Server Working' to 'Decided'
Dec 21 19:50:42 Web1-001 charon: 05[TNC] creating PB-TNC RESULT batch
Dec 21 19:50:42 Web1-001 charon: 05[TNC] adding IETF/PB-Assessment-Result message
Dec 21 19:50:42 Web1-001 charon: 05[TNC] adding IETF/PB-Access-Recommendation message
Dec 21 19:50:42 Web1-001 charon: 05[TNC] adding IETF/PB-Reason-String message
Dec 21 19:50:42 Web1-001 charon: 05[TNC] sending PB-TNC RESULT batch (109 bytes) for Connection ID 1
Dec 21 19:50:42 Web1-001 charon: 05[TNC] => 109 bytes @0x7f8dc8001320
Dec 21 19:50:42 Web1-001 charon: 05[TNC] 0: 02 80 00 03 00 00 00 6D 80 00 00 00 00 00 00 02 ....m........
Dec 21 19:50:42 Web1-001 charon: 05[TNC] 16: 00 00 00 10 00 00 00 04 00 00 00 00 00 00 00 03 ....
Dec 21 19:50:42 Web1-001 charon: 05[TNC] 32: 00 00 00 10 00 00 00 01 00 00 00 00 00 00 00 07 ....
Dec 21 19:50:42 Web1-001 charon: 05[TNC] 48: 00 00 00 45 00 00 00 32 49 4D 43 20 54 65 73 74 ...E...2IMC Test
Dec 21 19:50:42 Web1-001 charon: 05[TNC] 64: 20 77 61 73 20 6E 6F 74 20 63 6F 6E 66 69 67 75 was not configu
Dec 21 19:50:42 Web1-001 charon: 05[TNC] 80: 72 65 64 20 77 69 74 68 20 22 63 6F 6D 6D 61 6E red with "comman
Dec 21 19:50:42 Web1-001 charon: 05[TNC] 96: 64 20 3D 20 61 6C 6C 6F 77 22 02 65 6E d = allow".en
Dec 21 19:50:42 Web1-001 charon: 05[IKE] sending tunneled EAP-TTLS AVP [EAP/REQ/PT]
Dec 21 19:50:42 Web1-001 charon: 05[ENC] generating IKE_AUTH response 9 [EAP/REQ/TTLS]
Dec 21 19:50:42 Web1-001 charon: 05[NET] sending packet: from 192.168.10.100[4500] to 72.205.223.155[47396] (268 bytes)
Dec 21 19:50:42 Web1-001 charon: 03[NET] received packet: from 72.205.223.155[47396] to 192.168.10.100[4500] (156 bytes)
Dec 21 19:50:42 Web1-001 charon: 03[ENC] parsed IKE_AUTH request 10 [EAP/RES/TTLS]
Dec 21 19:50:42 Web1-001 charon: 03[IKE] received tunneled EAP-TTLS AVP [EAP/RES/PT]
Dec 21 19:50:42 Web1-001 charon: 03[TNC] received TNCCS batch (8 bytes) for Connection ID 1
Dec 21 19:50:42 Web1-001 charon: 03[TNC] => 8 bytes @ 0x7f8dc4002df6
Dec 21 19:50:42 Web1-001 charon: 03[TNC] 0: 02 00 00 06 00 00 00 08 ....
Dec 21 19:50:42 Web1-001 charon: 03[TNC] PB-TNC state transition from 'Decided' to 'End'
Dec 21 19:50:42 Web1-001 charon: 03[TNC] processing PB-TNC CLOSE batch
Dec 21 19:50:42 Web1-001 charon: 03[TNC] final recommendation is 'allow' and evaluation is 'don't know'
Dec 21 19:50:42 Web1-001 charon: 03[TNC] policy enforced on peer 'alexander@mydomain.org' is 'allow'
Dec 21 19:50:42 Web1-001 charon: 03[TNC] policy enforcement point added group membership 'allow'
Dec 21 19:50:42 Web1-001 charon: 03[IKE] EAP_TTLS phase2 authentication of 'alexander@mydomain.org' with EAP_PT_EAP successful
Dec 21 19:50:42 Web1-001 charon: 03[IMV] IMV 1 "Test" deleted the state of Connection ID 1
Dec 21 19:50:42 Web1-001 charon: 03[IMV] IMV 2 "Scanner" deleted the state of Connection ID 1
Dec 21 19:50:42 Web1-001 charon: 03[TNC] removed TNCCS Connection ID 1
Dec 21 19:50:42 Web1-001 charon: 03[TLS] sending TLS close notify
Dec 21 19:50:42 Web1-001 charon: 03[ENC] generating IKE_AUTH response 10 [EAP/REQ/TTLS]
Dec 21 19:50:42 Web1-001 charon: 03[NET] sending packet: from 192.168.10.100[4500] to 72.205.223.155[47396] (140 bytes)
Dec 21 19:50:42 Web1-001 charon: 01[NET] received packet: from 72.205.223.155[47396] to 192.168.10.100[4500] (140 bytes)
Dec 21 19:50:42 Web1-001 charon: 01[ENC] parsed IKE_AUTH request 11 [EAP/RES/TTLS]
Dec 21 19:50:42 Web1-001 charon: 01[IKE] EAP method EAP_TTLS succeeded, MSK established
Dec 21 19:50:42 Web1-001 charon: 01[ENC] generating IKE_AUTH response 11 [EAP/SUCC]
Dec 21 19:50:42 Web1-001 charon: 01[NET] sending packet: from 192.168.10.100[4500] to 72.205.223.155[47396] (76 bytes)
Dec 21 19:50:42 Web1-001 charon: 10[NET] received packet: from 72.205.223.155[47396] to 192.168.10.100[4500] (92 bytes)
Dec 21 19:50:42 Web1-001 charon: 10[ENC] parsed IKE_AUTH request 12 [AUTH]
Dec 21 19:50:42 Web1-001 charon: 10[IKE] authentication of 'alexander@mydomain.org' with EAP successful
Dec 21 19:50:42 Web1-001 charon: 10[IKE] authentication of 'mydomain.org' (myself) with EAP
Dec 21 19:50:42 Web1-001 charon: 10[IKE] IKE_SA rw-allow[1] established between 192.168.10.100[mydomain.org]...72.205.223.155[alexander@mydomain.org]
Dec 21 19:50:42 Web1-001 charon: 10[IKE] scheduling reauthentication in 3414s
Dec 21 19:50:42 Web1-001 charon: 10[IKE] maximum IKE_SA lifetime 3594s
Dec 21 19:50:42 Web1-001 charon: 10[IKE] peer requested virtual IP %any
Dec 21 19:50:42 Web1-001 charon: 10[CFG] assigning new lease to 'alexander@mydomain.org'
Dec 21 19:50:42 Web1-001 charon: 10[IKE] assigning virtual IP 10.1.0.1 to peer 'alexander@mydomain.org'
Dec 21 19:50:42 Web1-001 charon: 10[IKE] peer requested virtual IP %any6
Dec 21 19:50:42 Web1-001 charon: 10[IKE] no virtual IP found for %any6 requested by 'alexander@mydomain.org'
Dec 21 19:50:42 Web1-001 charon: 10[IKE] CHILD_SA rw-allow{1} established with SPIs cf55285a_i 97806d5a_o and TS 10.1.0.0/28 === 10.1.0.1/32

~~Dec 21 19:50:42 Web1-001 vpn: + alexander@mydomain.org 10.1.0.1/32 72.205.223.155 -~~ 192.168.10.100 10.1.0.0/28
Dec 21 19:50:42 Web1-001 charon: 10[ENC] generating IKE_AUTH response 12 [AUTH CPRP SA TSi TSr N(AUTH_LFT) N(MOBIKE_SUP) N(NO_ADD_ADDR)]
Dec 21 19:50:42 Web1-001 charon: 10[NET] sending packet: from 192.168.10.100[4500] to 72.205.223.155[47396] (236 bytes)
Dec 21 19:50:42 Web1-001 charon: 12[NET] received packet: from 72.205.223.155[47396] to 192.168.10.100[4500] (76 bytes)
Dec 21 19:50:42 Web1-001 charon: 12[ENC] parsed INFORMATIONAL request 13 [N(AUTH_FAILED)]
Dec 21 19:50:42 Web1-001 charon: 12[IKE] received DELETE for IKE_SA rw-allow[1]
Dec 21 19:50:42 Web1-001 charon: 12[IKE] deleting IKE_SA rw-allow[1] between 192.168.10.100[mydomain.org]...72.205.223.155[alexander@mydomain.org]
Dec 21 19:50:42 Web1-001 charon: 12[IKE] IKE_SA deleted
Dec 21 19:50:42 Web1-001 vpn: - alexander@mydomain.org 10.1.0.1/32 72.205.223.155 -- 192.168.10.100 10.1.0.0/28
Dec 21 19:50:42 Web1-001 charon: 12[ENC] generating INFORMATIONAL response 13 [ ]
Dec 21 19:50:42 Web1-001 charon: 12[NET] sending packet: from 192.168.10.100[4500] to 72.205.223.155[47396] (76 bytes)
Dec 21 19:50:42 Web1-001 charon: 12[CFG] lease 10.1.0.1 by 'alexander@mydomain.org' went offline

1. /etc/ipsec.conf - strongSwan IPsec configuration file

config setup
charondebug="tnc 3, imv 3"

conn %default
ikelifetime=60m
keylife=20m
rekeymargin=3m
keyingtries=1
keyexchange=ikev2

conn rw-allow
rightgroups=allow
leftsubnet=10.1.0.0/28
also=rw-eap
auto=add

conn rw-isolate
rightgroups=isolate
leftsubnet=10.1.0.16/28
also=rw-eap
auto=add

1. I added rightsourceip because it could not establish the virtual network.
   conn rw-eap
   left=192.168.10.100
   rightsourceip=10.1.0.0/28
   leftcert=vpnHostCert.pem
   leftid=mydomain.org
   leftauth=eap-ttls
   leftfirewall=yes
   rightauth=eap-ttls
   rightid=*@mydomain.org
   rightsendcert=never
   right=%any

1. /etc/strongswan.conf - strongSwan configuration file

charon {
load = aes des sha1 sha2 md5 pem pkcs1 gmp random nonce x509 curl revocation hmac stroke kernel-netlink socket-default eap-identity eap-ttls eap-md5 eap-tnc tnc-imv tnc-tnccs tnccs-20 updown

```
multiple_authentication = no

plugins {
    eap-ttls {
      phase2_method = md5
      phase2_piggyback = yes
      phase2_tnc = yes
    }
  }
```

```
}

libimcv {
plugins {
imv-test {
rounds = 1
}
}
}
```

1. /etc/ipsec.secrets - strongSwan IPsec secrets file

```
: RSA vpnHostKey.pem
alexander@mydomain.org : EAP "ZS629678"
```

History

#1 - 22.12.2014 06:49 - Andreas Steffen

- Status changed from New to Feedback

Hi Jim,

in order to do TNC measurement at least one IMV must be able to handle PA-TNC messages of the subtype 'IETF/Operating System'. Neither the Test nor Scan IMV that you currently use can do this. You must either add the OS IMV or Attestation IMV or both to the list in /etc/tnc_config. You can delete the Test IMV from the list since it doesn't have any use in an Android TNC Client scenario. And of course you must configure a strongTNC Policy manager as a backend for the TNC server. Otherwise no workitems are going to be generated. Have look at our strongTNC HOWTO:

Best regards

Andreas

#2 - 07.07.2015 16:16 - Tobias Brunner

- Status changed from Feedback to Closed

- Resolution set to No feedback