strongSwan - Bug #61

When recovering from DPD, firewall rules aren't added as necessary

15.09.2008 22:42 - Martin Willi

Status:	Closed	**Start date:**	
Priority:	High	**Due date:**	
Assignee:	Andreas Steffen	**Estimated time:**	0.00 hour
Category:	pluto		
Target version:			
Affected version:		**Resolution:**	

Description

1. Node A and node B are connected and both have the appropriate firewall rules automatically added, through leftfirewall. The link is using DPD.

2. Node B dies without a proper shutdown procedure.

3. Node B is rebooted and comes up.

4. Node A triggers a DPD reconnection.

5. Node B reestablishes the connection but does not execute the updown script and no rules are added.

The nodes do remain connected but no traffic can pass through, due to the missing rules.

This is the log output from Node A, running OpenSwan:

```
Sep 15 22:18:50 (none) kern.warn plutor23033: "solhemnet-jockenet" #2: DPD: No response from peer
- declaring peer dead
Sep 15 22:18:50 (none) kern.warn plutor23033: "solhemnet-jockenet" #2: DPD: Restarting Connection
Sep 15 22:18:50 (none) kern.warn plutor23033: "solhemnet-jockenet" #5: initiating Main Mode to rep
lace #2
Sep 15 22:18:50 (none) kern.warn plutor23033: "solhemnet-jockenet" #5: ignoring unknown Vendor ID
payload [af0a05e0bd37b0aba0135a194abb5b89]
Sep 15 22:18:50 (none) kern.warn plutor23033: "solhemnet-jockenet" #5: received Vendor ID payload
[XAUTH]
Sep 15 22:18:50 (none) kern.warn plutor23033: "solhemnet-jockenet" #5: received Vendor ID payload
[Dead Peer Detection]
Sep 15 22:18:50 (none) kern.warn plutor23033: "solhemnet-jockenet" #5: received Vendor ID payload
[RFC 3947] method set to=109
Sep 15 22:18:50 (none) kern.warn plutor23033: "solhemnet-jockenet" #5: enabling possible NAT-trave
rsal with method 3
Sep 15 22:18:50 (none) kern.warn plutor23033: "solhemnet-jockenet" #5: transition from state STATE
_MAIN_I1 to state STATE_MAIN_I2
Sep 15 22:18:50 (none) kern.warn plutor23033: "solhemnet-jockenet" #5: STATE_MAIN_I2: sent MI2, ex
pecting MR2
Sep 15 22:18:50 (none) kern.warn plutor23033: "solhemnet-jockenet" #5: NAT-Traversal: Result using
 3: no NAT detected
Sep 15 22:18:50 (none) kern.warn plutor23033: "solhemnet-jockenet" #5: I am sending my cert
Sep 15 22:18:50 (none) kern.warn plutor23033: "solhemnet-jockenet" #5: I am sending a certificate
request
Sep 15 22:18:50 (none) kern.warn plutor23033: "solhemnet-jockenet" #5: transition from state STATE
_MAIN_I2 to state STATE_MAIN_I3
Sep 15 22:18:50 (none) kern.warn plutor23033: "solhemnet-jockenet" #5: STATE_MAIN_I3: sent MI3, ex
pecting MR3
Sep 15 22:18:51 (none) kern.warn plutor23033: "solhemnet-jockenet" #5: Main mode peer ID is ID_DER
_ASN1_DN: 'C=SE, ST=SE, O=Spanga, CN=Solhem Wrt1'
Sep 15 22:18:51 (none) kern.warn plutor23033: "solhemnet-jockenet" #5: no crl from issuer "C=SE, S
T=SE, O=Spanga, CN=spanga.intra" found (strict=no)
Sep 15 22:18:51 (none) kern.warn plutor23033: "solhemnet-jockenet" #5: transition from state STATE
_MAIN_I3 to state STATE_MAIN_I4
Sep 15 22:18:51 (none) kern.warn plutor23033: "solhemnet-jockenet" #5: STATE_MAIN_I4: ISAKMP SA es
tablished {auth=OAKLEY_RSA_SIG cipher=aes_128 prf=oakley_sha group=modp1024}
```

```
Sep 15 22:18:51 (none) kern.warn plutor23033: "solhemnet-jockenet" #5: Dead Peer Detection (RFC 37
06): enabled
```

And Node B, which is running strongSwan U4.2.5/K2.6.25.16:

```
Sep 15 22:17:20 solhem-wrt1 authpriv.warn plutor1221: packet from 83.250.110.25:500: Informational
 Exchange is for an unknown (expired?) SA
Sep 15 22:17:50 solhem-wrt1 authpriv.warn plutor1221: packet from 83.250.110.25:500: Informational
 Exchange is for an unknown (expired?) SA
Sep 15 22:18:20 solhem-wrt1 authpriv.warn plutor1221: packet from 83.250.110.25:500: Informational
 Exchange is for an unknown (expired?) SA
Sep 15 22:18:50 solhem-wrt1 authpriv.warn plutor1221: packet from 83.250.110.25:500: Informational
 Exchange is for an unknown (expired?) SA
Sep 15 22:18:50 solhem-wrt1 authpriv.warn plutor1221: packet from 83.250.110.25:500: ignoring Vend
or ID payload [4f457a7d4646466667725f65]
Sep 15 22:18:50 solhem-wrt1 authpriv.warn plutor1221: packet from 83.250.110.25:500: received Vend
or ID payload [Dead Peer Detection]
Sep 15 22:18:50 solhem-wrt1 authpriv.warn plutor1221: packet from 83.250.110.25:500: received Vend
or ID payload [RFC 3947]
Sep 15 22:18:50 solhem-wrt1 authpriv.warn plutor1221: packet from 83.250.110.25:500: ignoring Vend
or ID payload [draft-ietf-ipsec-nat-t-ike-03]
Sep 15 22:18:50 solhem-wrt1 authpriv.warn plutor1221: packet from 83.250.110.25:500: ignoring Vend
or ID payload [draft-ietf-ipsec-nat-t-ike-02]
Sep 15 22:18:50 solhem-wrt1 authpriv.warn plutor1221: packet from 83.250.110.25:500: ignoring Vend
or ID payload [draft-ietf-ipsec-nat-t-ike-00]
Sep 15 22:18:50 solhem-wrt1 authpriv.warn plutor1221: "roadwarrior-wrt"r1 83.250.110.25 #3: respon
ding to Main Mode from unknown peer 83.250.110.25
Sep 15 22:18:50 solhem-wrt1 authpriv.warn plutor1221: "spanganet" #1: ignoring Delete SA payload:
PROTO_IPSEC_ESP SA(0xed415af0) not found (maybe expired)
Sep 15 22:18:50 solhem-wrt1 authpriv.warn plutor1221: packet from 81.232.63.153:500: Informational
 Exchange is for an unknown (expired?) SA
Sep 15 22:18:50 solhem-wrt1 authpriv.warn plutor1221: "roadwarrior-wrt"r1 83.250.110.25 #3: NAT-Tr
aversal: Result using RFC 3947: no NAT detected
Sep 15 22:18:50 solhem-wrt1 authpriv.warn plutor1221: "roadwarrior-wrt"r1 83.250.110.25 #3: Peer I
D is ID_DER_ASN1_DN: 'C=SE, ST=SE, O=Spanga, OU=Spanga, CN=jock.liotta.info'
Sep 15 22:18:50 solhem-wrt1 authpriv.warn plutor1221: "roadwarrior-wrt"r1 83.250.110.25 #3: crl no
t found
Sep 15 22:18:50 solhem-wrt1 authpriv.warn plutor1221: "roadwarrior-wrt"r1 83.250.110.25 #3: certif
icate status unknown
Sep 15 22:18:50 solhem-wrt1 authpriv.warn plutor1221: "roadwarrior-wrt"r1 83.250.110.25 #3: crl no
t found
Sep 15 22:18:50 solhem-wrt1 authpriv.warn plutor1221: "roadwarrior-wrt"r1 83.250.110.25 #3: certif
icate status unknown
Sep 15 22:18:50 solhem-wrt1 authpriv.warn plutor1221: "roadwarrior-wrt"r2 83.250.110.25 #3: deleti
ng connection "roadwarrior-wrt" instance with peer 83.250.110.25 {isakmp=#0/ipsec=#0}
Sep 15 22:18:50 solhem-wrt1 authpriv.warn plutor1221: "roadwarrior-wrt"r2 83.250.110.25 #3: we hav
e a cert and are sending it upon request
Sep 15 22:18:50 solhem-wrt1 authpriv.warn plutor1221: "roadwarrior-wrt"r2 83.250.110.25 #3: sent M
R3, ISAKMP SA established
```

Here is node B's ipsec.conf:

```
config setup
        interfaces=%defaultroute
        nat_traversal=yes               # required on both ends
        uniqueids=yes                   # makes sense on client, not server
        hidetos=no

conn %default
        authby=rsasig
        keyingtries=0
        rekeymargin=5m
        rekeyfuzz=10%
        keyexchange=ike
        left=%defaultroute
        leftrsasigkey=%cert
        rightrsasigkey=%cert
```

```
        dpdtimeout=30                   # keepalive must arrive within
        dpddelay=5                      # secs before keepalives start
        compress=no                     # breaks double nat installations
        pfs=yes
        esp=aes128-sha1,3des-sha1
        ike=aes128-sha-modp1024,3des-sha,3des-md5

conn roadwarrior-wrt
        leftcert=wrt1-spanga.cer
        leftsubnet=192.168.248.0/22
        leftsourceip=192.168.251.1
        leftfirewall=yes
        lefthostaccess=yes
        right=%any
        rightca="/C=SE/ST=SE/O=Spanga/CN=spanga.intra"
        rightsubnetwithin=192.168.0.0/16
        dpdaction=clear
        auto=add
```

Looking through 'iptables -L' confirms that no firewall rules have been added to node B. If, however ipsec is restarted, then when node A reconnects the proper rules are added to iptables. This can be confirmed by adding a logger checkpoint in the updown script. It does not seem to execute when recovering from DPD.

History

#1 - 15.09.2008 23:03 - Martin Willi

The necessary IP route is also missing from 'ip route list table 220', which should have been added by the updown script.

#2 - 06.05.2013 21:43 - Andreas Steffen

- Description updated

- Category changed from starter to pluto

- Status changed from New to Closed

Closed because we don't support the pluto IKEv1 daemon any more.