strongSwan - Bug #799

Usage statistics of IPsec SAs are incorrect after client's (NAT) endpoint changed

23.12.2014 09:04 - richard hu

Status:	Closed	**Start date:**	23.12.2014
Priority:	Normal	**Due date:**	
Assignee:	Tobias Brunner	**Estimated time:**	0.00 hour
Category:	charon		
Target version:	5.3.0		
Affected version:	5.2.1	**Resolution:**	Fixed

Description

iOS to strongswan server.
if use youtube, the final in and out packets recorded in radius is: | 1401069 | 38615402 |
if use pandora or netflix, the record is: | 1664 | 0 |
while in the same time tcpdump at iOS side or strongswan side, the network traffic is much more than this.

Associated revisions

Revision a3c2edb1 - 25.03.2015 12:00 - Tobias Brunner

kernel-netlink: Copy current usage stats to new SA in update_sa()

This is needed to fix usage stats sent via RADIUS Accounting if clients
use MOBIKE or e.g. the kernel notifies us about a changed NAT mapping.
The upper layers won't expect the stats to get reset if only the IPs have
changed (and some kernel interface might actually allow such updates
without reset).

It also fixes traffic based lifetimes in such situations.

Fixes #799.

History

#1 - 23.12.2014 09:44 - richard hu

above number is bytes in and out, acctinputoctets and acctoutputoctets

#2 - 25.12.2014 09:17 - richard hu

I found a clue for this:
when use pandora or netflix, server have log of:
NAT mappings of ESP CHILD_SA with SPI ccf564d5 and reqid {1} changed, queuing update job

found another thread discuss this error (but did not mention pandora or netflix), and said can comments out update_sa_job_create in kernel_handler.c
this can solve the radius input and output bytes issue but seems not a solution although the function looks ok after comments out.
any suggestion for this?

#3 - 26.12.2014 07:14 - richard hu

If "NAT mappings of ESP CHILD_SA...." is a normal behavior for client have multi IP, then why after update_sa_job_create the byte accounting number lost?

Here is rich log when doing above jobs:

```
Dec 26 05:57:51 11[KNL] NAT mappings of ESP CHILD_SA with SPI cd0ecf6b and reqid {1} changed, queuing update j
ob
Dec 26 05:57:51 11[CFG] not update_sa_job_create? zzz.ww.195.210[1363]
Dec 26 05:57:51 11[MGR] checkout IKE_SA by ID
Dec 26 05:57:51 13[JOB] watcher got notification, rebuilding
Dec 26 05:57:51 13[JOB]   watching 9 for reading
Dec 26 05:57:51 13[JOB]   watching 15 for reading
Dec 26 05:57:51 13[JOB]   watching 16 for reading
Dec 26 05:57:51 13[JOB] watcher going to select()
Dec 26 05:57:51 11[MGR] IKE_SA XauthRSA[1] successfully checked out
Dec 26 05:57:51 11[KNL] <XauthRSA|1> querying SAD entry with SPI cd0ecf6b for update
Dec 26 05:57:51 11[KNL] <XauthRSA|1> sending XFRM_MSG_GETSA: => 40 bytes @ 0x7fc7ae142420
Dec 26 05:57:51 11[KNL] <XauthRSA|1>    0: 28 00 00 00 12 00 01 00 D8 01 00 00 B8 BF 00 00  (...............
```

```
Dec 26 05:57:51 11[KNL] <XauthRSA|1>   16: 0A 00 00 40 00 00 00 00 00 00 00 00 00 00 00 00  ...@............
Dec 26 05:57:51 11[KNL] <XauthRSA|1>   32: CD 0E CF 6B 02 00 32 00                          ...k..2.
Dec 26 05:57:51 11[KNL] <XauthRSA|1> querying replay state from SAD entry with SPI cd0ecf6b
Dec 26 05:57:51 11[KNL] <XauthRSA|1> sending XFRM_MSG_GETAE: => 64 bytes @ 0x7fc7ae142820
Dec 26 05:57:51 11[KNL] <XauthRSA|1>    0: 40 00 00 00 1F 00 01 00 D9 01 00 00 B8 BF 00 00  @...............
Dec 26 05:57:51 11[KNL] <XauthRSA|1>   16: 0A 00 00 40 00 00 00 00 00 00 00 00 00 00 00 00  ...@............
Dec 26 05:57:51 11[KNL] <XauthRSA|1>   32: CD 0E CF 6B 02 00 32 00 00 00 00 00 00 00 00 00  ...k..2.........
Dec 26 05:57:51 11[KNL] <XauthRSA|1>   48: 00 00 00 00 00 00 00 00 02 00 00 00 00 00 00 00  ................
Dec 26 05:57:51 11[KNL] <XauthRSA|1> deleting SAD entry with SPI cd0ecf6b  (mark 0/0x00000000)
Dec 26 05:57:51 11[KNL] <XauthRSA|1> sending XFRM_MSG_DELSA: => 40 bytes @ 0x7fc7ae141f20
Dec 26 05:57:51 11[KNL] <XauthRSA|1>    0: 28 00 00 00 11 00 05 00 DA 01 00 00 B8 BF 00 00  (...............
Dec 26 05:57:51 11[KNL] <XauthRSA|1>   16: 0A 00 00 40 00 00 00 00 00 00 00 00 00 00 00 00  ...@............
Dec 26 05:57:51 11[KNL] <XauthRSA|1>   32: CD 0E CF 6B 02 00 32 00                          ...k..2.
Dec 26 05:57:51 11[KNL] <XauthRSA|1> deleted SAD entry with SPI cd0ecf6b (mark 0/0x00000000)
Dec 26 05:57:51 11[KNL] <XauthRSA|1> updating SAD entry with SPI cd0ecf6b from xxx.yy.212.14[4500]..10.0.0.64[
4500] to zzz.ww.195.210[1363]..10.0.0.64[4500]
Dec 26 05:57:51 11[KNL] <XauthRSA|1> sending XFRM_MSG_NEWSA: => 560 bytes @ 0x7fc7ae142420
Dec 26 05:57:51 11[KNL] <XauthRSA|1>    0: 30 02 00 00 10 00 05 00 DB 01 00 00 B8 BF 00 00  0...............
Dec 26 05:57:51 11[KNL] <XauthRSA|1>   16: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
Dec 26 05:57:51 11[KNL] <XauthRSA|1>   32: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
Dec 26 05:57:51 11[KNL] <XauthRSA|1>   48: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
Dec 26 05:57:51 11[KNL] <XauthRSA|1>   64: 00 00 00 00 00 00 00 00 0A 00 00 40 00 00 00 00  ...........@....
Dec 26 05:57:51 11[KNL] <XauthRSA|1>   80: 00 00 00 00 00 00 00 00 CD 0E CF 6B 32 00 00 00  ...........k2...
Dec 26 05:57:51 11[KNL] <XauthRSA|1>   96: DE 7E C3 D2 00 00 00 00 00 00 00 00 00 00 00 00  .~..............
Dec 26 05:57:51 11[KNL] <XauthRSA|1>  112: FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF  ................
Dec 26 05:57:51 11[KNL] <XauthRSA|1>  128: FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF  ................
Dec 26 05:57:51 11[KNL] <XauthRSA|1>  144: C9 27 00 00 00 00 00 00 30 2A 00 00 00 00 00 00  .'......0*......
Dec 26 05:57:51 11[KNL] <XauthRSA|1>  160: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
Dec 26 05:57:51 11[KNL] <XauthRSA|1>  176: D0 00 00 00 00 00 00 00 01 00 00 00 00 00 00 00  ................
Dec 26 05:57:51 11[KNL] <XauthRSA|1>  192: DF F8 9C 54 00 00 00 00 DF F8 9C 54 00 00 00 00  ...T.......T....
Dec 26 05:57:51 11[KNL] <XauthRSA|1>  208: 00 00 00 00 00 00 00 00 00 00 00 00 21 09 00 00  ............!...
Dec 26 05:57:51 11[KNL] <XauthRSA|1>  224: 01 00 00 00 02 00 01 20 20 00 00 00 00 00 00 00  .......  .......
Dec 26 05:57:51 11[KNL] <XauthRSA|1>  240: 5C 00 01 00 68 6D 61 63 28 73 68 61 31 29 00 00  \...hmac(sha1)..
Dec 26 05:57:51 11[KNL] <XauthRSA|1>  256: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
Dec 26 05:57:51 11[KNL] <XauthRSA|1>  272: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
Dec 26 05:57:51 11[KNL] <XauthRSA|1>  288: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
Dec 26 05:57:51 11[KNL] <XauthRSA|1>  304: 00 00 00 00 A0 00 00 00 DD A7 25 77 55 FF 32 AE  ..........%wU.2.
Dec 26 05:57:51 11[KNL] <XauthRSA|1>  320: 8E 89 0B 68 C5 07 FB C5 7F FD BC E6 60 00 14 00  ...h........`...
Dec 26 05:57:51 11[KNL] <XauthRSA|1>  336: 68 6D 61 63 28 73 68 61 31 29 00 00 00 00 00 00  hmac(sha1)......
Dec 26 05:57:51 11[KNL] <XauthRSA|1>  352: AC CB B2 98 03 88 FF FF 00 00 00 00 00 00 00 00  ................
Dec 26 05:57:51 11[KNL] <XauthRSA|1>  368: A0 CB B2 98 03 88 FF FF 00 00 00 00 00 00 00 00  ................
Dec 26 05:57:51 11[KNL] <XauthRSA|1>  384: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
Dec 26 05:57:51 11[KNL] <XauthRSA|1>  400: A0 00 00 00 00 60 00 00 00 DD A7 25 77 55 FF 32 AE  .....`.....%wU.2.
Dec 26 05:57:51 11[KNL] <XauthRSA|1>  416: 8E 89 0B 68 C5 07 FB C5 7F FD BC E6 58 00 02 00  ...h........X...
Dec 26 05:57:51 11[KNL] <XauthRSA|1>  432: 63 62 63 28 61 65 73 29 00 00 00 00 00 00 00 00  cbc(aes).........
Dec 26 05:57:51 11[KNL] <XauthRSA|1>  448: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
Dec 26 05:57:51 11[KNL] <XauthRSA|1>  464: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
Dec 26 05:57:51 11[KNL] <XauthRSA|1>  480: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
Dec 26 05:57:51 11[KNL] <XauthRSA|1>  496: 80 00 00 00 A1 F7 34 64 60 4F CC D9 6E D9 D8 A8  ......4d`O..n...
Dec 26 05:57:51 11[KNL] <XauthRSA|1>  512: 97 AA 91 92 1C 00 04 00 02 00 05 53 11 94 00 00  ...........S....
Dec 26 05:57:51 11[KNL] <XauthRSA|1>  528: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
Dec 26 05:57:51 11[KNL] <XauthRSA|1>  544: 10 00 0A 00 00 00 00 00 FA 02 00 00 FF FF FF FF  ................
Dec 26 05:57:51 11[KNL] <XauthRSA|1> querying SAD entry with SPI 0f2e26cb for update
Dec 26 05:57:51 11[KNL] <XauthRSA|1> sending XFRM_MSG_GETSA: => 40 bytes @ 0x7fc7ae142420
Dec 26 05:57:51 11[KNL] <XauthRSA|1>    0: 28 00 00 00 12 00 01 00 DC 01 00 00 B8 BF 00 00  (...............
Dec 26 05:57:51 11[KNL] <XauthRSA|1>   16: CA 41 D4 0E 00 00 00 00 00 00 00 00 00 00 00 00  .A..............
Dec 26 05:57:51 11[KNL] <XauthRSA|1>   32: 0F 2E 26 CB 02 00 32 00                          ..&...2.
Dec 26 05:57:51 11[KNL] <XauthRSA|1> querying replay state from SAD entry with SPI 0f2e26cb
Dec 26 05:57:51 11[KNL] <XauthRSA|1> sending XFRM_MSG_GETAE: => 64 bytes @ 0x7fc7ae142820
Dec 26 05:57:51 11[KNL] <XauthRSA|1>    0: 40 00 00 00 1F 00 01 00 DD 01 00 00 B8 BF 00 00  @...............
Dec 26 05:57:51 11[KNL] <XauthRSA|1>   16: CA 41 D4 0E 00 00 00 00 00 00 00 00 00 00 00 00  .A..............
Dec 26 05:57:51 11[KNL] <XauthRSA|1>   32: 0F 2E 26 CB 02 00 32 00 00 00 00 00 00 00 00 00  ..&...2.........
Dec 26 05:57:51 11[KNL] <XauthRSA|1>   48: 00 00 00 00 00 00 00 00 02 00 00 00 00 00 00 00  ................
Dec 26 05:57:51 11[KNL] <XauthRSA|1> deleting SAD entry with SPI 0f2e26cb  (mark 0/0x00000000)
Dec 26 05:57:51 11[KNL] <XauthRSA|1> sending XFRM_MSG_DELSA: => 40 bytes @ 0x7fc7ae141f20
Dec 26 05:57:51 11[KNL] <XauthRSA|1>    0: 28 00 00 00 11 00 05 00 DE 01 00 00 B8 BF 00 00  (...............
Dec 26 05:57:51 11[KNL] <XauthRSA|1>   16: CA 41 D4 0E 00 00 00 00 00 00 00 00 00 00 00 00  .A..............
Dec 26 05:57:51 11[KNL] <XauthRSA|1>   32: 0F 2E 26 CB 02 00 32 00                          ..&...2.
Dec 26 05:57:51 11[KNL] <XauthRSA|1> deleted SAD entry with SPI 0f2e26cb (mark 0/0x00000000)
Dec 26 05:57:51 11[KNL] <XauthRSA|1> updating SAD entry with SPI 0f2e26cb from 10.0.0.64[4500]..xxx.yy.212.14[
4500] to 10.0.0.64[4500]..zzz.ww.195.210[1363]
Dec 26 05:57:51 11[KNL] <XauthRSA|1> sending XFRM_MSG_NEWSA: => 560 bytes @ 0x7fc7ae142420
Dec 26 05:57:51 11[KNL] <XauthRSA|1>    0: 30 02 00 00 10 00 05 00 DF 01 00 00 B8 BF 00 00  0...............
Dec 26 05:57:51 11[KNL] <XauthRSA|1>   16: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
Dec 26 05:57:51 11[KNL] <XauthRSA|1>   32: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
```

```
Dec 26 05:57:51 11[KNL] <XauthRSA|1>   48: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
Dec 26 05:57:51 11[KNL] <XauthRSA|1>   64: 00 00 00 00 00 00 00 00 DE 7E C3 D2 00 00 00 00  .........~......
Dec 26 05:57:51 11[KNL] <XauthRSA|1>   80: 00 00 00 00 00 00 00 00 0F 2E 26 CB 32 00 00 00  ..........&.2...
Dec 26 05:57:51 11[KNL] <XauthRSA|1>   96: 0A 00 00 40 00 00 00 00 00 00 00 00 00 00 00 00  ...@............
Dec 26 05:57:51 11[KNL] <XauthRSA|1>  112: FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF  ................
Dec 26 05:57:51 11[KNL] <XauthRSA|1>  128: FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF  ................
Dec 26 05:57:51 11[KNL] <XauthRSA|1>  144: 91 26 00 00 00 00 00 00 30 2A 00 00 00 00 00 00  .&......0*......
Dec 26 05:57:51 11[KNL] <XauthRSA|1>  160: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
Dec 26 05:57:51 11[KNL] <XauthRSA|1>  176: 77 01 00 00 00 00 00 00 01 00 00 00 00 00 00 00  w...............
Dec 26 05:57:51 11[KNL] <XauthRSA|1>  192: DF F8 9C 54 00 00 00 00 DF F8 9C 54 00 00 00 00  ...T.......T....
Dec 26 05:57:51 11[KNL] <XauthRSA|1>  208: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
Dec 26 05:57:51 11[KNL] <XauthRSA|1>  224: 01 00 00 00 02 00 01 20 20 00 00 00 00 00 00 00  .......  .......
Dec 26 05:57:51 11[KNL] <XauthRSA|1>  240: 5C 00 01 00 68 6D 61 63 28 73 68 61 31 29 00 00  \...hmac(sha1)..
Dec 26 05:57:51 11[KNL] <XauthRSA|1>  256: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
Dec 26 05:57:51 11[KNL] <XauthRSA|1>  272: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
Dec 26 05:57:51 11[KNL] <XauthRSA|1>  288: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
Dec 26 05:57:51 11[KNL] <XauthRSA|1>  304: 00 00 00 00 A0 00 00 00 C4 87 F2 CB 9C CB 3E 22  ..............>"
Dec 26 05:57:51 11[KNL] <XauthRSA|1>  320: C4 72 64 F6 9C 45 EF 66 20 9B 4C BF 60 00 14 00  .rd..E.f .L.`...
Dec 26 05:57:51 11[KNL] <XauthRSA|1>  336: 68 6D 61 63 28 73 68 61 31 29 00 A4 03 88 FF FF  hmac(sha1)......
Dec 26 05:57:51 11[KNL] <XauthRSA|1>  352: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
Dec 26 05:57:51 11[KNL] <XauthRSA|1>  368: 00 00 00 00 00 00 00 00 37 04 0A 00 13 01 73 6F  ........7.....so
Dec 26 05:57:51 11[KNL] <XauthRSA|1>  384: 63 6B 65 74 2D 64 65 66 61 75 6C 74 2E 63 6F 00  cket-default.co.
Dec 26 05:57:51 11[KNL] <XauthRSA|1>  400: A0 00 00 00 60 00 00 00 C4 87 F2 CB 9C CB 3E 22  ....`.........>"
Dec 26 05:57:51 11[KNL] <XauthRSA|1>  416: C4 72 64 F6 9C 45 EF 66 20 9B 4C BF 58 00 02 00  .rd..E.f .L.X...
Dec 26 05:57:51 11[KNL] <XauthRSA|1>  432: 63 62 63 28 61 65 73 29 00 00 00 00 00 00 00 00  cbc(aes)........
Dec 26 05:57:51 11[KNL] <XauthRSA|1>  448: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
Dec 26 05:57:51 11[KNL] <XauthRSA|1>  464: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
Dec 26 05:57:51 11[KNL] <XauthRSA|1>  480: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
Dec 26 05:57:51 11[KNL] <XauthRSA|1>  496: 80 00 00 00 4A 3B BB 74 D0 24 D2 96 EC DF 64 93  ....J;.t.$....d.
Dec 26 05:57:51 11[KNL] <XauthRSA|1>  512: 65 04 C8 7C 1C 00 04 00 02 00 11 94 05 53 00 00  e..|.........S..
Dec 26 05:57:51 11[KNL] <XauthRSA|1>  528: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
Dec 26 05:57:51 11[KNL] <XauthRSA|1>  544: 10 00 0A 00 B5 06 00 00 00 00 00 00 00 00 00 00  ................
Dec 26 05:57:51 11[KNL] <XauthRSA|1> deleting policy 0.0.0.0/0 === 172.16.0.1/32 out  (mark 0/0x00000000)
Dec 26 05:57:51 11[KNL] <XauthRSA|1> policy still used by another CHILD_SA, not removed
Dec 26 05:57:51 11[KNL] <XauthRSA|1> updating policy 0.0.0.0/0 === 172.16.0.1/32 out  (mark 0/0x00000000)
Dec 26 05:57:51 11[KNL] <XauthRSA|1> sending XFRM_MSG_UPDPOLICY: => 184 bytes @ 0x7fc7ae142290
Dec 26 05:57:51 11[KNL] <XauthRSA|1>    0: B8 00 00 00 19 00 05 00 E0 01 00 00 B8 BF 00 00  ................
Dec 26 05:57:51 11[KNL] <XauthRSA|1>   16: AC 10 00 01 00 00 00 00 00 00 00 00 00 00 00 00  ................
Dec 26 05:57:51 11[KNL] <XauthRSA|1>   32: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
Dec 26 05:57:51 11[KNL] <XauthRSA|1>   48: 00 00 00 00 00 00 00 00 00 02 00 20 00 00 00 00  ........... .....
Dec 26 05:57:51 11[KNL] <XauthRSA|1>   64: 00 00 00 00 00 00 00 00 FF FF FF FF FF FF FF FF  ................
Dec 26 05:57:51 11[KNL] <XauthRSA|1>   80: FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF  ................
Dec 26 05:57:51 11[KNL] <XauthRSA|1>   96: FF FF FF FF FF FF FF FF 00 00 00 00 00 00 00 00  ................
Dec 26 05:57:51 11[KNL] <XauthRSA|1>  112: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
Dec 26 05:57:51 11[KNL] <XauthRSA|1>  128: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
Dec 26 05:57:51 11[KNL] <XauthRSA|1>  144: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
Dec 26 05:57:51 11[KNL] <XauthRSA|1>  160: 00 00 00 00 00 00 00 00 83 2F 00 00 00 00 00 00  ........./......
Dec 26 05:57:51 11[KNL] <XauthRSA|1>  176: 01 01 00 00 00 00 00 00                          ........
Dec 26 05:57:51 11[KNL] <XauthRSA|1> deleting policy 172.16.0.1/32 === 0.0.0.0/0 in  (mark 0/0x00000000)
Dec 26 05:57:51 11[KNL] <XauthRSA|1> policy still used by another CHILD_SA, not removed
Dec 26 05:57:51 11[KNL] <XauthRSA|1> updating policy 172.16.0.1/32 === 0.0.0.0/0 in  (mark 0/0x00000000)
Dec 26 05:57:51 11[KNL] <XauthRSA|1> sending XFRM_MSG_UPDPOLICY: => 184 bytes @ 0x7fc7ae142290
Dec 26 05:57:51 11[KNL] <XauthRSA|1>    0: B8 00 00 00 19 00 05 00 E1 01 00 00 B8 BF 00 00  ................
Dec 26 05:57:51 11[KNL] <XauthRSA|1>   16: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
Dec 26 05:57:51 11[KNL] <XauthRSA|1>   32: AC 10 00 01 00 00 00 00 00 00 00 00 00 00 00 00  ................
Dec 26 05:57:51 11[KNL] <XauthRSA|1>   48: 00 00 00 00 00 00 00 00 02 00 00 20 00 00 00 00  ........... ....
Dec 26 05:57:51 11[KNL] <XauthRSA|1>   64: 00 00 00 00 00 00 00 00 FF FF FF FF FF FF FF FF  ................
Dec 26 05:57:51 11[KNL] <XauthRSA|1>   80: FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF  ................
Dec 26 05:57:51 11[KNL] <XauthRSA|1>   96: FF FF FF FF FF FF FF FF 00 00 00 00 00 00 00 00  ................
Dec 26 05:57:51 11[KNL] <XauthRSA|1>  112: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
Dec 26 05:57:51 11[KNL] <XauthRSA|1>  128: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
Dec 26 05:57:51 11[KNL] <XauthRSA|1>  144: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
Dec 26 05:57:51 11[KNL] <XauthRSA|1>  160: 00 00 00 00 00 00 00 00 83 2F 00 00 00 00 00 00  ........./......
Dec 26 05:57:51 11[KNL] <XauthRSA|1>  176: 00 01 00 00 00 00 00 00                          ........
Dec 26 05:57:51 11[KNL] <XauthRSA|1> deleting policy 172.16.0.1/32 === 0.0.0.0/0 fwd  (mark 0/0x00000000)
Dec 26 05:57:51 11[KNL] <XauthRSA|1> policy still used by another CHILD_SA, not removed
Dec 26 05:57:51 11[KNL] <XauthRSA|1> updating policy 172.16.0.1/32 === 0.0.0.0/0 fwd  (mark 0/0x00000000)
Dec 26 05:57:51 11[KNL] <XauthRSA|1> sending XFRM_MSG_UPDPOLICY: => 184 bytes @ 0x7fc7ae142290
Dec 26 05:57:51 11[KNL] <XauthRSA|1>    0: B8 00 00 00 19 00 05 00 E2 01 00 00 B8 BF 00 00  ................
Dec 26 05:57:51 11[KNL] <XauthRSA|1>   16: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
Dec 26 05:57:51 11[KNL] <XauthRSA|1>   32: AC 10 00 01 00 00 00 00 00 00 00 00 00 00 00 00  ................
Dec 26 05:57:51 11[KNL] <XauthRSA|1>   48: 00 00 00 00 00 00 00 00 02 00 00 20 00 00 00 00  ........... ....
Dec 26 05:57:51 11[KNL] <XauthRSA|1>   64: 00 00 00 00 00 00 00 00 FF FF FF FF FF FF FF FF  ................
Dec 26 05:57:51 11[KNL] <XauthRSA|1>   80: FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF  ................
Dec 26 05:57:51 11[KNL] <XauthRSA|1>   96: FF FF FF FF FF FF FF FF 00 00 00 00 00 00 00 00  ................
```

```
Dec 26 05:57:51 11[KNL] <XauthRSA|1>  112: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
Dec 26 05:57:51 11[KNL] <XauthRSA|1>  128: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
Dec 26 05:57:51 11[KNL] <XauthRSA|1>  144: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
Dec 26 05:57:51 11[KNL] <XauthRSA|1>  160: 00 00 00 00 00 00 00 00 83 2F 00 00 00 00 00 00  ........./......
Dec 26 05:57:51 11[KNL] <XauthRSA|1>  176: 02 01 00 00 00 00 00 00                          ........
Dec 26 05:57:51 11[KNL] <XauthRSA|1> getting a local address in traffic selector 0.0.0.0/0
Dec 26 05:57:51 11[KNL] <XauthRSA|1> using host %any
Dec 26 05:57:51 11[KNL] <XauthRSA|1> sending RTM_GETROUTE: => 44 bytes @ 0x7fc7ae141da0
Dec 26 05:57:51 11[KNL] <XauthRSA|1>    0: 2C 00 00 00 1A 00 01 03 F4 00 00 00 B8 BF 00 00  ,...............
Dec 26 05:57:51 11[KNL] <XauthRSA|1>   16: 02 00 00 00 00 00 00 00 00 00 00 00 08 00 07 00  ................
Dec 26 05:57:51 11[KNL] <XauthRSA|1>   32: 0A 00 00 40 08 00 01 00 CA 41 D4 0E              ...@.....A..
Dec 26 05:57:51 11[KNL] <XauthRSA|1> using 10.0.0.1 as nexthop to reach xxx.yy.212.14/32
Dec 26 05:57:51 11[KNL] <XauthRSA|1> 10.0.0.64 is on interface eth0
Dec 26 05:57:51 11[KNL] <XauthRSA|1> policy 0.0.0.0/0 === 172.16.0.1/32 out  (mark 0/0x00000000) already exist
s, increasing refcount
Dec 26 05:57:51 11[KNL] <XauthRSA|1> updating policy 0.0.0.0/0 === 172.16.0.1/32 out  (mark 0/0x00000000)
Dec 26 05:57:51 11[KNL] <XauthRSA|1> sending XFRM_MSG_UPDPOLICY: => 252 bytes @ 0x7fc7ae142680
Dec 26 05:57:51 11[KNL] <XauthRSA|1>    0: FC 00 00 00 19 00 05 00 E3 01 00 00 B8 BF 00 00  ................
Dec 26 05:57:51 11[KNL] <XauthRSA|1>   16: AC 10 00 01 00 00 00 00 00 00 00 00 00 00 00 00  ................
Dec 26 05:57:51 11[KNL] <XauthRSA|1>   32: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
Dec 26 05:57:51 11[KNL] <XauthRSA|1>   48: 00 00 00 00 00 00 00 00 00 02 00 20 00 00 00 00  ......... .....
Dec 26 05:57:51 11[KNL] <XauthRSA|1>   64: 00 00 00 00 00 00 00 00 FF FF FF FF FF FF FF FF  ................
Dec 26 05:57:51 11[KNL] <XauthRSA|1>   80: FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF  ................
Dec 26 05:57:51 11[KNL] <XauthRSA|1>   96: FF FF FF FF FF FF FF FF 00 00 00 00 00 00 00 00  ................
Dec 26 05:57:51 11[KNL] <XauthRSA|1>  112: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
Dec 26 05:57:51 11[KNL] <XauthRSA|1>  128: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
Dec 26 05:57:51 11[KNL] <XauthRSA|1>  144: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
Dec 26 05:57:51 11[KNL] <XauthRSA|1>  160: 00 00 00 00 00 00 00 00 83 0B 00 00 00 00 00 00  ................
Dec 26 05:57:51 11[KNL] <XauthRSA|1>  176: 01 00 00 00 00 00 00 00 44 00 05 00 DE 7E C3 D2  ........D....~..
Dec 26 05:57:51 11[KNL] <XauthRSA|1>  192: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
Dec 26 05:57:51 11[KNL] <XauthRSA|1>  208: 32 00 00 00 02 00 00 00 0A 00 00 40 00 00 00 00  2..........@....
Dec 26 05:57:51 11[KNL] <XauthRSA|1>  224: 00 00 00 00 00 00 00 00 01 00 00 00 01 00 00 00  ................
Dec 26 05:57:51 11[KNL] <XauthRSA|1>  240: FF FF FF FF FF FF FF FF FF FF FF FF              ............
Dec 26 05:57:51 11[KNL] <XauthRSA|1> policy 172.16.0.1/32 === 0.0.0.0/0 in  (mark 0/0x00000000) already exists
, increasing refcount
Dec 26 05:57:51 11[KNL] <XauthRSA|1> updating policy 172.16.0.1/32 === 0.0.0.0/0 in  (mark 0/0x00000000)
Dec 26 05:57:51 11[KNL] <XauthRSA|1> sending XFRM_MSG_UPDPOLICY: => 252 bytes @ 0x7fc7ae142680
Dec 26 05:57:51 11[KNL] <XauthRSA|1>    0: FC 00 00 00 19 00 05 00 E4 01 00 00 B8 BF 00 00  ................
Dec 26 05:57:51 11[KNL] <XauthRSA|1>   16: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
Dec 26 05:57:51 11[KNL] <XauthRSA|1>   32: AC 10 00 01 00 00 00 00 00 00 00 00 00 00 00 00  ................
Dec 26 05:57:51 11[KNL] <XauthRSA|1>   48: 00 00 00 00 00 00 00 00 00 02 00 00 20 00 00 00  ........... ....
Dec 26 05:57:51 11[KNL] <XauthRSA|1>   64: 00 00 00 00 00 00 00 00 FF FF FF FF FF FF FF FF  ................
Dec 26 05:57:51 11[KNL] <XauthRSA|1>   80: FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF  ................
Dec 26 05:57:51 11[KNL] <XauthRSA|1>   96: FF FF FF FF FF FF FF FF 00 00 00 00 00 00 00 00  ................
Dec 26 05:57:51 11[KNL] <XauthRSA|1>  112: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
Dec 26 05:57:51 11[KNL] <XauthRSA|1>  128: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
Dec 26 05:57:51 11[KNL] <XauthRSA|1>  144: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
Dec 26 05:57:51 11[KNL] <XauthRSA|1>  160: 00 00 00 00 00 00 00 00 83 0B 00 00 00 00 00 00  ................
Dec 26 05:57:51 11[KNL] <XauthRSA|1>  176: 00 00 00 00 00 00 00 00 44 00 05 00 0A 00 00 40  ........D......@
Dec 26 05:57:51 11[KNL] <XauthRSA|1>  192: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
Dec 26 05:57:51 11[KNL] <XauthRSA|1>  208: 32 00 00 00 02 00 00 00 DE 7E C3 D2 00 00 00 00  2........~......
Dec 26 05:57:51 11[KNL] <XauthRSA|1>  224: 00 00 00 00 00 00 00 00 01 00 00 00 01 00 00 00  ................
Dec 26 05:57:51 11[KNL] <XauthRSA|1>  240: FF FF FF FF FF FF FF FF FF FF FF FF              ............
Dec 26 05:57:51 11[KNL] <XauthRSA|1> policy 172.16.0.1/32 === 0.0.0.0/0 fwd  (mark 0/0x00000000) already exist
s, increasing refcount
Dec 26 05:57:51 11[KNL] <XauthRSA|1> updating policy 172.16.0.1/32 === 0.0.0.0/0 fwd  (mark 0/0x00000000)
Dec 26 05:57:51 11[KNL] <XauthRSA|1> sending XFRM_MSG_UPDPOLICY: => 252 bytes @ 0x7fc7ae142680
Dec 26 05:57:51 11[KNL] <XauthRSA|1>    0: FC 00 00 00 19 00 05 00 E5 01 00 00 B8 BF 00 00  ................
Dec 26 05:57:51 11[KNL] <XauthRSA|1>   16: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
Dec 26 05:57:51 11[KNL] <XauthRSA|1>   32: AC 10 00 01 00 00 00 00 00 00 00 00 00 00 00 00  ................
Dec 26 05:57:51 11[KNL] <XauthRSA|1>   48: 00 00 00 00 00 00 00 00 00 02 00 00 20 00 00 00  ........... ....
Dec 26 05:57:51 11[KNL] <XauthRSA|1>   64: 00 00 00 00 00 00 00 00 FF FF FF FF FF FF FF FF  ................
Dec 26 05:57:51 11[KNL] <XauthRSA|1>   80: FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF  ................
Dec 26 05:57:51 11[KNL] <XauthRSA|1>   96: FF FF FF FF FF FF FF FF 00 00 00 00 00 00 00 00  ................
Dec 26 05:57:51 11[KNL] <XauthRSA|1>  112: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
Dec 26 05:57:51 11[KNL] <XauthRSA|1>  128: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
Dec 26 05:57:51 11[KNL] <XauthRSA|1>  144: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
Dec 26 05:57:51 11[KNL] <XauthRSA|1>  160: 00 00 00 00 00 00 00 00 83 0B 00 00 00 00 00 00  ................
Dec 26 05:57:51 11[KNL] <XauthRSA|1>  176: 02 00 00 00 00 00 00 00 44 00 05 00 0A 00 00 40  ........D......@
Dec 26 05:57:51 11[KNL] <XauthRSA|1>  192: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
Dec 26 05:57:51 11[KNL] <XauthRSA|1>  208: 32 00 00 00 02 00 00 00 DE 7E C3 D2 00 00 00 00  2........~......
Dec 26 05:57:51 11[KNL] <XauthRSA|1>  224: 00 00 00 00 00 00 00 00 01 00 00 00 01 00 00 00  ................
Dec 26 05:57:51 11[KNL] <XauthRSA|1>  240: FF FF FF FF FF FF FF FF FF FF FF FF              ............
Dec 26 05:57:51 11[KNL] <XauthRSA|1> getting a local address in traffic selector 0.0.0.0/0
Dec 26 05:57:51 11[KNL] <XauthRSA|1> using host %any
```

```
Dec 26 05:57:51 11[KNL] <XauthRSA|1> sending RTM_GETROUTE: => 44 bytes @ 0x7fc7ae142190
Dec 26 05:57:51 11[KNL] <XauthRSA|1>    0: 2C 00 00 00 1A 00 01 03 F5 00 00 00 B8 BF 00 00  ,...............
Dec 26 05:57:51 11[KNL] <XauthRSA|1>   16: 02 00 00 00 00 00 00 00 00 00 00 00 08 00 07 00  ................
Dec 26 05:57:51 11[KNL] <XauthRSA|1>   32: 0A 00 00 40 08 00 01 00 DE 7E C3 D2              ...@.....~..
Dec 26 05:57:51 11[KNL] <XauthRSA|1> using 10.0.0.1 as nexthop to reach zzz.ww.195.210/32
Dec 26 05:57:51 11[KNL] <XauthRSA|1> 10.0.0.64 is on interface eth0
Dec 26 05:57:51 11[MGR] <XauthRSA|1> checkin IKE_SA XauthRSA[1]
Dec 26 05:57:51 11[MGR] <XauthRSA|1> check-in of IKE_SA successful.
Dec 26 05:57:52 02[NET] received packet => 96 bytes @ 0x7fc7b29493e0
Dec 26 05:57:52 02[NET]    0: 00 00 00 00 12 26 6B 28 49 8A 93 2E 8B 6D D0 8D  .....&k(I....m..
Dec 26 05:57:52 02[NET]   16: E2 21 22 B0 08 10 05 01 57 44 1B 92 00 00 00 5C  .!".....WD.....\
Dec 26 05:57:52 02[NET]   32: 98 11 6F 3F C1 CE A3 8E 65 AB 16 1F 21 2E D0 E9  ..o?....e...!...
Dec 26 05:57:52 02[NET]   48: D3 E6 20 A0 35 86 94 7B E4 E2 BD 32 20 0F 53 AA  .. .5..{...2 .S.
Dec 26 05:57:52 02[NET]   64: 0E 73 CE D2 A8 7A F5 2D 2A 6C 91 4F 65 F0 4A DD  .s...z.-*l.Oe.J.
Dec 26 05:57:52 02[NET]   80: 49 F8 70 EF 2F 57 74 D9 93 DC 14 F6 7B 72 1F 59  I.p./Wt.....{r.Y
Dec 26 05:57:52 02[NET] received packet: from xxx.yy.212.14[4500] to 10.0.0.64[4500]
Dec 26 05:57:52 02[ENC] parsing header of message
Dec 26 05:57:52 02[ENC] parsing HEADER payload, 92 bytes left
Dec 26 05:57:52 02[ENC] parsing payload from => 92 bytes @ 0x7fc794000d14
Dec 26 05:57:52 02[ENC]    0: 12 26 6B 28 49 8A 93 2E 8B 6D D0 8D E2 21 22 B0  .&k(I....m...!".
Dec 26 05:57:52 02[ENC]   16: 08 10 05 01 57 44 1B 92 00 00 00 5C 98 11 6F 3F  ....WD.....\..o?
Dec 26 05:57:52 02[ENC]   32: C1 CE A3 8E 65 AB 16 1F 21 2E D0 E9 D3 E6 20 A0  ....e...!..... .
Dec 26 05:57:52 02[ENC]   48: 35 86 94 7B E4 E2 BD 32 20 0F 53 AA 0E 73 CE D2  5..{...2 .S..s..
Dec 26 05:57:52 02[ENC]   64: A8 7A F5 2D 2A 6C 91 4F 65 F0 4A DD 49 F8 70 EF  .z.-*l.Oe.J.I.p.
Dec 26 05:57:52 02[ENC]   80: 2F 57 74 D9 93 DC 14 F6 7B 72 1F 59              /Wt.....{r.Y
Dec 26 05:57:52 02[ENC]   parsing rule 0 IKE_SPI
Dec 26 05:57:52 02[ENC]    => 8 bytes @ 0x7fc794001288
Dec 26 05:57:52 02[ENC]    0: 12 26 6B 28 49 8A 93 2E                           .&k(I...
Dec 26 05:57:52 02[ENC]   parsing rule 1 IKE_SPI
Dec 26 05:57:52 02[ENC]    => 8 bytes @ 0x7fc794001290
Dec 26 05:57:52 02[ENC]    0: 8B 6D D0 8D E2 21 22 B0                           .m...!".
Dec 26 05:57:52 02[ENC]   parsing rule 2 U_INT_8
Dec 26 05:57:52 02[ENC]    => 8
Dec 26 05:57:52 02[ENC]   parsing rule 3 U_INT_4
Dec 26 05:57:52 02[ENC]    => 1
Dec 26 05:57:52 02[ENC]   parsing rule 4 U_INT_4
Dec 26 05:57:52 02[ENC]    => 0
Dec 26 05:57:52 02[ENC]   parsing rule 5 U_INT_8
Dec 26 05:57:52 02[ENC]    => 5
Dec 26 05:57:52 02[ENC]   parsing rule 6 RESERVED_BIT
Dec 26 05:57:52 02[ENC]    => 0
Dec 26 05:57:52 02[ENC]   parsing rule 7 RESERVED_BIT
Dec 26 05:57:52 02[ENC]    => 0
Dec 26 05:57:52 02[ENC]   parsing rule 8 FLAG
Dec 26 05:57:52 02[ENC]    => 0
Dec 26 05:57:52 02[ENC]   parsing rule 9 FLAG
Dec 26 05:57:52 02[ENC]    => 0
Dec 26 05:57:52 02[ENC]   parsing rule 10 FLAG
Dec 26 05:57:52 02[ENC]    => 0
Dec 26 05:57:52 02[ENC]   parsing rule 11 FLAG
Dec 26 05:57:52 02[ENC]    => 0
Dec 26 05:57:52 02[ENC]   parsing rule 12 FLAG
Dec 26 05:57:52 02[ENC]    => 0
Dec 26 05:57:52 02[ENC]   parsing rule 13 FLAG
Dec 26 05:57:52 02[ENC]    => 1
Dec 26 05:57:52 02[ENC]   parsing rule 14 U_INT_32
Dec 26 05:57:52 02[ENC]    => 1464081298
Dec 26 05:57:52 02[ENC]   parsing rule 15 HEADER_LENGTH
Dec 26 05:57:52 02[ENC]    => 92
Dec 26 05:57:52 02[ENC] parsing HEADER payload finished
Dec 26 05:57:52 02[ENC] parsed a INFORMATIONAL_V1 message header
Dec 26 05:57:52 02[NET] waiting for data on sockets
Dec 26 05:57:52 10[MGR] checkout IKE_SA by message
Dec 26 05:57:52 10[MGR] IKE_SA XauthRSA[1] successfully checked out
Dec 26 05:57:52 10[NET] <XauthRSA|1> received packet: from xxx.yy.212.14[4500] to 10.0.0.64[4500] (92 bytes)
Dec 26 05:57:52 10[ENC] <XauthRSA|1> parsing body of message, first payload is HASH_V1
Dec 26 05:57:52 10[ENC] <XauthRSA|1> parsing ENCRYPTED_V1 payload, 64 bytes left
Dec 26 05:57:52 10[ENC] <XauthRSA|1> parsing payload from => 64 bytes @ 0x7fc794000d30
Dec 26 05:57:52 10[ENC] <XauthRSA|1>    0: 98 11 6F 3F C1 CE A3 8E 65 AB 16 1F 21 2E D0 E9  ..o?....e...!...
Dec 26 05:57:52 10[ENC] <XauthRSA|1>   16: D3 E6 20 A0 35 86 94 7B E4 E2 BD 32 20 0F 53 AA  .. .5..{...2 .S.
Dec 26 05:57:52 10[ENC] <XauthRSA|1>   32: 0E 73 CE D2 A8 7A F5 2D 2A 6C 91 4F 65 F0 4A DD  .s...z.-*l.Oe.J.
Dec 26 05:57:52 10[ENC] <XauthRSA|1>   48: 49 F8 70 EF 2F 57 74 D9 93 DC 14 F6 7B 72 1F 59  I.p./Wt.....{r.Y
Dec 26 05:57:52 10[ENC] <XauthRSA|1>   parsing rule 0 ENCRYPTED_DATA
Dec 26 05:57:52 10[ENC] <XauthRSA|1>    => 64 bytes @ 0x7fc764007400
Dec 26 05:57:52 10[ENC] <XauthRSA|1>    0: 98 11 6F 3F C1 CE A3 8E 65 AB 16 1F 21 2E D0 E9  ..o?....e...!...
```

```
Dec 26 05:57:52 10[ENC] <XauthRSA|1>   16: D3 E6 20 A0 35 86 94 7B E4 E2 BD 32 20 0F 53 AA  .. .5..{...2 .S.
Dec 26 05:57:52 10[ENC] <XauthRSA|1>   32: 0E 73 CE D2 A8 7A F5 2D 2A 6C 91 4F 65 F0 4A DD  .s...z.-*l.Oe.J.
Dec 26 05:57:52 10[ENC] <XauthRSA|1>   48: 49 F8 70 EF 2F 57 74 D9 93 DC 14 F6 7B 72 1F 59  I.p./Wt.....{r.Y
Dec 26 05:57:52 10[ENC] <XauthRSA|1> parsing ENCRYPTED_V1 payload finished
Dec 26 05:57:52 10[ENC] <XauthRSA|1> process payload of type ENCRYPTED_V1
Dec 26 05:57:52 10[ENC] <XauthRSA|1> found an encrypted payload
Dec 26 05:57:52 10[IKE] <XauthRSA|1> next IV for MID 1464081298 => 16 bytes @ 0x7fc764006cc0
Dec 26 05:57:52 10[IKE] <XauthRSA|1>    0: E7 37 3C 5F 88 7D 87 5D F5 52 07 3A 78 C9 74 44  .7<_.}.].R.:x.tD
Dec 26 05:57:52 10[ENC] <XauthRSA|1> decrypting payloads:
Dec 26 05:57:52 10[ENC] <XauthRSA|1> encrypted => 64 bytes @ 0x7fc764007400
Dec 26 05:57:52 10[ENC] <XauthRSA|1>    0: 98 11 6F 3F C1 CE A3 8E 65 AB 16 1F 21 2E D0 E9  ..o?....e...!...
Dec 26 05:57:52 10[ENC] <XauthRSA|1>   16: D3 E6 20 A0 35 86 94 7B E4 E2 BD 32 20 0F 53 AA  .. .5..{...2 .S.
Dec 26 05:57:52 10[ENC] <XauthRSA|1>   32: 0E 73 CE D2 A8 7A F5 2D 2A 6C 91 4F 65 F0 4A DD  .s...z.-*l.Oe.J.
Dec 26 05:57:52 10[ENC] <XauthRSA|1>   48: 49 F8 70 EF 2F 57 74 D9 93 DC 14 F6 7B 72 1F 59  I.p./Wt.....{r.Y
Dec 26 05:57:52 10[ENC] <XauthRSA|1> plain => 64 bytes @ 0x7fc764007400
Dec 26 05:57:52 10[ENC] <XauthRSA|1>    0: 0B 00 00 18 26 4F 20 2B 0F EB F1 75 20 10 15 1B  ....&O +...u ...
Dec 26 05:57:52 10[ENC] <XauthRSA|1>   16: B5 40 65 07 3E 56 D5 FD 00 00 00 20 00 00 00 01  .@e.>V..... ....
Dec 26 05:57:52 10[ENC] <XauthRSA|1>   32: 01 10 8D 28 12 26 6B 28 49 8A 93 2E 8B 6D D0 8D  ...(.&k(I....m..
Dec 26 05:57:52 10[ENC] <XauthRSA|1>   48: E2 21 22 B0 00 00 08 D4 00 00 00 00 00 00 00 08  .!".............
Dec 26 05:57:52 10[ENC] <XauthRSA|1> parsing HASH_V1 payload, 64 bytes left
Dec 26 05:57:52 10[ENC] <XauthRSA|1> parsing payload from => 64 bytes @ 0x7fc764007400
Dec 26 05:57:52 10[ENC] <XauthRSA|1>    0: 0B 00 00 18 26 4F 20 2B 0F EB F1 75 20 10 15 1B  ....&O +...u ...
Dec 26 05:57:52 10[ENC] <XauthRSA|1>   16: B5 40 65 07 3E 56 D5 FD 00 00 00 20 00 00 00 01  .@e.>V..... ....
Dec 26 05:57:52 10[ENC] <XauthRSA|1>   32: 01 10 8D 28 12 26 6B 28 49 8A 93 2E 8B 6D D0 8D  ...(.&k(I....m..
Dec 26 05:57:52 10[ENC] <XauthRSA|1>   48: E2 21 22 B0 00 00 08 D4 00 00 00 00 00 00 00 08  .!".............
Dec 26 05:57:52 10[ENC] <XauthRSA|1>   parsing rule 0 U_INT_8
Dec 26 05:57:52 10[ENC] <XauthRSA|1>    => 11
Dec 26 05:57:52 10[ENC] <XauthRSA|1>   parsing rule 1 RESERVED_BYTE
Dec 26 05:57:52 10[ENC] <XauthRSA|1>    => 0
Dec 26 05:57:52 10[ENC] <XauthRSA|1>   parsing rule 2 PAYLOAD_LENGTH
Dec 26 05:57:52 10[ENC] <XauthRSA|1>    => 24
Dec 26 05:57:52 10[ENC] <XauthRSA|1>   parsing rule 3 CHUNK_DATA
Dec 26 05:57:52 10[ENC] <XauthRSA|1>    => 20 bytes @ 0x7fc7640073e0
Dec 26 05:57:52 10[ENC] <XauthRSA|1>    0: 26 4F 20 2B 0F EB F1 75 20 10 15 1B B5 40 65 07  &O +...u ....@e.
Dec 26 05:57:52 10[ENC] <XauthRSA|1>   16: 3E 56 D5 FD                                      >V..
Dec 26 05:57:52 10[ENC] <XauthRSA|1> parsing HASH_V1 payload finished
Dec 26 05:57:52 10[ENC] <XauthRSA|1> parsing NOTIFY_V1 payload, 40 bytes left
Dec 26 05:57:52 10[ENC] <XauthRSA|1> parsing payload from => 40 bytes @ 0x7fc764007418
Dec 26 05:57:52 10[ENC] <XauthRSA|1>    0: 00 00 00 20 00 00 00 01 01 10 8D 28 12 26 6B 28  ... .......(.&k(
Dec 26 05:57:52 10[ENC] <XauthRSA|1>   16: 49 8A 93 2E 8B 6D D0 8D E2 21 22 B0 00 00 08 D4  I....m...!".....
Dec 26 05:57:52 10[ENC] <XauthRSA|1>   32: 00 00 00 00 00 00 00 08                          ........
Dec 26 05:57:52 10[ENC] <XauthRSA|1>   parsing rule 0 U_INT_8
Dec 26 05:57:52 10[ENC] <XauthRSA|1>    => 0
Dec 26 05:57:52 10[ENC] <XauthRSA|1>   parsing rule 1 RESERVED_BIT
Dec 26 05:57:52 10[ENC] <XauthRSA|1>    => 0
Dec 26 05:57:52 10[ENC] <XauthRSA|1>   parsing rule 2 RESERVED_BIT
Dec 26 05:57:52 10[ENC] <XauthRSA|1>    => 0
Dec 26 05:57:52 10[ENC] <XauthRSA|1>   parsing rule 3 RESERVED_BIT
Dec 26 05:57:52 10[ENC] <XauthRSA|1>    => 0
Dec 26 05:57:52 10[ENC] <XauthRSA|1>   parsing rule 4 RESERVED_BIT
Dec 26 05:57:52 10[ENC] <XauthRSA|1>    => 0
Dec 26 05:57:52 10[ENC] <XauthRSA|1>   parsing rule 5 RESERVED_BIT
Dec 26 05:57:52 10[ENC] <XauthRSA|1>    => 0
Dec 26 05:57:52 10[ENC] <XauthRSA|1>   parsing rule 6 RESERVED_BIT
Dec 26 05:57:52 10[ENC] <XauthRSA|1>    => 0
Dec 26 05:57:52 10[ENC] <XauthRSA|1>   parsing rule 7 RESERVED_BIT
Dec 26 05:57:52 10[ENC] <XauthRSA|1>    => 0
Dec 26 05:57:52 10[ENC] <XauthRSA|1>   parsing rule 8 RESERVED_BIT
Dec 26 05:57:52 10[ENC] <XauthRSA|1>    => 0
Dec 26 05:57:52 10[ENC] <XauthRSA|1>   parsing rule 9 PAYLOAD_LENGTH
Dec 26 05:57:52 10[ENC] <XauthRSA|1>    => 32
Dec 26 05:57:52 10[ENC] <XauthRSA|1>   parsing rule 10 U_INT_32
Dec 26 05:57:52 10[ENC] <XauthRSA|1>    => 1
Dec 26 05:57:52 10[ENC] <XauthRSA|1>   parsing rule 11 U_INT_8
Dec 26 05:57:52 10[ENC] <XauthRSA|1>    => 1
Dec 26 05:57:52 10[ENC] <XauthRSA|1>   parsing rule 12 SPI_SIZE
Dec 26 05:57:52 10[ENC] <XauthRSA|1>    => 16
Dec 26 05:57:52 10[ENC] <XauthRSA|1>   parsing rule 13 U_INT_16
Dec 26 05:57:52 10[ENC] <XauthRSA|1>    => 36136
Dec 26 05:57:52 10[ENC] <XauthRSA|1>   parsing rule 14 SPI
Dec 26 05:57:52 10[ENC] <XauthRSA|1>    => 16 bytes @ 0x7fc7640063c0
Dec 26 05:57:52 10[ENC] <XauthRSA|1>    0: 12 26 6B 28 49 8A 93 2E 8B 6D D0 8D E2 21 22 B0  .&k(I....m...!".
Dec 26 05:57:52 10[ENC] <XauthRSA|1>   parsing rule 15 CHUNK_DATA
Dec 26 05:57:52 10[ENC] <XauthRSA|1>    => 4 bytes @ 0x7fc764007300
Dec 26 05:57:52 10[ENC] <XauthRSA|1>    0: 00 00 08 D4                                      ....
```

```
Dec 26 05:57:52 10[ENC] <XauthRSA|1> parsing NOTIFY_V1 payload finished
Dec 26 05:57:52 10[ENC] <XauthRSA|1> parsed content of encrypted payload
Dec 26 05:57:52 10[ENC] <XauthRSA|1> insert decrypted payload of type HASH_V1 at end of list
Dec 26 05:57:52 10[ENC] <XauthRSA|1> insert decrypted payload of type NOTIFY_V1 at end of list
Dec 26 05:57:52 10[ENC] <XauthRSA|1> verifying message structure
Dec 26 05:57:52 10[ENC] <XauthRSA|1> found payload of type NOTIFY_V1
Dec 26 05:57:52 10[ENC] <XauthRSA|1> found payload of type NOTIFY_V1
Dec 26 05:57:52 10[ENC] <XauthRSA|1> parsed INFORMATIONAL_V1 request 1464081298 [ HASH N(DPD) ]
Dec 26 05:57:52 10[IKE] <XauthRSA|1> Hash => 20 bytes @ 0x7fc764001150
Dec 26 05:57:52 10[IKE] <XauthRSA|1>    0: 26 4F 20 2B 0F EB F1 75 20 10 15 1B B5 40 65 07  &O +...u ....@e.
Dec 26 05:57:52 10[IKE] <XauthRSA|1>   16: 3E 56 D5 FD                                      >V..
Dec 26 05:57:52 10[ENC] <XauthRSA|1> HASH received => 20 bytes @ 0x7fc7640073e0
Dec 26 05:57:52 10[ENC] <XauthRSA|1>    0: 26 4F 20 2B 0F EB F1 75 20 10 15 1B B5 40 65 07  &O +...u ....@e.
Dec 26 05:57:52 10[ENC] <XauthRSA|1>   16: 3E 56 D5 FD                                      >V..
Dec 26 05:57:52 10[ENC] <XauthRSA|1> HASH expected => 20 bytes @ 0x7fc764001150
Dec 26 05:57:52 10[ENC] <XauthRSA|1>    0: 26 4F 20 2B 0F EB F1 75 20 10 15 1B B5 40 65 07  &O +...u ....@e.
Dec 26 05:57:52 10[ENC] <XauthRSA|1>   16: 3E 56 D5 FD                                      >V..
Dec 26 05:57:52 10[KNL] <XauthRSA|1> querying SAD entry with SPI cd0ecf6b for update
Dec 26 05:57:52 10[KNL] <XauthRSA|1> sending XFRM_MSG_GETSA: => 40 bytes @ 0x7fc7ae943290
Dec 26 05:57:52 10[KNL] <XauthRSA|1>    0: 28 00 00 00 12 00 01 00 E6 01 00 00 B8 BF 00 00  (...............
Dec 26 05:57:52 10[KNL] <XauthRSA|1>   16: 0A 00 00 40 00 00 00 00 00 00 00 00 00 00 00 00  ...@............
Dec 26 05:57:52 10[KNL] <XauthRSA|1>   32: CD 0E CF 6B 02 00 32 00                          ...k..2.
Dec 26 05:57:52 10[KNL] <XauthRSA|1> querying replay state from SAD entry with SPI cd0ecf6b
Dec 26 05:57:52 10[KNL] <XauthRSA|1> sending XFRM_MSG_GETAE: => 64 bytes @ 0x7fc7ae943690
Dec 26 05:57:52 10[KNL] <XauthRSA|1>    0: 40 00 00 00 1F 00 01 00 E7 01 00 00 B8 BF 00 00  @...............
Dec 26 05:57:52 10[KNL] <XauthRSA|1>   16: 0A 00 00 40 00 00 00 00 00 00 00 00 00 00 00 00  ...@............
Dec 26 05:57:52 10[KNL] <XauthRSA|1>   32: CD 0E CF 6B 02 00 32 00 00 00 00 00 00 00 00 00  ...k..2.........
Dec 26 05:57:52 10[KNL] <XauthRSA|1>   48: 00 00 00 00 00 00 00 00 02 00 00 00 00 00 00 00  ................
Dec 26 05:57:52 10[KNL] <XauthRSA|1> deleting SAD entry with SPI cd0ecf6b  (mark 0/0x00000000)
Dec 26 05:57:52 10[KNL] <XauthRSA|1> sending XFRM_MSG_DELSA: => 40 bytes @ 0x7fc7ae942d90
Dec 26 05:57:52 10[KNL] <XauthRSA|1>    0: 28 00 00 00 11 00 05 00 E8 01 00 00 B8 BF 00 00  (...............
Dec 26 05:57:52 10[KNL] <XauthRSA|1>   16: 0A 00 00 40 00 00 00 00 00 00 00 00 00 00 00 00  ...@............
Dec 26 05:57:52 10[KNL] <XauthRSA|1>   32: CD 0E CF 6B 02 00 32 00                          ...k..2.
Dec 26 05:57:52 10[KNL] <XauthRSA|1> deleted SAD entry with SPI cd0ecf6b (mark 0/0x00000000)
Dec 26 05:57:52 10[KNL] <XauthRSA|1> updating SAD entry with SPI cd0ecf6b from zzz.ww.195.210[1363]..10.0.0.64
[4500] to xxx.yy.212.14[4500]..10.0.0.64[4500]
Dec 26 05:57:52 10[KNL] <XauthRSA|1> sending XFRM_MSG_NEWSA: => 560 bytes @ 0x7fc7ae943290
Dec 26 05:57:52 10[KNL] <XauthRSA|1>    0: 30 02 00 00 10 00 05 00 E9 01 00 00 B8 BF 00 00  0...............
Dec 26 05:57:52 10[KNL] <XauthRSA|1>   16: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
Dec 26 05:57:52 10[KNL] <XauthRSA|1>   32: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
Dec 26 05:57:52 10[KNL] <XauthRSA|1>   48: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
Dec 26 05:57:52 10[KNL] <XauthRSA|1>   64: 00 00 00 00 00 00 00 00 00 0A 00 00 40 00 00 00  ............@...
Dec 26 05:57:52 10[KNL] <XauthRSA|1>   80: 00 00 00 00 00 00 00 00 CD 0E CF 6B 32 00 00 00  ...........k2...
Dec 26 05:57:52 10[KNL] <XauthRSA|1>   96: CA 41 D4 0E 00 00 00 00 00 00 00 00 00 00 00 00  .A..............
Dec 26 05:57:52 10[KNL] <XauthRSA|1>  112: FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF  ................
Dec 26 05:57:52 10[KNL] <XauthRSA|1>  128: FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF  ................
Dec 26 05:57:52 10[KNL] <XauthRSA|1>  144: C9 27 00 00 00 00 00 00 30 2A 00 00 00 00 00 00  .'......0*......
Dec 26 05:57:52 10[KNL] <XauthRSA|1>  160: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
Dec 26 05:57:52 10[KNL] <XauthRSA|1>  176: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
Dec 26 05:57:52 10[KNL] <XauthRSA|1>  192: DF F8 9C 54 00 00 00 00 00 00 00 00 00 00 00 00  ...T............
Dec 26 05:57:52 10[KNL] <XauthRSA|1>  208: 00 00 00 00 00 00 00 00 00 00 00 00 21 09 00 00  ............!...
Dec 26 05:57:52 10[KNL] <XauthRSA|1>  224: 01 00 00 00 02 00 01 20 20 00 00 00 00 00 00 00  .......  .......
Dec 26 05:57:52 10[KNL] <XauthRSA|1>  240: 5C 00 01 00 68 6D 61 63 28 73 68 61 31 29 00 00  \...hmac(sha1)..
Dec 26 05:57:52 10[KNL] <XauthRSA|1>  256: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
Dec 26 05:57:52 10[KNL] <XauthRSA|1>  272: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
Dec 26 05:57:52 10[KNL] <XauthRSA|1>  288: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
Dec 26 05:57:52 10[KNL] <XauthRSA|1>  304: 00 00 00 00 A0 00 00 00 DD A7 25 77 55 FF 32 AE  ..........%wU.2.
Dec 26 05:57:52 10[KNL] <XauthRSA|1>  320: 8E 89 0B 68 C5 07 FB C5 7F FD BC E6 60 00 14 00  ...h........`...
Dec 26 05:57:52 10[KNL] <XauthRSA|1>  336: 68 6D 61 63 28 73 68 61 31 29 00 00 00 00 00 00  hmac(sha1)......
Dec 26 05:57:52 10[KNL] <XauthRSA|1>  352: AC CB B2 98 03 88 FF FF 00 00 00 00 00 00 00 00  ................
Dec 26 05:57:52 10[KNL] <XauthRSA|1>  368: A0 CB B2 98 03 88 FF FF 00 00 00 00 00 00 00 00  ................
Dec 26 05:57:52 10[KNL] <XauthRSA|1>  384: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
Dec 26 05:57:52 10[KNL] <XauthRSA|1>  400: A0 00 00 00 00 60 00 00 00 00 DD A7 25 77 55 FF 32 AE  ....`.....%wU.2.
Dec 26 05:57:52 10[KNL] <XauthRSA|1>  416: 8E 89 0B 68 C5 07 FB C5 7F FD BC E6 58 00 02 00  ...h........X...
Dec 26 05:57:52 10[KNL] <XauthRSA|1>  432: 63 62 63 28 61 65 73 29 00 00 00 00 00 00 00 00  cbc(aes)........
Dec 26 05:57:52 10[KNL] <XauthRSA|1>  448: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
Dec 26 05:57:52 10[KNL] <XauthRSA|1>  464: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
Dec 26 05:57:52 10[KNL] <XauthRSA|1>  480: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
Dec 26 05:57:52 10[KNL] <XauthRSA|1>  496: 80 00 00 00 A1 F7 34 64 60 4F CC D9 6E D9 D8 A8  ......4d`O..n...
Dec 26 05:57:52 10[KNL] <XauthRSA|1>  512: 97 AA 91 92 1C 00 04 00 02 00 11 94 11 94 00 00  ................
Dec 26 05:57:52 10[KNL] <XauthRSA|1>  528: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
Dec 26 05:57:52 10[KNL] <XauthRSA|1>  544: 10 00 0A 00 00 00 00 00 FA 02 00 00 FF FF FF FF  ................
Dec 26 05:57:52 10[KNL] <XauthRSA|1> querying SAD entry with SPI 0f2e26cb for update
Dec 26 05:57:52 10[KNL] <XauthRSA|1> sending XFRM_MSG_GETSA: => 40 bytes @ 0x7fc7ae943290
Dec 26 05:57:52 10[KNL] <XauthRSA|1>    0: 28 00 00 00 12 00 01 00 EA 01 00 00 B8 BF 00 00  (...............
```

```
Dec 26 05:57:52 10[KNL] <XauthRSA|1>   16: DE 7E C3 D2 00 00 00 00 00 00 00 00 00 00 00 00  .~..............
Dec 26 05:57:52 10[KNL] <XauthRSA|1>   32: 0F 2E 26 CB 02 00 32 00                          ..&...2.
Dec 26 05:57:52 10[KNL] <XauthRSA|1> querying replay state from SAD entry with SPI 0f2e26cb
Dec 26 05:57:52 10[KNL] <XauthRSA|1> sending XFRM_MSG_GETAE: => 64 bytes @ 0x7fc7ae943690
Dec 26 05:57:52 10[KNL] <XauthRSA|1>    0: 40 00 00 00 1F 00 01 00 EB 01 00 00 B8 BF 00 00  @...............
Dec 26 05:57:52 10[KNL] <XauthRSA|1>   16: DE 7E C3 D2 00 00 00 00 00 00 00 00 00 00 00 00  .~..............
Dec 26 05:57:52 10[KNL] <XauthRSA|1>   32: 0F 2E 26 CB 02 00 32 00 00 00 00 00 00 00 00 00  ..&...2.........
Dec 26 05:57:52 10[KNL] <XauthRSA|1>   48: 00 00 00 00 00 00 00 00 02 00 00 00 00 00 00 00  ................
Dec 26 05:57:52 10[KNL] <XauthRSA|1> deleting SAD entry with SPI 0f2e26cb  (mark 0/0x00000000)
Dec 26 05:57:52 10[KNL] <XauthRSA|1> sending XFRM_MSG_DELSA: => 40 bytes @ 0x7fc7ae942d90
Dec 26 05:57:52 10[KNL] <XauthRSA|1>    0: 28 00 00 00 11 00 05 00 EC 01 00 00 B8 BF 00 00  (...............
Dec 26 05:57:52 10[KNL] <XauthRSA|1>   16: DE 7E C3 D2 00 00 00 00 00 00 00 00 00 00 00 00  .~..............
Dec 26 05:57:52 10[KNL] <XauthRSA|1>   32: 0F 2E 26 CB 02 00 32 00                          ..&...2.
Dec 26 05:57:52 10[KNL] <XauthRSA|1> deleted SAD entry with SPI 0f2e26cb (mark 0/0x00000000)
Dec 26 05:57:52 10[KNL] <XauthRSA|1> updating SAD entry with SPI 0f2e26cb from 10.0.0.64[4500]..zzz.ww.195.210
[1363] to 10.0.0.64[4500]..xxx.yy.212.14[4500]
Dec 26 05:57:52 10[KNL] <XauthRSA|1> sending XFRM_MSG_NEWSA: => 560 bytes @ 0x7fc7ae943290
Dec 26 05:57:52 10[KNL] <XauthRSA|1>    0: 30 02 00 00 10 00 05 00 ED 01 00 00 B8 BF 00 00  0...............
Dec 26 05:57:52 10[KNL] <XauthRSA|1>   16: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
Dec 26 05:57:52 10[KNL] <XauthRSA|1>   32: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
Dec 26 05:57:52 10[KNL] <XauthRSA|1>   48: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
Dec 26 05:57:52 10[KNL] <XauthRSA|1>   64: 00 00 00 00 00 00 00 00 CA 41 D4 0E 00 00 00 00  .........A......
Dec 26 05:57:52 10[KNL] <XauthRSA|1>   80: 00 00 00 00 00 00 00 00 0F 2E 26 CB 32 00 00 00  ..........&.2...
Dec 26 05:57:52 10[KNL] <XauthRSA|1>   96: 0A 00 00 40 00 00 00 00 00 00 00 00 00 00 00 00  ...@............
Dec 26 05:57:52 10[KNL] <XauthRSA|1>  112: FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF  ................
Dec 26 05:57:52 10[KNL] <XauthRSA|1>  128: FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF  ................
Dec 26 05:57:52 10[KNL] <XauthRSA|1>  144: 91 26 00 00 00 00 00 00 30 2A 00 00 00 00 00 00  .&......0*......
Dec 26 05:57:52 10[KNL] <XauthRSA|1>  160: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
Dec 26 05:57:52 10[KNL] <XauthRSA|1>  176: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
Dec 26 05:57:52 10[KNL] <XauthRSA|1>  192: DF F8 9C 54 00 00 00 00 00 00 00 00 00 00 00 00  ...T............
Dec 26 05:57:52 10[KNL] <XauthRSA|1>  208: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
Dec 26 05:57:52 10[KNL] <XauthRSA|1>  224: 01 00 00 00 02 00 01 20 20 00 00 00 00 00 00 00  .......  .......
Dec 26 05:57:52 10[KNL] <XauthRSA|1>  240: 5C 00 01 00 68 6D 61 63 28 73 68 61 31 29 00 00  \...hmac(sha1)..
Dec 26 05:57:52 10[KNL] <XauthRSA|1>  256: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
Dec 26 05:57:52 10[KNL] <XauthRSA|1>  272: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
Dec 26 05:57:52 10[KNL] <XauthRSA|1>  288: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
Dec 26 05:57:52 10[KNL] <XauthRSA|1>  304: 00 00 00 00 A0 00 00 00 C4 87 F2 CB 9C CB 3E 22  ..............>"
Dec 26 05:57:52 10[KNL] <XauthRSA|1>  320: C4 72 64 F6 9C 45 EF 66 20 9B 4C BF 60 00 14 00  .rd..E.f .L.`...
Dec 26 05:57:52 10[KNL] <XauthRSA|1>  336: 68 6D 61 63 28 73 68 61 31 29 00 A4 03 88 FF FF  hmac(sha1)......
Dec 26 05:57:52 10[KNL] <XauthRSA|1>  352: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
```

#4 - 18.02.2015 17:55 - Tobias Brunner

- Status changed from New to Feedback

- Assignee deleted (Martin Willi)

- Priority changed from Urgent to Normal

> If "NAT mappings of ESP CHILD_SA...." is a normal behavior for client have multi IP, then why after update_sa_job_create the byte accounting number lost?

If the kernel notices that the client's port and/or IP has changed it will notify the keying daemon and you'll see this message. It causes strongSwan to update the IPsec SAs with the new address. This is done by deleting and recreating the SA with the new address (since the tuple SPI, protocol, destination address is used as index we can't just update the SAs). We do copy all the properties from the old SAs to the new ones (including the ESP sequence numbers) but traffic counters are reset on the new SAs. Therefore, when the SAs are queried later when sending the RADIUS Accounting messages you'll only get stats since that last reset.

Unlike when an IPsec SA is rekeyed the RADIUS plugin does not get notified when the above happens. So it is not able to query the traffic counters on the old SAs before they get replaced. Actually, that there are new SAs at all (and therefore reset counters) depends on the kernel backend, so blindly querying the SA before the update and then add that to the number retrieved later could result in too high a number. So this definitely needs some more investigating to fix properly.

As a workaround you could e.g. patch the *kernel-netlink* plugin so that it always returns *NOT_SUPPORTED* from the update_sa() method, or you patch update_hosts() in source:src/libcharon/sa/ike_sa.c#L965 so it does not call update() on each CHILD_SA but instead just rekeyes them directly. Because if the CHILD_SA is rekeyed when the client's endpoint has changed the RADIUS plugin should be able to handle it correctly.

#5 - 24.03.2015 14:04 - Tobias Brunner

- File 0001-kernel-netlink-Copy-current-usage-stats-to-new-SA-in.patch added

- Tracker changed from Issue to Bug

> We do copy all the properties from the old SAs to the new ones (including the ESP sequence numbers) but traffic counters are reset on the new SAs.

I noticed that we can actually copy the traffic counters to the new SA. The attached patch should fix the issue.

#6 - 25.03.2015 12:05 - Tobias Brunner

- Subject changed from For some traffic, the output packets send to radius is not correct. to Usage statistics of IPsec SAs are incorrect after client's (NAT) endpoint changed

- Status changed from Feedback to Closed

- Assignee set to Tobias Brunner

- Target version set to 5.3.0

- Resolution set to Fixed

Files

0001-kernel-netlink-Copy-current-usage-stats-to-new-SA-in.patch	3.92 KB	24.03.2015	Tobias Brunner