# strongSwan - Bug #3198

## VICI child-updown event of the IKEv1 termination doesn't show the byte data correctly

09.10.2019 17:29 - Sung Kim

| | | | |
|---|---|---|---|
| **Status:** | Closed | **Start date:** | |
| **Priority:** | Normal | **Due date:** | |
| **Assignee:** | Tobias Brunner | **Estimated time:** | 0.00 hour |
| **Category:** | vici | | |
| **Target version:** | 5.8.2 | | |
| **Affected version:** | 5.8.0 | **Resolution:** | Fixed |

**Description**

Hi,
I have a question about the byte data in the VICI child-updown event ('down') from the IKEv1 termination. When the VPN connection is terminated, the child-updown event doesn't provide the byte data ("bytes-in" and "bytes-out"). They are just zeros and the child state is "DELETED". Is this the correct behavior?
However, the updown event ("down") of the IKEv2 termination shows the byte data correctly (the child state is "ESTABLISHED").

### Associated revisions

**Revision 08d0342c - 25.10.2019 16:15 - Tobias Brunner**

vici: List additional information for deleted CHILD_SAs

If a CHILD_SA is terminated, the updown event is triggered after the CHILD_SA is set to state CHILD_DELETED, so no usage stats or detail information like SPIs were reported. However, when an IKEv2 SA is terminated, the updown event for its children is triggered without changing the state first, that is, they usually remain in state INSTALLED and detailed data was reported in the event. IKEv1 CHILD_SAs are always terminated individually, i.e. with state change and no extra data so far.

With this change usage stats are also returned for individually deleted CHILD_SAs as long as the SA has not yet expired.

Fixes #3198.

### History

**#1 - 09.10.2019 18:09 - Tobias Brunner**

*- Category changed from vici to ikev1*

*- Status changed from New to Feedback*

<usualdisclaimer> **You shouldn't be using IKEv1 anymore.** </usualdisclaimer>

> When the VPN connection is terminated, the child-updown event doesn't provide the byte data ("bytes-in" and "bytes-out"). They are just zeros and the child state is "DELETED". Is this the correct behavior?
> However, the updown event ("down") of the IKEv2 termination shows the byte data correctly (the child state is "ESTABLISHED").

If you are referring to closing the complete IKE_SA then the different states are to be expected. For IKEv2, the individual CHILD_SAs are not deleted, an updown event is just triggered for them without changing the state first or logging anything about them etc. However, for IKEv1, each individual CHILD_SA is deleted separately because there is no strict relation between IKE and CHILD_SAs there, so the behavior is the same as manually terminating the CHILD_SAs (which changes the state and logs status information about the closed CHILD_SAs).

That the usage numbers are zero shouldn't be the case though. Unless the CHILD_SA actually never was used, or it already expired (the latter should produce errors in the log about querying a non-existent SA in the kernel). As mentioned above, status information is logged about closed IKEv1 CHILD_SAs, which includes usage numbers. Check what numbers are logged there.

**#2 - 09.10.2019 18:40 - Sung Kim**

> If you are referring to closing the complete IKE_SA then the different states are to be expected.

Yes, the termination was executed by the "vici.Session().terminate({"ike": ike_sa_name})"

> That the usage numbers are zero shouldn't be the case though. Unless the CHILD_SA actually never was used, or it already expired (the latter should produce errors in the log about querying a non-existent SA in the kernel). As mentioned above, status information is logged about closed IKEv1 CHILD_SAs, which includes usage numbers. Check what numbers are logged there.

I was confused about the numbers. The child SA ("DELETED") in the child-updown event **didn't have the byte data at all** (I've made some traffic though). Should it have the data?


```
"ike_sa_name": {
    "uniqueid": "2",
    "version": "1",
    "state": "ESTABLISHED",
    "local-host": "X.X.X.X",
    "local-port": "4500",
    "local-id": "XXXXXXXX",
    "remote-host": "X.X.X.X",
    "remote-port": "4500",
    "remote-id": "XXXXXXX",
    "initiator": "yes",
    "initiator-spi": "22dc527080c9c22d",
    "responder-spi": "6a01fa1d04097f10",
    "nat-local": "yes",
    "nat-remote": "yes",
    "nat-any": "yes",
    "encr-alg": "AES_CBC",
    "encr-keysize": "256",
    "integ-alg": "HMAC_SHA2_384_192",
    "prf-alg": "PRF_HMAC_SHA2_384",
    "dh-group": "ECP_384",
    "established": "15",
    "rekey-time": "14034",
    "local-vips": [
        "X.X.X.X"
    ],
    "tasks-queued": [
        "ISAKMP_DELETE"
    ],
    "tasks-active": [
        "QUICK_DELETE"
    ],
    "child-sas": {
        "child_sa_name": {
            "name": "child_sa_name",
            "uniqueid": "2",
            "reqid": "2",
            "state": "DELETED",
            "mode": "TUNNEL",
            "local-ts": [
                "x.x.x.x/x"
            ],
            "remote-ts": [
                "0.0.0.0/0"
            ]
        }
    }
}
```


#### #3 - 09.10.2019 19:27 - Tobias Brunner

*- Category changed from ikev1 to vici*

> I was confused about the numbers. The child SA ("DELETED") in the child-updown event **didn't have the byte data at all** (I've made some traffic though). Should it have the data?

Ah, I see. The *vici* plugin only returns some details about a CHILD_SA if it is in an "active" state (INSTALLED, REKEYING, REKEYED, see source:src/libcharon/plugins/vici/vici_query.c#L169). So neither DELETED, nor DELETING is included there and if the CHILD_SA is in either of these states you won't get usage numbers or other advanced info (like protocol, SPIs, marks, algorithms, lifetimes). That affects IKEv2 too if CHILD_SAs are terminated individually, as the state is set to DELETED before the event is triggered. But, as mentioned, not if the IKE_SA is deleted completely as the state just remains as is then.

I guess we could return some of the additional info for SAs in state DELETING/DELETED (but e.g. lifetimes don't really make sense). I'll have a look at this tomorrow.

#### #4 - 10.10.2019 15:54 - Tobias Brunner

*- Tracker changed from Issue to Bug*

*- Assignee set to Tobias Brunner*

*- Target version set to 5.8.2*

*- Resolution set to Fixed*

I pushed a fix for this to the *3198-vici-child-updown* branch (since lifetimes are reported as signed numbers, I left them in the message even for potentially expired or rekeyed SAs).

#### #5 - 10.10.2019 16:58 - Sung Kim

Thank you for the quick response. I'll let my server admin know this fix.
However, I have another question about the byte numbers in the child-updown event caused by dpd timeout during the child rekeying but I'll create a new issue for that.

#### #6 - 10.10.2019 17:06 - Sung Kim

> However, I have another question about the byte numbers in the child-updown event caused by ~~dpd timeout~~ the retransmission timeout during the child rekeying but I'll create a new issue for that.

Just for correcting my comment above

#### #7 - 10.10.2019 17:27 - Tobias Brunner

> However, I have another question about the byte numbers in the child-updown event caused by ~~dpd timeout~~ the retransmission timeout during the child rekeying but I'll create a new issue for that.

As mentioned, usage numbers are only provided if the CHILD_SA is still installed in the kernel. So if the CHILD_SA expires while retransmits of the rekeying request are sent, there won't be any numbers if the IKE_SA is later terminated due to DPD.

#### #8 - 25.10.2019 16:20 - Tobias Brunner

*- Status changed from Feedback to Closed*