strongSwan - Feature #2856

strongswan not including the Framed-IP-Address that was assigned by RADIUS in its Acct-Type: Stop record

10.12.2018 21:32 - James Dogopoulos

Status:	Closed	**Start date:**	
Priority:	Normal	**Due date:**	
Assignee:	Tobias Brunner	**Estimated time:**	0.00 hour
Category:	libcharon		
Target version:	5.7.2		
Resolution:	Fixed		

Description

When a connection fails for N(FAIL_CP_REQ) FAILED_CP_REQUIRED, strongswan is not including the Framed-IP-Address that was assigned by RADIUS in its Acct-Type: Stop request.

The result is the the IP stays leased in radius to the failed login on the VPN server, in this case N(FAIL_CP_REQ) FAILED_CP_REQUIRED causes it but it may present in other situations. This is a potential DoS issue as an attacker could use up all available IPs by flooding with failed logins before IP lease times expire in RADIUS. Assuming a small pool of IPs, someone merely trying to make a client machine work could also use up all available IPs and block further logins from other users.

The radiusd I'm testing with is FreeRADIUS, I didn't check if RFC requires the framed-ip-address to be sent here so this could be how FreeRADIUS is handling the Stop record, if it's not too difficult might as well just send the ip in the Stop record since it couldn't hurt.

```
Dec 10 12:12:16 avspam charon: 05[IKE] IKE_SA radius-pubkey-ike2[10] established between x.x.x.135
[CN=host.site.com]...y.y.y.102[jd]
Dec 10 12:12:16 avspam charon: 05[IKE] IKE_SA radius-pubkey-ike2[10] state change: CONNECTING => E
STABLISHED
Dec 10 12:12:16 avspam charon: 05[IKE] expected a virtual IP request, sending FAILED_CP_REQUIRED
Dec 10 12:12:16 avspam charon: 05[CFG] looking for a child config for 0.0.0.0/0 === 192.168.1.166/
32
Dec 10 12:12:16 avspam charon: 05[CFG] proposing traffic selectors for us:
Dec 10 12:12:16 avspam charon: 05[CFG]  0.0.0.0/0
Dec 10 12:12:16 avspam charon: 05[CFG] proposing traffic selectors for other:
Dec 10 12:12:16 avspam charon: 05[CFG]  dynamic
Dec 10 12:12:16 avspam charon: 05[IKE] traffic selectors 0.0.0.0/0 === 192.168.1.166/32 unacceptab
le
Dec 10 12:12:16 avspam charon: 05[IKE] failed to establish CHILD_SA, keeping IKE_SA
Dec 10 12:12:16 avspam charon: 05[CFG] RADIUS server 'primary' is candidate: 210
Dec 10 12:12:16 avspam charon: 05[CFG] sending RADIUS Accounting-Request to server 'primary'
Dec 10 12:12:16 avspam charon: 05[CFG] received RADIUS Accounting-Response from server 'primary'
Dec 10 12:12:16 avspam charon: 05[ENC] generating IKE_AUTH response 4 [ AUTH N(MOBIKE_SUP) N(ADD_6
_ADDR) N(FAIL_CP_REQ) N(TS_UNACCEPT) ]
Dec 10 12:12:16 avspam charon: 05[NET] sending packet: from x.x.x.135[4500] to y.y.y.102[58665] (1
60 bytes)
Dec 10 12:12:16 avspam charon: 05[MGR] checkin IKE_SA radius-pubkey-ike2[10]
Dec 10 12:12:16 avspam charon: 05[MGR] checkin of IKE_SA successful
Dec 10 12:12:16 avspam charon: 03[NET] sending packet: from x.x.x.135[4500] to y.y.y.102[58665]
Dec 10 12:12:16 avspam charon: 16[NET] received packet: from y.y.y.102[58665] to x.x.x.135[4500]
Dec 10 12:12:16 avspam charon: 16[NET] waiting for data on sockets
Dec 10 12:12:16 avspam charon: 07[MGR] checkout IKEv2 SA by message with SPIs c35645b5f77e16c5_i a
ea2e8e6ff66b31a_r
Dec 10 12:12:16 avspam charon: 07[MGR] IKE_SA radius-pubkey-ike2[10] successfully checked out
Dec 10 12:12:16 avspam charon: 07[NET] received packet: from y.y.y.102[58665] to x.x.x.135[4500] (
80 bytes)
Dec 10 12:12:16 avspam charon: 07[ENC] parsed INFORMATIONAL request 5 [ D ]
Dec 10 12:12:16 avspam charon: 07[IKE] received DELETE for IKE_SA radius-pubkey-ike2[10]
Dec 10 12:12:16 avspam charon: 07[IKE] deleting IKE_SA radius-pubkey-ike2[10] between x.x.x.135[CN
=host.site.com]...y.y.y.102[jd]
Dec 10 12:12:16 avspam charon: 07[IKE] IKE_SA radius-pubkey-ike2[10] state change: ESTABLISHED =>
DELETING
```

```
Dec 10 12:12:16 avspam charon: 07[IKE] IKE_SA deleted
Dec 10 12:12:16 avspam charon: 07[CFG] RADIUS server 'primary' is candidate: 210
Dec 10 12:12:16 avspam charon: 07[CFG] sending RADIUS Accounting-Request to server 'primary'
Dec 10 12:12:16 avspam charon: 07[CFG] received RADIUS Accounting-Response from server 'primary'
Dec 10 12:12:16 avspam charon: 07[ENC] generating INFORMATIONAL response 5 [ ]
Dec 10 12:12:16 avspam charon: 07[NET] sending packet: from x.x.x.135[4500] to y.y.y.102[58665] (8
0 bytes)
Dec 10 12:12:16 avspam charon: 07[MGR] checkin and destroy IKE_SA radius-pubkey-ike2[10]
Dec 10 12:12:16 avspam charon: 07[IKE] IKE_SA radius-pubkey-ike2[10] state change: DELETING => DES
TROYING
Dec 10 12:12:16 avspam charon: 03[NET] sending packet: from x.x.x.135[4500] to y.y.y.102[58665]
Dec 10 12:12:16 avspam charon: 07[MGR] checkin and destroy of IKE_SA successful
```

Associated revisions

Revision 03296451 - 18.12.2018 10:34 - Tobias Brunner

Merge branch 'radius-accounting-unclaimed'

Adds all IPs to RADIUS Accounting-Stop messages even those not claimed by
a client. For instance, if the connection fails with FAILED_CP_REQUIRED,
adding the unclaimed addresses allows the RADIUS server to release the
leases early.

Fixes #2856.

History

#1 - 11.12.2018 12:08 - Tobias Brunner

- Tracker changed from Issue to Feature

- Category set to libcharon

- Status changed from New to Feedback

- Assignee set to Tobias Brunner

- Target version set to 5.7.2

- Affected version deleted (5.7.1)

There is no code at all that releases IP addresses received from the RADIUS server explicitly, whether they were claimed or unclaimed by the client, only internal state is cleaned up (see source:src/libcharon/plugins/eap_radius/eap_radius_provider.c).

There is also no direct relation to RADIUS accounting (which is an optional feature anyway). Claimed IPs are just included in these messages for accounting reasons (i.e. just to provide additional information about the client to the RADIUS server, which, theoretically, also doesn't have to be the same server that handled the authentication and assigned the IP addresses, although, the *eap-radius* plugin currently doesn't support separate servers for authentication and accounting, but if multiple servers are configured, the messages could be sent to different ones).

I don't think there is a proper mechanism to actually release the received IPs to the authentication server. The Accounting Stop message is probably the only thing that comes close (but as mentioned, is optional and not necessarily sent to the same server). However, since an unclaimed IP is never assigned to the IKE_SA, adding it to that message is a bit tricky.

On the other hand, an attacker needs valid credentials to receive such an IP so you could maybe rate limit logins per client or cleanup leases not by the IP itself but by username (if you only allow single logins), or the class attribute (if sent and they're unique per user/session) or the session IDs (although these are currently only sent in accounting messages, RFC 2866 would allow them in Access-Request messages, too). Not sure if FreeRADIUS can be configured like that, though.

Anyway, I pushed a possible fix that adds unclaimed IPs to Accounting-Stop messages to the *2856-radius-unclaimed* branch.

#2 - 17.12.2018 19:28 - James Dogopoulos

This fixed the issue and it seems like the best bet if there are multiple access servers using the same IP pool.

#3 - 18.12.2018 10:40 - Tobias Brunner

- Status changed from Feedback to Closed

- Resolution set to Fixed

Thanks for testing. Pushed to master.