IPsec flowcache replacement

Steffen Klassert

secunet Security Networks AG

Dresden

Linux IPsec Workshop, Dresden, March 27, 2018
IPsec flowcache replacement
IPsec flowcache replacement

- The IPsec flowcache had a DoS problem (known since years)
- The IPsec flowcache was removed (Linux v4.14)
- The DoS problem with the flowcache went away.
- We lost the policy/SA lookup fastpath
- Slowpath lookup for policy + SA happens now for each packet
- How to solve this problem???
  - Fast lookup algorithm for policies and SAs (which one)?
  - Fast lookup algorithm for policies + cache SA at the policy?
  - Netfilter flowtable? (Pablo will tell more about that)
- Create an API to hook in different lookup methods?
  - Does that make sense?
IPsec flowcache replacement

- The IPsec flowcache had a DoS problem (known since years)
- The IPsec flowcache was removed (Linux v4.14)
- The DoS problem with the flowcache went away.
- We lost the policy/SA lookup fastpath
- Slowpath lookup for policy + SA happens now for each packet
- How to solve this problem???
  - Fast lookup algorithm for policies and SAs (which one)?
  - Fast lookup algorithm for policies + cache SA at the policy?
  - Netfilter flowtable? (Pablo will tell more about that)
- Create an API to hook in different lookup methods?
  - Does that make sense?
The IPsec flowcache had a DoS problem (known since years)

The IPsec flowcache was removed (Linux v4.14)

The DoS problem with the flowcache went away.

We lost the policy/SA lookup fastpath

Slowpath lookup for policy + SA happens now for each packet

How to solve this problem???

Fast lookup algorithm for policies and SAs (which one)?

Fast lookup algorithm for policies + cache SA at the policy?

Netfilter flowtable? (Pablo will tell more about that)

Create an API to hook in different lookup methods?

Does that make sense?
The IPsec flowcache had a DoS problem (known since years)
The IPsec flowcache was removed (Linux v4.14)
The DoS problem with the flowcache went away.
We lost the policy/SA lookup fastpath
Slowpath lookup for policy + SA happens now for each packet
How to solve this problem???
  Fast lookup algorithm for policies and SAs (which one)?
  Fast lookup algorithm for policies + cache SA at the policy?
  Netfilter flowtable? (Pablo will tell more about that)
Create an API to hook in different lookup methods?
  Does that make sense?
IPsec flowcache replacement

The IPsec flowcache had a DoS problem (known since years)
The IPsec flowcache was removed (Linux v4.14)
The DoS problem with the flowcache went away.
We lost the policy/SA lookup fastpath
Slowpath lookup for policy + SA happens now for each packet
How to solve this problem???
Fast lookup algorithm for policies and SAs (which one)?
Fast lookup algorithm for policies + cache SA at the policy?
Netfilter flowtable? (Pablo will tell more about that)
Create an API to hook in different lookup methods?
Does that make sense?
The IPsec flowcache had a DoS problem (known since years)
- The IPsec flowcache was removed (Linux v4.14)
- The DoS problem with the flowcache went away.
- We lost the policy/SA lookup fastpath
- Slowpath lookup for policy + SA happens now for each packet
- How to solve this problem???
  - Fast lookup algorithm for policies and SAs (which one)?
  - Fast lookup algorithm for policies + cache SA at the policy?
  - Netfilter flowtable? (Pablo will tell more about that)
- Create an API to hook in different lookup methods?
  - Does that make sense?
IPsec flowcache replacement

- The IPsec flowcache had a DoS problem (known since years)
- The IPsec flowcache was removed (Linux v4.14)
- The DoS problem with the flowcache went away.
- We lost the policy/SA lookup fastpath
- Slowpath lookup for policy + SA happens now for each packet
- How to solve this problem???
  - Fast lookup algorithm for policies and SAs (which one)?
  - Fast lookup algorithm for policies + cache SA at the policy?
  - Netfilter flowtable? (Pablo will tell more about that)
- Create an API to hook in different lookup methods?
  - Does that make sense?
IPsec flowcache replacement

- The IPsec flowcache had a DoS problem (known since years)
- The IPsec flowcache was removed (Linux v4.14)
- The DoS problem with the flowcache went away.
- We lost the policy/SA lookup fastpath
- Slowpath lookup for policy + SA happens now for each packet
- How to solve this problem???
  - Fast lookup algorithm for policies and SAs (which one)?
    - Fast lookup algorithm for policies + cache SA at the policy?
    - Netfilter flowtable? (Pablo will tell more about that)
  - Create an API to hook in different lookup methods?
    - Does that make sense?
IPsec flowcache replacement

- The IPsec flowcache had a DoS problem (known since years)
- The IPsec flowcache was removed (Linux v4.14)
- The DoS problem with the flowcache went away.
- We lost the policy/SA lookup fastpath
- Slowpath lookup for policy + SA happens now for each packet
- How to solve this problem???
  - Fast lookup algorithm for policies and SAs (which one)?
  - Fast lookup algorithm for policies + cache SA at the policy?
    - Netfilter flowtable? (Pablo will tell more about that)
  - Create an API to hook in different lookup methods?
    - Does that make sense?
The IPsec flowcache had a DoS problem (known since years)

The IPsec flowcache was removed (Linux v4.14)

The DoS problem with the flowcache went away.

We lost the policy/SA lookup fastpath

Slowpath lookup for policy + SA happens now for each packet

How to solve this problem???

- Fast lookup algorithm for policies and SAs (which one)?
- Fast lookup algorithm for policies + cache SA at the policy?
- Netfilter flowtable? (Pablo will tell more about that)

Create an API to hook in different lookup methods?

Does that make sense?
IPsec flowcache replacement

- The IPsec flowcache had a DoS problem (known since years)
- The IPsec flowcache was removed (Linux v4.14)
- The DoS problem with the flowcache went away.
- We lost the policy/SA lookup fastpath
- Slowpath lookup for policy + SA happens now for each packet
- How to solve this problem???
  - Fast lookup algorithm for policies and SAs (which one)?
  - Fast lookup algorithm for policies + cache SA at the policy?
  - Netfilter flowtable? (Pablo will tell more about that)
- Create an API to hook in different lookup methods?
  - Does that make sense?
IPsec flowcache replacement

- The IPsec flowcache had a DoS problem (known since years)
- The IPsec flowcache was removed (Linux v4.14)
- The DoS problem with the flowcache went away.
- We lost the policy/SA lookup fastpath
- Slowpath lookup for policy + SA happens now for each packet
- How to solve this problem???
  - Fast lookup algorithm for policies and SAs (which one)?
  - Fast lookup algorithm for policies + cache SA at the policy?
  - Netfilter flowtable? (Pablo will tell more about that)
- Create an API to hook in different lookup methods?
  - Does that make sense?