Software-Defined Networking (SDN)-based IPsec Flow Protection

(draft-ietf-i2nsf-sdn-ipsec-flow-protection-00)

Presenter: Gabriel López-Millán

Rafael Marín-López

(University of Murcia)

SDN-based IPsec

- **Architecture** for the SDN-based IPsec mgmt to centralize the establishment and management of IPsec security associations
- To define (so far) the **NSF facing interfaces** required to manage and monitor the IPsec SAs in the NSF from a SC.
- Case 1) The NSF implements IKE, SPD, SAD and PAD
  - SC provisioning the NSF with information to IKE, SPD and PAD
- Case 2) The NSF implements the IPsec databases (no IKE).
  - The SC provides the NSF the required parameters to create valid entries in the SPD and SAD
  - The NSF only support for IPsec, while automated key management functionality is moved to the SC

Update (Changes in ietf-…-00)

- Improved 5.3. Case 1 vs Case 2 discussion
  - Added text about NSF restart behavior
    - It may lose part or all the IPsec state.
    - By default, the SC can assume that all the state has been lost and therefore it will have to send:
      - IKEv2, SPD and PAD information to the NSF in case 1
      - SPD and SAD information in case 2
    - Other more optimized options can be considered (e.g. making iKEv2 configuration permanent between reboots)

Update (Changes in ietf-…-00)

- Improved YANG configuration data model → comments received in the mailing-list (https://mailarchive.ietf.org/arch/msg/i2nsf/OzLJ2IPG_2F78qQv1OZ5euhinzY/?qid=8c890a079867d021dd5265f00a047e33)
  - SAD model:
    - ah and esp descriptions aligned
    - Modified combined-enc-intr boolean for esp-sa element
    - Added espencap for encap element to allow ESPinTCP, ESPinTLS and ESPinUDP
    - Added sadb_bad-spi notification to inform the SC that packets with unknown SPI are received

Update (Changes in ietf-…-00)

- Improved YANG configuration data models (cont.)
  - IKEv2
    - Updated autostartup element to represent the states: alwayson, initiate-on-demand and respond-only
    - Added encap element, sport, sport and oaddr for nat-traversal options
    - Added combined-enc-intr
    - List of pfs_group allowed
    - Removed phase1-authby → Already in PAD
    - Removed phase2 elements (lifetime, authalg, encalg), local and remote addresses → represented by the SPD model

Update (Changes in ietf-…-00)

- Interim meeting minutes: https://datatracker.ietf.org/meeting/interim-2017-i2nsf-01/materials/minutes-interim-2017-i2nsf-01-201709061600/
- New section Security Considerations
  - Shares the security issues in [ITU-T.Y.3300] and [RFC8192]
  - Case 1
    - SC sends IKE creds (PSK, public/private keys, certificates, etc.) to NSFs
    - Recommendation → SC NEVER stores the IKE creds after distributing
    - NSFs MUST NOT allow the reading of these values once they have been applied by the SC (i.e. write only operations)
    - Avoid impersonation in IKE
      - If PSK, immediately after distributing it, the SC should remove it
      - If raw public keys, the SC should remove the associate private key immediately after distributing them to the NSF
      - If certificates, the NSF may generate the private key and exports the public key for certification in the SC

Update (Changes in ietf-…-00)

- New section Security Considerations
  - Case 2
    - That key material are symmetric keys to protect data traffic
    - the SC NEVER stores the keys after distributing them
    - the NSFs MUST NOT allow the reading of these values once they have been applied by the SC (i.e. write only operations)
    - if attacker has access to the SC during the period of time that key material is generated, he may have access to the key material used in the distributed IPsec SAs

Next steps

- To continue the Configuration Data model revision
- To start the definition of the State Data model for case 1 and case 2

Software-Defined Networking (SDN)-based IPsec Flow Protection

(draft-ietf-i2nsf-sdn-ipsec-flow-protection-00)

Presenter: Gabriel López-Millán

Rafael Marín-López

(University of Murcia)

YANG Model Trees

Update - SPD model (tree)

```
+--rw spd
|  +--rw spd-entry* [rule-number]
|     +--rw rule-number        uint64
|     +--rw priority?          uint32
|     +--rw names* [name]
|     |  +--rw name-type?   ipsec-spd-name
|     |  +--rw name         string
|     +--rw condition
|     |  +--rw traffic-selector-list* [ts-number]
|     |     +--rw ts-number              uint32
|     |     +--rw direction?             ipsec-traffic-direction
|     |     +--rw local-addresses* [start end]
|     |     |  +--rw start    inet:ip-address
|     |     |  +--rw end      inet:ip-address
|     |     +--rw remote-addresses* [start end]
|     |     |  +--rw start    inet:ip-address
|     |     |  +--rw end      inet:ip-address
|     |     +--rw next-layer-protocol*   ipsec-next-layer-proto
|     |     +--rw local-ports* [start end]
|     |     |  +--rw start    inet:port-number
|     |     |  +--rw end      inet:port-number
|     |     +--rw remote-ports* [start end]
|     |     |  +--rw start    inet:port-number
|     |     |  +--rw end      inet:port-number
|     |     +--rw selector-priority?     uint32
|     +--rw processing-info
|     |  +--rw action          ipsec-spd-operation
|     |  +--rw ipsec-sa-cfg
|     |     +--rw pfp-flag?            boolean
|     |     +--rw extSeqNum?           boolean
|     |     +--rw seqOverflow?         boolean
|     |     +--rw statefulfragCheck?   boolean
|     |     +--rw security-protocol?   ipsec-protocol
|     |     +--rw mode?                ipsec-mode
|     |     +--rw ah-algorithms
|     |     |  +--rw ah-algorithm*   integrity-algorithm-t
|     |     +--rw esp-algorithms
|     |     |  +--rw authentication*   integrity-algorithm-t
|     |     |  +--rw encryption*       encryption-algorithm-t
|     |     +--rw tunnel
|     |        +--rw local?          inet:ip-address
|     |        +--rw remote?         inet:ip-address
|     |        +--rw bypass-df?      boolean
|     |        +--rw bypass-dscp?    boolean
|     |        +--rw dscp-mapping?   yang:hex-string
|     |        +--rw ecn?            boolean
|     +--rw spd-lifetime
|        +--rw time-soft?       uint32
|        +--rw time-hard?       uint32
|        +--rw time-use-soft?   uint32
|        +--rw time-use-hard?   uint32
|        +--rw byte-soft?       uint32
|        +--rw byte-hard?       uint32
|        +--rw packet-soft?     uint32
|        +--rw packet-hard?     uint32
```

Update - SAD model (tree)

```
+--rw sad {case2}?
|  +--rw sad-entry* [spi]
|     +--rw spi                          ipsec-spi
|     +--rw seq-number?                  uint64
|     +--rw seq-number-overflow-flag?    boolean
|     +--rw anti-replay-window?          uint16
|     +--rw rule-number?                 uint32
|     +--rw local-addresses* [start end]
|     |  +--rw start    inet:ip-address
|     |  +--rw end      inet:ip-address
|     +--rw remote-addresses* [start end]
|     |  +--rw start    inet:ip-address
|     |  +--rw end      inet:ip-address
|     +--rw next-layer-protocol*         ipsec-next-layer-proto
|     +--rw local-ports* [start end]
|     |  +--rw start    inet:port-number
|     |  +--rw end      inet:port-number
```

```
|     +--rw remote-ports* [start end]
|     |  +--rw start    inet:port-number
|     |  +--rw end      inet:port-number
|     +--rw security-protocol?          ipsec-protocol
|     +--rw ah-sa
|     |  +--rw integrity
|     |     +--rw integrity-algorithm?   integrity-algorithm-t
|     |     +--rw key?                   string
|     +--rw esp-sa
|     |  +--rw encryption
|     |  |  +--rw encryption-algorithm?   encryption-algorithm-t
|     |  |  +--rw key?                    string
|     |  |  +--rw iv?                     string
|     |  +--rw integrity
|     |  |  +--rw integrity-algorithm?   integrity-algorithm-t
|     |  |  +--rw key?                   string
|     |  +--rw combined-enc-intr?   boolean
|     +--rw sa-lifetime
|     |  +--rw time-soft?       uint32
|     |  +--rw time-hard?       uint32
|     |  +--rw time-use-soft?   uint32
|     |  +--rw time-use-hard?   uint32
|     |  +--rw byte-soft?       uint32
|     |  +--rw byte-hard?       uint32
|     |  +--rw packet-soft?     uint32
|     |  +--rw packet-hard?     uint32
|     |  +--rw action?          lifetime-action
|     +--rw mode?                         ipsec-mode
|     +--rw statefulfragCheck?            boolean
|     +--rw dscp?                         yang:hex-string
|     +--rw tunnel
|     |  +--rw local?          inet:ip-address
|     |  +--rw remote?         inet:ip-address
|     |  +--rw bypass-df?      boolean
|     |  +--rw bypass-dscp?    boolean
|     |  +--rw dscp-mapping?   yang:hex-string
|     |  +--rw ecn?            boolean
|     +--rw path-mtu?                     uint16
|     +--rw encap
|        +--rw espencap?   esp-encap
|        +--rw sport?      inet:port-number
|        +--rw dport?      inet:port-number
|        +--rw oaddr?      inet:ip-address
```

Update - SAD model (tree)

```
rpcs:
+---x sadb_register
    +---w input
    |  +---w base-list* [version]
    |     +---w version        string
    |     +---w msg_type?      sadb-msg-type
    |     +---w msg_satype?    sadb-msg-satype
    |     +---w msg_seq?       uint32
    +--ro output
    +--ro base-list* [version]
       |  +--ro version        string
       |  +--ro msg_type?      sadb-msg-type
       |  +--ro msg_satype?    sadb-msg-satype
       |  +--ro msg_seq?       uint32
       +--ro algorithm-supported*
          +--ro authentication
          |  +--ro name?        integrity-algorithm-t
          |  +--ro ivlen?       uint8
          |  +--ro min-bits?    uint16
          |  +--ro max-bits?    uint16
          +--ro encryption
             +--ro name?        encryption-algorithm-t
             +--ro ivlen?       uint8
             +--ro min-bits?    uint16
             +--ro max-bits?    uint16

notifications:
+---n spdb_expire
|  +--ro index?   uint64
+---n sadb_acquire
|  +--ro state    uint32
+---n sadb_expire
|  +--ro state    uint32
+---n sadb_bad-spi
   +--ro state    ipsec-spi
```

Update - PAD model (tree)

```
+--rw pad {case1}?
   +--rw pad-entries* [pad-entry-id]
   +--rw pad-entry-id              uint64
   +--rw (identity)?
   |  +--:(ipv4-address)
   |  |  +--rw ipv4-address?            inet:ipv4-address
   |  +--:(ipv6-address)
   |  |  +--rw ipv6-address?            inet:ipv6-address
   |  +--:(fqdn-string)
   |  |  +--rw fqdn-string?             inet:domain-name
   |  +--:(rfc822-address-string)
   |  |  +--rw rfc822-address-string?   string
   |  +--:(dnX509)
   |  |  +--rw dnX509?                  string
   |  +--:(id_key)
   |     +--rw id_key?                  string
   +--rw pad-auth-protocol?       auth-protocol-type
   +--rw auth-method
      +--rw auth-m?          auth-method-type
      +--rw pre-shared
      |  +--rw secret?   string
      +--rw rsa-signature
         +--rw key-data?    string
         +--rw key-file?    string
         +--rw ca-data*     string
         +--rw ca-file?     string
         +--rw cert-data?   string
         +--rw cert-file?   string
         +--rw crl-data?    string
         +--rw crl-file?    string
```

Update - IKE model (tree)

```
+--rw ikev2 {case1}?
|  +--rw ike-connection
|     +--rw ike-conn-entries* [conn-name]
|        +--rw conn-name            string
|        +--rw autostartup          type-autostartup
|        +--rw nat-traversal?       boolean
|        +--rw encap
|        |  +--rw espencap?   esp-encap
|        |  +--rw sport?      inet:port-number
|        |  +--rw dport?      inet:port-number
|        |  +--rw oaddr?      inet:ip-address
|        +--rw version?             enumeration
|        +--rw phase1-lifetime      uint32
|        +--rw phase1-authalg*      integrity-algorithm-t
|        +--rw phase1-encalg*       encryption-algorithm-t
|        +--rw combined-enc-intr?   boolean
|        +--rw dh_group             uint32
|        +--rw local
|        |  +--rw (my-identifier-type)?
|        |  |  +--:(ipv4)
|        |  |  |  +--rw ipv4?            inet:ipv4-address
|        |  |  +--:(ipv6)
|        |  |  |  +--rw ipv6?            inet:ipv6-address
|        |  |  +--:(fqdn)
|        |  |  |  +--rw fqdn?            inet:domain-name
|        |  |  +--:(dn)
|        |  |  |  +--rw dn?              string
|        |  |  +--:(user_fqdn)
|        |  |     +--rw user_fqdn?       string
|        |  +--rw my-identifier    string
|        +--rw remote
|        |  +--rw (my-identifier-type)?
|        |  |  +--:(ipv4)
|        |  |  |  +--rw ipv4?            inet:ipv4-address
|        |  |  +--:(ipv6)
|        |  |  |  +--rw ipv6?            inet:ipv6-address
|        |  |  +--:(fqdn)
|        |  |  |  +--rw fqdn?            inet:domain-name
|        |  |  +--:(dn)
|        |  |  |  +--rw dn?              string
|        |  |  +--:(user_fqdn)
|        |  |     +--rw user_fqdn?       string
|        |  +--rw my-identifier    string
|        +--rw pfs_group*           uint32
```