Service Function Chaining (SFC) Architecture
draft-ietf-sfc-architecture

Prepared by
Carlos Pignataro
and Joel Halpern

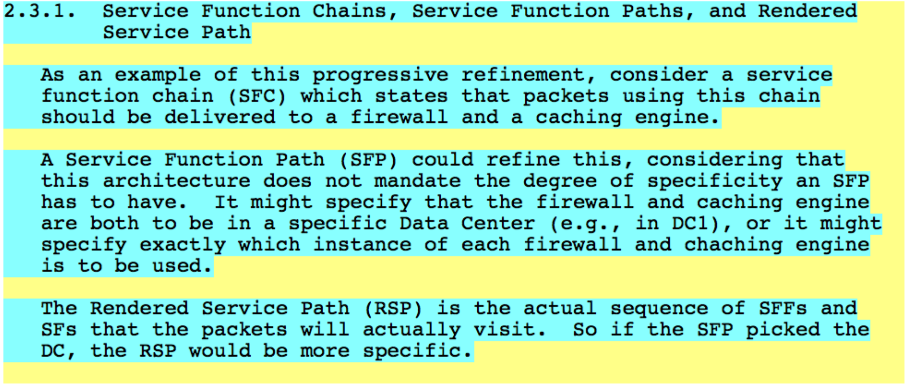
Update from IESG Evaluation (from -08)

Progress thus far… 1/5

- Alvaro Retana DISCUSS and COMMENT
  - Comments on Scope and Control Plane -> Clarified
  - Discuss on Intended Status -> Informational

Progress thus far… 2/5

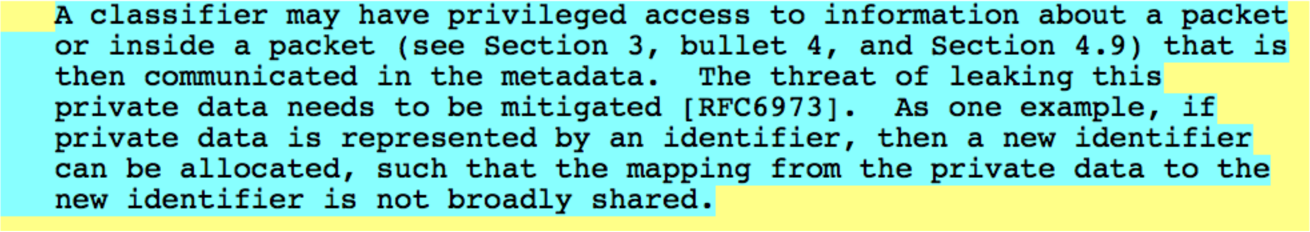
- Benoit Claise DISCUSS and COMMENT
  - Many Clarifying comments -> THANK YOU! Greatly improved the document
    - Editorials throughout
    - Notably: Definition of SFC and RSP, new Section 2.3.1. on SFC/SFP/RSP
  - Discuss on Consulting with Ops (IESG discussion, NOOP for editors)



```
2.3.1.  Service Function Chains, Service Function Paths, and Rendered
        Service Path

   As an example of this progressive refinement, consider a service
   function chain (SFC) which states that packets using this chain
   should be delivered to a firewall and a caching engine.

   A Service Function Path (SFP) could refine this, considering that
   this architecture does not mandate the degree of specificity an SFP
   has to have.  It might specify that the firewall and caching engine
   are both to be in a specific Data Center (e.g., in DC1), or it might
   specify exactly which instance of each firewall and chaching engine
   is to be used.

   The Rendered Service Path (RSP) is the actual sequence of SFFs and
   SFs that the packets will actually visit.  So if the SFP picked the
   DC, the RSP would be more specific.
```

Progress thus far... 3/5

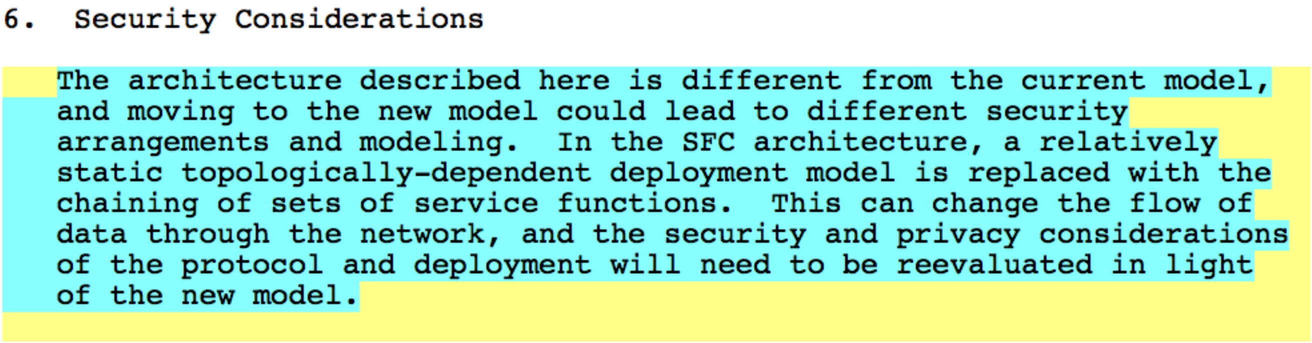
- Kathleen Moriarty DISCUSS and COMMENT
  - Privacy
  - Updated
    Security Considerations



A classifier may have privileged access to information about a packet or inside a packet (see Section 3, bullet 4, and Section 4.9) that is then communicated in the metadata. The threat of leaking this private data needs to be mitigated [RFC6973]. As one example, if private data is represented by an identifier, then a new identifier can be allocated, such that the mapping from the private data to the new identifier is not broadly shared.

Progress thus far…

- Stephen Farrell DISCUSS and COMMENT
  - Updated the Security Considerations based on Sec-Dir Review
  - DISCUSS outstanding

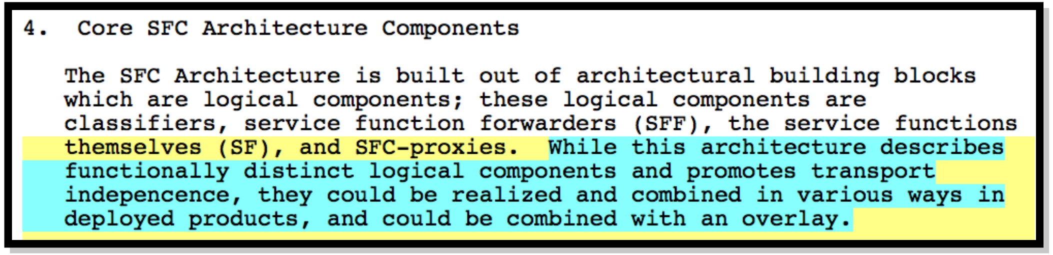


6. Security Considerations

The architecture described here is different from the current model, and moving to the new model could lead to different security arrangements and modeling. In the SFC architecture, a relatively static topologically-dependent deployment model is replaced with the chaining of sets of service functions. This can change the flow of data through the network, and the security and privacy considerations of the protocol and deployment will need to be reevaluated in light of the new model.

Progress thus far…

- Comments from Uri Elzur
  - Clarification on Logical Components and overlay
  - Clarification on Figure 3 and missing Classifier
  - Changes in working copy (to be submitted as -10)



4. Core SFC Architecture Components

The SFC Architecture is built out of architectural building blocks which are logical components; these logical components are classifiers, service function forwarders (SFF), the service functions themselves (SF), and SFC-proxies. While this architecture describes functionally distinct logical components and promotes transport indepencence, they could be realized and combined in various ways in deployed products, and could be combined with an overlay.

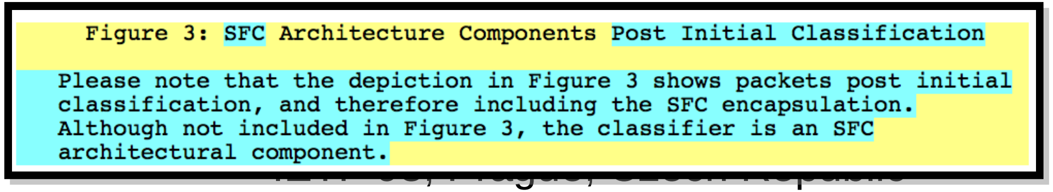
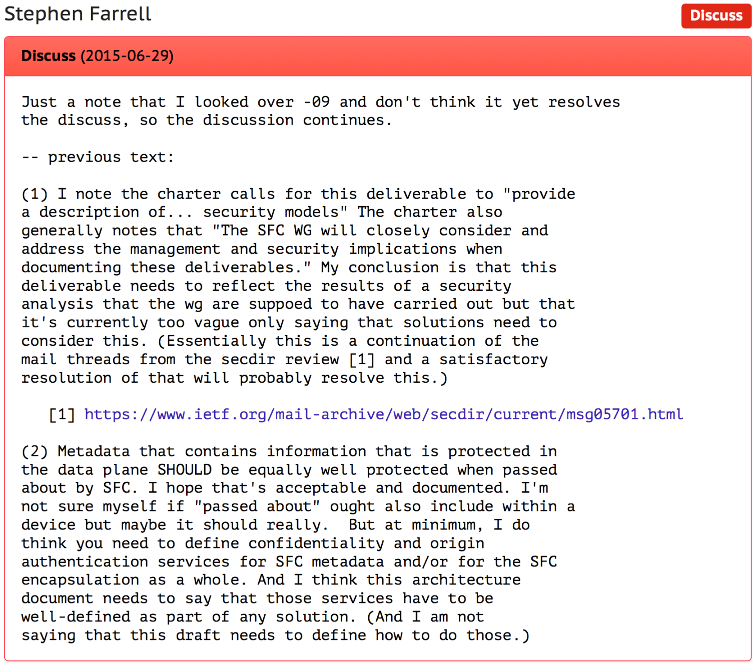


Figure 3: SFC Architecture Components Post Initial Classification

Please note that the depiction in Figure 3 shows packets post initial classification, and therefore including the SFC encapsulation. Although not included in Figure 3, the classifier is an SFC architectural component.

Next Steps

- Outstanding DISCUSS from Stephen Farrell



Stephen Farrell

Discuss (2015-06-29)

```
Just a note that I looked over -09 and don't think it yet resolves
the discuss, so the discussion continues.

-- previous text:

(1) I note the charter calls for this deliverable to "provide
a description of... security models" The charter also
generally notes that "The SFC WG will closely consider and
address the management and security implications when
documenting these deliverables." My conclusion is that this
deliverable needs to reflect the results of a security
analysis that the wg are suppoed to have carried out but that
it's currently too vague only saying that solutions need to
consider this. (Essentially this is a continuation of the
mail threads from the secdir review [1] and a satisfactory
resolution of that will probably resolve this.)

   [1] https://www.ietf.org/mail-archive/web/secdir/current/msg05701.html

(2) Metadata that contains information that is protected in
the data plane SHOULD be equally well protected when passed
about by SFC. I hope that's acceptable and documented. I'm
not sure myself if "passed about" ought also include within a
device but maybe it should really.  But at minimum, I do
think you need to define confidentiality and origin
authentication services for SFC metadata and/or for the SFC
encapsulation as a whole. And I think this architecture
document needs to say that those services have to be
well-defined as part of any solution. (And I am not
saying that this draft needs to define how to do those.)
```

Proposal 1/3

- Working with Chris Inacio (CERT)

Boundaries: Specific requirements may need to be enforced at the boundaries of an SFC-enabled domain. These include, for example, to avoid leaking SFC information, and to protect its borders against various forms of attacks. **If untrusted parties can inject packets which will be treated as being properly classified for service chaining, there are a large range of attacks which can be mounted against the resulting system. Depending upon deployment details, these likely include spoofing packets from users and creating DDoS and reflection attacks of various kinds. Thus, when a transport mechanisms are selected for use with SFC, they MUST ensure that outside parties can not inject SFC packets which will be accepted for processing into the domain. This border security MUST include any tunnels to other domains. If those tunnels are to be used for SFC without reclassification, then the tunnel MUST include additional techniques to ensure the integrity and validity of such packets.**

Proposal 2/3

- Working with Chris Inacio (CERT)

SFC Encapsulation: The SFC Encapsulation provides at a minimum SFP identification, and carries metadata. An operator may consider the SFC Metadata as sensitive. From a privacy perspective, a user may be concerned about the operator revealing data about (and not belonging to) the customer. Therefore, solutions should consider whether there is a risk of sensitive information slipping out of the operators control. Issues of information exposure should also consider flow analysis. **Further, when a specific metadata element is defined, it should be carefully considered whether origin authentication is needed for it.**

Proposal 3/3

- Working with Chris Inacio (CERT)

Some metadata added to and carried in SFC packets is sensitive for various reasons, including potentially revealing personally identifying information. Realizations of the architecture MUST protect to ensure that such information is handled with suitable care and precautions against inappropriate dissemination of the information. This can have implications to the data plane, the control plane, or both. Data plane protocol definitions for SFC can include suitable provision for protect such information for use when handling sensitive information, with packet or SFP granularity. Equally, the control mechanisms use with SFC can have provisions to determine that such mechanisms are available, and to ensure that they are used when needed. Inability to do so needs to result in error indications to appropriate management systems. In particular, when the control systems know that sensitive information may potentially be added to packets at certain points on certain service chains, the control mechanism MUST verify that appropriate protective treatment of NSH information is available from the point where the information is added to the point where it will be removed. If such mechanisms are unavailable, error notifications SHOULD be generated.

Thank you!