       Software-Defined Networking (SDN)-based IPsec Flow Protection
               draft-abad-sdnrg-sdn-ipsec-flow-protection-01

Abstract

   This document describes the use case for providing IPsec flow
   protection by means of a Software-Defined Network (SDN) controller
   and raises the requirements to support this service. It considers
   two main scenarios: (i) gateway-to-gateway and (ii) host-to-gateway
   (Road Warrior). For the gateway-to-gateway scenario, this document
   describes a mechanism to support the bootstrapping of key material
   between network resources to protect data traffic with IPsec and IKE,
   both in intra and inter-SDN cases. The host-to-gateway case defines
   a mechanism to bootstrap key material to protect data with IPsec
   between an end user's device and a gateway.

Status of This Memo

   This Internet-Draft is submitted in full conformance with the
   provisions of BCP 78 and BCP 79.

   Internet-Drafts are working documents of the Internet Engineering
   Task Force (IETF). Note that other groups may also distribute
   working documents as Internet-Drafts. The list of current Internet-
   Drafts is at http://datatracker.ietf.org/drafts/current/.

   Internet-Drafts are draft documents valid for a maximum of six months
   and may be updated, replaced, or obsoleted by other documents at any
   time. It is inappropriate to use Internet-Drafts as reference
   material or to cite them other than as "work in progress."

   This Internet-Draft will expire on April 21, 2016.

Copyright Notice

Table of Contents

1. Introduction

Software-Defined Networking (SDN) is an architecture that enables
users to directly program, orchestrate, control and manage network
resources through software. SDN paradigm relocates the control of
network resources to a dedicated network element, namely SDN
controller. The SDN controller manages and configures the
distributed network resources and provides an abstracted view of the
network resources to the SDN applications. The SDN application can
customize and automate the operations (including management) of the
abstracted network resources in a programmable manner via this
interface [RFC7149][ITU-T.Y.3300]
[ONF-SDN-Architecture][ONF-OpenFlow].

Typically, traditional IPsec VPN concentrators and, in general,
gateways supporting IKE/IPsec, are configured manually. This makes
the IPsec security association (SA) management difficult and
generates a lack of flexibility, specially if the number of security
policies and SAs to handle is high. With the grow of SDN-based

scenarios where network resources are deployed in an autonomous
manner, a mechanism to manage IPsec SAs according to the SDN
architecture becomes more relevant. Thus, the SDN-based service
described in this document will autonomously deal with IPsec-based
data protection also in such as an autonomous manner.

First, this document exposes the requirements to support the
protection of data flows using IPsec [RFC4301]. We consider two
cases: 1) Where the network resource implements the IKE protocol, the
IPsec Security Policy Database (SPD) and the Security Association
Database (SAD), and the SDN controller is in charge of provisioning
with required information both IKE and the SPD in the network
resource; 2) Where the SDN controller handles the IPsec SPD and takes
the role of an Internet Key Exchange (IKE) entity in the IPsec
architecture. In this sense, it will provision the required
parameters to create valid entries in the Security Association
Database (SAD), which we assumed to be in the data plane. Therefore,
the data plane will have only support for IPsec while SPD and IKE
functionality is moved to the control plane. In both cases, to carry
out this provisioning, an interface/protocol will be required between
the SDN controller and the data plane to send: the policies to be
applied in the SPD and the credentials for the IKE negotiation (case
1); or the required IPsec SA parameters such as keys, cryptographic
algorithms, IP addresses, IPsec protocol (AH or ESP), IPsec protocol
mode (tunnel or transport), lifetime of the SA, etc (case 2). An
example for case 1 using NETFCONF/YANG can be found in [netconf-vpn].
A YANG model for IPsec can be found in [I-D.wang-ipsecme-ipsec-yang].

Second, this document considers two scenarios to manage autonomously
IPsec SAs: gateway-to-gateway and host-to-gateway [RFC6071]. The
gateway-to-gateway scenario shows how flow protection services are
useful when data is to be protected across gateways in the network.
More precisely, the use case described in Section 8.1 depicts how
these services could be used to protect IP traffic among various
geographically distributed networks under the domain of the same SDN
controller. A variant of this scenario is also covered in
Section 8.2, where the network devices are under different SDN
controllers.

The host-to-gateway scenario described in Section 8.3 covers the case
where one end user belonging to a network wants to access securely
its network from another external network. In such a case, an IPsec
SA needs to be established between the end user's host and the
gateway. In this document, we describe how the SDN controller can
still configure automatically the IPsec SA in the gateway but after
an IKE negotiation.

2. Requirements Language

   The key words "MUST", "MUST NOT", "REQUIRED", "SHALL", "SHALL NOT",
   "SHOULD", "SHOULD NOT", "RECOMMENDED", "MAY", and "OPTIONAL" in this
   document are to be interpreted as described in RFC 2119 [RFC2119].
   When these words appear in lower case, they have their natural
   language meaning.

3. Terminology

   This document uses the terminology described in [RFC7149], [RFC4301],
   [ITU-T.Y.3300], [ONF-SDN-Architecture], [ONF-OpenFlow],
   [ITU-T.X.1252], and [ITU-T.X.800]. In addition, the following terms
   are defined below:

   o Software-Defined Networking: A set of techniques enabling to
      directly program, orchestrate, control, and manage network
      resources, which facilitates the design, delivery and operation of
      network services in a dynamic and scalable manner [ITU-T.Y.3300].

   o Flow / Data Flow: Set of network packets sharing a set of
      characteristics, for example IP dst/src values or QoS parameters.

   o Network Resources: Network devices that can perform packet
      forwarding in a network system. The network resources include
      network switch, router, gateway, VPN concentrators, and similar
      devices. This document makes no difference if these network
      devices are physical or virtual.

   o Flow Protection Policy: The set of rules defining the conditions
      under which a data flow MUST be protected, and the rules that MUST
      be applied to the specific flow.

   o IKE: Protocol to establish IPsec Security Associations (SAs). It
      requires information about the required authentication method
      (i.e. preshared keys), DH groups, modes and algorithms for IKE
      phase 1, etc.

   o SPD: IPsec Security Policy Database. It includes information
      about IPsec policies direction (in, out), local and remote
      addresses, inbound and outboud SAs, etc.

   o SAD: IPsec Security Associations Database. It includes
      information about IPsec security associations, such as SPI,
      destination addresses, authentication and encryption algorithms
      and keys.

4. Objectives

   o Flow-based data protection: SDN-based flow protection services
      based on IPsec to allow the protection of specific data flows
      based on defined security policies.

   o Bootstrapping security associations: SDN-based flow protection
      allow the centralized bootstrapping of IKE credentials (case 1)
      and IPsec key material for AH and ESP (case 2) to eventually
      protect specific data flows among network resources and end users.

5. Case 1: IKE/IPsec in the network resource

   In this case, the SDN controller is in charge of controlling and
   applying SPD entries in the network resource. It also has to derive
   and deliver IKE credentials (for example a pre-shared key) to the
   network resource for the IKE authentication. With these policies and
   credentials, the IKE implementation runs to build the IPsec SAs. The
   application (administrator) will send the IPsec requirements and end
   points information, and the SDN controller will translate those
   requirements into SPD Policies that will be installed in the network
   resource. With that information, the network resources can just run
   IKE to establish the IPsec SA. Figure 1 shows the different layers
   and corresponding functionality.

   Advantages: It is simple since network resources typically have and
   IKE/IPsec implementations.

   Disadvantages: 1) IKE implementations needs to renegotiate IPsec SAs
   upon SPD entries changes without restarting IKE daemon. 2) Data plane
   more complex.

```
             +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
             |              Security Application       | Application
             |   (e.g., IKE/SPD Management/Orchestration) | Layer
             +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
                                  |
             +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
             |             Application Support         |
             +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+ SDN Controller
             | IKE Credential and SPD Policies Distribution| Layer
             +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
                                  |
             +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
             |              Control Support            |
             +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+ Network
             |   IKEv2   |           IPsec(SPD)        | Resource
             +-----------------------------------------+ Layer
             |  IPsec (SAD) Data Protection and Forwarding |
             +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
```
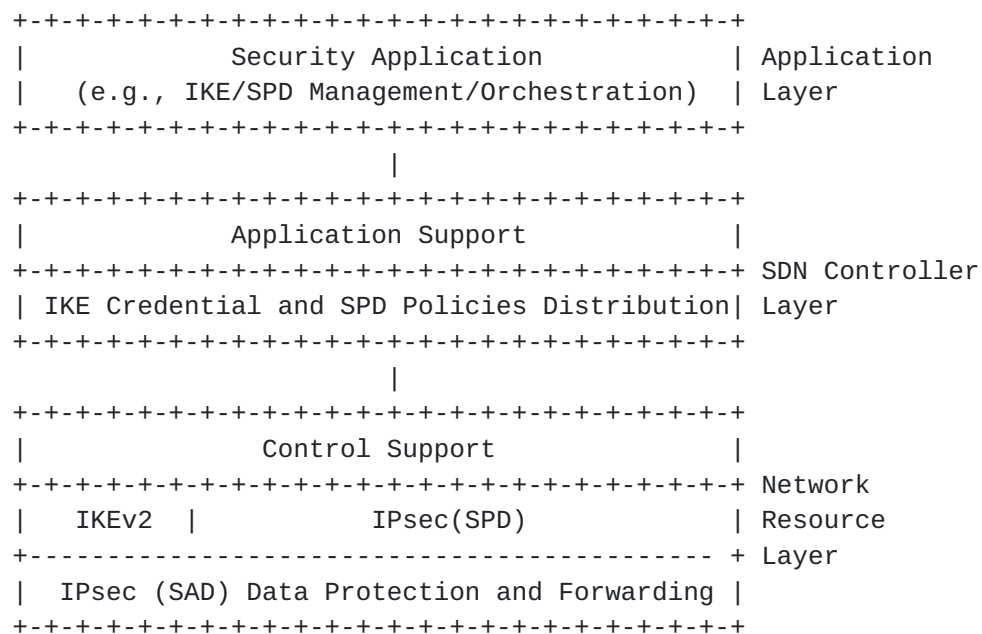
Figure 1: Case 1) High-level Architecture for SDN-based IPsec Flow
                  Protection Services

5.1. Requirements

SDN-based IPsec flow protection services provide dynamic and flexible
network resource management to protect data flows among network
resources and end users. In order to support this capability in case
1, the following requirements are to be met:

o The network resource MUST implement IKE, IPsec, SPD and the SADs.
   It MUST provide an (southbound) interface to configure SPD
   policies and IKE credentials.

o A southbound protocol MUST support sending these SPD Policies and
   IKE Credentials to the network resource.

o It requires an (northbound) application interface in the SDN
   controller allowing the management of IPsec Policies.

o In scenarios where multiple controllers are implicated, SDN-based
   flow protection service may require a mechanism to discover which
   SDN controller is controlling a specific network resource.

6. Case 2: IKE and SPD in the SDN Controller

This section describes the referenced architecture to support SDN-
based IPsec flow protection where the SDN controller owns the SPD and
the IKE implementation.

```
        +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
        |             Security Application        | Application
        |  (e.g., IKE/SDP Management/Orchestration)| Layer
        +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
                          |
        +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
        |             Application Support         |
        +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+ SDN
        |     IKEv2    |       IPsec (SPD)         | Controller
        +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+ Layer
        |       Key Derivation and Distribution   |
        +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
                          |
        +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
        |               Control Support           | Network
        +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+ Resource
        | IPsec (SAD)  Data Protection and Forwarding | Layer
        +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
```
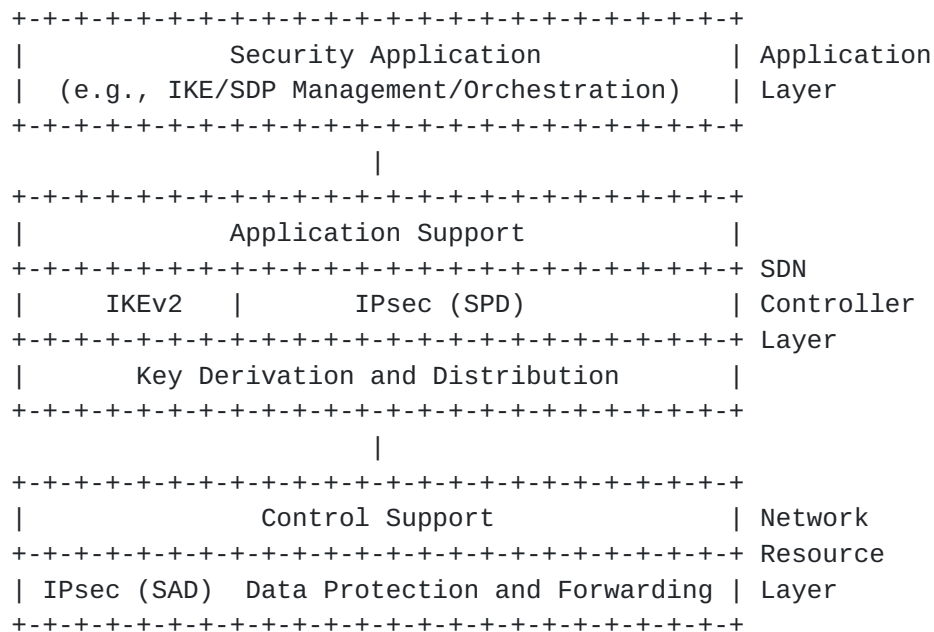
Figure 2: Case 2) SDN Controller holds the SPD and has IKE
                        implementation

As shown in Figure 2, applications for flow protection run on the top
of the SDN controller [ITU-T.Y.3300][ONF-SDN-Architecture]. When an
administrator enforces flow protection policies through an
application interface, the SDN controller inserts the corresponding
flow protection policies into its Security Policy Database (SPD) to
meet such flow protection policies in an autonomous manner.

According to these policies, when the controller decides that a flow
MUST be protected by means of IPsec, it inserts a new flow entry into
the corresponding network resources' flow tables, along with an entry
in the Security Associations Database (SAD) including all IPsec
parameters needed to protect the flow (keys, ESP or AH, transport or
tunnel, ...). This enforcement MAY be triggered by the network
resource when it does not know how to handle the IP packet.
Basically, it forwards the IP packet to the controller so that it can
take a decision based on the SPD. This allow network resources to
protect data flows based in rules dynamically enforced by the SDN
controller.

Advantages: 1) There is clear separation of data plane (IPsec
protection per flow) and control plane (IKE and SPD policies).
Hence, it allows less complex data planes. 2) IKE does not need to be
run in gateway-to-gateway scenario with a single controller (see
Section 8.1).

Disadvantages: 1) The overload of IKE negotiation is shifted to the
SDN controller. 2) IPSec SPD and SAD management need to be decoupled,
changing the traditional paradigm defined in IPsec where SPD and SAD
are placed in the network resource

6.1. Requirements

In order to support this capability in case 2, the following
requirements are to be met:

o It requires the provision of flow entries in network resources.
   Flow entries may need to include fields such as AH or ESP
   parameters, tunnel or transport mode and crypto material to
   process an IP packet with IPsec (in the end, the Security
   Association Database (SADs) is managed by the network resource).
   In the same way a southbound protocol MUST support sending this
   information to the network resource.

o Network resources MUST be capable to protect data flows with
   IPsec, such as the capability to forward data through an IPsec
   tunnel.

o It requires an (northbound) application interface in the SDN
   controller allowing the management of IPsec policies.

o In scenarios where multiple controllers are implicated, SDN-based
   flow protection service may require a mechanism to discover which
   SDN controller is managing a specific network resource.

7. Relationship with I2NSF

According to [I-D.dunbar-i2nsf-problem-statement] a Network Security
Function (NSF) is a function that ensures "integrity, confidentiality
and availability of network communications" among other aspects. As
such, the network resource we describe in this document can be
considered as a NSF with IPsec support. Additionally, the SDN
controller can be considered as a Security controller. In
[I-D.merged-i2nsf-framework-02] a framework for Interface to Network
Security Functions is described. Three possible interfaces are
described: Client Facing (service layer) Interface; NSF Facing
(capability) Interface and Vendor Facing Interface.

Figure 3 and Figure 4 describe the mapping with our use case. In the
right side of the figure each entity follows the same terminology
than [I-D.merged-i2nsf-framework-02].

```
                    +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
                    |              Security Application      | Client or
                    |   (e.g., IKE/SPD Management/Orchestration) |  App
Gateway
                    +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
                                        |   Client Facing (service layer)
Interface
                    +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
        Vendor      |           Application Support          |
        Facing <--->+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+ Security
        Interface   | IKE Credential and SPD Policies Distribution| Controller
                    +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
                                        |    NSF Facing (capability)
Interface
                    +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
                    |              Control Support           |
                    +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+ Network
                    |   IKEv2  |          IPsec(SPD)          | Security
                    +-----------------------------------------+ Function
(NSF)
                    | IPsec (SAD) Data Protection and Forwarding |
                    +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
```

                  Figure 3: Case 1) Mapping with I2NSF Framework

```
                    +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
                    |              Security Application      | Client or
                    |   (e.g., IKE/SPD Management/Orchestration) |  App
Gateway
                    +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
                                        |   Client Facing (service layer)
Interface
                    +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
        Vendor      |           Application Support          |
        Facing <--->+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+ Security
        Interface   | IKEv2   |        IPsec (SPD)           | Controller
                    +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
                    |        Key Derivation and Distribution |
                    +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
                                        |    NSF Facing (capability)
Interface
                    +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
                    |              Control Support           | Network
                    +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+ Security
                    | IPsec (SAD) Data Protection and Forwarding | Function
(NSF)
                    +-----------------------------------------+
```
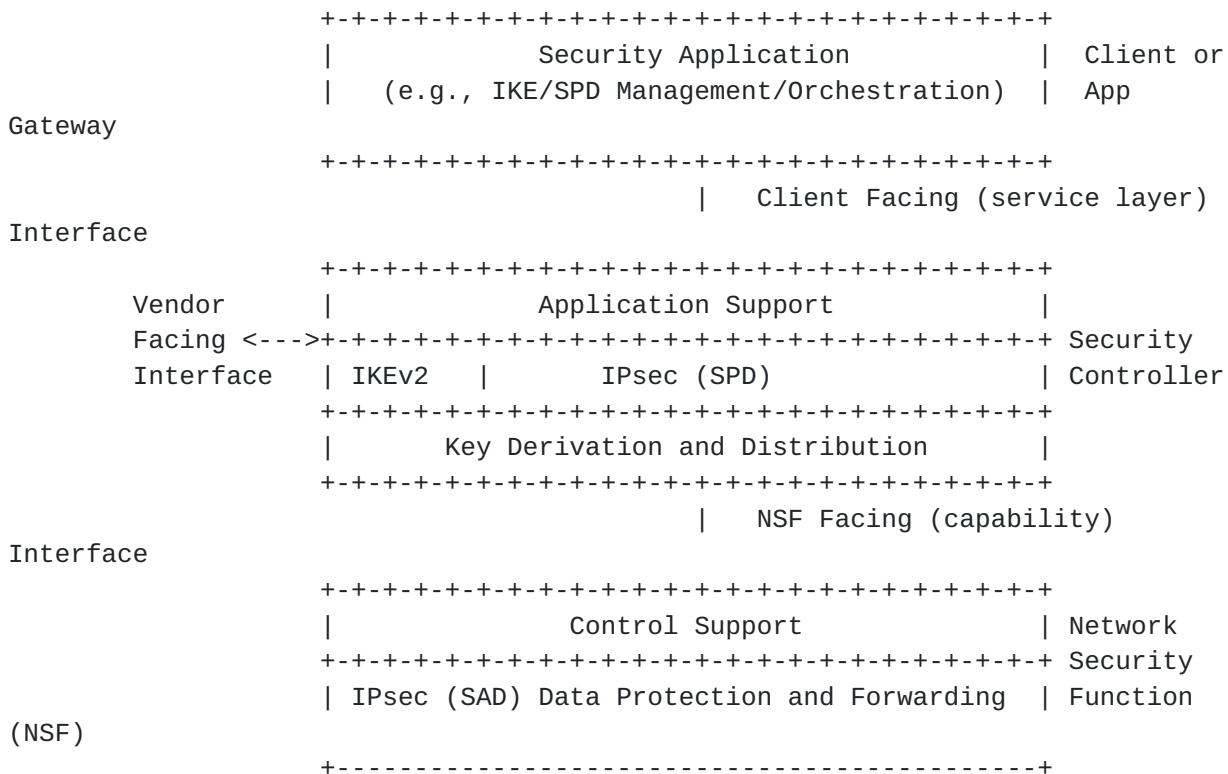
Figure 4: Case 2) Mapping with I2NSF Framework

NOTE: We believe these use cases can be considered as additional uses
cases to the work proposed in
[I-D.jeong-i2nsf-sdn-security-services-03] though we have found some
differences between the mapping to I2NSF we show in this document and
that reference. That is something that we will have to analyze in
the future.

8. Scenarios

   This section explains three use cases as examples for the SDN-based
   IPsec Flow Protection Service.

8.1. Gateway-to-gateway under the same controller

   Enterprise A has a headquarter office (HQ) and several branch offices
   (BO) interconnected through an Internet connection provided by an
   Internet Service Provicer (ISP). This ISP has deployed a SDN-based
   architecture to provide connectivity to all its clients, including HQ
   and BOs, so the HQ is provided with a gateway that acts as a router
   between Internet and each BO's internal network.

   Now, Enterprise A requires that all traffic between the HQ and BOs
   MUST be protected, for example, with confidentiality and integrity.
   The Entrepise A's administrator has to configure flow protection
   policies in the ISP's SDN controller, determining that all traffic
   among Enterprise A's HQ (HQ A) and each BO MUST be protected. Let us
   assume, for example, with an IPsec ESP tunnel.

   On the one hand, in case 1, these policies are translated into IPsec
   SPD entries and the SDN controller enforces these entries in the
   network resources.

```
                +-----------------------------------------+
                |               SDN Controller            |
                |                                         |
            (1)|   +--------------+ (2)+--------------+ |
      Flow ---------->| Translate    |--->| South. Prot. | |
      Protect. Pol.   |IPsec Policies|    |              | |
                |   +--------------+    +--------------+ |
                |                        |    |    |
                |                        |    |    |
                +------------------------|-----|-------+
                                         |    |
                                         | (3) |
                |------------------------+    +---|
       From         V                                V         To
       HQ A   +------------------+           +------------------+ BO
      ------>|      GW1          |============>|      GW2         |------->
             |IKE/IPsec(SPD/SAD)|            |IKE/IPsec(SPD/SAD)|
             +------------------+     (4)    +------------------+
```
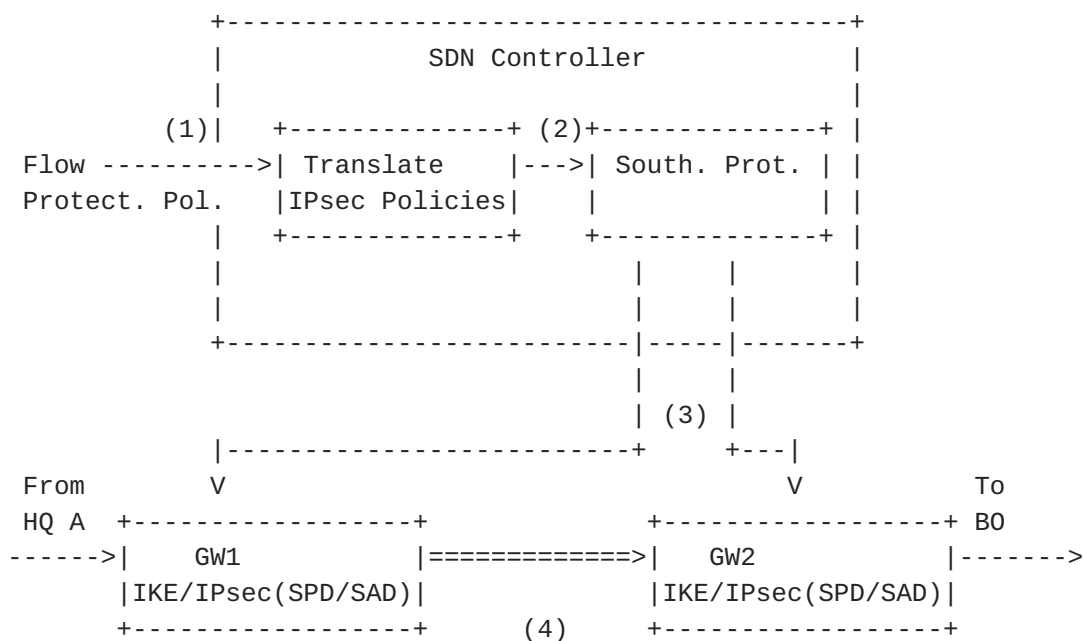
   Figure 5: Gateway-to-Gateway single controller flow for case 1 .

   Figure 5 describes the data and control communication planes in case
   1, when a data packet is sent from HQ A with destination BO :

1. The administrator establishes a general Flow Protection Policies.

2. The SDN controller translates into IPsec Policies entries.

3. The SDN Controller looks for the network resources involved (GW1
    and GW2) and inserts the IPsec SPD entries in both GW1 and GW2
    IPsec SPDs and keys and configuration information related with
    IKE.

4. All packets belonging to the flow that matches the IPsec SDP
    inserted by the SDN controller triggers the IKE negotiation in
    GW1 and GW2 by using the enforced configuration keys and
    parameters.

On the other hand, in case 2, these Flow Protection Policies defined
by the administrator are translated into IPsec SPD entries and
inserted into the SDN controller that represents the IPsec SPD.

```
              +-----------------------------------------+
              |    (0)       SDN Controller             |
   Flow Prot. ---------|                                |
   Pol.       |        V                                |
              |   +-------+       +----------------+    |
        ------->| IPSec |------>|  South. Prot.  |    |
              |  |   | (SPD) |       |                |    |
              |  |   +-------+  (2)  +----------------+    |
              |  |                      |    |              |
              |  |                      |    |              |
       (1) |    +------------------  | --- | -----------+
              |                        |    |
              |                        | (3) |
              |   |-------------------+      +---|
    From      |   V                              V      To
    HQ A   +----------+                    +----------+  BO
   ------->|    GW1    |=================>|    GW2    |------->
          |IPsec(SAD)|                    |IPsec(SAD)|
          +----------+        (4)         +----------+
```
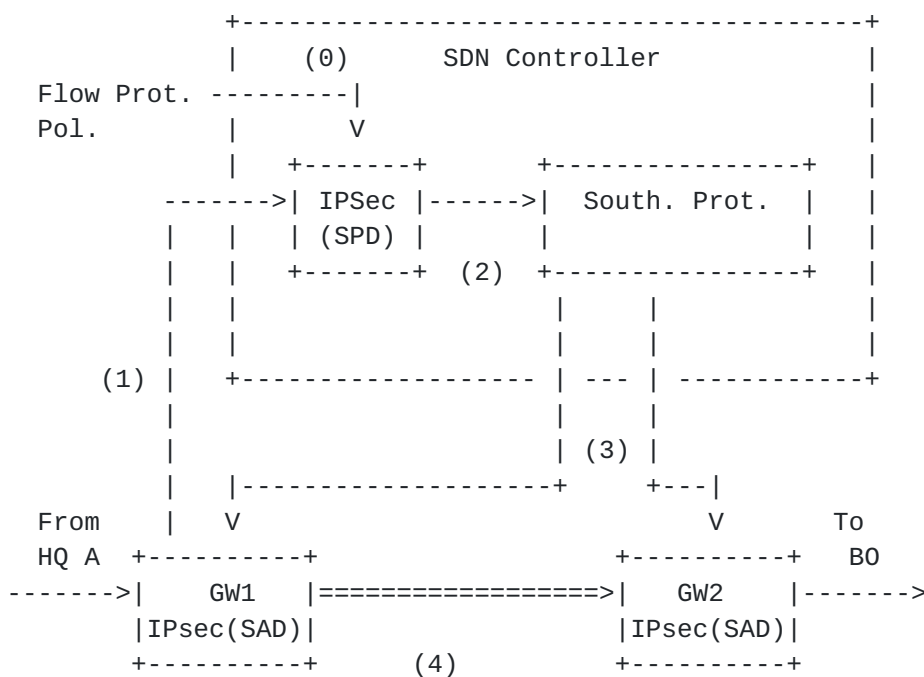
        Figure 6: Gateway-to-Gateway single controller flow for case 2.

Assuming that configuration step has happened (0), Figure 6 describes
the data and control communication planes in case 2, when a data
packet is sent from HQ A with destination BO :

1. When the data packet arrives for first time to the gateway in HQ
    A (GW1), it sends the packet to the SDN Controller.

2. The SDN Controller looks for security policies in its SPD table
    and decides that the flow MUST be protected, for example, with
    IPsec ESP in tunnel mode.

3. The SDN controller derives keys for the IPsec tunnel and enforces
    them, along with other information required, such as IPsec mode
    (ESP or AH), into both gateways' IPsec Security Association
    Database (SAD).

4. All packets belonging to the flow are tunneled between GW1 and
    GW2 by using the enforced configuration keys and parameters. No
    need to run IKE between GW1 and GW2.

In general (for case 1 and case2), this system presents various
advantages to the ISP: (i) it allows to create a security association
among two network resources, with only the application of specific
security policies at the application layer. Thus, the ISP can manage
all security associations in a centralized point and with an
abstracted view of the network; (ii) All new resources deployed after
the application of the new policies will not need to be manually
configured, thus allowing its deployment in an automated manner.

8.2. Gateway-to-gateway under different SDN controllers

Two organizations, Enterprise A and Enterprise B, have its
headquarters interconnected through an Internet connection provided
by different ISPs, called ISP_A and ISP_B. They have deployed a SDN-
based architecture to provide Internet connectivity to all its
clients, so Enterprise A's headquarters is provisioned with a gateway
deployed by ISP_A and Enterprise B's headquarters is provisioned with
a gateway deployed by ISP_B.

Now, these organizations require that all traffic among its
headquarters to be protected with confidentiality and integrity, so
the ISPs have to configure Flow Protection Policies in their SDN
Controllers. Those policies are translated into flow protection
policy rules into the SDN Controller's of each ISP, so all traffic
exchanged among these headquarters will be protected, for example, by
means of an IPsec ESP tunnel.

```
                 +-------------+                  +-------------+
                 |   ISP_A's   |                  |   ISP_B's   |
     Flow Prot.  |    SDN      |<===============>|     SDN     |
     Protect. ---> Controller  |      (2)        |  Controller |
          (1) |                |                  |            |
                 +-------------+                  +-------------+
                       |                                |
                       | (3)                       (3) |
       From            V                                V           To
       HQ A    +------------------+        +------------------+ BO
     ------->|      GW1           |============>|     GW2           |------->
             |IKE/IPsec(SPD/SAD)|              |IKE/IPsec(SPD/SAD)|
             +------------------+      (4)     +------------------+
```
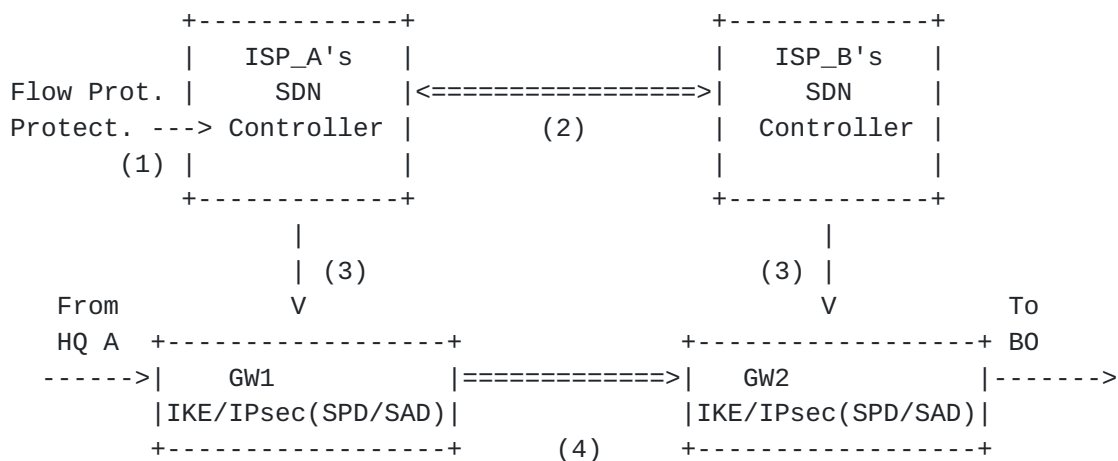
        Figure 7: Gateway-to-gateway multi controller flow in case 1

   On the one hand, case 1, Figure 7 describes the data and control
   plane communications required when a data packet is sent from
   Enterprise A's HQ (HQ A) to destination Enterprise B's HQ (HQ B):

   1. The administrator establishes a general Flow Protection Policies,
       which the SDN controller translates into IPsec Policies.

   2. The ISP_A's SDN Controller realizes that traffic between GW1 and
       GW2 MUST be protected. Nevertheless, the controller notices that
       GW2 is under the control of another SDN controller, so it starts
       negotiations with the other controller to agree on the IPsec SPD
       policies and IKE credentials for their respective gateway NOTE:
       This may require extensions in the East/West interface.

   3. Then, both SDN controllers enforce the IKE credentials and
       related parameters and the IPsec SPD Policies entries in their
       respective gateways.

   4. All packets belonging to the flow that matches the IPsec SDP
       inserted by the SDN controller triggers the IKE negotiation GW1
       and GW2 by using the enforced configuration keys and parameters.

```
         +--------------+                    +--------------+
         |    ISP_A's   |                    |    ISP_B's   |
    Flow. --->
    Prot. |    SDN       |<================>|     SDN      |
    Pol.(0)|  Controller |          (2)       |  Controller  |
         |IKE/IPsec(SPD)|                    |IKE/IPsec(SPD)|
         +--------------+                    +--------------+
            A   |                                  |
          (1) |   | (3)                          (3) |
      From     |    V                               V           To
      HQ A     +-----------+       (4)          +-----------+  HQ B
    --------->|    GW1      |===================>|    GW2     |------->
             |IPsec (SAD)|                      |IPsec (SAD)|
             +-----------+                      +-----------+
```
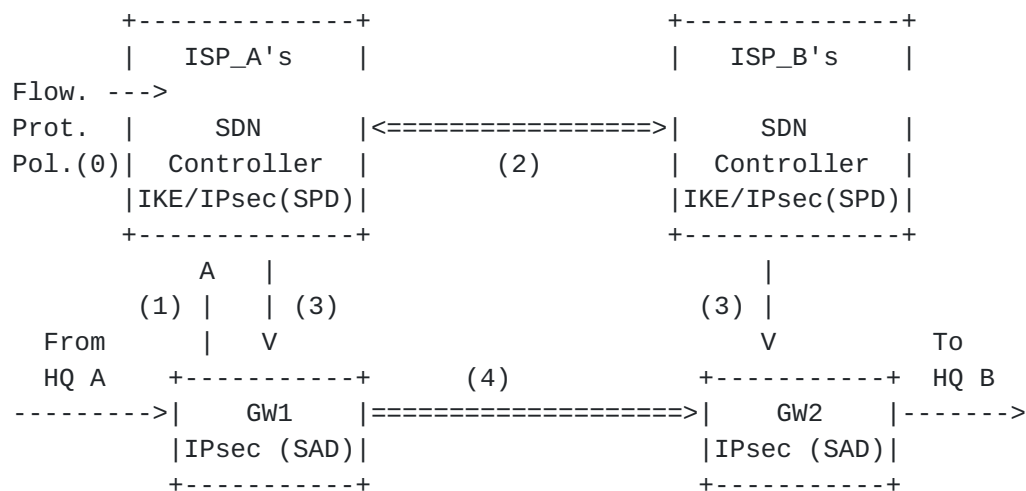
          Figure 8: Gateway-to-gateway multi controller flow in case 2

   On the other hand, case 2, Figure 8 describes the data and control
   plane communications required when a data packet is sent from
   Enterprise A's HQ (HQ A) to destination Enterprise B's HQ (HQ B):

   1. When the data packet arrives for first time to the gateway in
       Enterprise A's headquarters (GW1), it sends the packet to its SDN
       Controller.

   2. The ISP_A's SDN Controller looks for security policies in its SPD
       table and decides that the flow between GW1 and GW2 MUST be
       protected, for example, with IPsec ESP in tunnel mode.
       Nevertheless, the controller notices that GW2 is under the
       control of another SDN controller, so it starts negotiations with
       the other controller in order to generate key material. This
       could be performed by running IKEv2 (NOTE:more discussion is
       required).

   3. Once the controllers have generated shared key material, both
       enforce these keys into their respective gateways' Security
       Association Databases (SAD) along with the IPsec mode and other
       parameters that may be required.

   4. Therefore, all packets belonging to the flow are protected
       between GW1 and GW2 by using the enforced configuration keys and
       parameters.

   In general (case 1 and case 2), this system presents various
   advantages to both ISPs: (i) it allows to create a security
   association among two network resources across ISPs, from each ISP
   point of view, only the application of specific Flow Protection
   Policies at the application layer is needed, so they can manage all

security associations in a centralized point and with an abstracted
view of the network; (ii) All new resources deployed after the
application of the new policies will not need to be manually
configured, thus allowing its deployment in an automated manner.

8.3. Host-to-gateway

Alice is a member of Enterprise A who needs to connect to the HQ's
internal network. Enterprise A has deployed a IPsec-based VPN
concentrator in its HQ to allow members of the organization, like
Alice, to connect to the HQ's internal network in a secure manner.

Traditionally, VPN concentrators are built as appliances, configured
manually to authenticate and establish secure associations with
incoming users, for example, by running IKEv2 to establish an IPsec
tunnel. With the SDN-base management of IPsec protection service we
can automate these configuration.

In case 1, as we can see in Figure 10, the administrator configures a
Flow Protection Policy in the SDN controller (1). The SDN controller
translates that into IPsec Policies and installs those SPD entries
and IKE credentials in the corresponding gateway (VPN concentrator)
(2). With those policies and IKE credentials, end user and gateway
can negotiate IKE.

```
                   +------------------------------------------+
                   |                 SDN Controller           |
                   |                                          |
               (1)|   +--------------+    +--------------+ |
        Flow ---------->| Translate    |--->| South. Prot. | |
        Protect. Pol.   |IPsec Policies|    |              | |
                   |   +--------------+    +--------------+ |
                   |                         |              |
                   |                  (2)  |              |
                   +-----------------------|------------+
                                  |-------+
                                  V
     +----------+                    +------------------+
     | End user |                    |    Gateway       |  To
     | (Alice)  |                    |  (VPN conc.)     |  HQ
     | IKE/IPsec|===================>| IKE/IPsec(SPD/SAD)|------->
     +----------+         (3)        +------------------+
```
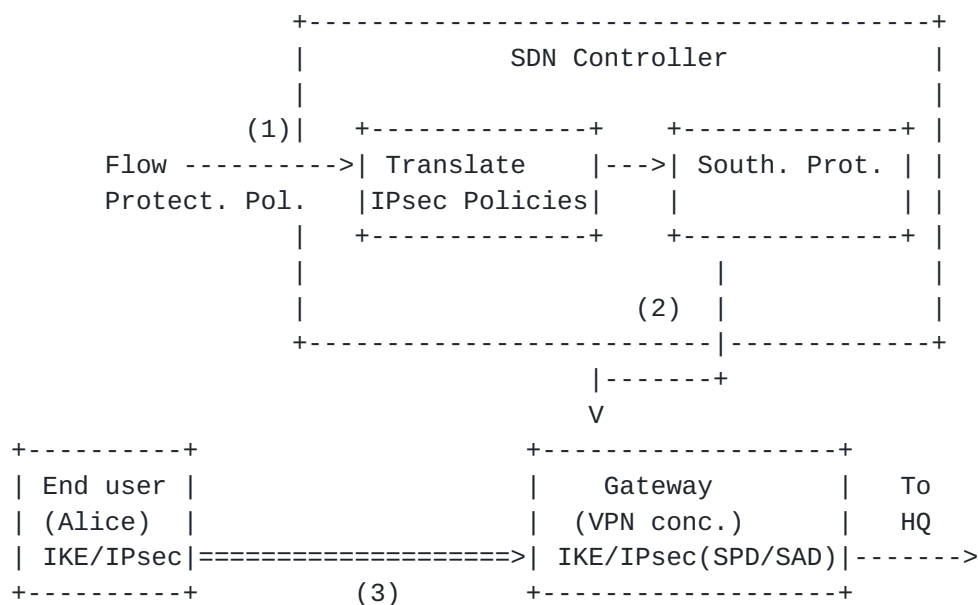
        Figure 9: Host-to-gateway flow protection in case 1.

In case 2, the role of running IKEv2 now resides in the SDN control
plane (i.e. the SDN controller), as we can see in Figure 10. Here,
the gateway forwards IKE packets to the controller. Therefore, the

IKEv2 negotiation is performed by the end user and the SDN controller
(1), being this fact completely transparent for the end user.

Once the IKEv2 negotiation has been successfully completed, new key
material is available in the end user and in the SDN controller.
This key material, along with other parameters like the IPsec mode,
are to be provisioned into the gateway's SAD (2). Now the end user
and the gateway share key material, thus being able to establish an
IPsec tunnel to protect all traffic among them (3).

In general, this feature allows the configuration of network
resources such as VPN concentrators as a service, so these could be
deployed and disposed as required by policies, such as network load,
in an autonomous manner.

```
                                  +----------------------------------+
                                  |           SDN Controller         |
                                  |                                  |
                                  |  +----------+   +-------------+   |
                                  |  |   IKE    |-->| South. Prot.|   |
                                  |  |IPsec(SPD)|   |             |   |
                                  |  +----------    +-------------+   |
                                  |       A                |         |
                                  |       |                |         |
                                  +------ | -----------  | -----------+
                                          |              |
                                    (1)   |         |----- (2)
                                          |         V
        +----------+        (1)      +---|-----------+
        |          |<----------------------|               |
        | End user |                   |    Gateway    |   To
        | (Alice)  |                   |  (VPN conc.)  |   HQ
        | IKE/IPsec|==================>|   IPsec(SAD)  |------->
        +----------+        (3)        +---------------+
```
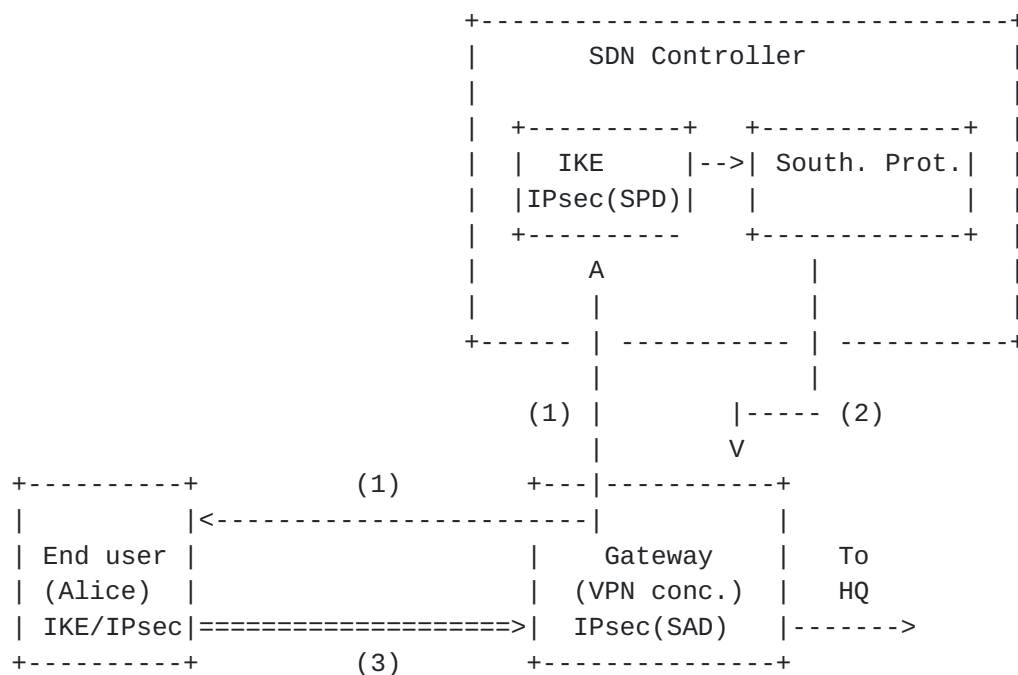
                Figure 10: Host-to-gateway flow in case 2.

9. Security Considerations

TBD.

10. Acknowledgements

Authors want to thank Carlos J. Bernardos and Alejandro Perez-Mendez
for their valuable comments.

11. References

11.1. Normative References

[RFC2119] Bradner, S., "Key words for use in RFCs to Indicate
           Requirement Levels", BCP 14, RFC 2119, DOI 10.17487/
           RFC2119, March 1997,
           <http://www.rfc-editor.org/info/rfc2119>.

[RFC5226] Narten, T. and H. Alvestrand, "Guidelines for Writing an
           IANA Considerations Section in RFCs", BCP 26, RFC 5226,
           DOI 10.17487/RFC5226, May 2008,
           <http://www.rfc-editor.org/info/rfc5226>.

11.2. Informative References

[I-D.dunbar-i2nsf-problem-statement]
           Dunbar, L., Zarny, M., Jacquenet, C., Boucadair, M., and
           S. Chakrabarty, "Interface to Network Security Functions
           (I2NSF) Problem Statement", draft-dunbar-i2nsf-problem-
           statement-05 (work in progress), May 2015.

[I-D.jeong-i2nsf-sdn-security-services-03]
           Jeong, J. and J. Park, "Software-Defined Networking Based
           Security Services using Interface to Network Security
           Functions", draft-jeong-i2nsf-sdn-security-services-03
           (work in progress), October 2015.

[I-D.merged-i2nsf-framework-02]
           Lopez, E., Lopez, D., Zhuang, X., Dunbar, L., Parrott, J.,
           Krishnan, R., and SR. Durbha, "Framework for Interface to
           Network Security Functions", draft-merged-i2nsf-framework-
           02.txt (work in progress), June 2015.

[I-D.wang-ipsecme-ipsec-yang]
           Wang, H., Nagaraj, V., and X. Chen, "Yang Data Model for
           IPsec", draft-wang-ipsecme-ipsec-yang-00 (work in
           progress), June 2015.

[ITU-T.X.1252]
           "Baseline Identity Management Terms and Definitions",
           April 2010.

[ITU-T.X.800]
           "Security Architecture for Open Systems Interconnection
           for CCITT Applications", March 1991.

   [ITU-T.Y.3300]
             "Recommendation ITU-T Y.3300", June 2014.

   [netconf-vpn]
             Stefan Wallin, "Tutorial: NETCONF and YANG", January 2014.

   [ONF-OpenFlow]
             ONF, "OpenFlow Switch Specification (Version 1.4.0)",
             October 2013.

   [ONF-SDN-Architecture]
             "SDN Architecture", June 2014.

   [RFC4301] Kent, S. and K. Seo, "Security Architecture for the
             Internet Protocol", RFC 4301, DOI 10.17487/RFC4301,
             December 2005, <http://www.rfc-editor.org/info/rfc4301>.

   [RFC6071] Frankel, S. and S. Krishnan, "IP Security (IPsec) and
             Internet Key Exchange (IKE) Document Roadmap", RFC 6071,
             DOI 10.17487/RFC6071, February 2011,
             <http://www.rfc-editor.org/info/rfc6071>.

   [RFC7149] Boucadair, M. and C. Jacquenet, "Software-Defined
             Networking: A Perspective from within a Service Provider
             Environment", RFC 7149, DOI 10.17487/RFC7149, March 2014,
             <http://www.rfc-editor.org/info/rfc7149>.

Authors' Addresses

   Alejandro Abad-Carrascosa
   University of Murcia
   Campus de Espinardo S/N, Faculty of Computer Science
   Murcia 30100
   Spain

   Email: alejandroprimitivo.abad@um.es

   Rafa Marin-Lopez
   University of Murcia
   Campus de Espinardo S/N, Faculty of Computer Science
   Murcia 30100
   Spain

   Phone: +34 868 88 85 01
   Email: rafa@um.es

Gabriel Lopez-Millan
University of Murcia
Campus de Espinardo S/N, Faculty of Computer Science
Murcia 30100
Spain

Phone: +34 868 88 85 04
Email: gabilm@um.es