IKEv2 Alternate Outer IP Address Extension

draft-mglt-ipsecme-alternate-outer-address-00.txt

D. Migault

12/03/2013- IETF86- Orlando
Addressed Problem

This draft considers the following situation:

- A VPN Client is attached to a Security Gateway (IKEv2 + VPN)
- At least one has multiple interfaces
- We want different paths for the IKEv2 and VPN channel
- We want to be able to use multiple interfaces (i.e., multiple VPNs) with a single IKEv2 channel

The problem addressed is: How can a VPN Client negotiate the outer IP addresses of a SA

- Negotiation of the outer IP address occurs during the SA negotiation
- We define the Alternate Outer IP Address (OADD) Transform
VPN End User with Multiple Interfaces

Addressed Problem

Use cases

VPN End User

Security Gateway

Interface_0 : VPN_0

Interface_1 : VPN_1
Security Gateway with Multiple Interfaces

+---------------------------------------------------+   +---------------------------------------------------+
|                VPN                             |          |                Security Gateway                    |
|              End User                       |          |                                |
| +-----------------+     +-----------------+   |                                |
|     Interface_0 : VPN_0                         | v       |     Interface_1 : VPN_1                     |
|     ============= Security =============         |       |
|          ^ ============                       |       |
|
Distributed Security Gateways

IKEv2 Interface_0 IKE Security Gateway

VPN Channel 📩 Security

End User

VPN Channel 📩 Security Interface_1 Gateway

+------------------+
| Interface_i       |
| VPN Gateway       |
| Security          |
+------------------+
SA Payload Structure

SA Payload
|-- Proposal #1 ( Proto ID = ESP(3), SPI size = 4,
|    7 transforms, SPI = 0x052357bb )
   |-- Transform ENCR ( Name = ENCR_AES_CBC )
      |-- Attribute ( Key Length = 128 )
   |-- Transform ENCR ( Name = ENCR_AES_CBC )
      |-- Attribute ( Key Length = 256 )
   |-- Transform INTEG ( Name = AUTH_HMAC_SHA1_96 )
   |-- Transform INTEG ( Name = AUTH_AES_XCBC_96 )
   |-- Transform ESN ( Name = ESNs )
   |-- Transform ESN ( Name = No ESNs )
OADD Transform Description

Here are the new entities involved:

- A new Transform: OADD
- New Transform Type: INIT and RESP
- New Attributes: IP and ANY_IP

To advertise that Alternate Outer IP addresses can negotiated:

- ALTERNATE_OUTER_IP_ADDRESS_SUPPORTED
Basic Exchange

Initiator                                    Responder
---------------------------------------------

Initiator Responder

--- From this exchange:
- the Initiator and the Responder support
the alternate outer IP address extension
- no NAT has been detected

---

HDR, SAi1, KEi, Ni    -->
N(ALTERNATE_OUTER_IP_ADDRESS_SUPPORTED)
N(NAT_DETECTION_SOURCE_IP),
N(NAT_DETECTION_DESTINATION_IP)

<--    HDR, SAr1, KEr, Nr, [CERTREQ]
N(ALTERNATE_OUTER_IP_ADDRESS_SUPPORTED)
N(NAT_DETECTION_SOURCE_IP),
N(NAT_DETECTION_DESTINATION_IP)
Basic Exchange

Initiator                                           Responder
----------------------------------------------------

HDR, SK {IDi, [CERT,] [CERTREQ,] [IDr,] AUTH, TSi, TSr
SAi2( Proposal(ENCR, INTEG, ESN, < proposes IP1, IP2
    OADD(INIT, IP1), for the init., ANY
    OADD(INIT, IP2), IP for the resp.
    OADD(RESP, ANY_IP))
Proposal(ENCR, INTEG, ESN)))} < proposes to use
    --> IKEv2 IP for the VPN outer IP

<--  HDR, SK {IDr, [CERT,] AUTH, TSi, TSr,
    SAr2(Proposal(ENCR, INTEG, ESN,
        OADD(INIT, IP1),
        OADD(RESP, IPr)))}