Configuration payload
<draft-dukes-ikev2-config-payload-00.txt>

Status of this Memo

This document is an Internet-Draft and is in full conformance with all provisions of Section 10 of RFC2026 [1].

Internet-Drafts are working documents of the Internet Engineering Task Force (IETF), its areas, and its working groups. Note that other groups may also distribute working documents as Internet-Drafts. 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."

The list of current Internet-Drafts can be accessed at http://www.ietf.org/ietf/1id-abstracts.txt
The list of Internet-Draft Shadow Directories can be accessed at http://www.ietf.org/shadow.html.

Abstract

This document proposes changes to IKEv2 [IKEv2] to allow configuration data to be securely distributed to IPsec Remote Access Clients (IRACs) by IPsec Remote Access Servers (IRASs). It is assumed this draft will be merged with the IKEv2 draft [IKEv2] and refers to sections in that draft, preceded by "****ö. This draft, on its own, is not intended to progress to any RFC status.

Comments regarding this draft should be sent to ddukes@cisco.com or ipsec@lists.tislabs.com

Conventions used in this document

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 [2].
1. Introduction

1.1. Changes from draft-dukes-ike-mode-cfg-02.txt

1.2. Reader Prerequisites
In remote access scenarios it is desirable and often necessary for an IRAS to provide configuration data, such as an internal IP address, to an IRAC before Child-SAs are created. This document describes requirements on TSi and TSr, and an additional Configuration Payload in message 3 and 4 (IKE_SA_AUTH) of IKE-SA creation in order to provide configuration data necessary for the creation of Child-SAs. The Configuration Payload MAY also be used within an Informational Exchange protected by an IKE-SA to request or set configuration data from or to an IKE peer.

1.1. Changes from draft-dukes-ike-mode-cfg-02.txt

This document is similar to draft-dukes-ike-mode-cfg-02.txt for IKEv1 [IKE], but is not intended to interoperate directly with implementations of that draft.

Some differences for IKEv2
1 - No transaction exchange, use the Informational exchange and the IKE_SA_AUTH exchange.
2 - The payload was called Attribute payload in the IKEv1 modecfg, it is called Configuration payload in IKEv2.
3 - No Identifier in the Configuration Payload since this was a major point of confusion in the IKEv1 modecfg draft, with no known use other than XAUTH.
4 - Configuration payloads are always secured via the IKE-SA.

1.2. Reader Prerequisites

It is assumed that the reader is familiar with Proposal for the Internet Key Exchange (IKEv2) Protocol [IKEv2]

2. IKE_SA_AUTH Exchange changes

**** [Below are changes to section 3.1 of [IKEv2], Message 3 and 4 are modified to include the Configuration Payload and additional description of CP and TS requirements are added]

HDR, SAi1, KEi, Ni, Nr,
SK {IDi, [CERT,] [CERTREQ,] [IDr,] AUTH, [CP], SAi2, TSi, TSr}     -->

The optional CP (Configuration Payload) MAY be sent by the initiator to request configuration data. If CP is used to request an internal IP address (as is often the case when the initiator is an IRAC) the initiator may not know what to place in the TSi payload, in this case she MUST include at least one Traffic Selector in TSi with a suitable range of ports, and addresses. As an example, if the initiator did not have a selector trigger SA creation (as may be the case when an IRAC starts up) she may include the selector (0.0.0.0-255.255.255.255) all ports and protocols. At least one suitable selector MUST be included in TSr. Continuing with this example, the initiator may not have any knowledge of the addresses secured by the responder so she MAY include the selector (0.0.0.0-255.255.255.255) all ports and protocols, requiring the responder to choose a
narrower selector if necessary.

\[ 
\text{\ldots HDR, SK \{IDr, [CERT,] AUTH, [CP], SAr2, TSi, TSr\}} 
\]

If CP was present in message 3 there MUST be a corresponding CP in message 4. When the responder sends a CP containing an internal IP address in message 4, he MUST limit the traffic selector(s) in TSi to contain only the address, or addresses, in the CP. The responder MAY choose to limit TSr as described in section 4.9 Negotiating Traffic Selectors of [IKEv2].

2. Informational (Phase 2) Exchanges

**** [This is an amendment to [IKEv2] section 3.3, paragraph 5 and the exchange description at the end of that section]

Messages in an Informational Exchange may contain zero or one Configuration Payloads. If there is a Configuration Payload in a request there MUST be a corresponding Configuration Payload in the response.

The Informational Exchange is defined as:

\[
\begin{align*}
\text{Initiator} & \rightarrow \text{Responder} \\
\text{HDR, SK \{N, \ldots, D, \ldots, CP, \ldots\}} & \rightarrow \\
\text{HDR, SK \{N, \ldots, D, \ldots, CP, \ldots\}} & \leftarrow
\end{align*}
\]

3. Configuration Payload

**** [This should be added to [IKEv2] section 5.]

A Configuration payload, denoted CP in this document, is used to exchange configuration information between IKE peers. Typically the peers would be an IRAC and IRAS. A Configuration Payload MAY appear in an Informational exchange, or an IKE_SA_AUTH exchange, and MUST NOT be in any other exchanges.

Configuration payloads are of type CFG_REQUEST/CFG_REPLY or CFG_SET/CFG_ACK (see CFG Type in the payload description below)

- "CFG_REQUEST/CFG_REPLY" allows an IRAC to request information from an IRAS. If an attribute in the CFG_REQUEST Configuration Payload is not zero length it is taken as a suggestion for that attribute. The CFG_REPLY Configuration Payload MAY return that attribute, or a new one. It MAY also add new attributes and not include some requested ones.

A CFG_REPLY MUST be sent when a CFG_REQUEST is received, even if it is empty, or missing attributes from the CFG_REQUEST. This merely means that the requested attributes were not available or unknown.
"CFG_SET/CFG_ACK" allows an IRAS to push configuration data to an IRAC. In this case the CFG_SET Configuration Payload contains attributes the initiator wants its peer to alter. The responder MUST return a Configuration Payload and it MUST contain the zero length attributes that the responder accepted. Those attributes that it did not accept MUST NOT be in the CFG_ACK Configuration Payload.

<table>
<thead>
<tr>
<th>Initiator</th>
<th>Responder</th>
</tr>
</thead>
<tbody>
<tr>
<td>HDR, SK{CP(CFG_SET)}</td>
<td>--&gt;</td>
</tr>
<tr>
<td>HDR, SK{CP(CFG_ACK)}</td>
<td>&lt;--</td>
</tr>
</tbody>
</table>

The Configuration Payload is defined as follows:

```
+-------------------+-------+-------------------+-------+
| Next Payload      | !     | Payload Length    | !     |
+-------------------+-------+-------------------+-------+
| CFG Type          | !     | RESERVED          | !     |
+-------------------+-------+-------------------+-------+
| Configuration Attributes | ~     |                    | ~     |
+-------------------+-------+-------------------+-------+
```

- **CFG Type** (1 octet) - The type of exchange represented by the Configuration Attributes.

<table>
<thead>
<tr>
<th>Types</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>RESERVED</td>
<td>0</td>
</tr>
<tr>
<td>CFG_REQUEST</td>
<td>1</td>
</tr>
<tr>
<td>CFG_REPLY</td>
<td>2</td>
</tr>
<tr>
<td>CFG_SET</td>
<td>3</td>
</tr>
<tr>
<td>CFG_ACK</td>
<td>4</td>
</tr>
</tbody>
</table>

Values 5-127 are reserved to IANA. Values 128-255 are for private use among mutually consenting parties.

- **RESERVED** (3 octets) - MUST be sent as zero; MUST be ignored.

```
IKEv2 Configuration Payload December 2002
```

- **Configuration Attribute** (variable length) - These are type length values specific to the Configuration Payload and are defined below. There may be zero or more Configuration Attributes in this payload.

The payload type for the Configuration Payload is **TBD** (**TBD**).

### 3.1. Configuration Attributes
Reserved (1 bit) - This bit MUST be set to zero and MUST be ignored.

Attribute Type (7 bits) - A unique identifier for each of the Configuration Attribute Types, the following are currently defined:

<table>
<thead>
<tr>
<th>Attribute Type</th>
<th>Value</th>
<th>Support</th>
<th>Length</th>
</tr>
</thead>
<tbody>
<tr>
<td>RESERVED</td>
<td>0</td>
<td></td>
<td></td>
</tr>
<tr>
<td>INTERNAL_IP4_ADDRESS</td>
<td>1</td>
<td>YES</td>
<td>0 or 4 octets</td>
</tr>
<tr>
<td>INTERNAL_IP4_NETMASK</td>
<td>2</td>
<td>NO</td>
<td>0 or 4 octets</td>
</tr>
<tr>
<td>INTERNAL_IP4_DNS</td>
<td>3</td>
<td>NO</td>
<td>0 or 4 octets</td>
</tr>
<tr>
<td>INTERNAL_IP4_NBNS</td>
<td>4</td>
<td>NO</td>
<td>0 or 4 octets</td>
</tr>
<tr>
<td>INTERNAL_ADDRESS_EXPIRY</td>
<td>5</td>
<td>YES</td>
<td>0 or 4 octets</td>
</tr>
<tr>
<td>INTERNAL_IP4_DHCP</td>
<td>6</td>
<td>NO</td>
<td>0 or 4 octets</td>
</tr>
<tr>
<td>APPLICATION_VERSION</td>
<td>7</td>
<td>YES</td>
<td>0 or more</td>
</tr>
<tr>
<td>INTERNAL_IP6_ADDRESS</td>
<td>8</td>
<td>YES</td>
<td>0 or 16 octets</td>
</tr>
<tr>
<td>INTERNAL_IP6_NETMASK</td>
<td>9</td>
<td>NO</td>
<td>0 or 16 octets</td>
</tr>
<tr>
<td>INTERNAL_IP6_DNS</td>
<td>10</td>
<td>NO</td>
<td>0 or 16 octets</td>
</tr>
<tr>
<td>INTERNAL_IP6_NBNS</td>
<td>11</td>
<td>NO</td>
<td>0 or 16 octets</td>
</tr>
<tr>
<td>INTERNAL_IP6_DHCP</td>
<td>12</td>
<td>NO</td>
<td>0 or 16 octets</td>
</tr>
<tr>
<td>INTERNAL_IP6_SUBNET</td>
<td>13</td>
<td>YES</td>
<td>0 or 8 octets</td>
</tr>
<tr>
<td>SUPPORTED_ATTRIBUTES</td>
<td>14</td>
<td>YES</td>
<td>0 or multiples of 2</td>
</tr>
<tr>
<td>INTERNAL_IP6_SUBSET</td>
<td>15</td>
<td>YES</td>
<td>0 or 17 octets</td>
</tr>
</tbody>
</table>

Values 16-16383 are reserved to IANA. Values 16384-32767 are for private use among mutually consenting parties.

o INTERNAL_IP4_ADDRESS, INTERNAL_IP6_ADDRESS - An address on the internal network, sometimes called a red node address or private address and MAY be a private address on the Internet. Multiple internal addresses MAY be requested by requesting multiple internal address attributes. The responder MAY only send up to the number of addresses requested.

The requested address is valid until the expiry time defined with the INTERNAL_ADDRESS_EXPIRY attribute or there are no IKE-SAs between the peers.
o INTERNAL_IP4_NETMASK, INTERNAL_IP6_NETMASK - The internal network's netmask. Only one netmask is allowed in the request and reply messages (e.g. 255.255.255.0) and it MUST be used only with an INTERNAL_ADDRESS attribute.

o INTERNAL_IP4_DNS, INTERNAL_IP6_DNS - Specifies an address of a DNS server within the network. Multiple DNS servers MAY be requested. The responder MAY respond with zero or more DNS server attributes.

o INTERNAL_IP4_NBNS, INTERNAL_IP6_NBNS - Specifies an address of a NetBios Name Server (WINS) within the network. Multiple NBNS servers MAY be requested. The responder MAY respond with zero or more NBNS server attributes.

o INTERNAL_ADDRESS_EXPIRY - Specifies the number of seconds that the host can use the internal IP address. The host MUST renew the IP address before this expiry time. Only one of these attributes MAY be present in the reply.

o INTERNAL_IP4_DHCP, INTERNAL_IP6_DHCP - Instructs the host to send any internal DHCP requests to the address contained within the attribute. Multiple DHCP servers MAY be requested. The responder MAY respond with zero or more DHCP server attributes.

o APPLICATION_VERSION - The version or application information of the IPSec host. This is a string of printable ASCII characters that is NOT null terminated.

o INTERNAL_IP4_SUBNET - The protected sub-networks that this edge-device protects. This attribute is made up of two fields; the first being an IP address and the second being a netmask. Multiple sub-networks MAY be requested. The responder MAY respond with zero or more sub-network attributes.

o SUPPORTED_ATTRIBUTES - When used within a Request, this attribute must be zero length and specifies a query to the responder to reply back with all of the attributes that it supports. The response contains an attribute that contains a set of attribute identifiers each in 2 octets. The length divided by 2 (bytes) would state the number of supported attributes contained in the response.

Note that no recommendations are made in this document how an implementation actually figures out what information to send in a reply. i.e. we do not recommend any specific method of an IRAS determining which DNS server should be returned to a requesting IRAC.
4. Notify Message Types

**INTERNAL-ADDRESS-FAILURE**

Indicates an error assigning an internal address (i.e., INTERNAL_IP4_ADDRESS or INTERNAL_IP6_ADDRESS) during the processing of a Configuration Payload by a Responder. If this error is generated within an IKE_SA_AUTH exchange no Child-SA will be created.

5. Implementation Notes

The following descriptions detail how to perform specific functions using the configuration payload. Other functions are possible and thus this list is not a complete list of all of the possibilities. While other functions are possible, the functions listed below MUST be performed as detailed in this document to preserve interoperability among different vendor's implementations.

5.1. Requesting an Internal Address

This function provides address allocation to an IRAC trying to tunnel into a network protected by an IRAS. Since the IKE_SA_AUTH exchange creates an IKE-SA and a Child-SA the IRAC MUST request the internal address, and optionally other information concerning the internal network, in the IKE_SA_AUTH exchange. The IRAS may procure an internal address for the IRAC from any number of sources such as a DHCP/BOOTP server or its own address pool.

<table>
<thead>
<tr>
<th>Initiator</th>
<th>Responder</th>
</tr>
</thead>
<tbody>
<tr>
<td>HDR, SAi1, KEi, Ni, Nr, SK {IDi, [CERT,] [CERTREQ,] [IDr,] AUTH, CP(CFG_REQUEST), SAi2, TSi, TSr} --</td>
<td>-- HDR, SK {IDr, [CERT,] AUTH, CP(CFG_REPLY), SAr2, TSi, TSr}</td>
</tr>
</tbody>
</table>

CP(CFG_REQUEST) MUST contain at least an INTERNAL_ADDRESS attribute (either IPv4 or IPv6) but MAY contain any number of additional attributes the initiator wants returned in the response.
For example, message from Initiator to Responder:

```
CP(CFG_REQUEST)=
    INTERNAL_ADDRESS(0.0.0.0)
    INTERNAL_NETMASK(0.0.0.0)
    INTERNAL_DNS(0.0.0.0)
TSi = (0, 0-65536,0.0.0.0-255.255.255.255)
TSr = (0, 0-65536,0.0.0.0-255.255.255.255)
```

NOTE: Traffic Selectors are a (protocol, port range, address range)

message from Responder to Initiator:

```
CP(CFG_REPLY)=
    INTERNAL_ADDRESS(192.168.219.202)
    INTERNAL_NETMASK(255.255.255.0)
    INTERNAL_SUBNET(192.168.219.0/255.255.255.0)
TSi = (0, 0-65536,192.168.219.202-192.168.219.202)
TSr = (0, 0-65536,192.168.219.0-192.168.219.255)
```

All returned values will be implementation dependent. As can be seen in the above example, the IRAS MAY also send other attributes that were not included in CP(CFG_REQUEST) and MAY ignore the non-mandatory attributes that it does not support.

5.2. Requesting the Peer’s Version

An IKE peer wishing to inquire about the other peer’s version information MUST use the method below. This is an example of a configuration request within an Informational Exchange, after the IKE-SA and first Child-SA have been created.

<table>
<thead>
<tr>
<th>Initiator</th>
<th>Responder</th>
</tr>
</thead>
<tbody>
<tr>
<td>HDR, SK{CP(CFG_REQUEST)}</td>
<td>--&gt;</td>
</tr>
<tr>
<td>&lt;&lt; HDR, SK{CP(CFG_REPLY)}</td>
<td></td>
</tr>
</tbody>
</table>

Dukes

IKEv2 Configuration Payload December 2002

```
CP(CFG_REQUEST)=
    APPLICATION_VERSION(""")

CP(CFG_REPLY)
    APPLICATION_VERSION("foobar v1.3beta, (c) Foo Bar Inc.")
```

6. Enterprise Management Considerations

****[ Something similar to this section could be placed in an appendix to [IKEv2] as well]

The method defined in this document SHOULD NOT be used for wide scale management. Its main intent is to provide a bootstrap mechanism to exchange information within IPSec from IRAS to IRAC. While it MAY be useful to use such a method to exchange information between some Security Gateways (SGW) or small networks, existing management protocols such as DHCP [DHCP], RADIUS [RADIUS], SNMP or
LDAP [LDAP] should be considered for enterprise management as well as subsequent information exchanges.

7. Security Considerations

This draft defines a payload for the Informational Exchange and MUST be protected by an IKE-SA.

8. References


[IKE] D. Harkins, D. Carrel, "The Internet Key Exchange (IKE)", RFC2400

[IKEv2] Charlie Kaufman, "Internet Key Exchange(IKEv2) Protocol", draft-ietf-ipsec-ikev2-03.txt


Dukes
Cisco Systems Co.
2000 Innovation Drive
Kanata, ON, Canada
Phone: 1-613-254-3679
Email: ddukes@cisco.com

IKEv2 Configuration Payload December 2002


. Acknowledgments

The editor would like to thank Stephane Beaulieu, Dan Harkins, Derrell Piper, and Paul Hauffman.

0. Author’s Addresses

Darren Dukes
Cisco Systems Co.
2000 Innovation Drive
Kanata, ON, Canada
Phone: 1-613-254-3679
Email: ddukes@cisco.com
ulll Copyright Statement

"Copyright (C) The Internet Society (date). All Rights Reserved. This
document and translations of it may be copied and furnished to
others, and derivative works that comment on or otherwise explain it
or assist in its implementation may be prepared, copied, published
and distributed, in whole or in part, without restriction of any
kind, provided that the above copyright notice and this paragraph
are included on all such copies and derivative works. However, this
document itself may not be modified in any way, such as by removing
the copyright notice or references to the Internet Society or other
Internet organizations, except as needed for the purpose of
developing Internet standards in which case the procedures for
copyrights defined in the Internet Standards process must be
followed, or as required to translate it into

This Internet Draft expires July 2003