DIAMETER
IP Security Policy Extensions
<draft-calhoun-diameter-ipsec-policy-00.txt>

Status of this Memo

This document is an Internet-Draft. 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. Internet-Drafts may be updated, replaced, or obsoleted by other documents at any time. It is not appropriate to use Internet-Drafts as reference material or to cite them other than as a "working draft" or "work in progress."

To learn the current status of any Internet-Draft, please check the lid-abstracts.txt listing contained in the Internet-Drafts Shadow Directories on ds.internic.net, nic.nordu.net, ftp.nisc.sri.com, or munnari.oz.au.

Abstract

The DIAMETER User Authentication/Authorization extension defines a mechanism which is used by a Network Access Server (NAS) to authenticate dial-up users. IP Security defines a mechanism of establishing a secure link between two entities over a network.

This document defines a mechanism for DIAMETER to inform the NAS of the security policies required for secure communication with a host.

Table of Contents

1.0 Introduction
1.1 Conventions
2.0 Operation
2.1 Login User
2.2 Tunneled User
3.0 Policy Building
4.0 Security Gateway Support
5.0  Attribute Format, Name and Code
6.0  RADIUS Attributes
   6.1  Transform
   6.2  Encryption-Algorithm
   6.3  Authentication-Algorithm
   6.4  Authentication-Method
   6.5  SA-Life-Seconds
   6.6  SA-Life-Kbs
   6.7  DH-Group
   6.8  Key-Length
   6.9  Key-Round
   6.10  Enapsulation-Mode
   6.11  Local-Id
   6.12  Remote-Id
   6.13  SA-Destination
   6.14  Policy
   6.15  Next-Hop
   6.16  SA-Direction
   6.17  Anti-Replay
   6.18  Table of Attributes
7.0  References
8.0  Author’s Address

1.0  Introduction

DIA METER is a proposed protocol for dial-up user authentication, authorization and accounting. In the case of "login" or tunneled users, where the NAS initiates a connection to a specified host on behalf of the user [1][2], the authorization information returned in the DIAMETER message contains the target host information. The only current security mechanism used to secure the connection is to rely on the source IP address of the target host (which is very weak security).

The IP Security (IPSEC) protocol suite is used by entities in order to communicate in a secure fashion over an untrusted network. In order for the NAS to be able to establish a secure link with a destination host or network it requires a set of security policies which defines the target as well as the different transforms which are to be used during the communication. These policies need to be pre-configured on the NAS prior to establishing the secure link.

Since an ISPs users will connect to a variety of hosts over the internet, it becomes very difficult to statically configure these policies for every possible host which a dial-up user may need to connect to. In the case of tunneling, where customers are outsourcing their dial-up services to a service provider this becomes even more complex. It would therefore be desirable to have this information maintained by an AAA server.
The fact that ROAMOPS is creating standards to allow users to roam to any service provider to get internet access complicates the problem even further. It is clear in this scenario that the AAA protocol MUST be able to download IPSEC Security Policies to a NAS.

1.1 Conventions

The following language conventions are used in the items of specification in this document:

- MUST, SHALL, or MANDATORY -- This item is an absolute requirement of the specification.

- SHOULD or RECOMMEND -- This item should generally be followed for all but exceptional circumstances.

- MAY or OPTIONAL -- This item is truly optional and may be followed or ignored according to the needs of the implementor.
2.0 Operation

In this section we will examine two possible types of users. In the first example we will describe a login user, and the second will define how a tunneled user would use the extensions used in this document.

2.1 Login User

In this section we will look at an example of a login user. The user, named joe, dials into a NAS which authenticates the user with the assistance of a local DIAMETER Server. The user’s DIAMETER profile is shown below:

```
  Joe     Password = password
          Service-Type = Login,
          Login-Service = Telnet,
          Login-IP-Host = 10.1.1.1,
          Login-Port = 23
```

As the user’s profile depicts, once the user is authenticated the NAS will create a telnet session to target host 10.1.1.1 on behalf of the user. In this case the NAS is used as a terminal server and sends all of the user’s asynchronous data to the target encapsulated within a telnet session.

As stated above IPSEC is a mechanism used by the NAS and the target to establish a secure telnet connection for the user. Traditionally the NAS must have security policies defined locally which state that all communication with the target host for the user must be secured, and more importantly how secure the communication must be.

2.2 Tunneled User

Document [3] defines a protocol which is used by a NAS to "tunnel" all
PPP data from the user to a destination host. This encapsulation is done in order to allow a user to connect to a destination network from the internet as well as to allow multi-protocol over an IP network.

Document [2] defines RADIUS attributes which may be sent from the DIAMETER Server to the NAS which contain tunneling information, such as the target tunnel endpoint.

In this example we will examine a user named bill which dials into a NAS which authenticates the user using a local DIAMETER Server. The DIAMETER Server informs the NAS that tunneling must occur for the user as shown in the user’s profile below.

```
bill
Password = password
Service-Type = Framed,
Framed-Protocol = PPP,
Framed-IP-Netmask = 255.255.255.255,
Framed-MTU = 1500,
Framed-IP-Address = 2.3.4.5 ,
Tunnel-Type = L2TP,
Tunnel-Medium-Type = IP,
Tunnel-Server-Endpoint = 10.1.1.2,
Tunnel-Password = password
```

As the user’s profile states, once the user is authenticated the NAS will create an L2TP tunnel with the target tunnel endpoint 10.1.1.2. Once the tunnel is established all PPP traffic will be encapsulated and forwarded to the target.

```
+-----+    +-----+    +-----+    +-----+
|     |    |     |    |     |
| Bill|----| NAS |----| DIA |
|     |    |     |    |     |
| PSTN|
|     |
|     |
|     |
------

As stated above IPSEC is a mechanism used by the NAS and the target to establish a secure tunnel for the user. Traditionally the NAS must have security policies defined locally which state that all communication with the target host for the user must be secured, and more importantly how secure the communication must be.

3.0 Policy Building
This section will define how Policies are built, and most importantly why this is so complex.

ISAKMP has the ability for an initiator to offer multiple protection suites (a.k.a. proposals), with preferences associated to them. The idea is that the peer has the ability to choose from one of the proposals offered. In addition it is possible for a proposal to contain more than one transform for a given protocol (analogous to a sub-proposal defined below) which the peer can use.

The following is an example of a complex, yet valid ISAKMP proposal:

```
+-- Protection Suite 1 --+
|               +-----+  |
|           +---|SHA-1|  |
|   +----+  |   +-----+  |
| +-| AH |--+ OR         |
| | +----+  |   +-----+  |
| |         +---| MD5 |  |
|+-----|-+ AND         +-----+  |
|     | |                      |
|     | | +----+   +-----+     |
|     | +-| ESP|---| DES |     |
|     |   +----+   +-----+     |
|     +------------------------+
|     | OR
|+-----|---| ESP|---| 3DES|     |
|   +----+   +-----+     |
|------------------------+
```

In this scenario a requestor proposes two different protection suites, one which consists of both AH and ESP, however note that the AH proposal can use either SHA-1 OR MD5 (note that a preference would be assigned to them). In addition ESP must be used with DES.

The requestor also proposes a second protection suite which only consists of ESP using 3DES.

This type of complexity was not initially designed in the existing DIAMETER protocol, since it is not necessary to correlate many attributes to form a single "proposal". However, document [2] does introduce this complexity with the use of the tag field. This document will make use of this mechanism, but also requires additional information within the DIAMETER attribute to include preference information.
The new header format as described in section 5.0 is necessary in order to be able to "build" policies as defined above. Such a policy could be represented as follow:

Tag = 1
  Protocol = AH / Preference = 1,
  Transform = SHA-1,
  Auth-Algorithm HMAC-SHA-1,
  SA-Life-Seconds = 28800,
  Encapsulation-Mode = Tunnel
  Protocol = AH / Preference = 2,
  Transform MD5,
  Auth-Algorithm HMAC-MD5,
  SA-Life-Kbs = 1024,
  Encapsulation-Mode = Tunnel
  Protocol = ESP / Preference = 1
  Transform DES,
  SA-Life-Seconds = 57600,
  Encapsulation-Mode = Tunnel

Tag = 2
  Protocol = ESP / Preference = 1
  Transform = 3DES,
  Auth-Algorithm DES-MAC,
  SA-Life-Seconds = 57600,
  SA-Life-Kbs = 2048,
  Encapsulation-Mode = Tunnel

Tag = 3
  Protocol = ESP / Preference = 1
  Transform = 3DES,
  Auth-Algorithm HMAC-SHA-1,
  SA-Life-Seconds = 57600,
  SA-Life-Kbs = 2048,
  Encapsulation-Mode = Transport

The above defined policy states that Tag #1 has two AH transforms, the preferred using SHA-1, the alternate using MD5. In addition ESP is to be used with DES as the transform. The second proposal is to only use ESP with 3DES as the transform. The third proposal is added for completeness and depicts a simple policy using only ESP with 3DES in transport mode.

Note that since both the Protocol and the Preference fields are used to "classify" groups of attributes to form a single sub-proposal it is not possible to have more than one protocol type with the same preference number within a given tag.

4.0 Security Gateway Support
The IPSEC Architecture specification[9] defines the concept of a security gateway, which is an intermediate node which provides some security functions. This means that although security from the NAS to the target host may be required, it also means that security from the NAS to the intermediate node is also required.

This functionality further complicates this document since support for such devices must be included.

Consider the following diagram which depicts such a configuration:

```
+-----+                   +-----+   |  |     |
|     |    PSTN    |     |   |  +-----+    +-----+
| Bill|--| DIA |----|Targ.|
|     |    |     |    |     |
| IP   +-----+    +-----+
```

In this scenario the NAS is informed that it must first establish an ESP tunnel to the Security Gateway (SG), and then use AH in transport mode to the target host shown above.

Due to this requirement, it must now be possible to associate the peer with a given policy (as shown in section 3.0). Although it is possible to create a new header format to support the above case it would be preferable to simply use the format defined in section 5.0.

Using the header format defined in section 5.0 it is now possible to define a security hierarchy as shown below:

```
Tag = 4
Protocol = First Host,
SA-Destination = SG,
Direction = Initiator,
Remote-ID = foo,
Policy = 1 / Preference = 1,
Policy = 2 / Preference = 2,
Next Hop = Target

Tag = 5
Protocol = NULL,
SA-Destination = Target,
SA-Direction = Initiator,
Remote-ID = bar,
```

Vakil, Calhoun          expires September 1998          [Page 8]
Policy = 3 / Preference = 1

The above example describes that a secure link must be established with the Security Gateway using either Policy 1 or 2 (with preference given to #1). Once this is complete, a secure link must be established with the target host using policy 3. Note that the Policy number is essentially the tag number assigned to the policies described in section 3.0

Given the mechanism described above it is now possible to build complex hierarchies of security systems which must be penetrated in order to reach the target host. Note that the last hop will not necessarily be the target host since a Security Gateway may be protecting the network instead.

Since Phase 2 security association are unidirectional, it is necessary to specify if the given policy is for the initiator or for the responder. In the example given above, the "policies" are what the NAS is to offer to the peer. When the SA-Direction is set to responder, it informs the NAS what policies it may accept from the peer.

5.0 Attribute Format, Name and Code

This section will define the DIAMETER Attributes which are used to send Security Policies or security hierarchies to the NAS for a given user connection.

The new attribute format is shown below:

```
+-----------------+-----------------+-----------------+
| Attribute Type  | Length          | Flags           |
+-----------------+-----------------+-----------------+
| Vendor ID (opt) | Tag             | Protocol        |
+-----------------+-----------------+-----------------+
| Preference      |                 |                 |
+-----------------+-----------------+-----------------+
```

Flag

This draft defines a new flag bit in the DIAMETER flag field:

4 - (T Bit) Indicates the presence of the Tag, Protocol and Preference fields.
Tag

The Tag field is one octet in length and is intended to provide a means of grouping attributes in the same packet which refer to the same policy or security hierarchy.

Protocol

A Protocol identifier. The following values are supported:

1 - Authentication Header (AH)
2 - Encapsulation Security Payload Header (ESP)
3 - Internet Security Association Key Management Protocol (ISAKMP)
4 - IP Compression (IPCOMP)
255 - First Host (First Host in a chain)

If the protocol identifier in the attributes is ISAKMP, the resulting policy is meant for a Phase 1 exchange. A Phase 1 exchange creates ISAKMP SAs which protect further negotiation traffic between the ISAKMP peers.

If the protocol identifier in the attribute is a protocol type other than ISAKMP, the resulting policy is meant for use in a Phase 2 exchange. A Phase 2 exchange happens under the protection of a pre-existing Phase 1 SA, and negotiates a SA for the protocol specified in the attribute.

Preference

The specific preference for the stated protocol.

Attribute Name: Transform
Attribute Code: 278

Attribute Name: Encryption-Algorithm
Attribute Code: 279

Attribute Name: Hash-Algorithm
Attribute Code: 280

Attribute Name: Authentication-Mechanism
Attribute Code: 281

Attribute Name: SA-Life-Seconds
Attribute Code: 282

Attribute Name: SA-Life-Kbs
Attribute Code: 283
Attribute Name: DH-Group
Attribute Code: 284
Attribute Name: Key-Length
Attribute Code: 285
Attribute Name: Key-Round
Attribute Code: 286
Attribute Name: Encapsulation-Mode
Attribute Code: 287
Attribute Name: Initiator-Id
Attribute Code: 288
Attribute Name: Responder-Id
Attribute Code: 289
Attribute Name: SA-Destination
Attribute Code: 290
Attribute Name: Policy
Attribute Code: 291
Attribute Name: Next-Hop
Attribute Code: 292
Attribute Name: SA-Direction
Attribute Code: 293
Attribute Name: Anti-Replay
Attribute Code: 294

6.0 Attribute Meanings

6.1 Transform

This attributes states the desired transform for the protocol.

<table>
<thead>
<tr>
<th>0</th>
<th>1</th>
<th>2</th>
<th>3</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>1</td>
<td>2</td>
<td>3</td>
</tr>
<tr>
<td>4</td>
<td>5</td>
<td>6</td>
<td>7</td>
</tr>
<tr>
<td>8</td>
<td>9</td>
<td>0</td>
<td>1</td>
</tr>
<tr>
<td>2</td>
<td>3</td>
<td>4</td>
<td>5</td>
</tr>
<tr>
<td>6</td>
<td>7</td>
<td>8</td>
<td>9</td>
</tr>
<tr>
<td>0</td>
<td>1</td>
<td>2</td>
<td>3</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Attribute Type</th>
<th>Length</th>
</tr>
</thead>
<tbody>
<tr>
<td>Flags</td>
<td>Tag</td>
</tr>
<tr>
<td>Protocol</td>
<td>Preference</td>
</tr>
</tbody>
</table>
Attribute Type

278 for Transform

Length

12

Tag

The Tag field is one octet in length and is intended to provide a means of grouping attributes in the same packet which refer to the same policy. This value is also used as a policy identifier.

Protocol

The Protocol field identifies for which protocol this attribute is to be used with as defined previously.

Flag

The Flag field has no meaning with this attribute.

Preference

The Preference field identifies the preference of the current transform within the proposal. The policy with the lowest preference value is preferred.

Value

The value field contains the transform ID. Note that this field is used in conjunction with the protocol ID in order to identify the specific transform. The following values are supported:

0 - NULL (ESP Only)
1 - DES (ESP and AH)
2 - 3DES (ESP Only)
3 - DES_IV64 (ESP Only)
4 - RC5 (ESP Only)
5 - IDEA (ESP Only)
6 - CAST (ESP Only)
7 - Blowfish (ESP Only)
8 - 3IDEA (ESP Only)
9 - DES_IV32 (ESP Only)
10 - ARCFour (ESP Only)
11 - MD5 (AH Only)
12 - SHA-1 (AH Only)
13 - Oakley (ISAKMP Only)
14 - LZS (IPCOMP Only)
15 - V.42bis (IPCOMP Only)
16 - DEFLATE (IPCOMP Only)

It is considered invalid to specify a value which is not relevant to the stated protocol ID in the attribute header.

6.2 Encryption-Algorithm

This attribute states the desired encryption algorithm for ISAKMP phase 1 exchange.

<table>
<thead>
<tr>
<th>0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1</th>
</tr>
</thead>
<tbody>
<tr>
<td>Attribute Type</td>
</tr>
<tr>
<td>-----------------------------------------------</td>
</tr>
<tr>
<td>Flags</td>
</tr>
<tr>
<td>-----------------------------------------------</td>
</tr>
<tr>
<td>Value</td>
</tr>
</tbody>
</table>

Attribute Type

279 for Encryption-Algorithm

Length

12

Tag

The Tag field is one octet in length and is intended to provide a means of grouping attributes in the same packet which refer to the same policy. This value is also used as a policy identifier.
The Protocol field MUST be set to ISAKMP.

Flag

The Flag field has no meaning with this attribute.

Preference

The Preference field identifies the preference of the current policy. The policy with the lowest preference value is preferred.

Value

The value field contains the transform ID. Note that this field is used in conjunction with the protocol ID in order to identify the specific transform. The following values are supported:

1 - DES-CBC
2 - IDEA-CBC
3 - Blowfish-CBC
4 - RC5-R16-B64-CBC
5 - 3DES-CBC
6 - CAST-CBC

6.3 Hash-Algorithm

This attribute states the desired hash algorithm for ISAKMP phase 1 exchange.

<table>
<thead>
<tr>
<th>0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1</th>
</tr>
</thead>
<tbody>
<tr>
<td>Attribute Type</td>
</tr>
<tr>
<td>Flags</td>
</tr>
<tr>
<td>Value</td>
</tr>
</tbody>
</table>

Attribute Type

280 for Hash-Algorithm

Length
Tag

The Tag field is one octet in length and is intended to provide a means of grouping attributes in the same packet which refer to the same policy. This value is also used as a policy identifier.

Protocol

The Protocol field MUST be set to ISAKMP.

Flag

The Flag field has no meaning with this attribute.

Preference

The Preference field identifies the preference of the current policy. The policy with the lowest preference value is preferred.

Value

The value field contains the transform ID. Note that this field is used in conjunction with the protocol ID in order to identify the specific transform. The following values are supported:
1 - MD5
2 - SHA
3 - Tiger

6.4 Authentication-Method

This attribute states the desired authentication algorithm for the IPSEC protocols.
Attribute Type

281 for Authentication-Method

Length

12

Tag

The Tag field is one octet in length and is intended to provide a means of grouping attributes in the same packet which refer to the same policy. This value is also used as a policy identifier.

Protocol

The Protocol field identifies for which protocol this attribute is to be used with as defined previously.

Flag

The Flag field has no meaning with this attribute.

Preference

The Preference field identifies the preference of the current policy. The policy with the lowest preference value is preferred.

Value

The value field contains the transform ID. Note that this field is used in conjunction with the protocol ID in order to identify the specific transform. The following values are supported:

1 - HMAC-MD5 (ESP and AH)
2 - HMAC-SHA-1 (ESP and AH)
3 - DES-MAC (ESP and AH)
4 - Pre-Shared key (ISAKMP Only)
5 - DSS-Signature (ISAKMP Only)
6 - RSA-Signature (ISAKMP Only)
7 - RSA-Encryption (ISAKMP Only)
8 - Revised-RSA-Encryption (ISAKMP Only)
9 - GSSAPI-Authentication (ISAKMP Only)
10 - KPDK (AH Only - MUST be used with MD5 as transform only)
It is considered invalid to specify a value which is not relevant to the stated protocol ID in the attribute header.

6.5 SA-Life-Seconds

This attribute states the lifetime for the generated Security Association for the IPSEC protocol requested. This attribute defines the lifetime in the number of seconds once the SA is established.

```
<table>
<thead>
<tr>
<th>Flags</th>
<th>Tag</th>
<th>Protocol</th>
<th>Preference</th>
</tr>
</thead>
</table>
| | | | | +-----------------+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|                             Value                             |
```

Attribute Type

282 for SA-Life-Seconds

Length

12

Tag

The Tag field is one octet in length and is intended to provide a means of grouping attributes in the same packet which refer to the same policy. This value is also used as a policy identifier.

Protocol

The Protocol field identifies for which protocol this attribute is to be used with as defined previously.

Flag

The Flag field has no meaning with this attribute.

Preference
The Preference field identifies the preference of the current policy. The policy with the lowest preference value is preferred.

Value

The value field contains the number of seconds before the Security Association must be renegotiated.

6.6 SA-Life-Kbs

This attribute states the lifetime for the generated Security Association for the IPSEC protocol requested. This attribute defines the lifetime in the number of kilobytes transmitted once the SA is established.

<table>
<thead>
<tr>
<th>Attribute Type</th>
<th>Length</th>
</tr>
</thead>
<tbody>
<tr>
<td>Flags</td>
<td>Tag</td>
</tr>
<tr>
<td>Protocol</td>
<td>Preference</td>
</tr>
<tr>
<td></td>
<td>Value</td>
</tr>
</tbody>
</table>

Attribute Type

283 for SA-Life-Kbs

Length

12

Tag

The Tag field is one octet in length and is intended to provide a means of grouping attributes in the same packet which refer to the same policy. This value is also used as a policy identifier.

Protocol

The Protocol field identifies for which protocol this attribute is to be used with as defined previously.
Flag

The Flag field has no meaning with this attribute.

Preference

The Preference field identifies the preference of the current policy. The policy with the lowest preference value is preferred.

Value

The value field contains the number of kilobytes before the Security Association must be renegotiated.

6.7 DH-Group

This attribute is used to indicate the Diffie-Hellman group for the phase 2 exchange. If perfect forward secrecy is desired, this attribute must be included. It allows for the negotiation of a fresh DH key for phase 2. This new ephemeral DH key can then be used instead of the phase 1 DH key, to derive session keys for the negotiated transforms.

The attribute’s format is as follows:

```
  0  1  2  3  4  5  6  7  8  9  a  b  c  d  e  f
+-----------------------------------------------+
<table>
<thead>
<tr>
<th>Attribute Type</th>
<th>Length</th>
</tr>
</thead>
<tbody>
<tr>
<td>Flags</td>
<td>Tag</td>
</tr>
<tr>
<td>--------------------------------</td>
<td>--------------------------------</td>
</tr>
<tr>
<td>Value</td>
<td></td>
</tr>
</tbody>
</table>
+-----------------------------------------------+
```

Attribute Type

284 for DH-Group

Length

12

Tag
The Tag field is one octet in length and is intended to provide a means of grouping attributes in the same packet which refer to the same policy. This value is also used as a policy identifier.

Protocol

The Protocol field identifies for which protocol this attribute is to be used with as defined previously. This attribute is not valid for IPCOMP.

Flag

The Flag field has no meaning with this attribute.

Preference

The Preference field identifies the preference of the current policy. The policy with the lowest preference value is preferred.

Value

The value field contains the Diffie-Hellman group and may have one of the following values:

1 - First-Oakley-Group (MODP 768 bit)
2 - Second-Oakley-Group (MODP 1024 bit)
3 - Third-Oakley-Group (EC2N on GP[2^155])
4 - Fourth-Oakley-Group (EC2N on GP[2^185])

6.8 Key-Length

For transforms that take variable length keys, this attribute can be used to indicate the key length desired. Its format is as follows:

```
<table>
<thead>
<tr>
<th>Attribute Type</th>
<th>Length</th>
</tr>
</thead>
<tbody>
<tr>
<td>Flags</td>
<td>Tag</td>
</tr>
<tr>
<td>----------------</td>
<td>--------</td>
</tr>
<tr>
<td>----------------</td>
<td>--------</td>
</tr>
<tr>
<td>----------------</td>
<td>--------</td>
</tr>
</tbody>
</table>
```

6.8.1 Attribute Type
285 for Key-Length

Length

12

Tag

The Tag field is one octet in length and is intended to provide a means of grouping attributes in the same packet which refer to the same policy. This value is also used as a policy identifier.

Protocol

The Protocol field identifies for which protocol this attribute is to be used with as defined previously. This attribute is not valid for IPCOMP.

Flag

The Flag field has no meaning with this attribute.

Preference

The Preference field identifies the preference of the current policy. The policy with the lowest preference value is preferred.

Value

This field contains a non-zero length for the key.

6.9 Key-Round

For transforms that have varying number of rounds, this attribute can be used to indicate the desired number of rounds. Its format is as follows:

<table>
<thead>
<tr>
<th>0</th>
<th>1</th>
<th>2</th>
<th>3</th>
</tr>
</thead>
<tbody>
<tr>
<td>0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Attribute Type</th>
<th>Length</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td>Flags</td>
<td>Tag</td>
</tr>
<tr>
<td>-------------------------------</td>
<td>-------------------------------</td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Vakil, Calhoun  expires September 1998
Attribute Type

286 for Key-Rounds

Length

12

Tag

The Tag field is one octet in length and is intended to provide a means of grouping attributes in the same packet which refer to the same policy. This value is also used as a policy identifier.

Protocol

The Protocol field identifies for which protocol this attribute is to be used with as defined previously. This attribute is not valid for IPCOMP.

Flag

The Flag field has no meaning with this attribute.

Preference

The Preference field identifies the preference of the current policy. The policy with the lowest preference value is prefered.

Value

This field contains a non-zero key round value.

6.10 Encapsulation-Mode

This attribute indicates the encapsulation mode for the given protocol. The attribute's format is as follows:
Attribute Type

287 for Encapsulation-Mode

Length

12

Tag

The Tag field is one octet in length and is intended to provide a means of grouping attributes in the same packet which refer to the same policy. This value is also used as a policy identifier.

Protocol

The Protocol field identifies for which protocol this attribute is to be used with as defined previously.

Flag

The Flag field has no meaning with this attribute.

Preference

The Preference field identifies the preference of the current policy. The policy with the lowest preference value is prefered.

Value

The value field may have one of the following values:
1 - Tunnel-Mode
2 - Transport-Mode
6.11 Initiator-Id

This attribute is used to indicate the identity of the ISAKMP exchange initiator.

If the protocol field is ISAKMP, the identity is meant for a Phase 1 exchange (IDii in [4]). If the NAS happens to be the initiator, it knows its local identity. In this case, the attribute SHOULD not be sent in the Access-Accept. However, if the attribute is sent in the Access-Accept, the NAS has an option of ignoring it. If the attribute is not present in the Access-Accept, the NAS MUST assume that it is to provide its own identity.

If the protocol field is anything but ISAKMP, the attribute provides the user identity on the initiator side for a Phase 2 exchange (IDui in [4]).

<table>
<thead>
<tr>
<th>0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1</th>
</tr>
</thead>
<tbody>
<tr>
<td>Attribute Type</td>
</tr>
<tr>
<td>----------------</td>
</tr>
<tr>
<td>Flags</td>
</tr>
<tr>
<td>ID Type</td>
</tr>
</tbody>
</table>

Attribute Type

288 for Initiator-Id

Length

>10

Tag

The Tag field is one octet in length and is intended to provide a means of grouping attributes in the same packet which refer to the same policy. This value is also used as a policy identifier.

Protocol

The Protocol field identifies for which protocol this attribute is to be used with as defined previously. This attribute is not valid for ISAKMP.
Flag

The Flag field has no meaning with this attribute.

Preference

The Preference field identifies the preference of the current policy. The policy with the lowest preference value is preferred.

ID Type

The ID Type field is one octet in length and represents the format of the address. The following values are supported:

1 - IPV4-Address (4 octets)
2 - IPV6-Address (20 octets)
3 - FQ-Domain-Name (e.g. 3com.com)
4 - FQ-User-Name (e.g. lobo@3com.com)
5 - IPV4-Subnet (4 octets address followed by 4 octets subnet mask)
6 - IPV4-Range (4 octets start address followed by a 4 octet end address)
7 - X.500-Distinguished-Name
8 - X.500-General-Name
9 - Vendor-Specific (pre-shared key identity)

String

The string field contains the local identifier.

6.12 Responder-Id

This attribute is used to indicate the identity of the ISAKMP exchange responder.

If the protocol field is ISAKMP, the identity is meant for a Phase 1 exchange (IDir in [4]). If the NAS happens to be the responder, it knows its local identity. In this case, the attribute SHOULD not be sent in the Access-Accept. However, if the attribute is sent in the Access-Accept, the NAS has an option of ignoring it. If the attribute is not present in the Access-Accept, the NAS MUST assume that it is to provide its own identity.

If the protocol field is anything but ISAKMP, the attribute provides the user identity on the responder side for a Phase 2 exchange (IDur in [4]).
### Attribute Type

289 for Remote-Id

### Length

>10

### Tag

The Tag field is one octet in length and is intended to provide a means of grouping attributes in the same packet which refer to the same Security Association Endpoint.

### Protocol

The Protocol field identifies for which protocol this attribute is to be used with as defined previously.

### Flag

The Flag field has no meaning with this attribute.

### Preference

The Preference field identifies the preference of the current policy. The policy with the lowest preference value is prefered.

### ID Type

The ID Type field is one octet in length and represents the format of the address. The following values are supported:

- 1 - IPV4-Address (4 octets)
2 - IPV6-Address (20 octets)
3 - FQ-Domain-Name (e.g. 3com.com)
4 - FQ-User-Name (e.g. lobo@3com.com)
5 - IPV4-Subnet (4 octets address followed by 4 octets subnet mask)
6 - IPV4-Range (4 octets start address followed by a 4 octet end address)
7 - X.500-Distinguished-Name
8 - X.500-General-Name
9 - Vendor-Specific (pre-shared key identity)

Value

The value field contains the remote identifier.

6.13 SA-Destination

This attribute defines the destination address with which the Security Association will be established.

<table>
<thead>
<tr>
<th>0</th>
<th>1</th>
<th>2</th>
<th>3</th>
</tr>
</thead>
<tbody>
<tr>
<td>0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Attribute Type</th>
<th>Length</th>
</tr>
</thead>
<tbody>
<tr>
<td>+-----------------------------+-------------</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Flags</th>
<th>Tag</th>
<th>Protocol</th>
<th>Preference</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>+-----------------------------+-------------</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Attribute Type

290 for SA-Destination

Length

12

Tag

The Tag field is one octet in length and is intended to provide a means of grouping attributes in the same packet which refer to the same Security Association Endpoint.
Protocol

The Protocol field has no meaning for this attribute.

Flag

The Flag field is used in order to identify the first host in a chain of Security Associations. The S bit is enabled if this host is the first security hop to the target. Note that this bit MUST be enabled even if the first hop is also the last hop.

Preference

The Preference field has no meaning for this attribute.

Value

The value field contains the address of the IPSEC destination, which may be the target host or an intervening Security Gateway.

6.14 Policy

This attribute is used to reference a specific policy for the user. When more than a single instance of this attribute is present within a given tag, the preference field is used in order to identify the preferred policy.

<table>
<thead>
<tr>
<th>Attribute Type</th>
<th>Length</th>
<th>Flags</th>
<th>Tag</th>
<th>Protocol</th>
<th>Preference</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>291</td>
<td>12</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Attribute Type

291 for Policy

Length

12
Tag

The Tag field is one octet in length and is intended to provide a means of grouping attributes in the same packet which refer to the same Security Association Endpoint.

Protocol

The Protocol field has no meaning for this attribute.

Flag

The Flag field has no meaning with this attribute.

Preference

The Preference field identifies the preference of the stated policy. The policy with the lowest preference value is preferred.

Value

The Value field contains the policy identifier as described above. When used with the Preference field it is used in order to associate preferred policies to use for a given SA-Destination.

6.15 Next-Hop

This attribute is used in order to identify the next hop in a chain of security associations. This attribute is used when it is necessary to establish a secure link with a security gateway in order to reach a host using IPSEC or in the case of multiple security gateways.

| Attribute Type | Length |
| Flags | Tag | Protocol | Preference |
| Value |

Attribute Type
292 for Next-Hop

Length

12

Tag

The Tag field is one octet in length and is intended to provide a means of grouping attributes in the same packet which refer to the same Security Association Endpoint.

Protocol

The Protocol field has no meaning for this attribute.

Flag

The Flag field has no meaning with this attribute.

Preference

The Preference field has no meaning with this attribute.

Value

The value field contains the address of the next hop.

6.16 SA-Direction

A Phase 2 SA is unidirectional. This means that a pair of SAs are required to secure a session. If the NAS is initiating the Phase 2 SA exchange, it needs a set of protection suites that it can propose to its peer.

On the other hand, if the NAS is responding to a Phase 2 SA exchange, it receives a set of protection suites from its peer. In this case, it needs a set of local protection suites to compare the proposed suites against. Hence it becomes necessary to provide the NAS with two sets of protection suites; one for use when it is the initiator, and the other when it is the responder.
Attribute Type

293 for SA-Direction

Length

12

Tag

The Tag field is one octet in length and is intended to provide a means of grouping attributes in the same packet which refer to the same Security Association Endpoint.

Protocol

The Protocol field has no meaning for this attribute.

Flag

The Flag field has no meaning with this attribute.

Preference

The Preference field has no meaning with this attribute.

Value

The value field contains the direction of the Security Association. The following values are supported:

1 - Initiator
2 - Reponder
6.17 Anti-Replay

The Anti-Replay attribute is used in order to identify whether anti-replay is to be used for the policy.

<table>
<thead>
<tr>
<th>Attribute Type</th>
<th>Length</th>
</tr>
</thead>
<tbody>
<tr>
<td>Flags</td>
<td>Tag</td>
</tr>
<tr>
<td>Value</td>
<td></td>
</tr>
</tbody>
</table>

Attribute Type

294 for Anti-Replay

Length

12

Tag

The Tag field is one octet in length and is intended to provide a means of grouping attributes in the same packet which refer to the same policy. This value is also used as a policy identifier.

Protocol

The Protocol field identifies for which protocol this attribute is to be used with as defined previously. This attribute is only valid for ESP.

Flag

The Flag field has no meaning with this attribute.

Preference

The Preference field identifies the preference of the current policy. The policy with the lowest preference value is preferred.
Value

The value field may have one of the following values:
1 - Anti-Replay-Enabled
2 - Anti-Replay-Disabled

6.18 Table of Attributes

The following table provides a guide to which of the above attributes may be found in which kinds of packets, and in what quantity.

<table>
<thead>
<tr>
<th>Authentication-Request</th>
<th>Success</th>
<th>Reject</th>
<th>Attribute Number</th>
<th>Name</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>0+</td>
<td>0</td>
<td>278</td>
<td>Transform</td>
</tr>
<tr>
<td>0</td>
<td>0+</td>
<td>0</td>
<td>279</td>
<td>Encryption-Algorithm</td>
</tr>
<tr>
<td>0</td>
<td>0+</td>
<td>0</td>
<td>280</td>
<td>Hash-Algorithm</td>
</tr>
<tr>
<td>0</td>
<td>0+</td>
<td>0</td>
<td>281</td>
<td>Authentication-Mechanism</td>
</tr>
<tr>
<td>0</td>
<td>0+</td>
<td>0</td>
<td>282</td>
<td>SA-Life-Seconds</td>
</tr>
<tr>
<td>0</td>
<td>0+</td>
<td>0</td>
<td>283</td>
<td>SA-Life-Kbs</td>
</tr>
<tr>
<td>0</td>
<td>0+</td>
<td>0</td>
<td>284</td>
<td>DH-Group</td>
</tr>
<tr>
<td>0</td>
<td>0+</td>
<td>0</td>
<td>285</td>
<td>Key-Length</td>
</tr>
<tr>
<td>0</td>
<td>0+</td>
<td>0</td>
<td>286</td>
<td>Key-Round</td>
</tr>
<tr>
<td>0</td>
<td>0+</td>
<td>0</td>
<td>287</td>
<td>Encapsulation-Mode</td>
</tr>
<tr>
<td>0</td>
<td>0+</td>
<td>0</td>
<td>288</td>
<td>Initiator-Id</td>
</tr>
<tr>
<td>0</td>
<td>0+</td>
<td>0</td>
<td>289</td>
<td>Responder-Id</td>
</tr>
<tr>
<td>0</td>
<td>0+</td>
<td>0</td>
<td>290</td>
<td>SA-Destination</td>
</tr>
<tr>
<td>0</td>
<td>0+</td>
<td>0</td>
<td>291</td>
<td>Policy</td>
</tr>
<tr>
<td>0</td>
<td>0+</td>
<td>0</td>
<td>292</td>
<td>Next-Hop</td>
</tr>
<tr>
<td>0</td>
<td>0+</td>
<td>0</td>
<td>293</td>
<td>SA-Direction</td>
</tr>
<tr>
<td>0</td>
<td>0+</td>
<td>0</td>
<td>294</td>
<td>Anti-Replay</td>
</tr>
</tbody>
</table>

The following table defines the meaning of the above table entries.

0     This attribute MUST NOT be present in packet.
0+    Zero or more instances of this attribute MAY be present in packet.
0-1   Zero or one instance of this attribute MAY be present in packet.

7.0 References


8.0 Author’s Address

Questions about this memo can also be directed to:

Sumit A. Vakil  
3Com Corporation  
1800 W. Central Rd.  
Mount Prospect, Il, 60056  
USA

Phone: 1-847-342-6892  
Fax: 1-847-222-2424  
E-mail: Sumit_Vakil@MW.3Com.Com

Pat R. Calhoun  
Technology Development  
Sun Microsystems, Inc.  
15 Network Circle

Vakil, Calhoun expires September 1998