Teldat Router

IPSec

Doc. *DM739-I* Rev. *10.10*
August, 2003

INDEX

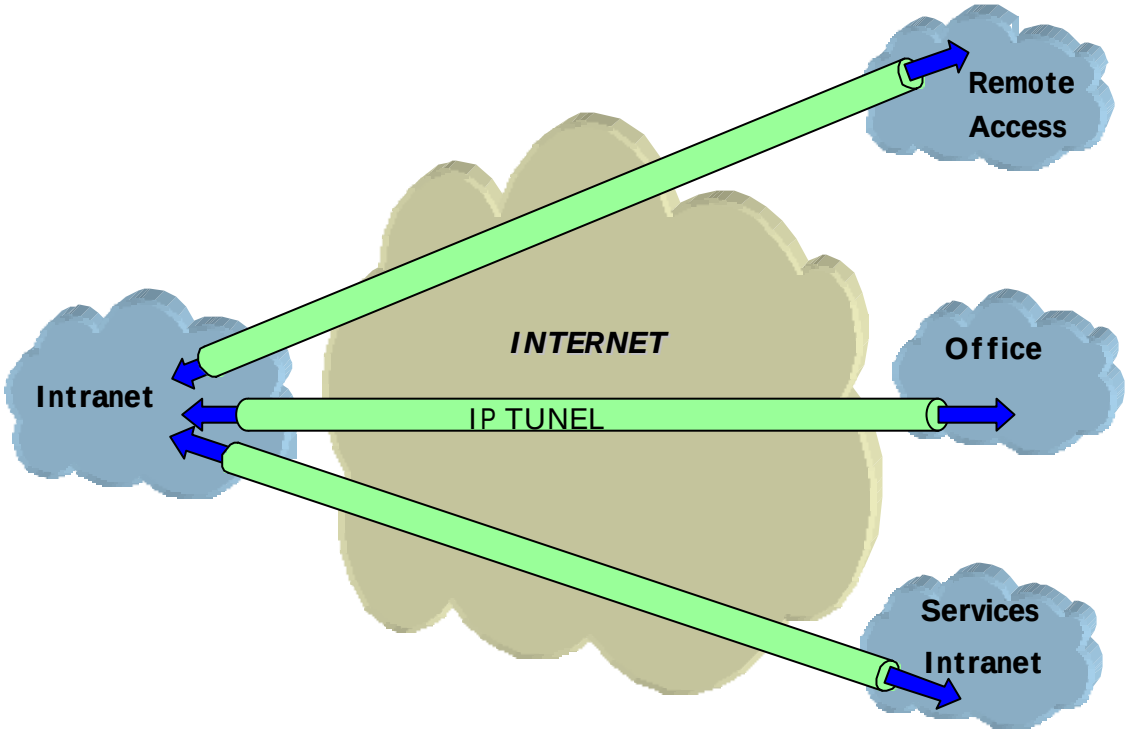
Chapter 1
Introduction

1. Virtual Private Networks

Until now, companies have traditionally used the Internet to promote their services and products through Web Sites. Today more and more companies use the Internet to communicate between their branches, offices or R+D centers. In short, the Internet could take the place of expensive private and less flexible telephone lines. Furthermore, the e-business requires global access (World Wide Web) offered by the Internet.

The packets which circle public networks, such as the Internet, are moved by multiple nodes that cannot be controlled or watched over. The route of these packets for the same destination is variable and therefore security mechanisms need to be established to prevent any intruder from accessing the information that you send through this type of network.

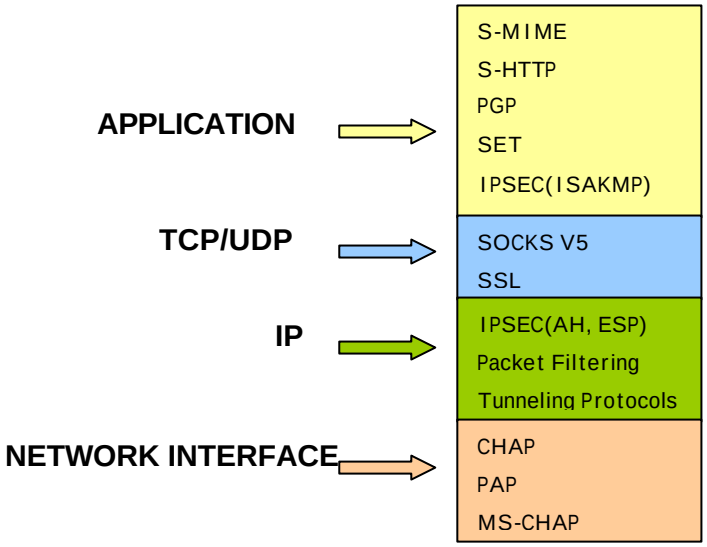
The purpose of a Virtual Private Network (VPN) is to extend a company's Intranet through a public network such as Internet: creating secure communications with Private Tunnels.



Different types of VPN solutions exist that can be classified depending on the OSI level of the protocol where these are implemented:

- The implemented VPNs in the *application* level: Authenticate and/or encrypt the message but not the source and destination address of the packets that these route.
- The VPNs based in the *link* level: Like L2TP, these can only authenticate the Tunnel's extreme end nodes but not each packet separately.
- The VPNs implemented in the *network* level: Like IPSec, protects the data and IP source and destination address without the user having to modify the applications. However outside of the Tunnel, for example in the company's Intranet, no protection is provided.

In conclusion, it is best to combine application level VPNs with the network level VPNs to obtain an adequate security level.



2. IPSec

IPSec is a security platform at the *network* level developed by the *IETF IPSec Working Group*. This provides the ability to accommodate new encryption and authentication algorithms in a flexible and robust way.

IPSec focuses on the following security problems:

- Authentication of data sources: verifies that the received data has been sent by the person who says they have sent it.
- Data integrity: verifies that the received data has not been modified en route.

  The term data authentication is usually used to indicate both the integrity of the data as well as source authentication.
- Data Confidentiality: conceals the data using an encryption algorithm.
- Protection Anti-Replay: prevents an intruder from re-sending one of your messages and you are unable to detect it.
- Automatic cryptography keys management.

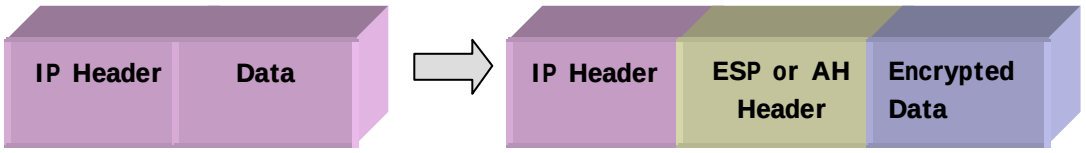
In order to resolve these aspects, IPSec defines two distinct security services:

- **ESP:** *Encapsulating Security Payload*: provides confidentiality, address source authentication in each IP packet, integrity and protection from copies being made.
- **AH:** *Authentication Header*: provides address source authentication in each IP packet, integrity and protection against copies being made, however this does not offer data confidentiality. This service is appropriate in cases where you only need to affirm the origin of the data.

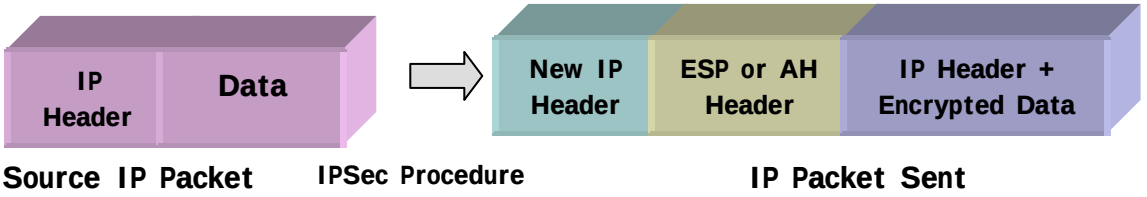
2.1. IPSec Tunnels

The IPSec platform permits two operation modes. You can use either of the two security services, ESP or AH, in each of them:

- The **Transport Mode** permits secure communications, normally established between the two hosts (e.g. communication between a workstation and a server or between two servers). However, in neither case does this mask the source or destination address of the packet to be sent. In transport mode, IPSec only acts over the IP packet internal data, without modifying the packet header. E.g. over a TCP or UDP segment or an ICMP packet.



- The IPSec **Tunnel Mode** encapsulates the whole of the original IP packet in a new IP packet, thus hiding all the original content. In this way the information is routed through a 'tunnel' from one point in the network to another without anyone being able to examine the content. This mode is the most appropriate one to be used in communications between a router and an external host or between two routers.



2.2. IPSec Architecture

a) Security Policy Database (SPD)

The IPSec platform must know which *security policies* to apply to the IP packet, depending on the header fields, also known as *selectors*. The security policies decide which encryption and authentication algorithms should be used in the secure connection.

The ***Security Policy Database*** (**SPD**) stores the entries that contain the selectors and the associated security policies.

After checking the security policies database, within the policies applicable to an IP packet, three possibilities exist:

- Discard the packet
- Route the packet normally.
- Apply the IPSec Security with some determined encryption or authentication algorithms that depend on the obligations of the security-efficiency adopted. For example, if you consider the processing speed as being more important than security, choose the DES encryption policy instead of the Triple DES.

b) Security Association (SA´s)

A packet whose selector coincides with one of the ***SPD*** entrances will be processed in accordance to the policy associated to this selector. A *Security Association* is the security connection that is created after the ***SPD*** has been consulted and contains the security information (authentication keys and encryption) required to process the packet.

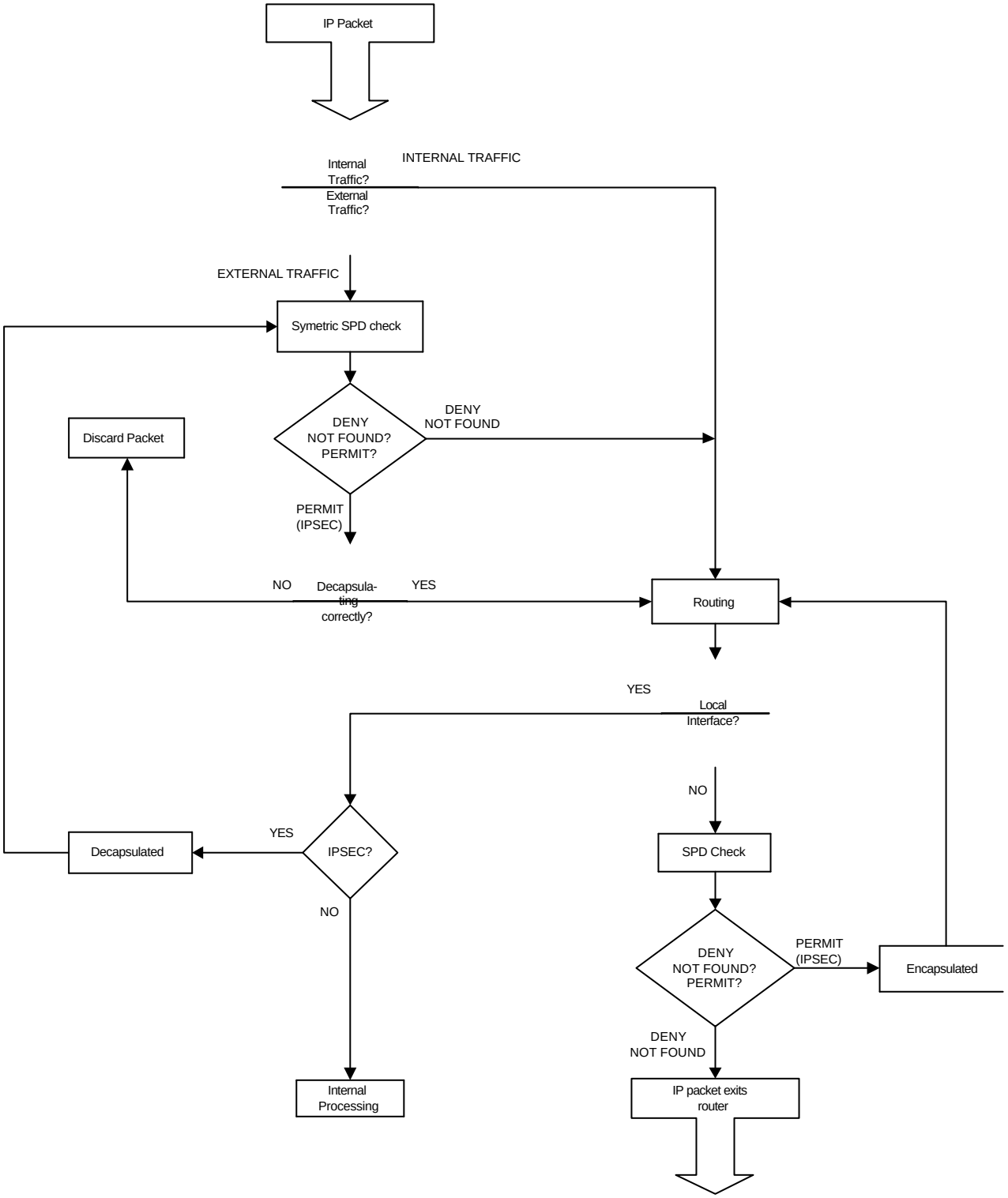
Within each of these security services (ESP or AH) we can choose different types of encryption algorithms, (DES, TRIPLE DES etc), or authentication (MD5, SHA1, etc.).

c) Packet processing with IPSEC-Router

There exists a single ***SPD*** or policies database that the user defines. This database is defined for the outgoing router traffic, while the incoming traffic is controlled through an ***implicit SPD***, symmetric to the previous one. In this way, all the incoming packets are processed in the same way the outgoing packets are sent: if certain outgoing traffic is defined to be sent with a specific security IPSec policy, this waits for the corresponding incoming traffic to comply with the same policy. In the same way, if the action defined for the outgoing traffic is route / discard, the incoming traffic will also be route / discard.

After carrying out the internal routing, the ***SPD*** is checked, this time for the outgoing traffic and similarly the decision must be taken between IPSec encapsulation, routing or elimination.

The following diagram describes the processing of an IP packet in **Teldat Router** with IPSec protocol:


IP Packet
Internal Traffic?
External Traffic?
INTERNAL TRAFFIC
EXTERNAL TRAFFIC
Symetric SPD check
DENY NOT FOUND? PERMIT?
DENY NOT FOUND
Discard Packet
PERMIT (IPSEC)
NO
Decapsula-ting correctly?
YES
Routing
YES
Local Interface?
NO
SPD Check
DENY NOT FOUND? PERMIT?
PERMIT (IPSEC)
Encapsulated
DENY NOT FOUND
IP packet exits router
YES
IPSEC?
Decapsulated
NO
Internal Processing

2.3. Advanced IPSec

a) Keys management

The entire security platform based on secret keys stops being secure if the keys are not periodically renewed.

The shorter the refresh time, the greater security of our system against Cryptanalysis tools.

There are two possible general work modes for the management of the security parameters and passwords in IPSec: manual (IPSec manual) and automatic or dynamic (IPSec IKE). These modes refer to the way in which an agreement is reached between peers on security parameters established for the Tunnel.

b) Manual IPSec

In the IPSEC manual, "manual-keying", the keys used in the encryption and/or authentication process for each SA are introduced by the user. The user should introduce the same security parameters (keys, encryption and authentication algorithms) for both ends of the Tunnel so that secure communication can be carried out. This is practical for small relatively static environments. When your VPN begins to grow, the manual renewal of the keys can be a costly task.

c) IKE IPSec

The IPSec platform permits this process to be automated, thanks to the *IKE Internet Key Exchange* protocol (based on the OAKLEY key exchange protocol and the ISAKMP platform). The two ends of the Tunnel automatically negotiate the secure communication parameters (keys, encryption and authentication algorithms). In order to generate this negotiation, the ends must first carry out a **first phase** where they agree on the security parameters that will protect the negotiation. Additionally in this first phase, authentication of the Tunnel ends is carried out, using a common key (*Pre-Shared Key*) manually introduced at both ends, digital signatures or with a public key algorithm.

There are two pre negotiation modes: *Main Mode* and *Aggressive Mode*.

- *Main Mode* masks the identities of the Tunnel's end routers. This type of negotiation is required when both ends know the security server's IP addresses that they confront.
- *Aggressive Mode* does not mask these identities and improves the authentication processing rate. Additionally, it is unnecessary to know the IP address at the other end of the Tunnel. This permits you to establish a Tunnel with an unknown security router provided that the security policy applicable to the packet permits this.

IPSec IKE has four operation modes for the first phase, depending on the type of Authentication used to negotiate the SAs security parameters.

· Authentication with Pre-shared Key

The same key (Pre-shared Key) is manually introduced in the two SECURITY ROUTERs permitting mutual authentication.

Two types of exchanges exist with the Pre-shared Key: *Main Mode* and *Aggressive Mode*.

- The Main Mode masks the identities of the Tunnel end Routers.
- The Aggressive Mode does not mask these identities and improves the authentication processing speed.

Every time the life span of a SA times out, new key material will be exchanged between the two security routers prior to authentication with the manual Pre-shared key.

Conversely, IPSEC "manual-keying" and IPSEC with Pre-shared Key means you need to know the IP address of the Tunnel end (Security Router IP address with which you are operating).

However the following types of IPSec IKEs permit, automatically and dynamically, to establish a Tunnel with an unknown Security Router if the security policy applied to the packet permits this. In these types of IPSec IKE, you do not need to introduce a common key at the Tunnel ends as this is automatically obtained through the below described processes.

· *Authentication with Signatures*

The authentication of the two Tunnel ends is carried out through a digital signature and the key exchange system "Diffie Hellman".

Two types of exchanges exist: *Main Mode* and *Aggressive Mode*.

- The *Main Mode* masks the identities of the Tunnel end Routers.
- The *Aggressive Mode* does not mask the identities and improves the authentication processing speed.

· *Authentication with Public Key Encryption*

Authentication is carried out by RSA with previous knowledge of the public key of the other router. The public keys of the other end of the Tunnel can be obtained through *certificates*.

Two types of exchanges also exist: *Main Mode* and *Aggressive Mode*. If the public key is frequently updated, the Aggressive Mode is just as secure as the Main Mode and is faster.

In addition the Authentication with Public Key Encryption provides greater security with respect to the Signature Authentication and Authentication with a Pre-shared Key, by combining the RSA public key system and the "Diffie Hellman" key exchange system. However the processing time of the Authentication with Public Key Encryption is greater.

· *Authentication with a Revised Public Key Encryption*

Authentication is also carried out by RSA with previous knowledge of the public key of the other ROUTER. The public keys of the other end of the Tunnel can be obtained through *certificates*.

However, operations are reduced with public key with an insignificant loss of security, but improving the authentication services.

Two types of exchanges exist: Main Mode and Aggressive Mode. If the public key is frequently updated, the Aggressive Mode is just as secure as the Main Mode and is faster.

d) High Security

The keys used to encrypt or authenticate a communication are obtained from *Material for Keys*. If this material has not originated nor will originate other keys to encrypt or authenticate other communications, then we say that ***Perfect Forward Secrecy*** has been attained.

The **Teldat Router** in high security mode permits you to achieve Perfect Forward Secrecy at the cost of a higher computation rate when establishing the IPSec Tunnels.

The high security mode also generates more secure keys material using the OAKELEY Groups, which are more resistant to Cryptanalysis.

e) Certificates

The certificates permit you to know the public keys of other security Routers through which it is possible to establish an IPSec Tunnel. These public keys will be used in the two IKE authentication modes with public key.

Chapter 2
Configuration

1. Introduction

As seen in the chapter 1 section 2.2 "IPSec Architecture", the processing of an IP packet by the IPSEC module, is based on applying the security policies configured for the said packet. This information is stored in the ***Security Policy Database (SPD)***, where the selectors and the associated security policies are found. In this way, the IPSEC configuration in the device is reduced to the definition of the ***SPD*** elements.

In the **Teldat Router**, the configuration of an SPD element is carried out in three steps. Firstly an element or an Access Control List (LCA) entry is defined i.e. some determined control selectors, which assigns a previously configured generic access list to IPSec. A type of decision is configured for each entry in the list: permit a packet to pass without applying the corresponding process to the protocol or feature which was assigned to this list (Deny) or apply the corresponding process in this IPSec case (Permit). Subsequently the **Templates** or IPSec security policies are created where the IPSec Tunnel security parameters are defined. Finally an access control list assigned to IPSec is associated (mapped) with a specific **Template**.

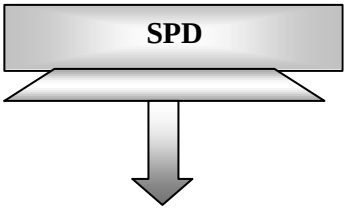
Access 1 control list	
Entry 1	✓ Source IP ✓ Permit ✓ Protocol
Entry 2	✓ Source IP ✓ Permit ✓ Ports ✓ Connection
...	...
Entry n	✓ Source IP ✓ Deny ✓ Protocols

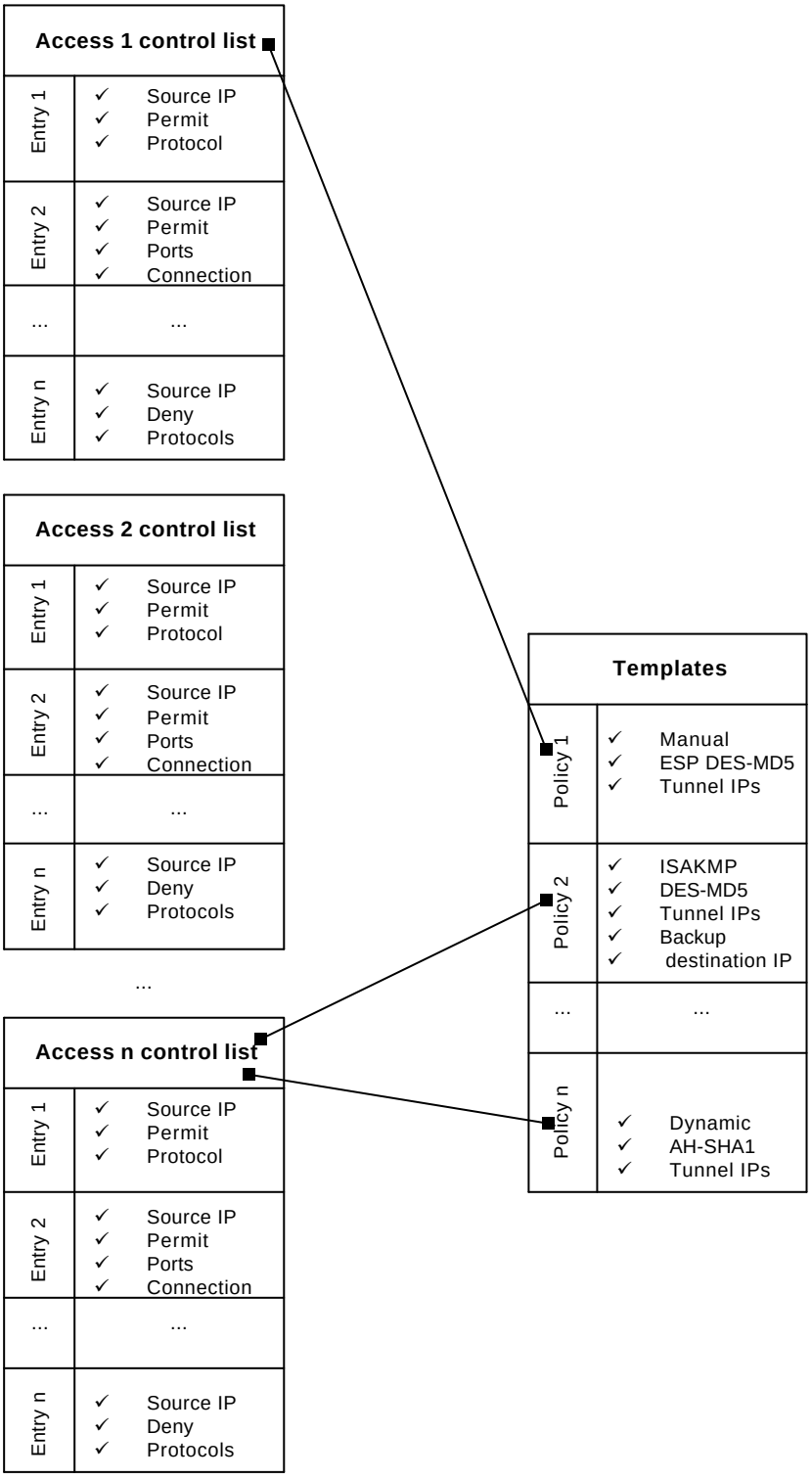
Access 2 control list	
Entry 1	✓ Source IP ✓ Permit ✓ Protocol
Entry 2	✓ Source IP ✓ Permit ✓ Ports ✓ Connection
...	...
Entry n	✓ Source IP ✓ Deny ✓ Protocols

...

Access n control list	
Entry 1	✓ Source IP ✓ Permit ✓ Protocol
Entry 2	✓ Source IP ✓ Permit ✓ Ports ✓ Connection
...	...
Entry n	✓ Source IP ✓ Deny ✓ Protocols

Templates	
Policy 1	✓ Manual ✓ ESP DES-MD5 ✓ Tunnel IPs
Policy 2	✓ ISAKMP ✓ DES-MD5 ✓ Tunnel IPs ✓ Backup ✓ destination IP
...	...
Policy n	✓ Dynamic ✓ AH-SHA1 ✓ Tunnel IPs




Access 1 control list
Entry 1
✓ Source IP
✓ Permit
✓ Protocol
Entry 2
✓ Source IP
✓ Permit
✓ Ports
✓ Connection
...
...
Entry n
✓ Source IP
✓ Deny
✓ Protocols
Access 2 control list
Entry 1
✓ Source IP
✓ Permit
✓ Protocol
Entry 2
✓ Source IP
✓ Permit
✓ Ports
✓ Connection
...
...
Entry n
✓ Source IP
✓ Deny
✓ Protocols
...
Access n control list
Entry 1
✓ Source IP
✓ Permit
✓ Protocol
Entry 2
✓ Source IP
✓ Permit
✓ Ports
✓ Connection
...
...
Entry n
✓ Source IP
✓ Deny
✓ Protocols
Templates
Policy 1
✓ Manual
✓ ESP DES-MD5
✓ Tunnel IPs
Policy 2
✓ ISAKMP
✓ DES-MD5
✓ Tunnel IPs
✓ Backup
✓ destination IP
...
...
Policy n
✓ Dynamic
✓ AH-SHA1
✓ Tunnel IPs

2. First Steps

2.1. Initial configurations

Given that the access to the device permits modifying the IPSec parameters, you first need to configure the access passwords for Telnet and the device Console.

In cases of using certificates, you need to adequately configure the date and time of the device in order to prevent validation problems with these (in this version, this step is unnecessary).

If you carry out an updating of old software to software with IPSec, you need to know that IPSec is disabled by default; therefore it does not execute any queries to the ***SPD***. Now you can begin to configure the ***SPD*** without affecting the traffic. The traffic is transparently processed as prior to the updating. Once the IPSec is configured and enabled, you need to save the configuration and restart the device in order to activate it.

If you wish to install the security router in a new network, without permitting any packet to exit or enter with consulting the ***SPD***, first you need to establish that any incoming packet is discarded and the IPSec is enabled (these actions will be explained in detail further on in the manual) and then connect the router to the network. Subsequently through configuration, you can permit any desired incoming traffic.

DISABLE / ENABLE Commands

The **DISABLE** command, found in IPSec configuration menu, permits you to disable the IPSec.

```
Config>PROTOCOL IP

-- Internet protocol user configuration --
IP config>IPSEC

-- IPSec user configuration --
IPSec config>DISABLE
IPSec config>
```

Simply write the **ENABLE** command to enable it.

In Nucleox Plus devices, you also need to enable the encryption card interruptions. The access password for this configuration, if this is not changed, is **teldat**.

```
Config>UCI CHANGE CFG

User Password? ******


Configuration

Interruption mode  (y/other)? (YES) y
Test RSA when starting (y/other)? (NO)
Max NRIs (10-500)? (100)
Flag Crypto? (NO)
You must restart so that the new configuration becomes effective
    Updating encrypt configuration...
```

3. IPSec Configuration

3.1. Commands for correct configuration

Once the device is connected to the private and public network, the ***SPD*** must be configured for incoming and outgoing packets.

The recommended steps to execute to generate a configuration are:

a) Configure the IPSec Access Control List.
b) Configure the Templates (security parameters).
c) Create the SPD.

3.2. Configuration

This section describes the steps to be followed in order to configure the IPSec in the **Teldat Router**. To access the IPSec configuration protocol environment, you must introduce the following commands:

```
Config>PROTOCOL IP

-- Internet protocol user configuration --
IP config>IPSEC

-- IPSec user configuration --
IPSec config>
```

Within the IPSec configuration protocol environment (indicated by the **IPSec config>** prompt) the following commands are available.

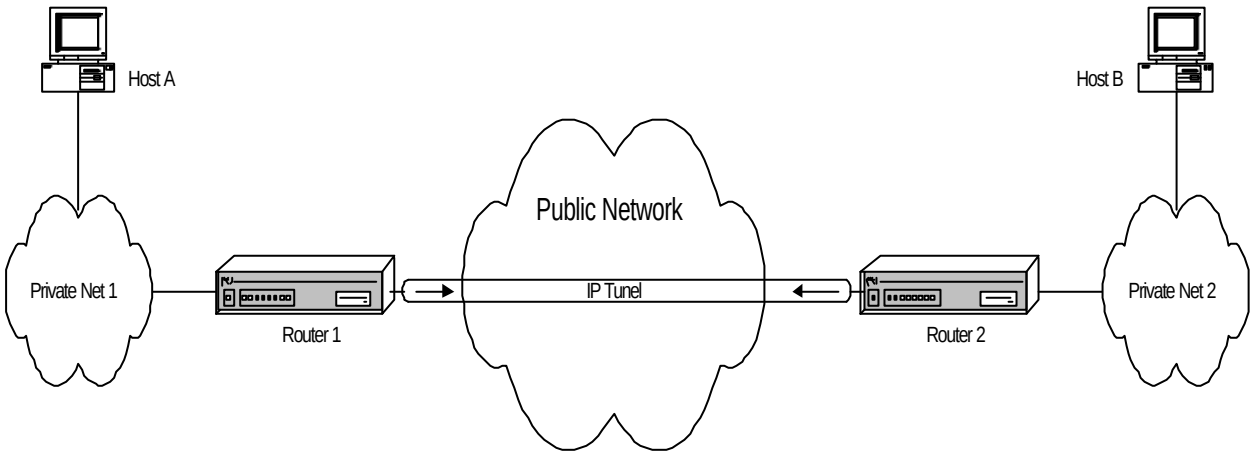
Command	Operation
? (HELP)	Lists the available commands or options.
ENABLE	Permits you to enable the IPSec and filter the events to be viewed.
DISABLE	Disable the IPSec.
ASSIGN-ACCESS-LIST	Assigns an access control list to the IPSec protocol.
TEMPLATE	Command to configure security policies parameters for the IPSec Tunnels.
MAP-TEMPLATE	Command that associates (mapping) an element in the access control list with a Template.
ASSOCIATE-KEY	Associates a key to an access control list.
KEY	This is used and described in the section on Dynamic Templates (IPSec IKE).
EVENT	Permits you to configure a filter to limit the events to be viewed or to display all of them.
QOS-PRE-CLASSIFY	Enables pre-filtering of packets (for BRS).
ADVANCED	Configuration of Advanced parameters.
LIST	Lists the IPSec configuration.
NO	Deletes elements from the Templates and Access Control lists, undoes mappings or deletes the whole of the configuration.
EXIT	Exits the IPSec configuration prompt.

In general, if you do not introduce all of the parameters required in the line commands to complete the command, the device will then request the information, except where there is an option to write subcommands. In either case, you can always enter the command or subcommand followed by '**?**' in order to get help.

```
IPSec config>?
ENABLE                  Enables IPSec
DISABLE                 Disables IPSec
ASSIGN-ACCESS-LIST      Assigns access lists to IPSec (used as SPD selectors)
TEMPLATE                Configures security policies params for IPSec tunnels
MAP-TEMPLATE            Associates an element in the LCA with a template
ASSOCIATE-KEY           Associates a key to an access list
KEY                     Adds preshared or RSA keys
EVENT                   Adds a filter for IPSec events or enables all of them
QOS-PRE-CLASSIFY        Enables QOS Preclasiffy
ADVANCED                Configuration of advanced IPSec parameters
LIST                    Lists the IPSec configuration
NO                      Disables options, deletes items or sets default values
EXIT                    Exits IPSec configuration menu
IPSec config>
```

a) IPSec access control list configuration

As already mentioned, there exists an access control list. Each entry in this list is a block of selectors and an *action*, which is defined by a unique number (the entry identifier or ID field). The block of selectors is made up of the source IP address (or range of addresses), an IP destination address (or range of IP destination addresses), a protocol (or range of protocols), source and destination ports (or a range of ports), and the identifier of the connection between interfaces through which the packet is transported. It is not necessary to specify all of these, only those you wish. The *action* represents the procedure assigned to the packets coinciding with the associated block of selectors: PERMIT or DENY.



As already explained on analyzing the ***SPD***, the specification of the LCA entries or elements are always established for **outgoing packets** through the router interfaces. As an example, in the previous figure we wished to establish an IPSec secure Tunnel for packets being routed between host A and host B. For this the control entry to be established in the LCA will contain the following selectors (as a minimum):

- Host A source IP address;
- Host B destination IP address;
- Action: PERMIT (IPSec processing);

Any packet that travels from A to B will in this way be encapsulated by IPSec. Implicitly on defining this entry, any packet arriving from B with address A must arrive with the same encapsulation. In this way the secure Tunnel between both ends is completely defined.

The order in the Access Control List is important in cases where the information offered the selectors overlaps between different LAC elements.

However, this order doe not give the identifier ID for each entry, just the order in which they are listed (this can be modified). I.e. if on searching through the list, beginning with the first element or entry that appears, you find an element that fits with your search, the search will not continue and the action indicated in the said element will be applied.

IPSec makes use of the generic and extended access control lists defined in the root menu of the device configuration ***Config*> FEATURE ACCESS-LISTS.** The lists created in this menu must be assigned to the IPSec protocol through the ***IPSec config***>**ASSIGN-ACCESS-LIST** command**.**

A generic and extended access control list is made up of a series of *entries* which define the properties that a packet must have in order to consider that it pertains to this entry and consequently to this list. Subsequently, this generic access control list is assigned to a protocol.

The first step consists in creating the access control list through the **ACCESS-LIST #** command. E.g., **ACCESS-LIST 100** accesses the ***Extended Access List 100*>** menu. Here you can register entries through the command **ENTRY # subcommand**.

Subsequently, the access control lists are made up of entries that admit the following subcommands:

Command	Operation
PERMIT	Type of action (IPSec processing in cases where the list is assigned to this protocol).
DENY	Type of action: does not carry out any process.
SOURCE ADDRESS	Defines the List entry source IP address selector.
SOURCE PORT-RANGE	Defines the entry source port selector.
DESTINATION ADDRESS	Defines the entry destination IP address selector.
DESTINATION PORT-RANGE	Defines the entry destination port selector.
PROTOCOL-RANGE	Defines the entry protocol selector.
DSCP	Diff Serv codepoint.
CONNECTION	Selector identifier for the connection between interfaces.

And the special commands:

Command	Function
LIST	To list the entries.
MOVE-ENTRY	To change the order of the entries.
NO	To delete an entry.

As an example we are going to display all the formats of all the subcommands together with an example of each in a possible configuration.

"ENTRY [ID] PERMIT"

Identifies the entry as a permitted type. In cases of IPSec this indicates that IPSec must be carried out. Therefore the entry in the access control list with this action specifies who the *Tunnel clients* will be i.e. defines the traffic to be transmitted through the Tunnel. The ID field is the integer which identifies the entry or element in the access control list.

Example:

```
Extended Access List 100>ENTRY 10 permit
```

"ENTRY [ID] DENY"

Identifies the entry as a non-permitted type. In cases of IPSec, this indicates that IPSec should not be carried out.

Example:

```
Extended Access List 100>ENTRY 10 deny
```

"ENTRY [ID] SOURCE ADDRESS [IP ADD] [MASK]"

To establish the IP source address selector for a possible packet. The range of addresses chosen is indicated in the form of a subnet mask. Once more, the ID field is the integer that identifies the element or entry in the access control list.

This address may be unnumbered i.e. you can set an address associated to an interface which is unknown at the time of configuring the device as, for example, it will be assigned by another mechanism such as PPP.

Example 1:

```
Extended Access List 100>ENTRY 10 source address 192.168.4.5 255.255.255.255
```

Example 2:

```
Extended Access List 100>ENTRY 10 source address 192.168.4.0 255.255.255.0
```

In Example 1, there is only one IP source address, and in Example 2 the source address for the entire subnet is 192.168.4.0 with a 255.255.255.0 mask. Please note that on using the same ID (10), the new information is added to or substitutes that already existing for this element. In this way the final entry is modified as shown in the following example.

As already said, you can choose not to introduce all the parameters for a command or subcommand or request help ('**?**'), and the router itself will progressively request these. In the following example, you can see how this works in the case of introducing the same data as that displayed in the previous example (Example 2):

```
Extended Access List 100>ENTRY 10 source address
Source IP address [0.0.0.0]? 192.168.4.0
Source IP mask [0.0.0.0]? 255.255.255.0
```

"ENTRY [ID] SOURCE PORT-RANGE [LOW] [HIGH]"

Establishes the selector for the Source Port. You can also select a range using the LOW and HIGH fields as port identifiers or a single port by setting both to the same value.

Example:

```
Extended Access List 100>ENTRY 10 source port-range 21 25
```

"ENTRY [ID] DESTINATION ADDRESS [IP ADD] [MASK]"

This command is similar to the one which establishes the source IP address selector of a possible packet. However this one is used to establish the selector for the destination IP address.

Example:

```
Extended Access List 100>ENTRY 10 destination address 192.168.10.0 255.255.255.0
```

"ENTRY [ID] DESTINATION PORT-RANGE [LOW] [HIGH]"

Establishes the selector for the Destination Port. In the same way, you can select a range by using the LOW and HIGH fields as port identifiers or a single port by setting both to the same value.

Example:

```
Extended Access List 100>ENTRY 10 destination port-range 1000 2000
```

If, once entered, you wish to eliminate the destination port control (or the source port control), as originally found, simply introduce the complete range. In this case:

```
Extended Access List 100>ENTRY 10 destination port-range 0 65535
```

On specifying the complete range, by default the corresponding selector does not appear.

"ENTRY [ID] PROTOCOL-RANGE [LOW] [HIGH]"

To establish the selector for the protocol or the protocol range of the packet. The LOW field is the protocol identifier in the lowest limit of the range. The HIGH field is the identifier in the highest limit. In cases where you do not want a range, simply set both to the same value.

Example:

```
Extended Access List 100>ENTRY 10 protocol-range 1 9
```

"ENTRY [ID] CONNECTION [ID CONN]"

Permits you to establish the identifier of the connection between interfaces for an LCA entry. This connection identifies the logical interface through which the packet is routed; this is configured in the IP rules. On establishing this relation, IPSec can associate traffic not only by the packet source, destination address etc., but also by the specific connection interface. The ID field is the integer that identifies the entry or element in the access control list.

Example:

Supposing that the following rule defined in IP exists:

ID	Local Address --> Remote Address	Timeout	Firewall	NAPT
1	172.24.70.1 --> 172.24.70.2	0	NO	NO

This identifies a specific connection between a router's local address and an end (the rest of the parameters are not considered). We therefore define an entry in the LCA, with the identifier of this connection (**1**) as selector:

```
Extended Access List 100>ENTRY 10 connection 1
```

Leaving the connection without specifying it or setting it to zero means that the connection will not be considered on checking the LCA.

A question mark will appear beside the connection (e.g. **Conn:1?**) should this not exist, together with a warning message.

Through this, all the selectors for an element in the access list are configured. If you do not configure one of these, this will not be taken into account when checking the packet against the control list.

Therefore what is left to define is the action to execute over a packet that coincides with this selection and also modification, if priority for this entry over the rest in the list is considered necessary. In order to do this, use the following subcommands:

"MOVE-ENTRY [ID_TO_MOVE][ID_BEFORE]"

Modifies the priority of an entry, placing the "ID_TO_MOVE" element in front of the "ID_BEFORE" element in the access control list, thus giving priority to the "ID_TO_MOVE" element versus "ID_BEFORE".

Example:

In order to display this, we will assume that we have to introduce a second entry:

```
Extended Access List 100, assigned to IPSec

10    PERMIT  SRC=192.168.4.0/24  DES=192.168.10.0/24  Conn:0
        PROT=1-9  SPORT=21-25  DPORT=1000-2000

11    DENY    SRC=192.168.4.8/32  DES=192.168.10.27/32  Conn:0
        PROT=1-9  SPORT=21-25  DPORT=1000-2000
```

The aim of this second entry is to permit certain transparent traffic to pass between two network hosts, 192.168.4.0/24 and 192.168.10.0/24, however the previous entry makes this ineffective. In order to avoid this situation, the entry order must be modified:

```
Extended Access List 100>MOVE 11 10
```

The order of the list and priority is now:

```
Extended Access List 100, assigned to IPSec

11    DENY    SRC=192.168.4.8/32  DES=192.168.10.27/32  Conn:0
        PROT=1-9  SPORT=21-25  DPORT=1000-2000

10    PERMIT  SRC=192.168.4.0/24  DES=192.168.10.0/24  Conn:0
        PROT=1-9  SPORT=21-25  DPORT=1000-2000
```

If you send a packet between hosts' 192.168.4.8 and 192.168.10.27 (with the adequate protocol etc), this will coincide with LCA entry with identifier 11, the first on the list, therefore the packet can transparently pass. Regarding traffic between the rest of the network hosts, 192.168.4.0/24 and 192.168.10.0/24, on checking the list, coincidence with the first entry will not be found. Consequently this will pass to the second entry (identifier 10). In cases where the packet coincides with the protocol, source port etc., this will be processed via IPSec Tunnel.

"LIST ALL-ENTRIES"

Displays all the access control list elements.

Example:

```
Extended Access List 100>LIST ALL-ENTRIES

Extended Access List 100, assigned to IPSec

11    DENY    SRC=192.168.4.8/32  DES=192.168.10.27/32  Conn:0
        PROT=1-9  SPORT=21-25  DPORT=1000-2000

10    PERMIT  SRC=192.168.4.0/24  DES=192.168.10.0/24  Conn:0
        PROT=1-9  SPORT=21-25  DPORT=1000-2000
```

You can achieve the same result if you execute the "LIST ACCESS-LISTS ALL-ENTRIES" command found in the IPSec config> menu.

```
IPSec config>LIST ACCESS-LISTS ALL-ENTRIES

Extended Access List 100, assigned to IPSec

11    DENY    SRC=192.168.4.8/32  DES=192.168.10.27/32  Conn:0
        PROT=1-9  SPORT=21-25  DPORT=1000-2000

10    PERMIT  SRC=192.168.4.0/24  DES=192.168.10.0/24  Conn:0
        PROT=1-9  SPORT=21-25  DPORT=1000-2000
```

"LIST ADDRESS-FILTER-ENTRIES [IP ADD] [MASK]"

Displays the access control list elements with source or destination IP address that is included within the [IP ADD] and the [MASK] defined range.

Example:

```
Extended Access List 100>LIST ADDRESS-FILTER-ENTRIES 192.168.4.8 255.255.255.255

Extended Access List 100, assigned to IPSec

11    DENY    SRC=192.168.4.8/32  DES=192.168.10.27/32  Conn:0
        PROT=1-9  SPORT=21-25  DPORT=1000-2000
```

You can achieve the same result if you execute the "LIST ACCESS-LISTS ADDRESS-FILTER-ENTRIES" command found in the IPSec config> menu.

```
IPSec config>LIST ACCESS-LISTS ADDRESS-FILTER-ENTRIES 192.168.4.8 255.255.255.255

Extended Access List 100, assigned to IPSec

11    DENY    SRC=192.168.4.8/32  DES=192.168.10.27/32  Conn:0
        PROT=1-9  SPORT=21-25  DPORT=1000-2000
```

"LIST ENTRY [ID]"

Displays the access control list identifier [ID] entry.

Example:

```
Extended Access List 100>LIST ENTRY 10

Extended Access List 100, assigned to IPSec

10    PERMIT  SRC=192.168.4.0/24  DES=192.168.10.0/24  Conn:0
        PROT=1-9  SPORT=21-25  DPORT=1000-2000
```

"NO ENTRY [ID]"

Command used to delete an identifier entry [ID] from the access list.

Example:

```
Extended Access List 100>NO ENTRY 10
```

b) Configuring the Templates (security parameters)

The Templates are IPSec security policies that can be associated to one or various elements in the Access Control List. Only the generic lists that have been previously assigned to IPSec can be associated to a Template.

In each Template, the IP addresses of the two ends of the Tunnel you wish to establish are defined (corresponding to the security routers); IPSec Tunnels key management authentication or encryption algorithms and the **manual** (manual IPSec) or **dynamic mode** (IKE IPSec) as well as a Template identifier (ID) number.

Each **mode** has a series of commands associated, some are common to both and others being specific to each, although when you are listing these in the Template the meanings of the configured mode will be shown.

First of all the **manual IPSec** configuration will be described and subsequently **IKE IPSec** will be displayed.

· *Manual Templates*

In the IPSec manual, "manual-keying", the keys used in encryption processing and/or authentication for each SA, are introduced by the user. The user must introduce the same security parameters (keys, encoded algorithms and authentication) for both ends of the Tunnel in order to carry out secure communication.

The following subcommands are available within the TEMPLATE command in order to configure the manual Templates:

Command	Operation
DEFAULT	Sets the default values for a Template.
MANUAL	Creates a static Template with a security service (ESP or AH).
SOURCE-ADDRESS	Introduces the address of the Tunnel source end in the Template.
DESTINATION-ADDRESS	Introduces the address of the Tunnel destination end in the Template.
SPI	Introduces the security configuration identifier number (SA) defined by the Template.
KEY	Introduces a DES key into Template.
TKEY	Introduces a Triple DES key into Template.
MD5KEY	Introduces a MD5 key into Template.
SHA1KEY	Introduces a SHA1 key in the Template.

The first thing to define in a Template (manual or dynamic) is the security service you wish to use, ESP or AH. The ESP service (Encapsulating Security Payload) is a confidential service that encrypts data with an option to authenticate these. The AH service (Authentication Header) only permits authentication:

"TEMPLATE [ID] DEFAULT]"

Sets the default values for a Template.

Example:

```
IPSec config>TEMPLATE 4 default
```

"TEMPLATE [ID] MANUAL ESP [ENCRYPT] [AUTHEN]"

This command defines a Manual Template with ESP security service.

The possible encryption algorithms are "DES" (Data Encryption Standard), "TDES"(Triple Data Encryption Standard)".

You can choose the "MD5", or "SHA1" or "NONE" authentication algorithms

The "ID" field is the Template identification number.

Example:

```
IPSec config>TEMPLATE 4 manual esp des md5
```

"TEMPLATE [ID] MANUAL AH [AUTHEN]"

This defines a manual Template with AH security service.

The possible authentication algorithms are "MD5" or "SHA1".

The "ID" field identifies the Template.

Example:

```
IPSec config>TEMPLATE 5 manual ah sha1
```

Once the security service has been defined, you need to enter the IP addresses for the secure Tunnel ends, the SA identifier created from the Template (SPI) and the keys to be used with the chosen encryption and authentication algorithms.

"TEMPLATE [ID] SOURCE-ADDRESS [IP ADD]"

This introduces the Tunnel's local IP address for the Template identified by [ID].

Example:

```
IPSec config>TEMPLATE 4 source-address 192.100.1.2
```

"TEMPLATE [ID] DESTINATION-ADDRESS [IP ADD]"

This introduces the IP address of the other remote end of the Tunnel.

Example:

```
IPSec config>TEMPLATE 4 destination-address 192.100.1.1
```

"TEMPLATE [ID] SPI [INTEGER > 256]"

Permits you to introduce the "Security Parameter Index" for the Template identified by [ID]. This number is an integer, [INTEGER], that must be higher than 256. The **SPI** must be the same at both ends, identifying a Template with respect to other Templates with the same Tunnel destination address and with the same security service (ESP or AH).

Example:

```
IPSec config>TEMPLATE 4 spi 280
```

You cannot define two policies that have identical values for the three said parameters: Tunnel destination IP address, security service and SPI.

"TEMPLATE [ID] KEY [8 bytes key]"

In order to introduce the key in cases where you have selected DES as the encryption algorithm. "8 bytes Key" represents the Template encryption DES key (you can introduce this in Hexadecimal, beginning with 0x, or in ASCII).

Example:

```
IPSec config>TEMPLATE 4 key 0x0123456789ABCDEF
```

Please note, if you decide to introduce the key in hexadecimal, you must introduce double the amount of characters (between 0-9 and A-F), as two hexadecimal characters define one byte.

"TEMPLATE [ID] TKEY [24 bytes key]"

In cases where you have selected Triple DES as encryption algorithm. "24 bytes Key" contains the Triple DES key (you can introduce this in Hexadecimal, beginning with 0x, or in ASCII).

Example:

```
IPSec config>TEMPLATE 4 tkey 0123456789abcdefghijklmn
```

"TEMPLATE [ID] MD5KEY [16 bytes key]"

If you have chosen MD5 for authentication, you need to provide a "16 bytes Key" (you can introduce this in Hexadecimal, beginning with 0x, or in ASCII).

Example:

```
IPSec config>TEMPLATE 4 md5key teldatsateldatsa
```

"TEMPLATE [ID] SHA1KEY [20 bytes key]"

In cases of selecting SHA1 for authentication, you must enter a "20 bytes Key" (you can introduce this in Hexadecimal, beginning with 0x, or in ASCII).

Example:

```
IPSec config>TEMPLATE 4 sha1key teldatsateldatsa1234
```

Once all the corresponding parameters and keys are defined, you need to introduce these in the other router through which you are going to establish the Tunnel. The final step is the association (mapping) between the LCA entries and the Templates i.e. the creation of the **SPDs** entries. This will be explained after configuring the dynamic Templates.

You can view or delete configured Templates through the same **LIST** and **NO** commands used for the access lists:

Command	Operation
LIST TEMPLATE	Displays the elements from the Templates list.
NO TEMPLATE	Deletes elements from the Templates list.

"LIST TEMPLATE ALL"

Displays all the elements in the Templates list.

Example:

```
IPSec config>LIST TEMPLATE ALL
TEMPLATES
4 manual  ESP-DES  ESP-MD5  SRC=192.100.1.2 DES=192.100.1.1 SPI=280

5 manual  AH-SHA1  SRC=192.100.1.2 DES=192.100.1.10  SPI=280
```

"LIST TEMPLATE ADDRESS-FILTER [IP ADD] [MASK]"

Displays the elements in the Templates list with Tunnel source or destination IP address that is included within the range defined by [IP ADD] and [MASK].

Example:

```
IPSec config>LIST TEMPLATE ADDRESS-FILTER 192.100.1.10  255.255.255.255
TEMPLATES
5 manual  AH-SHA1  SRC=192.100.1.2 DES=192.100.1.10  SPI=280
```

"NO TEMPLATE [ID]"

Deletes the element from the Templates list identified by [ID].

Example:

```
IPSec config>NO TEMPLATE 5
IPSec config>LIST TEMPLATE ALL
TEMPLATES
4 manual  ESP-DES  ESP-MD5  SRC=192.100.1.2 DES=192.100.1.1 SPI=280
```

· *Dynamic Templates (IPSec IKE)*

The IKE IPSec (dynamic IPSec) configuration requires two types of Templates: those known as **dynamic Templates**, which are the equivalent to the Templates configured in manual mode, and the **ISAKMP Templates**. At this point you need to negotiate the algorithms and the keys between the Tunnel ends in order to establish a communication SA. This is carried out in two phases:

- In the first phase, certain security parameters that protect the negotiation are agreed as well as authenticating both ends. These parameters are defined in the ISAKMP Templates.
- The second phase consists of the SA negotiation for the Tunnel. This is based in dynamic Templates.

As regards the TEMPLATE subcommands to create these Templates, some are common and others are only applicable to some of the other two types.

Command	Operation
DYNAMIC	Creates a dynamic Template with a security service (ESP or AH).
ISAKMP	Creates an ISAKMP Template with some security parameters.
SOURCE-ADDRESS	Introduces the address of the Tunnel source end in the Template.
DESTINATION-ADDRESS	Introduces the address of the Tunnel destination end in the Template.
BACKUP-DESTINATION	Adds a backup destination address.
ANTIREPLAY	Activates the Anti-Replay service in the Template.
NO ANTIREPLAY	Deactivates the Anti-Replay service in the Template.
PADDING-CHECK	Checks that the IPSec header padding field takes the value indicated in the RFC.
NO PADDING-CHECK	The value of the IPSec header padding field is ignored.
UDP-ENCAPSULATION	To encapsulate IPSec packets in UDP packets.
NO UDP-ENCAPSULATION	To disable the option of encapsulating IPSec packets in UDP packets.
UDP-IKE	To encapsulate the IPSec IKE packets in UDP packets.
NO UDP-IKE	To disable the option of encapsulating the IPSec IKE packets in UDP packets.
AGGRESSIVE	Configures the sending of the encryption/clear from the third IKE message in aggressive mode.
ENCAP	Configures the Tunnel or Transport operation mode.
LIFE	Introduces the SAs life span created from the Template.
IKE	Configures parameters relative to the IPSec IKE mode.
KEEPALIVE	Enables or disables the available keepalive services.
NO	Deletes a backup address or disables an option.

The section will begin by describing the ISAKMP as this is the first step in the negotiations.

The first thing to establish is the security parameters for the ISAKMP Template, under which the connection SA negotiation is carried out. As regards the ISAKMP Template, this also gives rise to a negotiation SA, or ISAKMP SA:

"TEMPLATE [ID] ISAKMP [ENCRYPT] [AUTHEN]"

The Template ISAKMP is created based on encryption and authentication algorithms. For encryption, the options are DES and Triple DES (TDES), and as authentication MD5 and SHA1. Despite the similarity, this is not the ESP service and the selection of an authentication algorithm is compulsory.

Example:

```
IPSec config>TEMPLATE 2 isakmp tdes sha1
```

Now you need to specify the address of the Tunnel end. The ISAKMP Templates do not require the source address.

"TEMPLATE [ID] DESTINATION [IP ADD]"

Example:

```
IPSec config>TEMPLATE 2 destination-address 192.100.1.1
```

"TEMPLATE [ID] BACKUP-DESTINATION [IP ADD]"

Adds a backup destination address.

It's possible to establish up to three backup destination addresses in the ISAKMP Templates, so that in cases where the Tunnel cannot be established with the main address, the backup addresses are used.

Example:

```
IPSec config>TEMPLATE 2 backup-destination 192.100.1.2
```

"TEMPLATE [ID] NO BACKUP-DESTINATION [IP ADD]"

Deletes a backup destination address.

Example:

```
IPSec config>TEMPLATE 2 no backup-destination 192.100.1.2
```

Finally, there are various optional parameters with default values. However these can be modified if necessary:

"TEMPLATE [ID] UDP-ENCAPSULATION"

This command indicates if the IPSec packets should be encapsulated in UDP packets. This is usually used to cross Firewalls or devices executing NAPT without needing to change the configuration. This makes sense in cases of ISAKMP Templates.

Example:

```
IPSec config>TEMPLATE 2 udp-encapsulation
```

"TEMPLATE [ID] NO UDP-ENCAPSULATION"

This command indicates that IPSec packets are not encapsulated in UDP packets i.e. normal operation. This makes sense for ISAKMP Templates.

Example:

```
IPSec config>TEMPLATE 2 no udp-encapsulation
```

"TEMPLATE [ID] UDP-IKE"

This command indicates that the IPSec IKE packets must be encapsulated in UDP packets. This is usually used to cross Firewalls or devices executing NAPT, without having to change the configuration. This makes sense in cases of ISAKMP Templates.

Example:

```
IPSec config>TEMPLATE 2 udp-ike
```

"TEMPLATE [ID] NO UDP-IKE"

This command indicates that the negotiation IPSec packets should not be encapsulated in UDP packets, even though this encapsulation is being carried out with the data packets.

Example:

```
IPSec config>TEMPLATE 2 no udp-ike
```

"TEMPLATE [ID] AGGRESSIVE CIPHER/CLEAR"

This command indicates if the IKE negotiation third message in aggressive mode should be encrypted or not.

Example:

```
IPSec config>TEMPLATE 2 aggressive clear
```

"TEMPLATE [ID] ENCAP TUNNEL/TRANSPORT"

This command indicates if encapsulation is going to be carried out in tunnel or transport mode.

Example:

```
IPSec config>TEMPLATE 2 encap transport
```

"TEMPLATE [ID] LIFE DURATION SECONDS [VALUE]"

Permits you to introduce the lifetime of the SA negotiation, the default value is 3600 seconds (1 hour).

Example:

```
IPSec config>TEMPLATE 2 life duration seconds 1000
```

"TEMPLATE [ID] IKE MODE AGGRESSIVE/MAIN"

Phase 1 of the ISAKMP/IKE exchange can be carried out in two ways: Aggressive Mode and Main Mode. The first mode is faster than the second, but at the cost of a diminution of parameters to be negotiated.

Example:

```
IPSec config>TEMPLATE 2 ike mode aggressive
```

"TEMPLATE [ID] IKE METHOD PRESHARED/RSA"

Establishes the authentication method used by the device. In principal, only the Pre-shared key method is available.

Example:

```
IPSec config>TEMPLATE 2 ike method preshared
```

"TEMPLATE [ID] IKE IDTYPE IP/FQDN/UFQDN/KEYID/ASN-DN"

Phase 1 of the ISAKMP /IKE exchange can be carried out by using different types of identifiers. IP indicates that IP address itself is used as the device identifier. In the rest, the device name will be used, i.e. that configured with the SET HOSTNAME command in the configuration menu.

This method can only be used in the AGGRESSIVE mode.

The remote device will use the received identifier and will search in its key table (Pre-shared Keys) associated to devices (IP addresses or Hostnames) created with the KEY IP/HOSTNAME command (this will be seen further on).

Example:

```
IPSec config>TEMPLATE 2 ike idtype ip
```

"TEMPLATE [ID] IKE GROUP ONE/TWO"

Establishes the type of Oakley group. Group 1 is used by default.

Example:

```
IPSec config>TEMPLATE 2 ike group one
```

Through this, all the parameters relative to the ISAKMP Templates are configured. When the router wishes to establish a security Tunnel, it first sends its appropriate ISAKMP Template proposals to the other end (depending on the destination IP address) and both have to reach an agreement on which Template is to be used.

Once the SA negotiation is established, the agreement must take into account the **dynamic Template** in order to create the connection SA.

"TEMPLATE [ID] DYNAMIC ESP [ENCRYPT] [AUTHEN]"

A dynamic Template is defined with ESP security service, selecting encryption between DES and TDES and authentication between MD5, SHA1 or NONE.

Example:

```
IPSec config>TEMPLATE 4 dynamic esp tdes sha1
```

"TEMPLATE [ID] DYNAMIC AH [AUTHEN]"

A dynamic Template is defined with AH security service, choosing between MD5 or SHA1.

Example:

```
IPSec config>TEMPLATE 3 dynamic ah md5
```

"TEMPLATE [ID] SOURCE-ADDRESS [IP ADD]"

To introduce the local IP address of the Tunnel. Please note that is only necessary to define this for the dynamic Templates.

This address may be unnumbered i.e. you can set an address associated to an interface which is unknown at the time of configuring the device as, for example, it will be assigned by another mechanism such as PPP.

Example:

```
IPSec config>TEMPLATE 4 source-address 192.100.1.2
```

"TEMPLATE [ID] DESTINATION-ADDRESS [IP ADD]"

This introduces the IP address of the remote end of the Tunnel.

Example:

```
IPSec config>TEMPLATE 4 destination-address 192.100.1.1
```

If the remote Tunnel address is 0.0.0.0, this is considered unknown and is not a significant parameter for selecting the dynamic Template during negotiation. Given that the destination address is unknown, only the remote end can begin IKE negotiation.

The following subcommands refer to the established default values, however it might be appropriate to modify these depending on the circumstances.

"TEMPLATE [ID] ANTIREPLAY":

This command enables the Anti-Replay service. This is a security method to avoid attacks based on packet retransmission.

Example:

```
IPSec config>TEMPLATE 3 antireplay
```

"TEMPLATE [ID] NO ANTIREPLAY"

Disables the Anti-Replay service.

Example:

```
IPSec config>TEMPLATE 3 no antireplay
```

"TEMPLATE [ID] PADDING-CHECK"

The original IPSec RFC permitted you to fill out the IPSec header padding field with any random value. The current RFC however specifies a determined value for the said field. So that the router can operate with devices which comply with the original RFC, you can configure a parameter indicating if a check should be carried out on whether the padding field takes the value defined in the RFC or if this data should be ignored.

Example:

```
IPSec config>TEMPLATE 3 padding-check
```

"TEMPLATE [ID] NO PADDING-CHECK"

The IPSec header padding field will not be checked.

Example:

```
IPSec config>TEMPLATE 3 no padding-check
```

"TEMPLATE [ID] LIFE TYPE SECONDS/KBYTES/BOTH"

Permits you to introduce the type of life duration for the communication SA based on the dynamic Template. In the dynamic Templates, the lifetime can be represented as a time limit ("SECONDS"), in the same way as for the ISAKMP Templates, or also as a quantity limit of transmitted bytes (KBYTES") through the SA generated with this Template.

The third option ("BOTH") establishes both limits at the same time. In this case the SA will delete when one of the two limits expire.

Example:

```
IPSec config>TEMPLATE 4 life type both
```

"TEMPLATE [ID] LIFE DURATION SECONDS/KBYTES [VALUE]"

The chosen life duration is shown in the VALUE field. In cases where you have selected BOTH in the previous subcommand, you will have to enter the subcommand twice in order to give both types of values (seconds and kilobytes).

Example:

```
IPSec config>TEMPLATE 4 life duration seconds 20000
IPSec config>TEMPLATE 4 life duration kbytes 1000
```

"TEMPLATE [ID] IKE PFS"

This enables the Perfect Forward Secrecy service. This increases the security of the created SAs, making for a better management of the used keys.

Example:

```
IPSec config>TEMPLATE 4 ike pfs
```

"TEMPLATE [ID] IKE NO PFS"

This disables the Perfect Forward Secrecy service.

Example:

```
IPSec config>TEMPLATE 4 ike no pfs
```

"TEMPLATE [ID] KEEPALIVE KEEPALIVE"

Enables the Keep Alive service for maintenance of the SAs.

Example:

```
IPSec config>TEMPLATE 4 keepalive keepalive
```

"TEMPLATE [ID] KEEPALIVE NO KEEPALIVE"

Disables the Keep Alive service for maintenance of the SAs.

Example:

```
IPSec config>TEMPLATE 4 keepalive no keepalive
```

"TEMPLATE [ID] KEEPALIVE DPD"

Enables the DPD service (Dead Peer Detection) for maintenance of the SAs. This makes sense in cases of ISAKMP Templates.

Example:

```
IPSec config>TEMPLATE 2 keepalive dpd
```

"TEMPLATE [ID] KEEPALIVE NO DPD"

Disables the DPD service (Dead Peer Detection) for maintenance of the SAs. This makes sense in cases of ISAKMP Templates.

Example:

```
IPSec config>TEMPLATE 2 keepalive no dpd
```

In relation to the connection SAs created starting from the dynamic Templates, there is a command in the IPSec configuration's main menu that permits you to configure certain advanced characteristics. This command is **ADVANCED** and provides access to several subcommands:

Command	Operation
DPD	Service to ensure the maintenance of an SA connection.
KEEP-ALIVE	Service to ensure the maintenance of an SA connection.
PURGE-TIMEOUT	Configuration of SA's timeout.
RENEGOTIATION-TIME	Service to carry out SA re-negotiation.
NO	Establishes the default values for the IPSec configuration advanced parameters.

"ADVANCED DPD"

DPD (Dead Peer Detection) is a service which detects when communication with the other end of the Tunnel is lost. In order to use this, an ID vendor from the DPD is sent in phase 1 of any negotiation. This service consists of the exchange of notifications (an R-U-THERE petition and an R-U-THERE-ACK response) in phase 2 in the Tunnel when there is no data reception during a certain period of time. This is configurable as idle time.

If this is enabled in an ISAKMP Template, the router will send phase 2 DPD petitions in the Tunnels created from the said Template and will also respond to these notifications. In cases where this is not enabled, the router will not send petitions but will respond to any received.

Command	Operation
ALWAYS-SEND	Always sends the keepalive once the idle time has timed out.
ANTI-REPLAY	Enables the DPD packets anti-replay capacity.
IDLE-PERIOD	Idle period before sending DPD packets.
INTERVAL	Interval between DPD keepalives.
PACKETS	Maximum number of DPD packets without confirmation.
NO	Disables an option or establishes the default values for a parameter.

"ADVANCED DPD ALWAYS SEND"
Indicates that DPD exchanges must be carried out when the idle time times out.

"ADVANCED DPD NO ALWAYS SEND"
Indicates that you must wait for data after the idle time has timed out before executing the exchange.

"ADVANCED DPD ANTI-REPLAY"
Enables the anti-replay capacity for DPD packets.

"ADVANCED DPD NO ANTI-REPLAY"
Disables the anti-replay capacity for DPD packets.

"ADVANCED DPD IDLE-PERIOD [SECONDS]"
Idle time before carrying out DPD exchanges i.e. time without receiving data in the Tunnel. Default value is 60 seconds. This can be re-established by executing the "ADVANCED DPD NO IDLE-PERIOD" command.

"ADVANCED DPD INTERVAL [SECONDS]"
Wait interval (in seconds) between DPD petition transmissions when a response has not been received. The default value is 5 seconds which can be re-established by executing the "ADVANCED DPD NO INTERVAL" command.

"ADVANCED DPD PACKETS [MAX_PKTS]"
Maximum number of DPD petitions without receiving a response. The default value (3) can be re-established by executing the "ADVANCED DPD NO PACKETS" command.

Example:

```
IPSec config>ADVANCED DPD ALWAYS-SEND
IPSec config>ADVANCED DPD IDLE-PERIOD 60
IPSec config>ADVANCED DPD INTERVAL 5
IPSec config>ADVANCED DPD PACKETS 3
IPSec config>ADVANCED DPD ANTI-REPLAY
Keep Alive modified
Do not forget to enable DPD in the template configuration
```

As the final message indicates, you must individually enable the DPD service in each ISAKMP Template if you want it with "TEMPLATE [ID] KEEPALIVE DPD".

"ADVANCED KEEP-ALIVE"
Keep Alive is a service that deals with ensuring that the other end maintains its SA open, observing the time that this remains without showing signs of life. On introducing this command, the user is asked to define two parameters:

Command	Operation
PACKETS	Maximum number of packets without receiving a response.
TIMEOUT	Wait period (in seconds) after the last packet.
NO	Establishes the default value of any of the previous parameters.

Example:

```
IPSec config>ADVANCED KEEP-ALIVE PACKETS 4
Keep Alive modified
Do not forget to enable Keep Alive in the template configuration.
IPSec config>ADVANCED KEEP-ALIVE TIMEOUT 10
Keep Alive modified
Do not forget to enable Keep Alive in the template configuration.
```

As the final message indicates, you must individually enable the Keep Alive service in each dynamic Template if you want it with "TEMPLATE [ID] KEEPALIVE KEEPALIVE".

"ADVANCED PURGE-TIMEOUT [SECONDS]"

Permits you to configure the SAs timeout. This is for example, the time taken in deleting a negotiation SA when, during negotiation with a Tunnel, the destination does not respond. The "ADVANCED NO PURGE-TIMEOUT" command re-establishes the default value for this parameter (15 seconds).

Example:

```
IPSec config>ADVANCED PURGE-TIMEOUT 15
```

"ADVANCED RENEGOTIATION-TIME"

Renegotiation time is a limit that is established in relation to the end time of a connection SA lifespan. If between this limit and the end of the SA there is traffic, the router will automatically renegotiate a new SA before the current SA lifespan times out. This avoids the situation of losing traffic due to SA timeout.

This limit is interpreted as a percentage and is applied to each individual lifetime (only in seconds) for each SA, without allowing it to ever drop below one minute.

The default value for this parameter is 10 (10%) which can be re-established through the "ADVANCED NO RENEGOTIATION-TIME" command.

Example:

```
IPSec config>ADVANCED RENEGOTIATION-TIME 20
Check-out time (%) - from SA's end-lifetime - to renegotiate : 20
```

The last line is one of confirmation and describes the following behavior: when an SA has 20% of its time left until it finalizes, the router begins to check if there is traffic up until the end-lifetime. If there is traffic then the router renegotiates a new SA when it has one minute left.

Other parameters which are configurable from the ADVANCED submenu from the IPSec configuration main menu are as follows:

Command	Operation
EXPONENTATION-DEVICE	Service ensuring the maintenance of an SA connection.
LQUEUE	Length of the cipher queue.
NO LQUEUE	Establishes the default value for the cipher queue length.

"ADVANCED EXPONENTATION-DEVICE"

This command provides access to two other commands: HARDWARE and SOFTWARE. These permit you to configure the way in which operations are carried out for cipher packets processing. If you select the HARDWARE option, cipher will be carried out at the HARDWARE level (cipher card). The SOFTWARE option implies that the operations will be carried out by using the software code.

Example:

```
IPSec config>ADVANCED EXPONENTIATION-DEVICE ?
HARDWARE      A hardware device will be used to carry out cipher operations
SOFTWARE      Software will be used to carry out cipher operations
IPSec config>ADVANCED EXPONENTIATION-DEVICE HARDWARE
```

"ADVANCED LQUEUE"

Configures the length of the cipher queue.

Example:

```
IPSec config>ADVANCED LQUEUE
Size of the cypher queque:[50]? 25
IPSec config>
```

"ADVANCED NO LQUEUE"

Sets the cipher queue length to it's default value: 50.

Example:

```
IPSec config>ADVANCED NO LQUEUE
IPSec config>
```

This step finalizes the configuration of the ISAKMP and dynamic Templates required in order to carry out IPSec IKE. However there is a further parameter left to introduce to make these operational. This deals with the Pre-Shared Key that both security routers must have in order to mutually authenticate. This key is introduced from the main IPSec menu:

"KEY PRESHARED IP/HOSTNAME [ADDRESS/NAME] CIPHERED/PLAIN [KEY]"

This permits you to introduce the Pre-shared key associated to the remote IP address or device name depending how the Tunnel was configured when the "TEMPLATE IKE IDTYPE" command was used for the ISAKMP Templates.

Please note that this key however is not associated to a Template but to a remote IP address or host. Consequently, this does not require an [ID] identifier as in the rest of the commands.

The Pre-shared key can be introduced in plain (subcommand PLAIN) or ciphered (subcommand **C**IPHERED). If this is manually configured from the console, you normally introduce the key in plain. If you use the configuration saved in text mode however (precedent from the "SHOW CONFIG" command) the key will be ciphered. In cases where it is plain, the key can have a length between 1 and 32 bytes. This can be introduced in hexadecimal, beginning with 0x or in ASCII. Please note that if you introduce this in hexadecimal, you must introduce double the characters (between 0-9 and A-F). If the key is ciphered then it is always displayed in hexadecimal.

Example 1:

```
IPSec config>KEY PRESHARED IP 192.100.1.1 plain 1234567890
IPSec config>KEY PRESHARED HOSTNAME Router2 plain 1234567890teldat
IPSec config>KEY PRESHARED IP 192.100.1.1 plain 0x1234567890abcdef
```

The Pre-shared key admits networks with mask 0, 8, 16 and 24 bits in IP addresses.

Example 2:

```
IPSec config>KEY PRESHARED IP 192.100.1.0 plain 1234567890
```

This key is assigned to all the network 192.100.1.0 255.255.255.0

The Pre-shared key admits the wildcard character (asterisk) at the end of the hostname.

Example 3:

```
IPSec config>KEY PRESHARED HOSTNAME Router* plain 1234567890teldat
```

This key is assigned to Router1, RouterTeldat, Router, Router_234...

In cases where intersections exist, the most restrictive is always taken.

Example 4:

```
IPSec config>KEY PRESHARED HOSTNAME Router* plain 1234567890teldat
IPSec config>KEY PRESHARED HOSTNAME Router plain 1111111
```

If the hostname is Router, key 1111111 will be used.

```
IPSec config>KEY PRESHARED IP 192.100.1.0 plain 1234567890
IPSec config>KEY PRESHARED IP 192.100.1.163 plain aaaa
```

If the IP is 192.100.1.163 key aaaa will be used.

You can view the configured Pre-shared keys by using the "LIST KEY PRESHARED" command. The keys are not printed as such in the console but it is possible find out what IP addresses or hostnames have a Pre-shared key associated:

```
IPSec config>LIST KEY PRESHARED
5 key entries
   192.100.1.1 ************
   Router2 ************
   192.100.1.0 ************
   Router* ************
   Router ************
```

If you wish to delete a key associated to an IP address or hostname, simple execute the "NO KEY PRESHARED IP/HOSTNAME [ADDRESS/NAME]" command:

```
IPSec config>NO KEY PRESHARED IP 192.100.1.0
```

c) Creating the SPD

Finally, once the Access Control List and the Templates have been defined you have to create a policy database or SPD. Each input from this database is make up of an element from the Access Control List and an associated Template. The association is known as **mapping** and the command and its use for mapping the entries is shown as follows:

Command	Operation
ASSIGN-ACCESS-LIST	Assigns an access control list to the IPSec protocol
ASSOCIATE-KEY	Associates a key with an access control list.
MAP-TEMPLATE	Associates access control list elements with Templates.

"ASSIGN-ACCESS-LIST [LCA entry ID]"

Assigns a generic and extended access control list to the IPSec protocol.

Example:

```
IPSec config>ASSIGN-ACCESS-LIST 100
```

"ASSOCIATE-KEY IP/HOSTNAME [ACCESS_LIST] [ADDRESS/NAME KEY]"

One of the parameters negotiated during the opening of an IPSec Tunnel is the access control i.e. the *Tunnel clients*. In principal, the knowledge of a Pre-shared key permits the remote device to open a Tunnel to the local device with client independence. However occasionally this is not convenient and you need to provide certain controls for the devices which know one key and other controls to those that know another key.

In the example shown below, the following statements can be made:

- Only devices which know the key associated to the hostname *teldat_router* will be able to open a Tunnel accessing the whole of the 192.60.64.0/24 network.
- Devices which only know the key associated to *router*, **will not** be able to open a Tunnel accessing the whole of the 192.60.64.0/24 network.
- As the access control list 101 does not have a key associated, devices which know the key associated to *router* and that associated to *teldat_router* will be able to open a Tunnel accessing host 192.60.64.1

Example:

```
Extended Access List 101, assigned to IPSec

1     PERMIT  SRC=192.60.64.1/32  DES=0.0.0.0/16  Conn:0


Extended Access List 100, assigned to IPSec

10    PERMIT  SRC=192.60.64.0/24  DES=0.0.0.0/16  Conn:0
IPSec config> LIST KEY PRESHARED
2 key entries
   teldat_router ************
   router ************
IPSec config> ASSOCIATE-KEY HOSTNAME 100 teldat_router
```

"MAP [LCA entry ID] [Template ID]"

This command associates an element from the access control list with a Template, creating an SPD element.

Example:

```
IPSec config>MAP-TEMPLATE 100 4
```

When mapping is carried out, you can sometimes see some automatic entries not introduced by the user in the list of entries in the access control list found in the IPSec monitoring menu. These are distinguished by the words DYNAMIC ENTRY. These automatic entries are necessary so that both ends of the Tunnel can communicate control packets.

```
Extended Access List 101, assigned to IPSec

 ACCESS LIST ENTRIES
65534 DENY    SRC=0.0.0.0/0  DES=192.60.64.1/32  Conn:0
        PROT=17  SPORT=500
        DYNAMIC ENTRY
        Hits: 0

65533 DENY    SRC=0.0.0.0/0  DES=192.60.64.1/32  Conn:0
        PROT=17  SPORT=4500
        DYNAMIC ENTRY
        Hits: 0
```

```
65532 DENY    SRC=0.0.0.0/0  DES=192.60.64.1/32  Conn:0
        PROT=50-51
        DYNAMIC ENTRY
        Hits: 0

65531 PERMIT  SRC=192.60.64.2/32  DES=192.60.64.1/32  Conn:0
        DYNAMIC ENTRY
        Hits: 0

1     PERMIT  SRC=0.0.0.6/32  DES=192.60.64.1/32  Conn:0
        Hits: 0
```

Mapping is the last step required in order to configure the complete IPSec security service. Before considering the configuration completed you can check what has been carried out, modifying any errors and even determine which events you wish to view in the trace monitoring:

Command	**Operation**
LIST ALL	Displays all the configuration.
SHOW CONFIG	Displays the configuration commands.
NO ASSIGN-ACCESS-LIST	Eliminates the assignation of an access control list to the IPSec protocol.
NO ASSOCIATE-KEY	Eliminates the association of a key to an access control list.
NO MAP-TEMPLATE	Eliminates the association between LCA elements and Templates.
EVENT	Enables certain Events.
LIST ENABLED-EVENTS	Displays the filter configured for events monitoring (should there be one).
QOS-PRE-CLASSIFY	Classification of packets in their respective BRS classes.
NO QOS-PRE-CLASSIFY	Disables classification of packets in their respective BRS classes.

"LIST ALL"

Displays all of the configuration policies the SPD contains, i.e. the LCA elements and the list of Templates.

Example:

```
IPSec config>LIST ALL
IPSec Access Control.
Access Control is: enabled
QOS Preclassify is: disabled

Access Lists assigned to IPSec:
  Extended Access List 101
  Templates: 1


Extended Access List 101, assigned to IPSec

1     PERMIT  SRC=0.0.0.6/32  DES=192.60.64.1/32  Conn:0

TEMPLATES
1 dynamic ESP-3DES ESP-MD5  SRC=0.0.0.6 DES=192.60.64.1
   LifeTime:0h3m0s 100000 kbytes
   PFS disabled

2 dynamic ESP-DES ESP-SHA1  SRC=192.24.51.75 DES=192.24.51.74
   LifeTime:0h50m0s 100000 kbytes
   PFS disabled

3 dynamic AH-MD5  SRC=192.24.51.75 DES=192.24.51.74
   LifeTime:0h50m0s 100000 kbytes
   PFS disabled

4 dynamic AH-SHA1  SRC=192.24.51.75 DES=192.24.51.74
   LifeTime:0h50m0s 100000 kbytes
   PFS disabled

20 isakmp 3DES MD5  DES=192.60.64.1
   LifeTime:0h4m0s
   IKE AGGRESSIVE
   PRESHARED
   fqdn ID TYPE
   OAKLEY GROUP 1

4 key entries
   172.24.51.57 ************
   192.24.51.74 ************
   192.24.78.75 ************
   192.60.64.1 ************
0 rsakey entries
Id.           Date.         Len         CA.                   Cert sn.

KeepAlive Configuration:
   Maximum number of encoded packets without receiving an answer: 0.
   Timeout after last packet encoded: 0 seconds.

DPD Configuration:
Idle period(secs) before sending DPD keepalives: 60
Maximum number of DPD keepalives not acknowledged: 3
Period of time(secs) between DPD keepalives: 5
Always send keepalive after idle period expiration : ENABLED
Anti-replay : DISABLED

Check-out time (%) - from SA's end-lifetime - to renegotiate : 10

SA's purge timeout:  15

Use software exponentiation
IPSec config>
```

"SHOW CONFIG"

Displays the configuration commands. Please note that the values of the fields that coincide with the default value are not shown. In the example shown below, the result of the *SHOW CONFIG* command is displayed with the configuration of the example presented with the *LIST ALL* command.

Example:

```
IPSec config>SHOW CONFIG
; Showing System Configuration ...
; Router C5i IPSec 1 17 Version 10.0.0CAI

      enable
      assign-access-list 101
;
      template 1 create
      template 1 dynamic esp tdes md5
      template 1 source-address 0.0.0.6
      template 1 destination-address 192.60.64.1
      template 1 life type both
      template 1 life duration seconds 180
      template 1 life duration kbytes 100000
;
      template 2 create
      template 2 dynamic esp des sha1
      template 2 source-address 192.24.51.75
      template 2 destination-address 192.24.51.74
      template 2 life type both
      template 2 life duration seconds 3000
      template 2 life duration kbytes 100000
;
      template 3 create
      template 3 dynamic ah md5
      template 3 source-address 192.24.51.75
      template 3 destination-address 192.24.51.74
      template 3 life type both
      template 3 life duration seconds 3000
      template 3 life duration kbytes 100000
;
      template 4 create
      template 4 dynamic ah sha1
      template 4 source-address 192.24.51.75
      template 4 destination-address 192.24.51.74
      template 4 life type both
      template 4 life duration seconds 3000
      template 4 life duration kbytes 100000
;
      template 20 create
      template 20 isakmp tdes md5
      template 20 destination-address 192.60.64.1
      template 20 life duration seconds 240
      template 20 ike ca THAWTECA.CER
      template 20 ike mode aggressive
      template 20 ike idtype fqdn
;
      map-template 101 1
      key preshared ip 172.24.51.57 holas
      key preshared ip 192.24.51.74 ciphered 0xF85C0CB62556C562120794C28EB9334
      key preshared ip 192.24.78.75 ciphered 0xF85C0CB62556C562120794C28EB9334
      key preshared ip 192.60.64.1 ciphered 0xF85C0CB62556C562120794C28EB9334
IPSec config>
```

"NO ASSIGN-ACCESS-LIST [LCA entry ID]"

Eliminates the assignation of an access control list to the IPSec protocol.

Example:

```
IPSec config>NO ASSIGN-ACCESS-LIST 100
```

"NO ASSOCIATE-KEY [LCA entry ID]"

Eliminates the association of a key to an access control list.

Example:

```
IPSec config>NO ASSOCIATE-KEY 100
```

"NO MAP-TEMPLATE [LCA entry ID] [Template ID]"

Eliminates the association or mapping of an LCA element with the Template.

Example:

```
IPSec config>NO MAP-TEMPLATE 10 4
```

Even though you disable the mapping, the automatic entry that was generated remains. I.e. this has to be deleted if you do not require it.

"EVENT ALL"

This permits you to view all the events. The said events have to be enabled in the events monitoring process (P 3) and can be viewed in P 2.

Example:

```
IPSec config>EVENT ALL
```

"EVENT ADDRESS-FILTER [IP ADD][MASK]"

Once enabled, this only permits you to view those events with a source address or destination that is included within the range defined by [IP ADD][MASK].

Example:

```
IPSec config>EVENT ADD 192.100.1.2 255.255.255.255
```

"LIST ENABLED-EVENTS"

Displays the filter configured for event monitoring (should there be one).

Example:

```
IPSec config>LIST ENABLED-EVENTS

 Address/Subnet enabled : 192.100.1.2 with MASK : 255.255.255.255
```

"QOS- PRE-CLASSIFY"

Permits you to enable the classification of packets in their respective BRS classes before being ciphered.

```
IPSec config>QOS-PRE-CLASSIFY
IPSec config>
```

To disable this option, simple execute the "NO QOS-PRE-CLASSIFY" command:

```
IPSec config>NO QOS-PRE-CLASSIFY
IPSec config>
```

If this mode is enables, the packets will be classified before being ciphered therefore distinct traffic classes can be prioritized within the same IPSec Tunnel. Classification only operates in those access controls which are associated to an IP rule, contrariwise you will not know which interface the packets are going to exit through before being ciphered and therefore the BRS associated to this interface cannot be applied. If this mode is disabled, all traffic coming from the IPSec Tunnel will be classified in the same BRS class, as the header that will be analyzed is the IPSec Tunnel header.

· *ISAKMP Configuration Mode*

There is a method that permits you to configure the phase II parameters which are negotiated after finishing phase I. Through this method, you can reliably define the characteristics that the IPSec session negotiated in phase II will have in order to exchange data. When creating this documentation,

the details of the properties and operation mode for this configuration mode can be found in the draft: *The ISAKMP Configuration Mode*.

This method is usually used in star configurations, where the central node assigns the addresses that each of the ends connecting to the VPN are going to have during the session, which will be the name servers, if using PFS or the port over which NAT-T will be carried out is going to be used.

You will find the following parameters within the TEMPLATE menu which permit you to configure this method:

Command	Operation
IKE METHOD	Incorporates the "xauth-init-preshared" option.
CONFIG	Permits you to define if the device will initiate the configuration method, wait for a proposal or if it will behave as indicated by the IKE method used.

"IKE METHOD XAUTH-INIT-PRESHARED"

Through this command you add a new functionality to the previously described IKE METED command. This functionality is known as *Extended Authentication Preshared* described in the *Extended Authentication within ISAKMP/Oakle* draft when creating this documentation. On activating this parameter this indicates if you wish to carry out a pre-shared authentication where you wish to execute a *ISAKMP Configuration* process, where the initiator device must autentícate with a remote server. This latter can assign, among other things, the IP address within the VPN.

Example:

```
IPSec config>TEMPLATE 4 ike method xauth-init-preshared
```

"CONFIG INITIATOR"

This command indicates that the device will initiate the configuration method, carrying out the initial proposals and requesting the necessary parameters.

This parameter has no effect if the authentication method is xauth-init-preshared.

Example:

```
IPSec config>TEMPLATE 4 config initiator
```

"CONFIG RESPONDER"

This command indicates that the device will wait for the remote end to initiate the configuration method.

This parameter has no effect if the authentication method is xauth-init-preshared.

Example:

```
IPSec config>TEMPLATE 4 config responder
```

"CONFIG NONE"

This command indicates that the device will behave as the initiator or responder depending on that indicated by the used IKE method.

Example:

```
IPSec config>TEMPLATE 4 config none
```

"EXTENDED AUTHENTICATION"

Extended Authentication consists of authentication with a server device which asignes the parameters needed to establish a connection. This authentication is typically executed through a user and a password.

The commands described below permit you to associate a user and a password and an IP address or name.

Command	Operation
XAUTH-IP	Associates a user to an IP address.
XAUTH-HOSTNAME	Associates a user to a name.

"XAUTH-IP [dirección IP] USER [nombre de usuario]"

"XAUTH-IP [dirección IP] PASSWORD [password]"

Through these two commands you can define a user and a password that will be associated to the IP address which is introduced as a parameter.

In cases where this is the initiator this IP address will indicate the address with which the remote end identified itself.

In cases where this is the responder this IP address will indicate the address which will be assigned to the end initiator in the ISAKMP Configuration method negotiation.

Example:

```
IPSec config>xauth-ip 1.1.1.1 user router1
IPSec config>xauth-ip 1.1.1.1 password plain mykey
```

"XAUTH-HOSTNAME [hostname] USER [nombre de usuario]"

"XAUTH-HOSTNAME [hostname] PASSWORD [password]"

Through these two command you can define the user and password that will be associated to the name introduced as a parameter.

This name indicates the hostname through which the remote end identifies itself.

Example:

```
IPSec config>xauth-hostname remoterouter user router1
IPSec config>xauth-hostname remoterouter password plain mykey
```

"ASSIGNED IP ADDRESS DESTINATION"

The assigned IP address will become the NAT addressed used in the NAPT rules whose local address coincides with that being used in the negotiation.

I.e. if you have a device with this rule:

IP local = 80.33.21.187 // ADSL interface IP address.

IP NAPT = 0.0.0.0

NAPT = Yes

When you negotiate the ISAKMP configuration mode, through the ADSL interface and you receive the address, e.g. 10.123.1.13, you will have the following rule:

IP local = 80.33.21.187 // ADSL interface IP address.

IP NAPT = 10.123.1.13

NAPT = Yes

You can enter the following type of Access Control List:
Source = 0.0.0.0/0
Destination = 0.0.0.0/0

Which subsequent to negotiation will transform into:
Source = 10.123.1.13/32
Destination = 0.0.0.0/0

In this way all the devices are connected to the router LAN and exit through ADSL, passing through the open SA in IPSec in order to access any destination outside of the LAN.

· *IPComp*

IPComp defines a property that permits you to establish a context or SA where the data is compressed as specified in the *RFC 3173 IP Payload Compression Protocol (IPComp).*

This compresión method can only be configured when using IPSec, i.e. at present there does not exist a way to activate this method outside of the context of IPSec SA..

Within the TEMPLATE menu, you will find the following parameters which permit you to configure this mode:

Command	Operation
IPCOMP	IP compression mode.

"IPCOMP LZS"
Through this command you activate the IP compresión functionality (IPComp) using the LZS algorithm.

Example:

```
IPSec config>TEMPLATE 4 ipcomp lzs
```

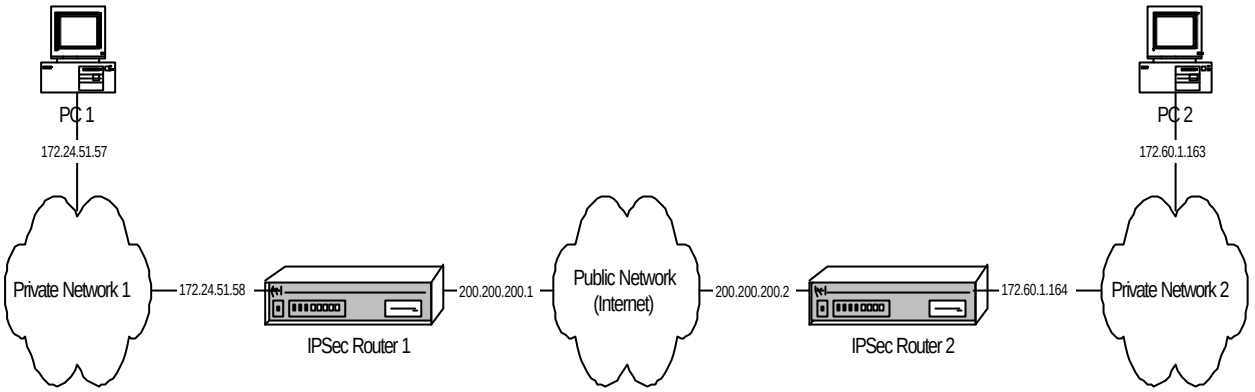
"IPCOMP NONE"
This command deactivates the IP compresión functionality (IPComp).

Example:

```
IPSec config>TEMPLATE 4 ipcomp none
```

4. Examples

4.1. Example 1: Manual Mode



This is the process of creating a new virtual private network (VPN) between Host A and Host B. The rest of the traffic between private networks will be allowed to pass in normal mode. Create an IPSec Tunnel with Triple DES encryption and SHA1 authentication in order to comply with the security requirements.

· *Creating the access control lists*

As already mentioned, the Tunnel clients are host A and host B.

Router 1:

```
Config>FEATURE ACCESS-LISTS

-- Access Lists user configuration --
Access Lists config> ACCESS-LIST
Access List number (1-99, 100-199)[1]? 101


Extended Access List 101> ENTRY 1
permit              configures type of entry or access control as permit
deny                configures type of entry or access control as deny
source              source menu: subnet or port
destination         destination menu: subnet or port
protocol-range      protocol range
dscp                Diff Serv codepoint
connection          IP connection identifier (rule)
Type an option []? source
address         ip address and mask of the source subnet
port-range      source port range
Type an option [address]?
Source IP address [0.0.0.0]? 172.24.51.57
Source IP mask [0.0.0.0]? 255.255.255.255
Extended Access List 101> ENTRY 1 destination
address         ip address and mask of the destination subnet
port-range      destination port range
Type an option [address]?
Destination IP address [0.0.0.0]? 172.60.1.163
Destination IP mask [0.0.0.0]? 255.255.255.255
Extended Access List 101>
```

The configured access list is as follows:

```
Extended Access List 101>LIST ALL-ENTRIES

Extended Access List 101, assigned to no protocol

1     PERMIT  SRC=172.24.51.57/32  DES=172.60.1.163/32  Conn:0

Extended Access List 101>
```

Through the "SHOW CONFIG" command the configuration can be displayed and used in the future by introducing this command in the console as shown below:

```
Access Lists config>SHOW CONFIG
; Showing System Configuration ...
; Router C5i IPSec 1 17 Version 10.0.0CAI

   access-list 101
;
      entry 1 permit
      entry 1 source address 172.24.51.57 255.255.255.255
      entry 1 destination address 172.60.1.163 255.255.255.255
;
   exit
;
Access Lists config>
```

I.e. you could have configured the required entry in the access list in the following way:

```
Access Lists config>
   access-list 101
      entry 1 permit
      entry 1 source address 172.24.51.57 255.255.255.255
      entry 1 destination address 172.60.1.163 255.255.255.255
```

Router 2:

```
Access Lists config>
   access-list 101
      entry 1 permit
      entry 1 source address 172.60.1.163 255.255.255.255
      entry 1 destination address 172.24.51.57 255.255.255.255
```

· *Creating Templates*

Subsequently the security patterns or Templates are created:

Router 1:

The first step is to enable IPSec.

```
Config>PROTOCOL IP

-- Internet protocol user configuration --
IP config> IPSEC

-- IPSec user configuration --
IPSec config> ENABLE
IPSec config>
```

Next you need to configure the required Template:

```
IPSec config>TEMPLATE 2
default                  sets default values to a template or creates a new one
dynamic                   dynamic template
manual                    manual template
isakmp                    isakmp template
source-address            tunnel's local IP address
destination-address       IP address of the other remote end of the tunnel
backup-destination        backup destination IP address
spi                       Security Parameter Index
key                       template encryption DES key
tkey                      triple DES key
md5key                    MD5 key
sha1key                   SHA1 key
antireplay                activates the Anti-Replay service
padding-check             enables padding check
udp-encapsulation         enables UDP encapsulation
life                     introduces the SAs life span created from the template
ike                       configures parameters relative to the IPSec IKE mode
keepalive                 enables the available keepalive services
no                        deletes a backup destination or disables an option
Type an option [default]? manual
esp      ESP security service (Encapsulating Security Payload)
ah       AH security service (Authentication Header)
Type an option [esp]?
des       encryption algorithm DES (Data Encryption Standard)
tdes      encryption algorithm TDES (Triple Data Encryption Standard)
Type an option [des]? tdes
md5       authentication algorithm MD5
sha1      authentication algorithm SHA1
none      no authentication algorithm
Type an option [md5]? sha1
IPSec config> TEMPLATE 2 source-address
IP address [0.0.0.0]? 200.200.200.1
IPSec config> TEMPLATE 2 destination-address
IP address [0.0.0.0]? 200.200.200.2
IPSec config> TEMPLATE 2 spi
Enter SPI (SPI > 256):[257]? 280
IPSec config> TEMPLATE 2 tkey h53s45ef46agv4646n2j8qpo

IPSec config> TEMPLATE 2 sha1key b74hd748ghzm67k6m6d1
```

The Template configuration is established as shown below:

```
IPSec config>LIST TEMPLATE ALL
TEMPLATES
2 manual ESP-3DES ESP-SHA1  SRC=200.200.200.1 DES=200.200.200.2 SPI=280

IPSec config>
```

Through the “SHOW CONFIG” command you obtain the following:

```
IPSec config>SHOW CONFIG
; Showing System Configuration ...
; Router C5i IPSec 1 17 Version 10.0.0CAI

      enable
;
      template 2 default
      template 2 manual esp tdes sha1
      template 2 source-address 200.200.200.1
      template 2 destination-address 200.200.200.2
      template 2 spi 280
      template 2 tkey h53s45ef46agv4646n2j8qpo
      template 2 sha1key b74hd748ghzm67k6m6d1
;
IPSec config>
```

I.e. The Template could also have been configured like this:

```
IPSec config>
      enable
      template 2 default
      template 2 manual esp tdes sha1
      template 2 source-address 200.200.200.1
      template 2 destination-address 200.200.200.2
      template 2 spi 280
      template 2 tkey h53s45ef46agv4646n2j8qpo
      template 2 sha1key b74hd748ghzm67k6m6d1
```

Router 2:

```
IPSec config>
      enable
      template 2 default
      template 2 manual esp tdes sha1
      template 2 source-address 200.200.200.2
      template 2 destination-address 200.200.200.1
      template 2 spi 280
      template 2 tkey h53s45ef46agv4646n2j8qpo
      template 2 sha1key b74hd748ghzm67k6m6d1
```

The SPI must be the same in both Routers.

· *Creating the SPDs*

In order to complete the Security Policies database (***SPD***), it is necessary to "map" the elements from the Access Control list to the chosen Templates.

Router 1:

```
IPSec config>assign-access-list
Enter extended access list id[100]? 101
IPSec config>map-template
Enter extended access list id[100]? 101
Enter template id[1]? 2
IPSec config>
```

Or:

```
IPSec config>
      assign-access-list 101
      map-template 101 2
```

The IPSec configuration is established as follows:

```
IPSec config>LIST ALL
IPSec Access Control.
Access Control is: enabled
QOS Preclassify is: disabled

Access Lists assigned to IPSec:
  Extended Access List 101
  Templates: 2


Extended Access List 101, assigned to IPSec
```

```
1     PERMIT  SRC=172.24.51.57/32  DES=172.60.1.163/32  Conn:0

TEMPLATES
2 manual ESP-3DES ESP-SHA1  SRC=200.200.200.1 DES=200.200.200.2 SPI=280

0 key entries
0 rsakey entries
Id.           Date.         Len         CA.                   Cert sn.

KeepAlive Configuration:
   Maximum number of encoded packets without receiving an answer: 0.
   Timeout after last packet encoded: 0 seconds.

DPD Configuration:
Idle period(secs) before sending DPD keepalives: 60
Maximum number of DPD keepalives not acknowledged: 3
Period of time(secs) between DPD keepalives: 5
Always send keepalive after idle period expiration : ENABLED
Anti-replay : DISABLED

Check-out time (%) - from SA's end-lifetime - to renegotiate : 10

SA's purge timeout:  15

Use software exponentiation

IPSec config>
```

Through the "SHOW CONFIG" command you obtain the following:

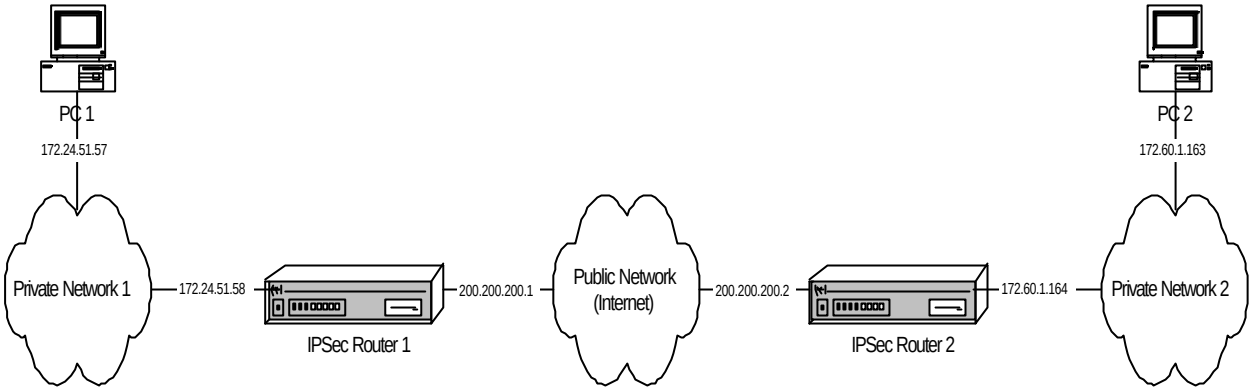
```
IPSec config>SHOW CONFIG
; Showing System Configuration ...
; Router C5i IPSec 1 17 Version 10.0.0CAI

      enable
      assign-access-list 101
;
      template 2 default
      template 2 manual esp tdes sha1
      template 2 source-address 200.200.200.1
      template 2 destination-address 200.200.200.2
      template 2 spi 280
      template 2 tkey h53s45ef46agv4646n2j8qpo
      template 2 sha1key b74hd748ghzm67k6m6d1
;
      map-template 101 2
IPSec config>
```

Router 2:

```
IPSec config>
      assign-access-list 101
      map-template 101 2
```

You can now save the configuration and restart the device to activate it; any communication between hosts A and B is now securely carried out regarding the said communication. However, the complete security of the communications system, based as well in the devices, introduced keys, modification permissions, etc., is the responsibility of the user.

4.2. Example 2: Dynamic mode (Main Mode IKE IPSEC)



The scenario for this example is the same as for the previous one. However the Tunnel is now going to be established based on dynamic Templates so that the communications, keys etc are automatically negotiated using the Main mode.

· *Creating the access control lists*

There is no further modification in this configuration with regard to example 1.

· *Creating Templates*

At this point you need to create the ISAKMP and dynamic Templates. The final command is important to introduce the Pre-shared key which must be the same in both devices. By default, the negotiation mode is Main Mode where the identities of the end routers for the Tunnel are masked. Although the same lifetimes have also been introduced, these parameters can be different and be negotiated.

Router 1:

```
IPSec config>ENABLE
IPSec config>TEMPLATE 1
default                 sets default values to a template or creates a new one
dynamic                  dynamic template
manual                   manual template
isakmp                   isakmp template
source-address           tunnel's local IP address
destination-address      IP address of the other remote end of the tunnel
backup-destination       backup destination IP address
spi                      Security Parameter Index
key                      template encryption DES key
tkey                     triple DES key
md5key                   MD5 key
sha1key                  SHA1 key
antireplay               activates the Anti-Replay service
padding-check            enables padding check
udp-encapsulation        enables UDP encapsulation
life                    introduces the SAs life span created from the template
ike                      configures parameters relative to the IPSec IKE mode
keepalive                enables the available keepalive services
no                       deletes a backup destination or disables an option
Type an option [default]? isakmp
des       encryption algorithm DES (Data Encryption Standard)
tdes      encryption algorithm TDES (Triple Data Encryption Standard)
Type an option [des]? tdes
md5       authentication algorithm MD5
sha1      authentication algorithm SHA1
```

```
Type an option [md5]? sha1
IPSec config> TEMPLATE 1 destination-address
IP address [0.0.0.0]? 200.200.200.2
IPSec config> TEMPLATE 1 life
type          type of life duration for the SA
duration      life duration
Type an option [type]? duration
seconds       lifetime in seconds
kbytes        lifetime in kbytes
Type an option [seconds]?
SECONDS[28800]? 43200

IPSec config> TEMPLATE 3 dynamic
esp      ESP security service (Encapsulating Security Payload)
ah       AH security service (Authentication Header)
Type an option [esp]?
des       encryption algorithm DES (Data Encryption Standard)
tdes      encryption algorithm TDES (Triple Data Encryption Standard)
Type an option [des]? tdes
md5       authentication algorithm MD5
sha1      authentication algorithm SHA1
none      no authentication algorithm
Type an option [md5]?
IPSec config> TEMPLATE 3 source-address
IP address [0.0.0.0]? 200.200.200.1
IPSec config> TEMPLATE 3 destination-address
IP address [0.0.0.0]? 200.200.200.2
IPSec config> TEMPLATE 3 life
type          type of life duration for the SA
duration      life duration
Type an option [type]?
seconds       lifetime in seconds
kbytes        lifetime in kbytes
both          lifetime in seconds and kbytes
Type an option [seconds]? both
IPSec config> TEMPLATE 3 life duration
seconds       lifetime in seconds
kbytes        lifetime in kbytes
Type an option [seconds]?
SECONDS[28800]? 14400
IPSec config> TEMPLATE 3 life duration
seconds       lifetime in seconds
kbytes        lifetime in kbytes
Type an option [seconds]? kbytes
KBYTES[0]?
IPSec config> KEY PRESHARED IP 200.200.200.2 plain 1234567890123456

IPSec config>
```

You could have also used the configuration in text mode (taken from that obtained through the "SHOW CONFIG" command).

```
IPSec config>
      enable
      template 1 default
      template 1 isakmp tdes sha1
      template 1 destination-address 200.200.200.2
      template 1 life duration seconds 43200
      template 3 default
      template 3 dynamic esp tdes md5
      template 3 source-address 200.200.200.1
      template 3 destination-address 200.200.200.2
      template 3 life type both
      template 3 life duration seconds 14400
      key preshared ip 200.200.200.2 plain 1234567890123456
```

Router 2:

```
IPSec config>
      enable
      template 1 default
      template 1 isakmp tdes sha1
      template 1 destination-address 200.200.200.1
      template 1 life duration seconds 43200
      template 3 default
      template 3 dynamic esp tdes md5
      template 3 source-address 200.200.200.2
      template 3 destination-address 200.200.200.1
      template 3 life type both
      template 3 life duration seconds 14400
      key preshared ip 200.200.200.1 plain 1234567890123456
```

· *Creating the SPD´s*

Finally, you need to establish the *SPD's*:

Router 1:

```
IPSec config>ASSIGN-ACCESS-LIST
Enter extended access list id[100]? 101
IPSec config>MAP-TEMPLATE
Enter extended access list id[100]? 101
Enter template id[1]? 3
IPSec config>
```

Or:

```
IPSec config>
      assign-access-list 101
      map-template 101 3
```

The IPSec final configuration is established as shown below:

```
IPSec config>LIST ALL
IPSec Access Control.
Access Control is: enabled
QOS Preclassify is: disabled

Access Lists assigned to IPSec:
  Extended Access List 101
  Templates: 3


Extended Access List 101, assigned to IPSec

1     PERMIT  SRC=172.24.51.57/32  DES=172.60.1.163/32  Conn:0

TEMPLATES
1 isakmp 3DES SHA1  DES=200.200.200.2
   LifeTime:12h0m0s
   IKE MAIN
   PRESHARED
   addr4 ID TYPE
   OAKLEY GROUP 1

3 dynamic ESP-3DES ESP-MD5  SRC=200.200.200.1 DES=200.200.200.2
   LifeTime:4h0m0s 0 kbytes
   PFS disabled

1 key entries
```

```
   200.200.200.2 ************
0 rsakey entries
Id.           Date.         Len         CA.                    Cert sn.

KeepAlive Configuration:
   Maximum number of encoded packets without receiving an answer: 0.
   Timeout after last packet encoded: 0 seconds.

DPD Configuration:
Idle period(secs) before sending DPD keepalives: 60
Maximum number of DPD keepalives not acknowledged: 3
Period of time(secs) between DPD keepalives: 5
Always send keepalive after idle period expiration : ENABLED
Anti-replay : DISABLED

Check-out time (%) - from SA's end-lifetime - to renegotiate : 10

SA's purge timeout:  15

Use software exponentiation

IPSec config>
```

With the "SHOW CONFIG" command:

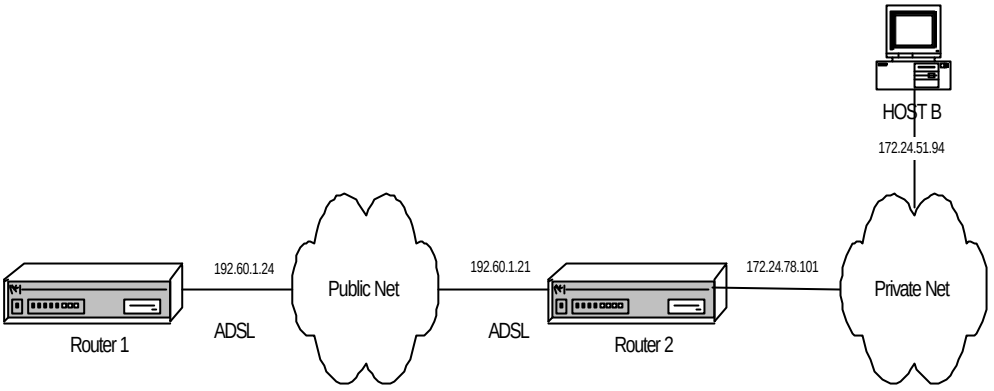
```
IPSec config>SHOW CONFIG
; Showing System Configuration ...
; Router C5i IPSec 1 17 Version 10.0.0CAI

      enable
      assign-access-list 101
;
      template 1 default
      template 1 isakmp tdes sha1
      template 1 destination-address 200.200.200.2
      template 1 life duration seconds 43200
;
      template 3 default
      template 3 dynamic esp tdes md5
      template 3 source-address 200.200.200.1
      template 3 destination-address 200.200.200.2
      template 3 life type both
      template 3 life duration seconds 14400
      template 3 life duration kbytes 0
;
      map-template 101 3
      key preshared ip 200.200.200.2 ciphered 0xE21C47018BC8B868FB72F48DC4363FC0
CFABF60C9FFE0286
IPSec config>
```

Router 2:

```
IPSec config>
      assign-access-list 101
      map-template 101 3
```

Once you have saved the configuration and restarted the device, the communication between hosts A and B is securely carried out, with the Pre-shared key as the only key to protect in this case.

4.3. Example 3: Dynamic mode (Aggressive mode IKE IPSEC) with one Tunnel end having an unknown address



This scenario reflects how to connect two routers through a virtual private network (VPN) using an ADSL line as the connection means. You create an IPSec Tunnel based on the dynamic Templates, with DES encryption and MD5 authentication as security requirements for the ISAKMP negotiation and ESP service with DES encryption and SHA1 authentication in the SA negotiation of the Tunnel. The Tunnel will be based on dynamic Templates so that the communications, keys, etc., are automatically negotiated using Aggressive mode.

The Aggressive mode has the advantage that Router 2 does not need to know the IP address of the other end of the Tunnel. This signifies that this configuration is perfectly adequate for many devices to connect to a single Router 2 by simply knowing the *hostname* and the common key between them. Router 1 must know the IP address of the router through which the Tunnel is going to be established, as it is this router that initiates the negotiation and must know which IP address it needs to connect to.

Firstly, we are going to give an in-depth explanation on how to configure Router 1. Once this has been configured, we will configure Router 2, going into detail on those parameters which differ from the Router 1 configuration.

a) Configuring the Router 1

· Configuring the hostname, IP addresses and rules

As previously indicated, authentication is carried out through the *hostname* rather than the IP addresses. Therefore, the first thing you have to configure is the name you are going to give to the device.

```
Teldat              (c)1996-2002

Router model C5i IPSec 1 17 CPU MPC860      S/N: 391/02415
1 LAN, 1 WAN Line, 1 ISDN Line, 1 ADSL Line


*PROCESS 4


Config>SET HOSTNAME GAS1
```

Subsequently, you need to assign the IP address for the ADSL interface. You also need to add a static route indicating that all the packets you are going to send to the private network are transmitted using the other end of the IPSec Tunnel as the link port.

You can also specify a connection identifier for the traffic between the routers. This is only necessary if you wish to treat the packets differently in different connections.

```
GAS1 Config>LIST DEVICES

 Interface       Con    Type of interface            CSR     CSR2  int
 ethernet0/0     LAN1   Quicc Ethernet           fa200a00 fa203c00   5e
 serial0/0       WAN1   X25                      fa200a20 fa203d00   5d
 atm0/0          ADSL1  Async Transfer Mode      fa200a60 fa203f00   55
 bri0/0          ISDN1  ISDN Basic Rate Int      fa200a40 fa203e00   5c
 x25-node        ---    Router->Node                    0             0
 ppp1            ---    Generic PPP                     0             0
 ppp2            ---    Generic PPP                     0             0
Config>

GAS1 Config>PROTOCOL IP
```

· *Creating the access control lists*

Once you have configured all the IP's own parameters, you need to configure the IPSec itself.

The first thing that you must configure is the access control lists. To do this, you need to access the generic lists configuration menu, select a number from the list corresponding to an extended list (between 100 and 199), indicate an entry ID within the list, in this case 1 and give the required value to the following parameters:

- The source IP address, this will be the one previously configured in the ADSL interface.
- The destination IP, this is the device with which you are going to establish an IPSec Tunnel, in our case this deals with a Router 2.
- The connection: you have to indicate the connection ID assigned to the Tunnel's traffic. This ID is displayed through the **LIST RULE** command. In this particular example, it is not necessary to assign the connection as no distinction is made when dealing with the packets according to the connection.
- The action to be taken in the packets, in this case, IPSec procedure (PERMIT).

```
GAS1 Config>FEATURE ACCESS-LISTS

-- Access Lists user configuration --
GAS1 Access Lists config>ACCESS-LIST
Access List number (1-99, 100-199)[1]? 102


GAS1 Extended Access List 102>ENTRY 1
permit              configures type of entry or access control as permit
deny                configures type of entry or access control as deny
source              source menu: subnet or port
destination         destination menu: subnet or port
protocol-range      protocol range
dscp                Diff Serv codepoint
connection          IP connection identifier (rule)
Type an option []? source
address          ip address and mask of the source subnet
port-range       source port range
Type an option [address]?
Source IP address [0.0.0.0]? 192.60.1.24
Source IP mask [0.0.0.0]? 255.255.255.255
GAS1 Extended Access List 102>entry 1 destination
address          ip address and mask of the destination subnet
port-range       destination port range
Type an option [address]?
Destination IP address [0.0.0.0]? 172.24.0.0
Destination IP mask [0.0.0.0]? 255.255.0.0
```

```
GAS1 Extended Access List 102>entry 1 permit
GAS1 Extended Access List 102>
```

Or:

```
GAS1 Access Lists config>
   access-list 102
      entry 1 permit
      entry 1 source address 192.60.1.24 255.255.255.255
      entry 1 destination address 172.24.0.0 255.255.0.0
```

· *Creating Templates*

Now you need to create the ISAKMP and dynamic Templates. The last command is important to introduce the Pre-Shared key that must be the same in both devices. The difference between this example and the previous one is that here the negotiation mode is Aggressive Mode, where the identities of the Tunnel's end routers are not masked and the IP address of the other end of the Tunnel is unknown.

Although you have also introduced the same lifetimes, these parameters may be different and be negotiated in such a way that the negotiation result will be the smallest configured at the Tunnel ends.

When creating the ISAKMP Template, you need to indicate the encryption type (DES) and the authentication (MD5) which are going to be used, as indicated in the initial security specifications.

On creating the Template, you need to indicate the ID number that will be used in the rest of the configuration for this Template. You also need to indicate the Tunnel's destination IP which you are going to connect to and additionally Aggressive mode will be used, as the authentication executed sends the hostname rather than the IP address. This is extremely useful when you do not know the IP address of the other end of the Tunnel a priori, as in the case of Router 2 in this example, where it does not need to know the IP address of the Routers to be connected to it. The IPSec Tunnel can be created by simply knowing the hostname.

Through the **TEMPLATE 1 IKE IDTYPE FQDN** command, you indicate that the authentication uses the hostname instead of the IP address which is the default option.

```
GAS1 Config>PROTOCOL IP

-- Internet protocol user configuration --
GAS1 IP config>IPSEC

-- IPSec user configuration --
GAS1 IPSec config>ENABLE
GAS1 IPSec config>TEMPLATE 1
default                  sets default values to a template or creates a new one
dynamic                   dynamic template
manual                    manual template
isakmp                    isakmp template
source-address            tunnel's local IP address
destination-address       IP address of the other remote end of the tunnel
backup-destination        backup destination IP address
spi                       Security Parameter Index
key                       template encryption DES key
tkey                      triple DES key
md5key                    MD5 key
sha1key                   SHA1 key
antireplay                activates the Anti-Replay service
padding-check             enables padding check
udp-encapsulation         enables UDP encapsulation
life                     introduces the SAs life span created from the template
ike                       configures parameters relative to the IPSec IKE mode
```

```
keepalive               enables the available keepalive services
no                      deletes a backup destination or disables an option
Type an option [default]? isakmp
des       encryption algorithm DES (Data Encryption Standard)
tdes      encryption algorithm TDES (Triple Data Encryption Standard)
Type an option [des]?
md5       authentication algorithm MD5
sha1      authentication algorithm SHA1
Type an option [md5]?
GAS1 IPSec config>TEMPLATE 1 destination-address
IP address [0.0.0.0]? 192.60.1.21
GAS1 IPSec config>TEMPLATE 1 ike
ca          CA
mode        mode in which phase I of the ISAKMP/IKE exchange is carried out
method      establishes the authentication method used by the device
pfs         enables the Perfect Forward Secrecy service
idtype      types of identifiers used during phase 1 of the ISAKMP/IKE exchange
crl         CRL
group       group
jfe         JFE
no          disables an IKE option
Type an option [ca]? mode
aggressive      aggressive mode
main            main mode
Type an option [aggressive]?
GAS1 IPSec config> TEMPLATE 1 ike idtype
ip          IP Address
fqdn        FQDN
ufqdn       UFQDN
keyid       keyid
asn-dn      asn-dn
Type an option [ip]? fqdn
GAS1 IPSec config>
```

Or in a more condensed form if you use the configuration in text mode:

```
GAS1 IPSec config>
    enable
    template 1 default
    template 1 isakmp des md5
    template 1 destination-address 192.60.1.21
    template 1 ike mode aggressive
    template 1 ike idtype fqdn
```

Once the ISAKMP Template has been created, you need to create the DYNAMIC Template.

Firstly, you indicate the type of service, ESP or AH. The ESP service provides confidentiality, authentication of the source address in each IP packet, integrity and protection against replays, while the AH service does not provide confidentiality. Subsequently you have to indicate that this is dealing with encryption (DES) and the type of authentication (SHA1), as indicated in the initial security specifications.

When indicating the Template ID, you must chose a different one from the above ISKMP Template (1), as contrariwise the previous configuration will be overwritten with the DYNAMIC Template configuration. In the example, the ID is 2.

In the same way as in the ISAKMP Template, you have to indicate the destination address, however you also have to indicate what the source address is i.e. the address of your ADSL interface. In this Template we have also enabled the KEEPALIVE option thus ensuring that the other end maintains its SA open.

```
GAS1 IPSec config>TEMPLATE 2 dynamic
esp      ESP security service (Encapsulating Security Payload)
ah       AH security service (Authentication Header)
Type an option [esp]?
des       encryption algorithm DES (Data Encryption Standard)
tdes      encryption algorithm TDES (Triple Data Encryption Standard)
Type an option [des]?
md5       authentication algorithm MD5
sha1      authentication algorithm SHA1
none      no authentication algorithm
Type an option [md5]? sha1
GAS1 IPSec config> TEMPLATE 2 source-address
IP address [0.0.0.0]? 192.60.1.24
GAS1 IPSec config> TEMPLATE 2 destination-address
IP address [0.0.0.0]? 192.60.1.21
GAS1 IPSec config> TEMPLATE 2 keepalive
keepalive      enables the available keepalive services
dpd            enables the DPD service (Dead Peer Detection)
no             disables the available keepalive services
Type an option [keepalive]?
GAS1 IPSec config>
```

Or:

```
GAS1 IPSec config>
      template 2 default
      template 2 dynamic esp des sha1
      template 2 source-address 192.60.1.24
      template 2 destination-address 192.60.1.21
      template 2 keepalive keepalive
```

Lastly, you need to configure the Pre-shared key. This key is common to both ends of the Tunnel.

When introducing the key, you need to indicate this is dealing with a Pre-shared key. We are also going to introduce a name instead of an IP address as previously explained.

The name to be introduced corresponds to the **domain name** of the other end of the Tunnel.

In addition to the device hostname, it's possible to configure the device domain. This can be carried out in the following way:

```
GAS1 IP config>DNS-DOMAIN-NAME
Domain name :  []? madrid.es
Domain name : madrid.es
Domain Name configured.
```

In this example, we have not used the domain name. Therefore, on displaying the domain name, this indicates that it is not configured and that the name to be used will be "**GAS1.**" This will be the name you need to configure when indicating the Pre-shared common keys at the other end of the Tunnel, i.e. in Router 2.

```
GAS1 IP config>LIST DNS-DOMAIN-NAME
No Domain Name configured.
Partial DNS name : GAS1.
```

In Router 1, you need to introduce the hostname to be used in the "**HOST.**" key as the domain in Router 2 has not been configured either. Only the device hostname as HOST has been configured.

```
GAS1 IPSec config>KEY PRESHARED HOSTNAME HOST. plain 1234567890123456
```

· Creating SDPs

Lastly, you need to establish the *SPD's* i.e. relating a control access to a created Template. In the below example, the configured generic list is 102, and the Template that this must be related to is dynamic i.e. ID 2.

```
GAS1 IPSec config>ASSIGN-ACCESS-LIST
Enter extended access list id[100]? 102
GAS1 IPSec config>MAP-TEMPLATE
Enter extended access list id[100]? 102
Enter template id[1]? 2
```

In text mode:

```
GAS1 IPSec config>
      assign-access-list 102
      map-template 102 2
```

The IPSec configuration in Router 1 is established as follows:

```
GAS1 IPSec config>LIST ALL
IPSec Access Control.
Access Control is: enabled
QOS Preclassify is: disabled

Access Lists assigned to IPSec:
  Extended Access List 102
  Templates: 2


Extended Access List 102, assigned to IPSec

1     PERMIT  SRC=192.60.1.24/32  DES=172.24.0.0/16  Conn:0

TEMPLATES
1 isakmp DES MD5  DES=192.60.1.21
   LifeTime:1h0m0s
   IKE AGGRESSIVE
   PRESHARED
   fqdn ID TYPE
   OAKLEY GROUP 1

2 dynamic ESP-DES ESP-SHA1  SRC=192.60.1.24 DES=192.60.1.21
   LifeTime:1h0m0s
   PFS disabled
   Keep Alive enabled

1 key entries
   HOST. ************
0 rsakey entries
Id.           Date.         Len         CA.                   Cert sn.

KeepAlive Configuration:
   Maximum number of encoded packets without receiving an answer: 0.
   Timeout after last packet encoded: 0 seconds.

DPD Configuration:
Idle period(secs) before sending DPD keepalives: 60
Maximum number of DPD keepalives not acknowledged: 3
```

```
Period of time(secs) between DPD keepalives: 5
Always send keepalive after idle period expiration : ENABLED
Anti-replay : DISABLED

Check-out time (%) - from SA's end-lifetime - to renegotiate : 10

SA's purge timeout:  15

Use software exponentiation

GAS1 IPSec config>
```

Through the "SHOW CONFIG" command, you obtain the following:

```
GAS1 IPSec config>SHOW CONFIG
; Showing Menu and Submenus Configuration ...
; Router C5i IPSec 1 17 Version 10.0.0CAI

      enable
      assign-access-list 102
;
      template 1 default
      template 1 isakmp des md5
      template 1 destination-address 192.60.1.21
      template 1 ike mode aggressive
      template 1 ike idtype fqdn
;
      template 2 default
      template 2 dynamic esp des sha1
      template 2 source-address 192.60.1.24
      template 2 destination-address 192.60.1.21
      template 2 keepalive keepalive
;
      map-template 102 2
      key preshared hostname HOST. ciphered 0xE21C47018BC8B868FB72F48DC4363FC0CF
ABF60C9FFE0286
GAS1 IPSec config>
```

b) Configuring the Router 2

· *Configuring the hostname, IP addresses and rules*

Hostname and the IP protocol parameters configuration is similar to that executed for Router 1.

```
Teldat              (c)1996-2002

Router model Centrix SEC (c) 1 36 CPU MPC860      S/N: 359/00144
1 LAN

*PROCESS 4
User Configuration
Config>SET HOSTNAME HOST
```

On configuring the IP protocol, care must be taken when configuring the interface addresses as the ethernet0/0 interface connects the network card with the 172.24.0.0 LAN. You also need to assign the IP address to the ADSL interface where the IPSec Tunnel connection is carried out.

```
HOST IP config>address atm0/0 192.60.1.24 255.255.255.0
HOST IP config>address ethernet0/0 172.24.78.101 255.255.0.0
```

· *Creating the access control lists*

Once all the IP parameters have been configured, you need to configure the IPSec itself.

Configuring the access control lists is similar to the way this was carried out for Router 1. Care must be taken when configuring the source and destination IP addresses.

```
HOST Access Lists config>
   access-list 103
      entry 1 permit
      entry 1 source address 172.24.0.0 255.255.0.0
      entry 1 destination address 192.60.1.24 255.255.255.255
```

· *Creating Templates*

As done for Router 1, you need to create the ISAKMP and dynamic Templates with Aggressive Mode as the negotiation mode. The Pre-shared key must be the same as that configured in Router 1, however in this case indicating that the key corresponds to the *hostname* "**GAS1**".

When creating the ISAKMP Template, you need to indicate the encryption type (DES) and the authentication (MD5) which are going to be used, as indicated in the initial security specifications. This coincides with that previously configured in Router 1.

On creating the Template, you need to indicate the ID number that will be used in the rest of the configuration for this Template. You also need to indicate the Tunnel's destination IP which you are going to connect to, however as the IP address of the device which is going to connect to Router 2 is unknown and we only know the *hostname*, the **destination IP** address will be **0.0.0.0**. Additionally you need to indicate you are going to use Aggressive mode and that the IDTYPE is FQDN so that the hostname is used in the authentication instead of the IP address which is the default option.

```
HOST IPSec config>
      enable
      template 1 default
      template 1 isakmp des md5
      template 1 destination-address 0.0.0.0
      template 1 ike mode aggressive
      template 1 ike idtype fqdn
```

Once the ISAKMP Template has been created, you need to create the DYNAMIC Template with ESP service, DES encryption and SHA1 authentication as done for Router 1. When indicating the Template ID, you must chose a different one from the above ISKMP Template (1), as contrariwise the previous configuration will be overwritten with the DYNAMIC Template configuration. In the example, the ID is 2.

In the same way as in the ISAKMP Template, you have to indicate the **destination address** (**0.0.0.0**), however you also have to indicate what the source address will be i.e. the address of your ADSL interface. The KEEPALIVE option is not enabled in this Template to free process time for Router 2 and it is the routers connecting to this that have to check that the SA is open.

```
HOST IPSec config>
      template 2 default
      template 2 dynamic esp des sha1
      template 2 source-address 192.60.1.21
      template 2 destination-address 0.0.0.0
      template 2 life duration seconds 1800
```

Lastly, you need to configure the Pre-shared key. This key is common to both ends of the Tunnel.

When introducing the key, you need to indicate this is dealing with a Pre-shared key. We are also going to introduce a name instead of an IP address as previously explained.

The name to be introduced corresponds to the **domain name** of the other end of the Tunnel as explained in the case of Router 1.

The name used in this example is "**GAS1.**" This is the Router 1 domain name.

```
HOST IPSec config> KEY PRESHARED HOSTNAME GAS1. plain 1234567890123456
HOST IPSec config>
```

If more routers apart from Router 1 are going to be connected to this Router, you must specify a hostname and the corresponding key for each of them.

· *Creating SPDs*

Lastly, you need to establish the *SPD's* i.e. relating a control access to a created Template. In the below example, the configured extended list that must be assigned to IPSec and associated with a Template is the 103, and the Template that must be related is the dynamic i.e. ID 2.

```
HOST IPSec config>
      assign-access-list 103
      map-template 103 2
```

Finally, you can free more Router 2 process time indicating the SA is not re-negotiated when this reaches the lifetime percentage specified and that the other end of the Tunnel (Router 1) will re-negotiate the SA.

```
HOST IPSec config>ADVANCED RENEGOTIATION-TIME 0
HOST IPSec config>
```

The resulting IPSec configuration is:

```
HOST IPSec config>LIST ALL
IPSec Access Control.
Access Control is: enabled
QOS Preclassify is: disabled

Access Lists assigned to IPSec:
  Extended Access List 103
  Templates: 2


Extended Access List 103, assigned to IPSec

1     PERMIT  SRC=172.24.0.0/16  DES=192.60.1.0/24  Conn:0

TEMPLATES
1 isakmp DES MD5  DES=0.0.0.0
   LifeTime:1h0m0s
   IKE AGGRESSIVE
   PRESHARED
   fqdn ID TYPE
   OAKLEY GROUP 1

2 dynamic ESP-DES ESP-SHA1  SRC=192.60.1.21 DES=0.0.0.0
```

```
   LifeTime:0h30m0s
   PFS disabled

1 key entries
   GAS1. ************
0 rsakey entries
Id.           Date.         Len         CA.                    Cert sn.

KeepAlive Configuration:
   Maximum number of encoded packets without receiving an answer: 0.
   Timeout after last packet encoded: 0 seconds.

DPD Configuration:
Idle period(secs) before sending DPD keepalives: 60
Maximum number of DPD keepalives not acknowledged: 3
Period of time(secs) between DPD keepalives: 5
Always send keepalive after idle period expiration : ENABLED
Anti-replay : DISABLED

Check-out time (%) - from SA's end-lifetime - to renegotiate : 0

SA's purge timeout:  15

Use software exponentiation

HOST IPSec config>
```

The following is displayed on executing the "SHOW CONFIG" command:

```
HOST IPSec config>SHOW CONFIG
; Showing System Configuration ...
; Router CENTRIX SEC (c) 1 36 Version 10.0.0CAI

      enable
      assign-access-list 103
;
      template 1 default
      template 1 isakmp des md5
      template 1 ike mode aggressive
      template 1 ike idtype fqdn
;
      template 2 default
      template 2 dynamic esp des sha1
      template 2 source-address 192.60.1.21
      template 2 life duration seconds 1800
;
      map-template 103 2
      key preshared hostname GAS1. ciphered 0xE21C47018BC8B868FB72F48DC4363FC0CF
ABF60C9FFE0286
      advanced renegotiation-time 0
HOST IPSec config>
```

Once the configuration of both devices has been saved and the devices have been restarted in order to activate the said configuration, the communication between the routers will be securely carried out, with the Pre-shared key as the only protected key in this case.

5. Certificates

When the authentication methods based on RSA are applied, you need to use RSA asymetric keys. These keys are usually used within the higher layer encapsulations known as *Certificates*. The Teldat Routers permit authentication based on RSA and require tools that are capable to manager Certificates for this.

We are going to describe how to operate with Certificates in this section, i.e. how to load them, how to assign them to Templates, how to create them, etc.

5.1. CERT Menu

The CERT menu is located within the IPSec menu. In the CERT menu you will find the CERTIFICATE command which has the following options:

Command	Operation
LOAD	Loads a CERTIFICATE from a disk to RAM memory.
UPDATE	Dynamically loads a CERTIFICATE from a disk to the RAM memory.
DELETE	Deletes a CERTIFICATE from a disk.
PRINT	Displays the content of a CERTIFICATE on screen.

"CERTIFICATE [CertFile] LOAD"

This command permits you to load a Certificate from a disk to the device RAM memory. Before executing an operation with a Certificate, Certificate must be loaded in the RAM through this command.

Example:

```
CERTIFICATES config>certificate router.cer load
```

"CERTIFICATE [CertFile] UPDATE"

This command permits you to load a Certificate from a disk to the device RAM memory dynamically i.e. without needing to restart the device.

Example:

```
CERTIFICATES config>certificate router.cer update
```

"CERTIFICATE [CertFile] DELETE"

This command permits you to delete a Certificate from a disk.

Example:

```
CERTIFICATES config>certificate router.cer delete
```

"CERTIFICATE [CertFile] PRINT"

This command permits you to print the content of a previously loaded Certificate.

Example:

```
CERTIFICATES config>certificate router.cer print
Version                   : V3
Serial Number             : 547E D185 0000 0000 1E6E
Algorithm Identifier      : SHA1 With RSA
Issuer:
  CN (Common Name        ): SECTESTCA1
  OU (Organizational Unit): Microsoft, Interopability Testing Only
  O  (Organization Name  ): Microsoft, Interopability Testing Only
  L  (Locality           ): Redmond
  S  (State or Province  ): WA
  C  (Country Name       ): US
  E  (Email              ): testca@microsoft.com
Valid From                : Wed Jul 25 09:21:24 2001
Valid To                  : Thu Jul 25 09:31:24 2002
Subject:
  E  (Email              ): jiglesias@teldat.es
  CN (Common Name        ): router.teldat.es
  OU (Organizational Unit): ImasD
  O  (Organization Name  ): Teldat
  L  (Locality           ): Tres Cantos
  S  (State or Province  ): Madrid
  C  (Country Name       ): sp
Publick Key               :
  Algorithm Identifier    : RSA
  Modulus Length          : 512 Bits.
  Modulus                 :
    E1CF D175 90EE 43BC 4BC5 D215 695A 74CC D1E8 F301 4F09 2093 7B12 84C0
    2C07 DE4B E458 9D48 43CB 4F14 A075 0D09 FB57 71DB 4FC6 8FDF 1FEF AA6D
    13BB 96FB 88FA 1343
  Exponent                :
    01 00 01
Signature                 :
  Signature Algorithm     : SHA1 With RSA
  Signature Data Info     : 2048 Bits.
  Signature Data          :
    3C10 94F3 CE87 0040 C3D0 A59F 1F0E 84DC E21F CCFD CA7A 2A32 651B 3D27 F9D0
    F87A 6993 E22C 28F5 7954 ED49 1E90 A52C 8098 F686 5E51 18DA D713 D65E 81BB
    267A 1D70 957D FB2F C841 E155 AD3C 3B38 6796 FA62 F6EF 8D76 DEDF 09B2 52C3
    3496 AD4B BF06 1415 3111 DEDD B2BE 9C68 5584 0A3B BF41 90B3 05C4 5CA1 E079
    AADA 43B1 F48D 9DEE 9793 907E 262D 2CC5 325C F3D1 892C 54E7 4736 06A3 4883
    A239 B68D 5477 13A8 BDE0 D7F4 18C1 FD94 3116 48FC C701 BA86 D932 A5C8 C28C
    5FE0 D8CF BE39 CF77 5CCC A104 0189 FF0B 5598 DBB1 2EB5 6269 9683 31DF 19BB
    DDEB 8BC0 FFDA 4587 13E4 42FF 7AF1 BD63 ACE4 D469 37B7 03FA 78DD 4535 49FB
    36AA 4525 F6EF 33A8 F5DB 3934 5079 A536
```

5.2. KEY RSA Command

This command enables you to work with the RSA keys generated in the Router.

Command	Operation
GENERATE	Generates a pair of random RSA keys.
CA-CHANGE	Changes the CA associated to the generated RSA key.

"KEY RSA GENERATE [CA NAME][SIZE(512/1024/2048)]"

Through this command you can generate a random RSA key and associate a CA name. I.e. generate a pair of public and private keys which are stored in the device disk on saving the configuration.

After generating the pair of keys, the device asks if you wish to generate a CSR file, *Certificate Signing Request*.

Example:

```
IPSec config>key rsa generate caname 512
RSA Key Generation.
Please, wait for a few seconds.
 RSA Key Generation done.
Checking..OK
Key Generation Process Finished.
Generate CSR?
(Yes/No)? n
Do not forget to save RSA keys.
```

"KEY RSA CA-CHANGE"

This command permits you to change the CA associated with a previously generated RSA key.

Example:

```
IPSec config>list key rsa all
1 rsakey entries
Id.           Date.         Len         CA.                   Cert sn.
   1   06/18/03  11:46:16    512         caname                ---
atlaslocal IPSec config>key rsa ca-change 1 newca
Do not forget to save RSA keys changes.
IPSec config>lis key rsa all
1 rsakey entries
Id.           Date.         Len         CA.                   Cert sn.
   1   06/18/03  11:46:16    512           newca               ---
```

5.3. Obtaining certificates through CSR

You can obtain a certificate for a Teldat device by creating a Certificate Signing Request (CSR). The end objective is to achieve two files: the CA certificate *caname.cer*, and the Router one, *router.cer*. The steps to carry out are as follows:

1. If you have a private key generated, you must create a CSR associated to this key. In order to do this, you execute the make command from the CSR configuration menu. If you do not have a private key generated, you need to generate it (key rsa generate command) and respond postively when the devices asks if you wish to generate CSR. The private key will have a CA associated through a file name corresponding to the certificate installed in the device for this CA, *caname.cer*. (This operation can be carried out even if you do not have a CA certificate available.)
2. After generating the CSR you can save this in a file that later can be obtained through FTP or be printed through the console by executing the *print* command. Normally the CSR are encoded in base64.
3. The CSR must be delivered to the CA in order for a certificate is returned, *router.cer*. Normally at this point, the CA also sends a certificate from the CA itself, *caname.cer*.
4. The obtained certificates are installed in the device, sending them through FTP and executing the *quote site savebuffer* command.
5. Now, you need to enter the *CERT* menu and load the router certificate through the *certificate **router** update* command.
6. A template is created which will use the RSA method *template **1** ike method rsa*.
7. Finally the CA certificate is associated to the template being used, through the command *template **1** ike ca **caname***..
8. The last step is to save the configuration.

This means, the association between the components is as follows:

- **(Private Key, CSR)** = Association through the private key identifier.
- **(Private Key, CA)** = Association through the CA name.
- **(Private Key, Certificado de Equipo)** = Association through the CA and the certificate serial number. The CA must be associated to a template and the certificate must be loaded.

NOTE: Verisign does not admit certain characters in the CSR fields. The @ symbol is one of these, so an email address cannot be included. The error returned by Verisign is 105. This field must be left blank if the CSR is goingto be delivered to Verisign.

The *list template all* command displays how everything has gone:

```
IPSec config>list template all
TEMPLATES
1 isakmp 3DES MD5  DES=1.1.1.1
   LifeTime:1h0m0s
   IKE MAIN
   RSA SIGNATURE
      CA      : SECTEST.CER. Expired.
      CRL     : disabled
       USER    : ROUTER.CER. Signature ok. Expired. Without Private Key.
   fqdn ID TYPE
   OAKLEY GROUP 1
```

Chapter 3
Monitoring

1. Introduction

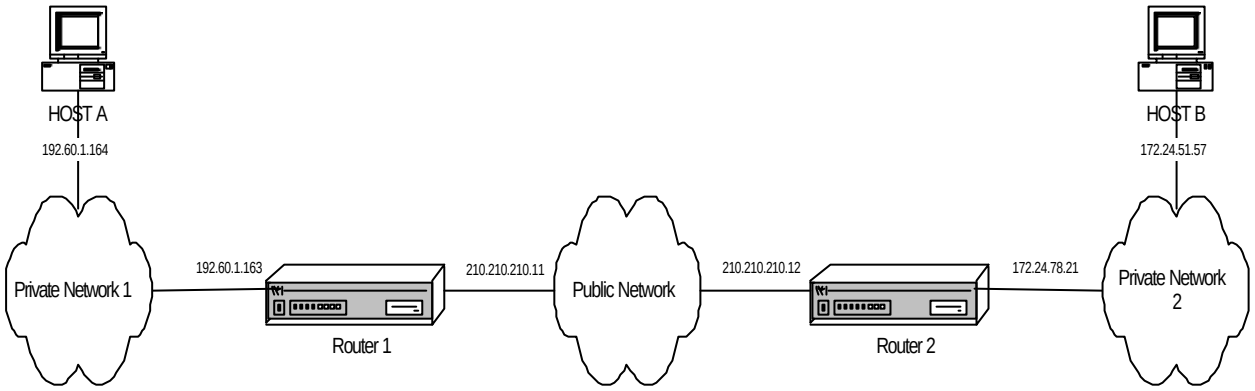
IPSec monitoring in the **Teldat Routers** is carried out once the SPD elements have been configured.

The difference with respect to the configuration is that now you are not going to vary any parameter. The parameters need to be listed and if they are varied, this will be temporary. Changes carried out in the monitoring will only be valid until the router is restarted.

The monitoring displays an operation list of the previously configured connections, the ISAKMP SAs or from the first phase and Dynamic and Manual SAs or the second phase. Additionally this permits you to eliminate the said connections.

In the first place the steps to follow are described in order to access to the said monitoring and secondly the SAs monitoring. Subsequently, you will see a command that will display the whole of the monitoring. Finally a problems and solutions reference is provided which can normally be found in the IPSec negotiations.

All of the examples seen for each monitoring command are based on the following scenario.



2. IPSec Monitoring

2.1. Initial Monitoring

This section describes the steps needed to access the IPSec monitoring in the **Teldat Router**. In order to enter the monitoring environment you must introduce the following commands:

```
*P 3
+PROTOCOL IP
IP>IPSEC
IPSEC protocol monitor
IPSEC>
```

Within the IPSec protocol monitoring environment the following commands are initially available:

Command	Operation
? (HELP)	Lists the commands or their available options.
CLEAR	Clears the cache memory and the SAs.
LIST	Lists the IPSEC monitoring.
EXIT	Exits the IPSEC configuration prompt.

2.2. Monitoring SAs

As seen in the introduction, the SAs (*Security Association*) are security connections that are created once the SPD has been consulted and contain the security information (authentication and encryption keys) needed in order to process the packet. Therefore when you create an SA, what you have is a connection established in order to securely transmit data between the two ends of the Tunnel.

There are two types of SAs, those of the first phase or ISAKMP and those of the second phase. The latter can be Dynamic SAs or Manual SAs.

You must take into account that in the SAs, there is a clear difference between the Dynamic SAs and the ISAKMP SAs, with respect to the Manual SAs. The Manual SAs are permanent connections, meaning that when the Manual Templates are configured a connection is established between Tunnel ends. Contrariwise, the Dynamic SAs and the ISAKMP SAs, as they are dynamic only appear when using the connection between the Tunnels ends, i.e. when the Tunnel is established.

SAs monitoring permits you to carry out two operations: cut the connection, i.e. delete the SAs with the **CLEAR** command or list all the established connections, i.e. all the SAs. This is executed with the **LIST** command.

a) CLEAR

With this command you can cut the established connection between the Tunnel ends. The said interruption will depend on which type of SA you have.

If the SA is a Manual SA there is no reason to eliminate it as seen earlier, the connection is permanent therefore cannot be cut. What can be done is to eliminate the Dynamic SAs and the ISAKMP SAs.

Command	Operation
NEGOTIATION	Eliminates the ISAKMP SAs or first phase SAs.
OUT	Eliminates the output Dynamic SAs.
IN	Eliminates the input Dynamic SAs.

"CLEAR SA NEGOTIATION ALL"

Eliminates all the ISAKMP SAs.

Example:

```
IPSEC>CLEAR SA NEGOTIATION ALL
Connection cleared
IPSEC>
```

"CLEAR SA NEGOTIATION CONNECTION [ID]"

The "ID" field is the SA identification number. This will only eliminate the ISAKMP SA defined by the "ID" number.

Example:

```
IPSEC>CLEAR SA NEGOTIATION CONNECTION 1
Connection 1 cleared
IPSEC>
```

"CLEAR SA NEGOTIATION ADDRESS-FILTER [IP ADD][MASK]"

Clears the ISAKMP SA with a source or destination address that is included within the range defined by [IP ADD][MASK].

Example:

```
IPSEC>CLEAR SA NEGOTIATION ADDRESS-FILTER 210.210.210.12  255.255.255.25
Connection 1 cleared
IPSEC>
```

"CLEAR SA OUT/IN ALL"

Clears all the Dynamic SAs, be they outputs or inputs.

Example:

```
IPSEC>CLEAR SA OUT ALL
All Connection cleared
IPSEC>
```

"CLEAR SA OUT /IN CONNECTION [ID]"

The "ID" field is the SA identification number. This only clears the Dynamic SAs defined by the "ID" number.

Example:

```
IPSEC>CLEAR SA OUT CONNECTION 1
Connection 1 cleared
IPSEC>
```

"CLEAR SA OUT/IN ADDRESS-FILTER [IP ADD][MASK]"

Clears the Dynamic or Manual SAs with a source or destination address included within the range defined by [IP ADD][MASK].

Example:

```
IPSEC>CLEAR SA OUT ADDRESS-FILTER 210.210.210.12  255.255.255.255
Connection 1 cleared
IPSEC>
```

b) LIST

You can display all the output or input connections, i.e. all the SAs with this command. With this list you will know if the connections are active or not.

The Manual SAs, since they are permanent connections, will always been seen on the list. However, the Dynamic SAs and the ISAKMP SAs as they are dynamic will only be seen if using the connection between Tunnel ends, i.e. you are transmitting data.

Command	Operation
NEGOTIATION	Lists the ISAKMP SAs or the first phase SAs.
OUT	Lists the output Dynamic and Manual SAs.
IN	Lists the input Dynamic and Manual SAs.

"LIST SA NEGOTIATION ALL"

Lists all the ISAKMP SAs that are active.

Example:

```
IPSEC>LIST SA NEGOTIATION ALL

SA NEGOTIATION
SA 1  Resp = 210.210.210.11
SRC=210.210.210.12 DES=210.210.210.11 STATE=5
LifeTime:23h59m0s (23h58m53s)
ClientSRC=192.60.1.164 ClientDES=172.24.51.57 ICMP SPORT=2048 DPORT=13416
ISAKMP_SA available:Purgetime=60
ISAKMP_NEGII (0x39330A0E/0x23951B2E)

SA 2  Resp = 200.200.200.1
SRC=200.200.200.2 DES=200.200.200.1 STATE=5
LifeTime:23h59m0s (23h58m53s)
ClientSRC=192.168.10.6 ClientDES= 192.168.4.5 ICMP SPORT=1500 DPORT=6000
ISAKMP_SA available:Purgetime=60
ISAKMP_NEGII (0x40530A0E/0x12351B2E)
IPSEC>
```

"LIST SA NEGOTIATION ADDRESS-FILTER [IP ADD][MASK]"

Lists the active ISAKMP SA with a source or destination address included within the range defined by [IP ADD][MASK].

Example:

```
IPSEC>LIST SA NEGOTIATION ADDRESS-FILTER 210.210.210.12  255.255.255.255

SA NEGOTIATION
SA 1  Resp = 210.210.210.11
SRC=210.210.210.12 DES=210.210.210.11 STATE=5
LifeTime:23h59m0s (23h58m53s)
ClientSRC=192.60.1.164 ClientDES=172.24.51.57 ICMP SPORT=2048 DPORT=13416
ISAKMP_SA available:Purgetime=60
ISAKMP_NEGII (0x39330A0E/0x23951B2E)
IPSEC>
```

"LIST SA OUT/IN ALL"

Lists all the active Dynamic SAs and the Manual SAs, whether they are outputs or inputs.

Example:

```
IPSEC>LIST SA OUT ALL

SA OUT
SA 3 SPI=0x23951B2E
SA UP, ESP-DES ESP-MD5 SRC=210.210.210.12 DES=210.210.210.11
LifeTime:24h0m0s 4608000 kbytes  (23h46m31s 4608000 kbytes )
encode pkts:0 (err:0), decode pkts:0 (err:0)

SA 4 SPI=0x12351B2E
SA UP, ESP-DES ESP-MD5 SRC=200.200.200.2 DES=200.200.200.1
LifeTime:24h0m0s 5008000 kbytes  (23h46m31s 5008000 kbytes )
encode pkts:0 (err:0), decode pkts:0 (err:0)
IPSEC>
```

"LIST SA OUT/IN ADDRESS-FILTER [IP ADD][MASK]"

List of the active Dynamic SAs or Manual SAs with source or destination address included within the range defined by [IP ADD][MASK].

Example:

```
IPSEC>LIST SA OUT ADDRESS-FILTER 210.210.210.12  255.255.255.255

SA OUT
SA 3 SPI=0x23951B2E
SA UP, ESP-DES ESP-MD5 SRC=210.210.210.12 DES=210.210.210.11
LifeTime:24h0m0s 4608000 kbytes  (23h46m31s 4608000 kbytes )
encode pkts:0 (err:0), decode pkts:0 (err:0)
IPSEC>
```

2.3. Monitoring List

Through the **LIST** command you can view a list of the entire monitoring process.

Command	Operation
ADDRESS-FILTER	Lists the monitoring for a determined address.
NEGOTIATION	Lists the IKE negotiation process.
NOTIFICATION	Displays IKE negotiations notification messages.
SA	Sas monitoring, previously seen in detail.
STATISTICS	Displays the IKE negotiations statistics.

"LIST ADDRESS-FILTER [IP ADD][MASK]"

Lists the whole of the monitoring with source or destination address included within the range defined by [IP ADD][MASK].

If no address is indicated, the whole of the monitoring is listed with all the source and destination addresses.

Example:

```
IPSEC>LIST ADDRESS-FILTER 210.210.210.12  255.255.255.255
SA OUT
SA 3 SPI=0x23951B2E
SA UP, ESP-DES ESP-MD5 SRC=210.210.210.12 DES=210.210.210.11
LifeTime:24h0m0s 4608000 kbytes  (23h46m31s 4608000 kbytes )
encode pkts:0 (err:0), decode pkts:0 (err:0)
```

```
SA IN
SA 2 SPI=0x39330A0E
SA UP, ESP-DES ESP-MD5 SRC=210.210.210.11 DES=210.210.210.12
LifeTime:24h0m0s 4608000 kbytes  (23h46m28s 4608000 kbytes )
encode pkts:0 (err:0), decode pkts:0 (err:0)

SA NEGOTIATION
SA 1  Resp = 210.210.210.11
SRC=210.210.210.12 DES=210.210.210.11 STATE=5
LifeTime:23h59m0s (23h58m53s)
ClientSRC=192.60.1.164 ClientDES=172.24.51.57 ICMP SPORT=2048 DPORT=13416
ISAKMP_SA available:Purgetime=60
ISAKMP_NEGII (0x39330A0E/0x23951B2E)
IPSEC>
```

"LIST NEGOTIATION"

Displays a list of the entire IKE negotiation process between the two Tunnel ends.

Example:

```
IPSEC>LIST NEGOTIATION

  (Time ************************************ 0h0m23s)
210.210.210.12:
  (* --------- Creating ISAKMP NEG ---------)(# 1(0x1))(HDR 0)(HDR sa)
  (prop 1 iskamp #1)(trans 1 id=1)(encryp des)(hash md5)(grp desc 1)(auth presh)
  (life sec)(duration 86340)
210.210.210.11: (HDR 0)(HDR sa)(prop 1 iskamp #1)(trans 1 id=1)(encryp des)
  (hash md5)(grp desc 1)(auth presh)(life sec)(duration 86340)
210.210.210.12:
  (* --------- Matching template ---------)(# 20(0x14))(HDR 0)(HDR keyx)
  (HDR nonce)
0.0.0.0: (Time ************************************ 0h0m1s)
210.210.210.11: (HDR 0)(HDR keyx)(HDR nonce)(vendor 10)
210.210.210.12:
  (* --------- Creating ISAKMP SA ---------)(HDR 0)(id addr4 prot=17 port=500)
  (# 0xd2d2d20c)(HDR hash)
210.210.210.11: (HDR 0)(id addr4 prot=17 port=500)(# 0xd2d2d20b)(HDR hash)
210.210.210.12:
  (* --------- Creating ISAKMP SA id ---------)(# -1629185295(0x9ee49af1))
  (HDR 9ee49af1)(HDR hash)(HDR sa)(prop 1 esp #1)(# 959646222(0x39330a0e))
  (trans 1 id=des)(encap tunnel)(grp desc presh)(life sec)(duration 86400)
  (life kbytes)(duration 4608000)(auth alg md5)(HDR nonce)(HDR keyx)
  (id addr4 prot=0 port=0)(# 0xc03c01a4)(id addr4 prot=0 port=0)(# 0xac183339)
0.0.0.0: (Time ************************************ 0h0m1s)
210.210.210.11: (HDR 9ee49af1)(HDR hash)(HDR sa)(prop 1 esp #1)
  (# 596974382(0x23951b2e))(trans 1 id=des)(encap tunnel)(life sec)
  (duration 86400)(life kbytes)(duration 4608000)(auth alg md5)(grp desc presh)
  (HDR nonce)(HDR keyx)(id addr4 prot=0 port=0)(# 0xc03c01a4)
  (id addr4 prot=0 port=0)(# 0xac183339)
210.210.210.12:
  (* --------- Matching template ---------)(# 1(0x1))(HDR 9ee49af1)(HDR hash)
  (* --------- Creating SA ---------)(# 959646222(0x39330a0e))
  (* --------- Creating SA ---------)(# 596974382(0x23951b2e))
0.0.0.0: (Time ************************************ 0h0m3s
```

"LIST NOTIFICATION"

Displays the IKE negotiation notification messages. The proposed failed negotiations, incompatible or deleted SAs, etc.

Example:

```
IPSEC>LIST NOTIFICATION

  (Time ************************************ 0h14m5s)
IPSEC>
```

"LIST STATISTICS"

IKE negotiation statistics

Example:

```
IPSec>LIST STATISTICS

----ESP/AH Statistics:----

Input Stats
-----------
  Frames ok    0
  Frames error 0
  ---> Out-of-Order frames      0
  ---> Unknown payload protocol 0
  ---> Internal errors          0
Output Stats
------------
  Frames ok    0
  No alg auth known errors 0


----IPSEC Forwarding Statistics:----

Sa in not found                 0
Sa out Template not found       0
Sa out not found(only manual)   0

----IKE Statistics:----
Negotiation phase I             0
Negotiation phase II            0
Check Hash Error phase I        0
Check Hash Error phase II       0
Drops Collision IKE messages    0
Drops Waiting IKE Processing    0

   Cypher queue empty:           0

IPSec>
```

2.4. Diagnosing problems in the IKE negotiation

In this section, we are going to give some typical example problems that often appear during IKE negotiation due to configuration errors. It is very important to know how to identify which phase the negotiation is in. To obtain this information, simply check the number associated to message header causing the error. If this is 0, this means that this is a phase 1 message and if it is distinct to zero, then it pertains to phase 2. The message producing the error usually is the one preceding the warning message indicating that an error has occurred. For example:

```
172.24.51.57: (HDR 0)(HDR sa)(prop 1 isakmp #1)(trans 1 id=1)(encryp des)
  (hash sha)(grp desc 1)(auth rsa)(life sec)(duration 600)(vendor 14)
172.24.78.15:
  (* --------- Creating ISAKMP NEG ---------)(# 57(0x39))(HDR 24343432)
  (notif isakmp no proposal chosen)
```

The message provoking the error was the one sent by 172.24.51.57 whose HDR has identifier 0. This means it is an error produced in the first phase of negotiation.

Another important piece of data is to know who initiated the negotiation, i.e. who was the *initiator*.

a) The device does not initiate the negotiation

Origin

The access control list has not been correctly configured.

This message is produced because the device could not correspond the packet which should set off the negotiation with an IPSec entry in the access control list.

Solution

Check the access control list parameters.

Addresses: Source and Destination. (Be careful with the subnets)
Mask.
Protocol.
Ports. Source and Destination.
Template: The corresponding dynamic Template must be mapped.

If you still cannot find the source of the error, check the result of the **LIST ACCESS OUT** monitoring command and check that the *hits* are increasing in the corresponding entry.

b) notif isakmp no proposal chosen. Phase 1

Initiator: `172.24.51.57`

```
172.24.51.57: (HDR 0)(HDR sa)(prop 1 isakmp #1)(trans 1 id=1)(encryp des)
  (hash sha)(grp desc 1)(auth rsa)(life sec)(duration 600)(vendor 14)
172.24.78.15:
  (* --------- Creating ISAKMP NEG ---------)(# 57(0x39))(HDR 0)
  (notif isakmp no proposal chosen)
```

Origin

The isakmp Template has not been correctly configured.

This message is produced because the device with address 172.24.78.15 has not been able to accept any of the proposals from device 172.24.51.57. In this phase of the negotiation, the proposals received are compared with those configured in the isakmp.

Solution

Check the isakmp Template parameters.

Authentication method: RSA_SIGNATURE, PRE-SHARED...
Encryption system: DES, TDES...
Authentication system: SHA1, MD5...
Type of lifetime: Seconds, Kbytes, both...
Group: 1 or 2.

c) notif isakmp payload malformed. Phase 1

Initiator: `172.24.51.57`

```
172.24.51.57: (HDR 0)(HDR sa)(prop 1 isakmp #1)(trans 1 id=1)(encryp des)
  (hash md5)(grp desc 1)(auth presh)(life sec)(duration 600)(vendor 14)
172.24.78.15:
  (* --------- Creating ISAKMP NEG ---------)(# 67(0x43))
  (* --------- Matching template ---------)(# 20(0x14))(HDR 0)(HDR sa)
  (prop 1 isakmp #1)(trans 1 id=1)(encryp des)(hash md5)(grp desc 1)(auth presh)
  (life sec)(duration 600)
172.24.51.57: (HDR 0)(HDR keyx)(HDR nonce)
172.24.78.15: (HDR 0)(HDR keyx)(HDR nonce)
  (* --------- Creating ISAKMP SA ---------)
172.24.51.57: (HDR 0)(id none prot=148 port=9841)(# 0x3c068321)(HDR 75 0)
172.24.78.15: (HDR 0)(notif isakmp payload malformed)
```

Origin

The Pre-shared key has not been correctly configured.

This message has been produced because the device with address 172.24.78.15 has not been able to correctly decode the encrypted message sent by device 172.24.51.57. In fact, on analyzing the erroneous message, you can see that some strange parameters have been received: unknown identifier, with protocol and port distinct to those configured, followed by an unknown header, .hdr 75 0.

Solution

Check the Pre-shared key and the ip_address – key, hostname-key associations.

d) notif esp no proposal chosen. Phase 2

Initiator: `172.24.51.57`

```
172.24.51.57: (HDR 53da7bd5)(HDR hash)(HDR sa)(prop 1 esp #2)
  (# -786612676(0xd11d3e3c))(trans 1 id=des)(life sec)(duration 300)
  (life kbytes)(duration 100000)(encap tunnel)(auth alg md5)(trans 2 id=des)
  (life sec)(duration 300)(life kbytes)(duration 100000)(encap tunnel)
  (auth alg sha)(prop 2 ah #2)(# -786612676(0xd11d3e3c))(trans 1 id=md5)
  (life sec)(duration 300)(life kbytes)(duration 100000)(encap tunnel)
  (auth alg md5)(trans 2 id=sha)(life sec)(duration 300)(life kbytes)
  (duration 100000)(encap tunnel)(auth alg sha)(HDR nonce)
  (id addr4 prot=0 port=0)(# 0xac183339)(id addr4 prot=0 port=0)(# 0xac184e0f)
172.24.78.15:
  (* --------- Creating ISAKMP SA id ---------)(# -583852704(0xdd331d60))
  (HDR dd331d60)(HDR hash)(notif esp no proposal chosen)
```

Origin

The isakmp Template has not been correctly configured.

This message is produced because the device with address 172.24.78.15 has not been able to accept any of the proposals from device 172.24.51.57. In this phase of the negotiation, the proposals received are compared with those configured in the dynamic Template associated with the corresponding access control list.

Solution

Check the dynamic Template parameters.

Type of encapsulation: Tunnel or Transport.
Encryption system: DES, TDES...
Authentication system: SHA1, MD5...
Type of lifetime: Seconds, Kbytes, both...
PFS: Check that the remote device admits PFS.

e) notif esp invalid id inform. Phase 2

Initiator: `172.24.51.57`

```
172.24.78.15: (HDR 0)(id addr4 prot=17 port=500)(# 0xac184e0f)(HDR hash)
  (* --------- Creating ISAKMP SA id ---------)(# 785093687(0x2ecb9437))
172.24.51.57: (HDR 2ecb9437)(HDR hash)(HDR sa)(prop 1 esp #2)
  (# 291357516(0x115dc34c))(trans 1 id=des)(life sec)(duration 300)(life kbytes)
  (duration 100000)(encap tunnel)(auth alg md5)(trans 2 id=des)(life sec)
  (duration 300)(life kbytes)(duration 100000)(encap tunnel)(auth alg sha)
  (prop 2 ah #2)(# 291357516(0x115dc34c))(trans 1 id=md5)(life sec)
  (duration 300)(life kbytes)(duration 100000)(encap tunnel)(auth alg md5)
  (trans 2 id=sha)(life sec)(duration 300)(life kbytes)(duration 100000)
  (encap tunnel)(auth alg sha)(HDR nonce)(id addr4 prot=0 port=0)(# 0xac183339)
  (id addr4 prot=16 port=0)(# 0xac184e0f)
172.24.78.15:
  (* --------- Creating ISAKMP SA id ---------)(# 1537079449(0x5b9df899))
  (HDR 5b9df899)(HDR hash)(notif esp invalid id inform)
```

Origin

The access control list has not been correctly configured.

This message is produced when the device with address 172.24.78.15 has not been able to accept the client identifier from device 172.24.51.57 *(id addr4 prot=0 port=0)(# 0xac183339) (id addr4 prot=16 port=0)(# 0xac184e0f).* In this phase of the negotiation, the proposals of the received identifiers are compared with those configured in the access control list.

Solution

Check the access control list parameters.

Addresses: Source and Destination. (Be careful with the subnets)
Mask.
Protocol.
Ports. Source and Destination.
Template: The corresponding dynamic Template must be mapped.

f) notif isakmp invalid cert authority. Phase 1. Initiator A

Initiator: `172.24.78.15`

```
172.24.78.15: (HDR 0)(HDR keyx)(HDR nonce)
172.24.51.57: (HDR 0)(HDR keyx)(HDR nonce)(certreq x509sig CERTREG 8)
172.24.78.15:
  (* --------- Creating ISAKMP SA ---------)(HDR 0)
  (notif isakmp invalid cert authority)
```

Origin

The isakmp Template has not been correctly configured.

This message is produced because the device with address 172.24.78.15 has not been able to find the CA configured in the corresponding isakmp Template.

Solution

Check the isakmp Template parameters.

Name of the CA.
Check that the CA name corresponds to a file in the device:

```
Router CERTIFICATES config>LIST EXIST
```

g) notif isakmp invalid cert authority. Phase 1. Initiator B

Initiator: `172.24.51.57`

```
172.24.78.15: (HDR 0)(HDR keyx)(HDR nonce)(certreq x509sig CERTREG 6)
  (* --------- Creating ISAKMP SA ---------)
172.24.51.57: (HDR 0)(id der_dn port=0 CERTREG 7)(cert x509sig CERTREG 8)
  (HDR sig)(certreq x509sig CERTREG 9)
172.24.78.15: (HDR 0)(notif isakmp invalid cert authority)
```

Origin

The isakmp Template has not been correctly configured.

This message is produced because the device with address 172.24.78.15 has not been able to find a CA configured in any isakmp Template that corresponds to that of the received certificate, in the example CERTREG 9

Solution

Check the isakmp Template parameters and compare them with the command execution result.

```
Router IPSec>LIST CERTIFICATE_NUMBER 9
```

Name of the CA.

Check that the CA name corresponds to a file in the device:

```
Router CERTIFICATES config>LIST EXIST
```

h) notif isakmp invalid cert. Phase 1

Initiator: `172.24.51.57`

```
172.24.51.57: (HDR 0)(HDR keyx)(HDR nonce)
172.24.78.15: (HDR 0)(HDR keyx)(HDR nonce)(certreq x509sig CERTREG 14)
  (* --------- Creating ISAKMP SA ---------)
172.24.51.57: (HDR 0)(id der_dn port=0 CERTREG 15)(cert x509sig CERTREG 16)
  (HDR sig)(certreq x509sig CERTREG 17)
172.24.78.15: (HDR 0)(notif isakmp invalid cert)
```

Origin

The received certificate is invalid.

Solution

Check that the received certificate is correct with the command:

```
Router IPSec>LIST CERTIFICATE_NUMBER 16
```

Check the parameters for:

Validity period.

The Issuer corresponds with the required CA.

```
Router IPSec>LIST CERTIFICATE_NUMBER 14
```

The certificate may be incorrectly signed.

i) notif isakmp cert unavailable. Phase 1

Initiator: `172.24.51.57`

```
172.24.51.57: (HDR 0)(HDR keyx)(HDR nonce)
172.24.78.15: (HDR 0)(HDR keyx)(HDR nonce)(certreq x509sig CERTREG 0)
  (* --------- Creating ISAKMP SA ---------)
172.24.51.57: (HDR 0)(id der_dn port=0 CERTREG 1)(cert x509sig CERTREG 2)
  (HDR sig)(certreq x509sig CERTREG 3)
172.24.78.15: (HDR 0)(notif isakmp cert unavailable)
```

Origin

There is no user certificate loaded for device 172.24.78.15 to send to the 172.24.51.57 end.

Solution

Check that there does exist a loaded certificate for the required CA.

First of all check which CA is required.

```
Router IPSec>LIST CERTIFICATE_NUMBER 3
```

If the required CA coincides with that sent. Execute a list of the isakmp Templates and check the result. This should indicate what the problem is.

If the required CA does not coincide with that sent, search in the CERTIFICATES menu to ensure there does exist a loaded certificate pertaining to this CA.

```
Router CERTIFICATES config>LIST LOADED PRINT ISSUER <certificate_name>
```

2.5. Monitoring options summary

SA Monitoring	Clear	"CLEAR SA NEGOTIATION ALL" "CLEAR SA NEGOTIATION CONNECTION [ID]" "CLEAR SA NEGOTIATION ADDRESS-FILTER [IP ADD][MASK]" "CLEAR OUT/IN ALL "CLEAR OUT /IN CONNECTION [ID]" "CLEAR OUT/IN ADDRESS-FILTER [IP ADD][MASK]"
	List	"LIST SA NEGOTIATION ALL" "LIST SA NEGOTIATION ADDRESS-FILTER [IP ADD][MASK]" "LIST SA OUT/IN ALL" "LIST SA OUT/IN ADDRESS-FILTER [IP ADD][MASK]"
Monitoring list	"LIST ADDRESS-FILTER[IP ADD][MASK]" "LIST NEGOTIATION" "LIST NOTIFICATION" "LIST STATISTICS"	