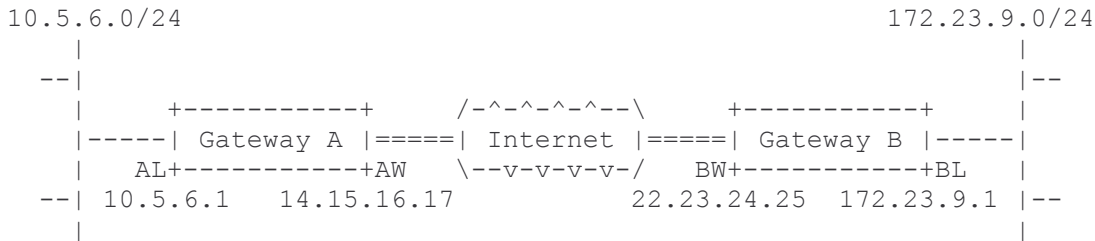




## SAFENET QUICKSEC TOOLKIT DOCUMENTATION PROFILE

This document describes the steps involved in configuring the SafeNet QuickSec toolkit for IPSec communication between two machines

### Scenario I: Gateway-to-Gateway communication using Pre Shared Keys



The **IKE Phase 1 parameters** used in Scenario 1 are:

- Main mode
- TripleDES
- SHA-1
- MODP group 2 (1024 bits)
- pre-shared secret of "hr5xb84l6aa9r6"
- SA lifetime of 28800 seconds (eight hours) with no kbytes rekeying

The **IKE Phase 2 parameters** used in Scenario 1 are:

- TripleDES
- SHA-1
- ESP tunnel mode
- MODP group 2 (1024 bits)
- Perfect forward secrecy for rekeying
- SA lifetime of 3600 seconds (one hour) with no kbytes rekeying
- Selectors for all IP protocols, all ports, between 10.5.6.0/24 and 172.23.9.0/24, using IPv4 subnets

▣ **Creating the security policy database file:**

- The configuration file on Gateway A will be as follows:

```
<?xml version="1.0" encoding="ISO-8859-1"?>
<!DOCTYPE quicksec PUBLIC "quicksec.dtd" "quicksec.dtd">
<quicksec>
  <params>
    <!-- Show statistics using the HTTP interface default port is 7368. -->
    <http-interface/>
  </params>
  <policy>
    <!-- How to speak IPSec between Host-A and Host-B. -->
    <tunnel name="hostb" ike-life="28800" transform="3des sha1 esp">
      <psk>hr5xb84l6aa9r6</psk>
      <peer>22.23.24.25</peer>
      <ike-groups>2</dh-groups>
      <pfs-groups level="request"></pfs-groups>
      <life type="seconds">3600</life>
    </tunnel>
    <rule to-tunnel="hostb">
      <src>10.5.6.0/24</src>
      <dst>172.23.9.0/24</dst>
    </rule>
    <rule from-tunnel="hostb">
      <src>172.23.9.0/24</src>
      <dst>10.5.6.0/24</dst>
    </rule>
  </policy>
</quicksec>
```

▣ **Starting the user mode policy manager:**

The policy manager is started from the command line as follows:

```
sshipsecpm -f filename
```

where *filename* is the name of the configuration file.

To see all the options provided by the policy manager use

```
sshipsecpm -h
```



## □ Configuring the Gateways to use Certificates for authentication

The configuration is similar to the previous scenario, the differences being the requirements for the private keys, certificate and CA certificate files.

The configuration file for Gateway A is as follows:

```
<?xml version="1.0" encoding="ISO-8859-1"?>
<!DOCTYPE quicksec PUBLIC "quicksec.dtd" "quicksec.dtd">
<quicksec>
  <params>
    <http-interface/>
    <externalkey type="software" init-info="directory(/tmp/ee)"/>
  </params>
  <policy>
    <tunnel name="hostb" ike-life="28800" transform="3des sha1 esp">
      <ca flags="no-crl" file="/tmp/test/ca-cert.ca"/>
      <peer>10.33.226.2</peer>
      <ike-groups>2</dh-groups>
      <pfs-groups level="request"></pfs-groups>
      <life type="seconds">3600</life>
    </tunnel>
    <rule to-tunnel="hostb">
      <src>192.168.1.0/24</src>
    </rule>
    <rule from-tunnel="hostb">
      <dst>192.168.1.0/24</dst>
    </rule>
  </policy>
</quicksec>
```

## □ Starting the user mode policy manager:

The policy manager is started from the command line as follows:

```
sshipsecpm -f filename
```

where *filename* is the name of the configuration file.

To see all the options provided by the policy manager use

```
sshipsecpm -h
```



**Notes:**

Scenarios developed by the Virtual Private Networks consortium ([www.vpnc.org](http://www.vpnc.org))

Contact [ipsec-support@safenet-inc.com](mailto:ipsec-support@safenet-inc.com) for further questions related to the SafeNet QuickSec toolkit.

For Evaluation and Sales – please contact [oemsales@safenet-inc.com](mailto:oemsales@safenet-inc.com)

For complete description and configuration information please refer to the SafeNet QuickSec for Access toolkit technical documentation.