TheGreenBow IPSec VPN Client

Configuration File Format
Release 6.1X

WebSite:	http://www.thegreenbow.com
Contact:	support@thegreenbow.com

Confidential, Property of TheGreenBow - Sistech SA - © 2001-2014

Table of Contents

1 INTRODUCTION 3

2 FILE LAYOUT 4
- 2.1 TEXT ENCODING 4

3 ROOT SECTIONS 5
- 3.1 [GENERAL] 5
- 3.2 [PHASE 1] 6
- 3.3 [PHASE 2] 6
- 3.4 [DEFAULT-PHASE-2-LIFETIME] 6
- 3.5 [TGBIKENG] 6

4 REFERRED-TO SECTIONS 7
- 4.1 <ISAKMPD-PEER> 7
- 4.2 <PHASE1-ID> 8
- 4.3 <ISAKMP-CONFIGURATION> 9
- 4.4 <ISAKMP-TRANSFORM> 9
- 4.5 <LIFETIME> 10
- 4.6 <IPSEC-CONNECTION> 10
- 4.7 <IPSEC-CONFIGURATION> 10
- 4.8 <IPSEC-SUITE> 11
- 4.9 <IPSEC-PROTOCOL> 11
- 4.10 <IPSEC-TRANSFORM> 11
- 4.11 <IPSEC-ID> 11
- 4.12 <X509-CERT> 12

5 PREDEFINED SECTIONS AND TAGS 13

6 IKEV2 14
- 6.1 XML FORMAT 14
- 6.2 MAIN TAGS 15

7 HEADER 19

8 RESTRICTIONS 20
- 8.1 PHASE1 OR PHASE 2 NAME 20
- 8.2 PHASE1 REMOTE GATEWAY 20
- 8.3 PHASE1 ADVANCED REDUNDANT GATEWAY 20
- 8.4 PHASE1 PRESHAREDKEY 20
- 8.5 PHASE1 OTHER PARAMETERS 20
- 8.1 PHASE2 SCRIPTS 20
- 8.2 PHASE2 DESKTOP SHARING ALIAS NAME 20

9 CONFIGURATION FILE SAMPLE 21

10 TGBCONFIG.XSD 25

Confidential, Property of TheGreenBow - Sistech SA - © 2001-2014

1 Introduction

TgbVpn.conf is the configuration file for TgbIKE daemon managing security association and key management for the IPsec layer at the NDIS level.

This document describes TgbVpn.conf general layout and deals with required and optional configuration elements. A sample configuration file with preshared key is also provided.

Confidential, Property of TheGreenBow - Sistech SA - © 2001-2014

2 File layout

TgbVpn.conf consists of sections, each beginning with a line looking like:

[Section name]

Between the brackets is the name of the section following this section header. Inside a section many tag/value pairs can be stored, each one looking like:

Tag=Value

Tag and Value must fit on a single line. Often the right-hand side values consist of other section names. This results in a tree structure. Some values are treated as a list of several scalar values. Such lists always use a comma character as the separator. Some values are formatted like this: X,Y:Z, which is an offer/accept syntax, where X is a value we offer and Y:Z is a range of accepted values, inclusive.

Comments can be put anywhere in the file by using a hash mark #'. The comment extends to the end of the current line.

For a IKEv2 Configuration see Chapter 6.

2.1 Text encoding

No UNICODE character is allowed in the VPN Configuration file.

All parameters are ASCII.

Confidential, Property of TheGreenBow - Sistech SA - © 2001-2014

3 Root sections

TgbVpn.conf must contain the following root sections for a IKEv1 Configuration [General], [Phase 1], [Phase 2], [Default-phase-2-lifetime]. [X509-Certificates] is required when authentication with X.509v3 certificates is needed.

IKEv2 Configuration is described in xml format inside the root section [TGBIKENG]

Below, we provided an exhaustive list of all tags within each root section.

3.1 [General]

This section root contains global configuration parameters:

Shared-SADB

Must be specified and always set to Defined.

Retransmits

How many times should a message be retransmitted before giving up.

Exchange-max-time

How many seconds should an exchange maximally take to set up before we give up.

Default-phase-1-lifetime

The default phase 1 lifetime.

Default-phase-2-lifetime

The default phase 2 lifetime.

Bitblocking

If set to 1 then only ISAKMP and IPSEC traffic are allowed.

Xauth-interval

The interval between watchdog checks of XAUTH authentication.

Rconf-interval

Time period between watchdog checks of Config Mode parameters negociation.

Dpd-interval

The interval between watchdog checks of DPD messages.

DPD_retrans

Number of retransmission of DPD messages

DPD_wait

Time period between two DPD messages if no response

Confidential, Property of TheGreenBow - Sistech SA - © 2001-2014

3.2 [Phase 1]

This root section contains ISAKMP SA peers:

<IP-address> or <DNS name>

A name of the ISAKMP peer at the given IP-address or DNS name. Look at <ISAKMP-peer> below.

3.3 [Phase 2]

This root section contains IPsec SA peers:

Passive-connections

A list of IPsec "passive connection" names we recognize and accept initiations for. . A tunnel from a passive connection can be established with traffic detection or user's action on GUI. Look at <IPsec-connection> below

Manual-connections

A list of IPsec "manual connection" names we recognize. A "manual connection" can only be established on user's action on GUI. Traffic detection does not work with this kind of connection. Look at <IPsec-connection> below.

3.4 [Default-phase-2-lifetime]

Phase 2 SA lifetime. Look at <Lifetime> below.

3.5 [TGBIKENG]

This root sections contains all IKEv2 Configuration.

Xml format is described on chapter 6.

Confidential, Property of TheGreenBow - Sistech SA - © 2001-2014

4 Referred-to sections

Referred-to sections extends Root sections to provide specific ISAKMP and IPSEC configuration. Below, we provided an exhaustive list of all Referred-to sections and their tags.

4.1 <ISAKMPD-peer>

This section provides parameters for negotiation with an ISAKMP peer:

Phase

The constant 1 as ISAKMP-peer.

Local-address

If exists, the Local IP-address to use.

Address

Peer IP-address

Transport

The name of the transport protocol, defaults to **UDP**

Port

In case of **UDP** the **UDP** port number to send to. This is optional; the default value is 500 which is the IANA-registered number for ISAKMP.

Configuration

The name of the ISAKMP-configuration section to use. Look at <ISAKMP-configuration> below.

Authentication

If existent, authentication data for this specific peer. In the case of preshared key, this is the key value itself.

ID

If existent, the name of the section that describes the local client ID that we should present to our peer. If not present, it defaults to the address of the local interface we are sending packets over to the remote daemon. Look at <Phase1-ID> below.

Remote-ID

If existent, the name of the section that describes the remote client ID we expect the remote daemon to send us. If not present, it defaults to the address of the remote daemon. Look at <Phase1-ID> below.

Xauth

If existent and set to **1**, an XAUTH authentication must be initiated by the peer.

Rconf

If existent and set to **1**, a Config Mode parameters negotiation must be initiated by the peer.

Confidential, Property of TheGreenBow - Sistech SA - © 2001-2014

Xpopup

If existent and set to **1**, Xauth parameters will be fetched from another application or process.

Xuser

Xauth user name.

Xpassword

Xauth password.

CertLocation

Location where certificate for this phase can be found. Accepted values: **localfile**, **smardcard**, **wincertstore**. The default value is localfile.

CertUser

Section name for the user certificate. Read <X509-cert> below.

CertKey

Section name for the private key of the user certificate. Read <X509-cert> section below. This tag can be omitted.

CertCa

Section name for the certification authority used by the user certificate. Read <X509-cert> section below. This tag can be omitted.

SmartCardReader

PCSC name of the smart card reader.

NATT_ENABLED

If set to 0, NAT-T payloads are not sent by the IKE daemon. If set to 1, NAT-T feature is supported

NATT_FORCED

If existent and set to 1, force NAT-T payload to be sent.

4.2 <Phase1-ID>

This section describes Phase 1 ID format:

ID-type

The Phase 1 ID type. Supported types are **IPV4_ADDR**, **IPV4_ADDR_SUBNET**, **FQDN**, **USER_FQDN**, **DER_ASN1_DN** and **KEY_ID**.

Address

If the ID-type is **IPV4_ADDR** this tag must exist and be an IP-address.

Network

If the ID-type is **IPV4_ADDR_SUBNET** this tag must exist and be a network address.

Confidential, Property of TheGreenBow - Sistech SA - © 2001-2014

Netmask

If the ID-type is **IPV4_ADDR_SUBNET** this tag must exist and be a network subnet mask.

Name

If the ID-type is **FQDN**, **USER_FQDN**, **DER_ASN1_DN** or **KEY_ID** this tag must exist and contain a domain name, an email address, a certificate subject or other identifying string respectively.

ReadFrom

Location from where Name value can be gotten. This tag only exists If the ID-type is DER_ASN1_DN. The only value available is **smartcard**.

4.3 <ISAKMP-configuration>

This section describes exchange type and defines the transform for protecting ISAKMP traffic:

DOI

The domain of interpretation. Normally **IPSEC** If unspecified, defaults to **IPSEC**

EXCHANGE_TYPE

The exchange type as given by the RFCs. For main mode this is **ID_PROT** and for aggressive mode it is **AGGRESSIVE**

Transforms

A proposed transform to use for protecting the ISAKMP traffic. Look at <ISAKMP-transform> below.

4.4 <ISAKMP-transform>

This section describes an ISAKMP transform:

ENCRYPTION_ALGORITHM

The encryption algorithm as the RFCs name it.

KEY_LENGTH

For encryption algorithms with variable key length, this is where the offered/accepted key lengths are described. The value is of the offer-accept kind described above.

HASH_ALGORITHM

The hash algorithm as the RFCs name it.

AUTHENTICATION_METHOD

The authentication method as the RFCs name it.

GROUP_DESCRIPTION

The group used for Diffie-Hellman exponentiations. The names are symbolic, like **MODP_768**, **MODP_1024**, **MODP_1536** and **MODP_2048**.

Life

Confidential, Property of TheGreenBow - Sistech SA - © 2001-2014

Name of the section that defines the lifetime. By default, use LIFE_MAIN_MODE or LIFE_QUICK_MODE. Look at <Lifetime> below.

4.5 <Lifetime>

This section defines the lifetime of an ISAKMP or an IPSEC SA.

LIFE_TYPE

Only **SECONDS** is supported.

LIFE_DURATION

An offer/accept kind of value. Format: default,minimal:maximal

4.6 <IPsec-connection>

This section provides parameters for an IPSEC connection:

Phase

The constant **2** as IPsec-connections.

ISAKMP-peer

The name of the ISAKMP-peer which to talk to in order to set up this connection. The value is the name of an <ISAKMP-peer> section. See above.

Configuration

The name of the IPsec-configuration section to use. Look at <IPsec-configuration> below.

Local-ID

The name of the section that describes the local client ID that we present to our peer. Look at <IPsec-ID> below.

Important note: if the local virtual address is undefined (i.e. 0.0.0.0 when sets through the GUI client), then the Local-ID tag must not be present in this section, and there is no local <IPsec-ID> section to create in the file.

Remote-ID

The name of the section that describes the remote client ID that we present to our peer. Look at <IPsec-ID> below.

AutoStart

If set to **1** then the IPSEC connection is started at boot.

USBStart

If set to **1** then configuration is loaded from USB key.

4.7 <IPsec-configuration>

This section describes an IPSEC configuration:

Confidential, Property of TheGreenBow - Sistech SA - © 2001-2014

DOI

The domain of interpretation as given by the RFCs. Normally **IPSEC** If unspecified, defaults to **IPSEC**

EXCHANGE_TYPE

The exchange type as given by the RFCs. For quick mode this is **QUICK_MODE**

Suites

A protection suite usable for protecting the IP traffic. It contains a name of an <IPsec-suite> section. See below.

4.8 <IPsec-suite>

Protocols

A name of an <IPsec-protocol> section. See below.

4.9 <IPsec-protocol>

This section describes an IPSEC protocol:

PROTOCOL_ID

The protocol as given by the RFCs. Only **IPSEC_ESP** is supported.

Transforms

A transform usable for implementing the protocol. It contains a name of an <IPsec-transform> section. See below.

4.10 <IPsec-transform>

This section describes an IPSEC transform:

TRANSFORM_ID

The transform ID as given by the RFCs.

AUTHENTICATION_ALGORITHM

The authentication algorithm as given by the RFCs.

GROUP_DESCRIPTION

An optional (provides PFS if present) Diffie-Hellman group description. The values are the same as GROUP_DESCRIPTION's in <ISAKMP-transform> sections shown above.

ENCAPSULATION_MODE

The encapsulation mode as given by the RFCs. Only TUNNEL is supported.

Life

Name of the section that defines the lifetime. Look at <Lifetime> above.

4.11 <IPsec-ID>

Confidential, Property of TheGreenBow - Sistech SA - © 2001-2014

This section describes Phase 2 ID format:

ID-type

The Phase 2 ID type. Supported types are **IPV4_ADDR** and **IPV4_ADDR_SUBNET**.

Address

If the ID-type is **IPV4_ADDR** this tag must exist and be an IP-address.

Network

If the ID-type is **IPV4_ADDR_SUBNET** this tag must exist and be a network address.

Netmask

If the ID-type is **IPV4_ADDR_SUBNET** this tag must exist and be a network subnet mask.

4.12 <X509-cert>

This section describes X509 certificate sections.

The certificate content must be delimited by -----BEGIN CERTIFICATE----- and -----END CERTIFICATE-----. These strings must be set from the beginning of a line. The base64 certificate content must start from the beginning of a line. The private key content must be delimited by -----BEGIN RSA PRIVATE KEY----- and -----END RSA PRIVATE KEY-----. These strings must be set from the beginning of a line. The base64 private key content must start from the beginning of a line.

Example:

[CnxVpn1-Public-Client-Key]
-----BEGIN CERTIFICATE-----
MIICwDCCAimgAwIBAgIJAJWR38h+E4nhMA0GCSqGSIb3DQEBBAUAMIGZMQswCQYD
VQQGEwJGUjEWMBQGA1UECBMNSWxlIGRlIEZyYW5jZTEOMAwGA1UEBxMFUGFyaXMx
FDASBgNVBAoTC1RoZUdyZWVuQm93MSQwIgYDVQQDExtvcGVuYnNkLmRldi50aGVn
cmVlbmJvdy5jb20xJjAkBgkqhkiG9w0BCQEWF3N1cHBvcnRAdGhlZ3JlZW5ib3cu
Y29tMB4XDTA2MDMyOTExMDMxNloXDTA3MDMyOTExMDMxNloweTELMAkGA1UEBhMC
RlIxDjAMBgNVBAcTBVBhcmlzMRQwEgYDVQQKEwtUaGVHcmVlbkJvdzEWMBQGA1UE
AxMNRXJpYyBCb3VkcmFuZDEsMCoGCSqGSIb3DQEJARYdZXJpYy5ib3VkcmFuZEB0
aGVncmVlbmJvdy5jb20wgZ8wDQYJKoZIhvcNAQEBBQADgY0AMIGJAoGBALjaPdJf
h/5b7wvncueEV/LlmEL5cUo3UjquP+dFjDk+UEeIePQ/CUbZ9Hg+r67kihnVPXdb
Y5TGFHN0eHSWH82CQw+bqQyN+VzCgHnEDmkCnUsurFxtsyCjlR0ppP7wwn90rvpZ
Hs93NEQKFV0D1pfDod/bj94zQUTA9Q2FdcFXAgMBAAGjLzAtMCsGA1UdEQEB/wQh
MB+BHWVyaWMuYm91ZHJhbmRAdGhlZ3JlZW5ib3cuY29tMA0GCSqGSIb3DQEBBAUA
A4GBAKTDEkXWbS0FJ36hEhlxIpguS8+7ZU4btXvF/nBC8uuO3OMmszu9nPZv2bcv
ylFgXb2G879LJfGvTZGmox07wjz94Tfnyi1xKUzF8woGewhfavvCdt3ZE4OV9eUm
BcukEPDU7U9fpvDtnWuxqqdOSMFjk1GcVVNQyWv44hYQg9+t
-----END CERTIFICATE-----

Confidential, Property of TheGreenBow - Sistech SA - © 2001-2014

5 Predefined sections and tags

Some predefined section names are recognized by the TgbIKE daemon, avoiding the need to fully specify the Main Mode transforms and Quick Mode suites, protocols, and transforms.

For Main Mode: { DES, 3DES, AES }-{ MD5, SHA }[-GRP{1, 2, 5, 14}][-{RSA_SIG}]

For Quick Mode: QM-ESP[-TRP]-{cipher}[-{hash}][-PFS[-{group}]]-SUITE

where
{cipher} is either DES, 3DES or AES
{hash} is either MD5 or SHA
{group} is either GRP1, GRP2, GRP5 or GRP14

For example, 3DES-SHA means: 3DES encryption, SHA hash, and authorization by pre-shared keys. Similarly, QM-ESP-3DES-SHA-PFS-SUITE means: ESP protocol, 3DES encryption, SHA hash, and use Perfect Forward Secrecy. Unless explicitly stated with -GRP1, 2, 5 or 14, transforms and PFS suites use DH group 2.

All autogenerated values can be overridden by manual entries by using the same section and tag names in the configuration file.

Confidential, Property of TheGreenBow - Sistech SA - © 2001-2014

6 IKEV2

6.1 XML Format

Under the root section [TGBIKENG], all IKEv2 configurations are described in a xml format.

XSD file described in section Tgbconfig.xsd contains all the available tags for IKEv2 configuration. This file is containing minimum and maximum occurrences for each tag and also possible values for the main XML type. Some XML tags are also described in the next subsection.

The following example is concerning a configuration for an IKEv2 connection with certificates.

[TGBIKENG]

```
<?xml version="1.0" encoding="iso-8859-1"?>
<tgbconfig>
  <cfg_ikev2>
    <cfg_connectionv2 name="StrongSwanIkeV2IPV4">
      <cfg_ike_sa name="StrongSwanIkeV2IPV4" family="AF_AUTO">
        <server>192.168.205.191</server>
        <port>500</port>
        <port_nat>4500</port_nat>
        <ikeauth_lifetime>1800</ikeauth_lifetime>
        <retries>4</retries>
        <cfg_dpd>
          <interval>60</interval>
          <retrans>3</retrans>
          <wait>15</wait>
        </cfg_dpd>
        <cfg_sa>
          <proposal protocol="IKE">
            <transform type="ENCR_ALGO" keylength="128">AES_CBC</transform>
            <transform type="PRF">PRF_HMAC_SHA2_512</transform>
            <transform type="INTEG">AUTH_HMAC_SHA2_512_256</transform>
            <transform type="DH_GROUP">DH_MODP_2048</transform>
          </proposal>
        </cfg_sa>
        <identity type="ID_DER_ASN1_DN" location="local">
          C = XX, ST = XX, L = XX, O = XX, OU = XX, CN = XX, name = XX1, emailAddress = XX
        </identity>
        <identity type="ID_DER_ASN1_DN" location="remote">
          C= XX/ ST = XX, L = XX, O = XX, OU = XX, CN = XX, name = XX, emailAddress = XX
        </identity>
        <authentication type="certificate" multipleauth="yes" sendcertrequest="yes">
          <cfg_eap type="EAP-MSCHAPV2">
            <identity>login</identity>
            <secret>pwd</secret>
          </cfg_eap>
          <certificate type="cacert" location="file">
            <public_key>
              -----BEGIN CERTIFICATE-----
              XX
              -----END CERTIFICATE-----
            </public_key>
          </certificate>
          <certificate type="user" location="file">
            <public_key>
              -----BEGIN CERTIFICATE-----
              XX
              -----END CERTIFICATE-----
            </public_key>
            <private_key>
              -----BEGIN RSA PRIVATE KEY-----
              XX
              -----END RSA PRIVATE KEY-----
            </private_key>
            <subject>
              C = XX, ST = XX, L = XX, O = XX, OU = XX, CN = XX, name = XX, emailAddress = XX
            </subject>
          </certificate>
```


Confidential, Property of TheGreenBow - Sistech SA - © 2001-2014

```
      </authentication>
    </cfg_ike_sa>
    <cfg_child_sa name="reseau163_1" family="AF_INET" requestconfig="false">
      <childsa_lifetime>3600</childsa_lifetime>
      <cfg_sa>
        <proposal protocol="ESP">
          <transform type="ENCR_ALGO" keylength="128">AES_CBC</transform>
          <transform type="INTEG">AUTH_HMAC_SHA2_512_256</transform>
          <transform type="DH_GROUP">DH_MODP_2048</transform>
          <transform type="ESN">NO_EXTENDED_SEQ_NUMBER</transform>
        </proposal>
      </cfg_sa>
      <cfg_ts type="IPV4_ADDR_RANGE" location="local">
        <protocol>0</protocol>
        <start_port>0</start_port>
        <end_port>65535</end_port>
        <starting_address>10.10.4.2</starting_address>
        <ending_address>10.10.4.2</ending_address>
      </cfg_ts>
      <cfg_ts type="IPV4_ADDR_RANGE" location="remote">
        <protocol>0</protocol>
        <start_port>0</start_port>
        <end_port>65535</end_port>
        <starting_address>192.168.163.0</starting_address>
        <ending_address>192.168.163.255</ending_address>
      </cfg_ts>
      <cfg_automation>
        <ginamode>yes</ginamode>
      </cfg_automation>
      <cfg_remotesharing>
        <remotecomputer alias="XX">192.168.XX.XX</remotecomputer>
      </cfg_remotesharing>
      <suffixdomain>XX.suff</suffixdomain>
    </cfg_child_sa>
  </cfg_connectionv2>
</cfg_ikev2>
</tgbconfig>
```

6.2 Main tags

cfg_connectionv2

This tag is containing all the parameters for an IKEv2 Tunnel. The two main subtags are *cfg_ike_sa* and *cfg_child_sa*. Tag *cfg_ike_sa* is related to IKE SA INIT and IKE AUTH exchange and *cfg_child_sa* to a CHILD SA exchange. One tag must contain 1 unique cfg_ike_sa tag and 1 tag cfg_child_sa at least (read Tgbconfig.xsd for details about occurrences).

cfg_ike_sa

This tag is containing all the parameters for KE SA INIT and IKE AUTH exchanges. It is the equivalent of IKEv2 Phase1. The “name” attribute is the same than the “name” attribute in *cfg_connectionv2* tag.

XML attribute “family” must be set to “AF_AUTO”. Network family (IPv6 or IPv4) is automatically detected from “server” tag content.

cfg_child_sa

This tag is containing all the parameters for a CHILD SA exchange. This is equivalent of IKEv1 phase 2.

XML attribute “name” content must be unique.

XML attribute “family” can be “AF_INET” or “AF_INET6” and is related to the IPV4/IPV6 button in the interface.

When XML attribute “requestconfig” is set to “yes”, client IP address and remote network will be requested with CP payload.

Confidential, Property of TheGreenBow - Sistech SA - © 2001-2014

identity

If this tag is a child tag of cfg_ike_sa, it contains the identities of each endpoints. There must be 2 “identity” tags, one with “local” attribute and one with “remote” attribute.

By default, type “

authentication

All authentication methods are described with tag ”authentication”. Three types can be used within this tag :

- “preshared” if a preshared key is used as authentication method,
- “certificate” when certificates with RSA signature are used or
- “eap” if EAP is used

The attributes for this tag are:

- “multipleauth” if two authentications are used at the same time. It works only with type “eap” and “certificate”. This attribute value must be “yes”. By default, it is set to “no”.
- “sendcertrequest” if set to “yes” a CERT_REQ will be sent. Default value is “yes”.

If a preshared key is used the XML tag should look like:

```
<authentication type="preshared">
 <preshared>aaaa</preshared>
</authentication>
```

If certificates are used the XML tag should look like:

```
<authentication type="certificate" sendcertrequest="no">
   <certificate type="cacert" location="file">
     <public_key>
       -----BEGIN CERTIFICATE-----

       -----END CERTIFICATE-----
     </public_key>
   </certificate>
   <certificate type="user" location="file">
     <public_key>
       -----BEGIN CERTIFICATE-----

       -----END CERTIFICATE-----
     </public_key>
     <private_key>
       -----BEGIN RSA PRIVATE KEY-----

       -----END RSA PRIVATE KEY-----
     </private_key>
   </certificate>
</authentication>
```

If certificates are used the XML tag should look like:

```
<authentication type="eap">
  <cfg_eap type="EAP-MSCHAPV2" popup="yes" />
</authentication>
```

If login and password are stored in the file then the XML tags must be:

```
<authentication type="eap">
  <cfg_eap type="EAP-MSCHAPV2">
    <identity>my_login</identity>
    <secret>my_password</secret>
  </cfg_eap>
</authentication>
```


Confidential, Property of TheGreenBow - Sistech SA - © 2001-2014

The following example can be used for multiple authentication :

```
<authentication type="eap" multipleauth="yes" sendcertrequest="yes">
 <cfg_eap type="EAP-MSCHAPV2">
   <identity>sss</identity>
   <secret>sss</secret>
 </cfg_eap>
 <certificate type="user" location="file">
   <public_key>
     -----BEGIN CERTIFICATE-----

     -----END CERTIFICATE-----
   </public_key>
   <private_key>
     -----BEGIN RSA PRIVATE KEY-----

     -----END RSA PRIVATE KEY-----
   </private_key>
 </certificate>
</authentication>
```

cfg_sa

Tag cfg_sa contains the algorithm negociated between the two endpoints. It is used for generating SA payload. It can contain one or more proposals, each one in the same “proposal” tag.

The following example is used for IKE SA INIT echange. The 4 types are mandatory.

```
<cfg_sa>
  <proposal protocol="IKE">
    <transform type="ENCR_ALGO">3DES</transform>
    <transform type="PRF">PRF_HMAC_SHA1</transform>
    <transform type="INTEG">AUTH_HMAC_SHA1_96</transform>
    <transform type="DH_GROUP">DH_MODP_1024</transform>
  </proposal>
</cfg_sa>
```

For CHILD SA Exchange, the XML configuration should be as following. Transform types ENCR_ALGO, INTEG and ESN are mandatory. Transform type DH_GROUP is optional. These settings are also used during IKE AUTH exchange (any DH_GROUP transform will be then removed).

```
<cfg_sa>
  <proposal protocol="ESP">
    <transform type="ENCR_ALGO">3DES</transform>
    <transform type="INTEG">AUTH_HMAC_SHA1_96</transform>
    <transform type="ESN">NO_EXTENDED_SEQ_NUMBER</transform>
  </proposal>
</cfg_sa>
```

transform

"Transform" type requires the attribute "type" with simpleType "transformType". Accepted values for "transformType" are : ENCR_ALGO, PRF, INTEG, DH_GROUP and ESN. Each item of "transformType" required specific values.

If "transform" tag type is "ENCR_ALGO", related values are defined in simpleType "encryptionAlgoType".

If "transform" tag type is "INTEG", related values are defined in simpleType "authAlgoType".

If "transform" tag type is "PRF", related values are defined in simpleType "prfAlgoType".

If "transform" tag type is "DH_GROUP", related values are defined in simpleType "dhGroupType".

If "transform" tag type is "ESN", related values are defined in simpleType "esnAlgoType".

Confidential, Property of TheGreenBow - Sistech SA - © 2001-2014

cfg_ts

XML tag "cfg_ts" is used for traffic selector configuration. There must be two cfg_ts tags for each cfg_child_sa.

The XML attributes are:

- "type" with possible values "IPV4_ADDR_RANGE" and "IPV6_ADDR_RANGE".
- "location" must be set to "local" for one cfg_ts and "remote" for the other one.

The following configuration can be used for the client IP address. The starting and the ending address are the same.

```
<cfg_ts type="IPV4_ADDR_RANGE" location="local">
  <protocol>0</protocol>
  <start_port>0</start_port>
  <end_port>65535</end_port>
  <starting_address>10.10.4.2</starting_address>
  <ending_address>10.10.4.2</ending_address>
</cfg_ts>
```

If the configuration is requested from the gateway, the XML tags must be :

```
<cfg_ts type="IPV6_ADDR_RANGE" location="local">
  <protocol>0</protocol>
  <start_port>0</start_port>
  <end_port>65535</end_port>
  <starting_address>::</starting_address>
  <ending_address>::</ending_address>
</cfg_ts>
<cfg_ts type="IPV6_ADDR_RANGE" location="remote">
  <protocol>0</protocol>
  <start_port>0</start_port>
  <end_port>65535</end_port>
  <starting_address>::</starting_address>
  <ending_address>FFFF:FFFF:FFFF:FFFF:FFFF:FFFF:FFFF:FFFF
        </ending_address>
</cfg_ts>
```


Confidential, Property of TheGreenBow - Sistech SA - © 2001-2014

7 Header

The VPN Configuration file must have the following header:

 # SIGNATURE MD5 = xxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxx
 # Creation Date : yyyy-mm-dd at hh:mm:ss
 # Written by ProductName Version

It is very important to have 24 x for the MD5 value. If it doesn't the vpn configuration can be imported.

Creation Date is the current date when VPN Configuration is created. For example: 2011-06-20 at 11:26:14.
Written by section is by default VpnConf 6.10. If you use another ProductName please inform us.

Confidential, Property of TheGreenBow - Sistech SA - © 2001-2014

8 Restrictions

8.1 Phase1 or Phase 2 Name

- Size: 1 to 49 characters max.
- Phase1 name must be unique. 2 phases 1 with the same name is forbidden.
- Phase2 name must be unique. 2 phases 2 with the same name is forbidden.
- Characters strictly forbidden: dash (-), space ( ).

8.2 Phase1 Remote Gateway

- Size: 1 to 127 characters max.
- Characters allowed: "abcdefghijklmnopqrstuvwxyzABCDEFGHIJKLMNOPQRSTUVWXYZ0123456789.-"

8.3 Phase1 Advanced Redundant Gateway

- Size: 1 to 127 characters max.
- Characters allowed: "abcdefghijklmnopqrstuvwxyzABCDEFGHIJKLMNOPQRSTUVWXYZ0123456789.-"

8.4 Phase1 PreSharedKey

- Size: 1 to 511 characters max.
- Characters allowed: "abcdefghijklmnopqrstuvwxyzABCDEFGHIJKLMNOPQRSTUVWXYZ0123456789.-"
- Characters strictly forbidden: quote (") or backslash (\).

8.5 Phase1 other parameters

- XAuth login: 1 to 31 characters max.
- XAuth Password: 1 to 31 characters max.
- LocalID Name: 1 to 1021 characters max.
- RemoteID Name: 1 to 1021 characters max.

8.1 Phase2 scripts

- Size: limited to 259 characters max.

8.2 Phase2 Desktop Sharing Alias Name

- Size: 1 to 31 characters max.
- Characters strictly forbidden: quote ("), dash (-), semicolon (;) and colon (:).

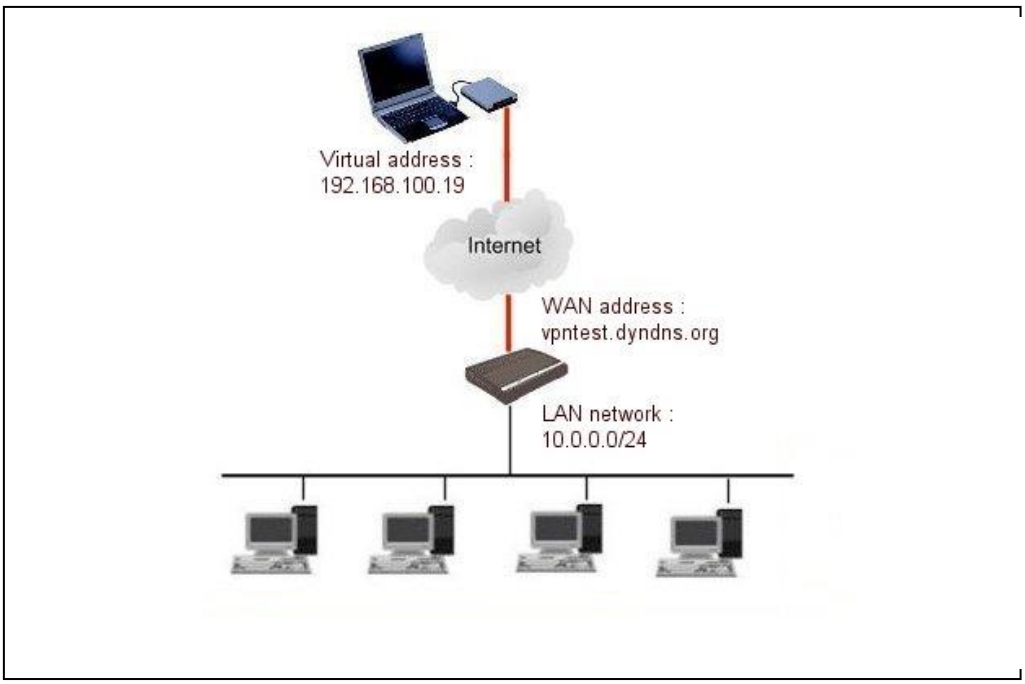
Confidential, Property of TheGreenBow - Sistech SA - © 2001-2014

9 Configuration File Sample

In this section, we provide a sample TgbVpn.conf file illustrating the network diagram shown below. We assume the following:

Gateway WAN address: vpntest.dyndns.org
ISAKMP Proposal: AES 128 – MD5 – GRP 1
IPSEC Proposal: AES 256 – SHA1 – GRP 2
Shared key: TheGreenBow

VPN client virtual IP address: 192.168.100.19
Remote network: 10.0.0.0/24



Sample network diagram

Confidential, Property of TheGreenBow - Sistech SA - © 2001-2014

TgbVpn.conf listening:

```
# SIGNATURE MD5 = xxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxx
# Creation Date : 2011-06-03 at 16:21:56
# Written by VpnConf 6.10
#

#  ===========
# Root sections
#  ===========

# Default phase 1 lifetime is 30 minutes, accepted range is 6 minutes to 8 hours.
# Tunnel establishment retries is 5. Whole exchange lifetime is 80 seconds.
[General]
Shared-SADB = Defined
Retransmits = 5
Exchange-max-time = 80
Default-phase-1-lifetime = 1800,360:28800
Bitblocking = 0
Xauth-interval = 20


# Default phase 2 lifetime is 20 minutes, accepted range is 5 minutes to 8 hours.
[Default-phase-2-lifetime]
LIFE_TYPE = SECONDS
LIFE_DURATION = 1200,300:28800


# Phase 1 connections list.
[Phase 1]
vpntest.dyndns.org = VpnTest1-P1

# Phase 2 connections list.
[Phase 2]
Passive-connections = VpnTest1-VpnTest2-P2


# =================
# Referred-to sections
# =================

# “VpnTest1-P1” configuration section :
#  Type : Phase 1 with a preshared key ( “TheGreenBow” ).
#  Remote peer address : vpntest.dyndns.org.
#  ISAKMP configuration section defined in “ VpnTest1-main-mode ”.
[VpnTest1-P1]
Phase = 1
Address = vpntest.dyndns.org
Transport = udp
Configuration = VpnTest1-main-mode
Authentication = TheGreenBow


# “VpnTest1-main-mode” configuration section :
# Type : Main Mode.
```


Confidential, Property of TheGreenBow - Sistech SA - © 2001-2014

```
# Proposal : “AES128-MD5-GRP1”.
[VpnTest1-main-mode]
DOI = IPSEC
EXCHANGE_TYPE = ID_PROT
Transforms = AES128-MD5-GRP1


# “AES128-MD5-GRP1” configuration section :
# Phase 1 proposal is AES128 – MD5 – Group 1.
[AES128-MD5-GRP1]
ENCRYPTION_ALGORITHM = AES_CBC
KEY_LENGTH = 128,128:256
HASH_ALGORITHM = MD5
GROUP_DESCRIPTION = MODP_768
AUTHENTICATION_METHOD = PRE_SHARED


# “VpnTest1-VpnTest2-P2” configuration section :
# Type : Phase 2 attached to “VpnTest1-P1” connection.
# Quick Mode section defined in VpnTest2-quick-mode.
# Local ID attributes defined in section “VpnTest2-local-addr”.
# Remote ID attributes defined in section “ VpnTest2-remote-addr ”.
[VpnTest1-VpnTest2-P2]
Phase = 2
ISAKMP-peer = VpnTest1-P1
Local-ID = VpnTest2-local-addr
Remote-ID = VpnTest2-remote-addr
Configuration = VpnTest2-quick-mode
AutoStart = 0
USBStart = 0
```


Confidential, Property of TheGreenBow - Sistech SA - © 2001-2014

```
# Local IPSEC ID :
# " VpnTest2-local-addr " defines an IP address 192.168.100.19.
[VpnTest2-local-addr]
ID-type = IPV4_ADDR
Address = 192.168.100.19


# Remote IPSEC ID :
# " VpnTest2-remote-addr " defines a subnet 10.0.0.0/24.
[VpnTest2-remote-addr]
ID-type = IPV4_ADDR_SUBNET
Network = 10.0.0.0
Netmask = 255.255.255.0


# "VpnTest2-quick-mode" quick mode configuration section :
# IPSEC suite defined in " VpnTest2-quick-mode-suite ".
[VpnTest2-quick-mode]
DOI = IPSEC
EXCHANGE_TYPE = QUICK_MODE
Suites = VpnTest2-quick-mode-suite


# " VpnTest2-quick-mode-suite " suite configuration section :
# IPSEC protocol defined in " TGBQM-ESP-AES256-SHA-PFSGRP2-TUN ".
[VpnTest2-quick-mode-suite]
Protocols = TGBQM-ESP-AES256-SHA-PFSGRP2-TUN

# "TGBQM-ESP-AES256-SHA-PFSGRP2-TUN" protocol configuration section :
# IPSEC protocol : ESP.
# IPSEC proposal defined in "TGBQM-ESP-AES256-SHA-PFSGRP2-TUN-XF ".
[TGBQM-ESP-AES256-SHA-PFSGRP2-TUN]
PROTOCOL_ID = IPSEC_ESP
Transforms = TGBQM-ESP-AES256-SHA-PFSGRP2-TUN-XF

# " TGBQM-ESP-AES256-SHA-PFSGRP2-TUN-XF " transform configuration section :
# IPSEC proposal  : AES128 – SHA – Group 2.
# Encapsulation : Tunnel mode.
# IPSEC SA lifetime defined in "Default-phase-2-lifetime".
[TGBQM-ESP-AES256-SHA-PFSGRP2-TUN-XF]
TRANSFORM_ID = AES
KEY_LENGTH = 256,128:256
AUTHENTICATION_ALGORITHM = HMAC_SHA
GROUP_DESCRIPTION = MODP_1024
ENCAPSULATION_MODE = TUNNEL
Life = Default-phase-2-lifetime
```


Confidential, Property of TheGreenBow - Sistech SA - © 2001-2014

10 Tgbconfig.xsd

```
<?xml version="1.0" encoding="UTF-8"?>
<xs:schema xmlns:xs="http://www.w3.org/2001/XMLSchema" elementFormDefault="qualified">
  <xs:simpleType name="authenticationType">
    <xs:restriction base="xs:string">
      <xs:enumeration value="eap" />
      <xs:enumeration value="preshared" />
      <xs:enumeration value="certificate" />
    </xs:restriction>
  </xs:simpleType>
  <xs:simpleType name="booleanType">
    <xs:restriction base="xs:string">
      <xs:enumeration value="yes" />
      <xs:enumeration value="no" />
    </xs:restriction>
  </xs:simpleType>
  <xs:simpleType name="certificateType">
    <xs:restriction base="xs:string">
      <xs:enumeration value="cacert" />
      <xs:enumeration value="user" />
    </xs:restriction>
  </xs:simpleType>
  <xs:simpleType name="certificateLocation">
    <xs:restriction base="xs:string">
      <xs:enumeration value="file" />
      <xs:enumeration value="smartcard" />
      <xs:enumeration value="winstore" />
    </xs:restriction>
  </xs:simpleType>
  <xs:simpleType name="identityType">
    <xs:restriction base="xs:string">
      <xs:enumeration value="ID_IPV4_ADDR" />
      <xs:enumeration value="ID_FQDN" />
      <xs:enumeration value="ID_RFC822_ADDR" />
      <xs:enumeration value="ID_IPV6_ADDR" />
      <xs:enumeration value="ID_DER_ASN1_DN" />
      <xs:enumeration value="ID_DER_ASN1_GN" />
      <xs:enumeration value="ID_KEY_ID" />
      <xs:enumeration value="ID_FC_NAME" />
    </xs:restriction>
  </xs:simpleType>
  <xs:simpleType name="locationType">
    <xs:restriction base="xs:string">
      <xs:enumeration value="remote" />
      <xs:enumeration value="local" />
    </xs:restriction>
  </xs:simpleType>
  <xs:simpleType name="protocolType">
    <xs:restriction base="xs:string">
      <xs:enumeration value="IKE" />
      <xs:enumeration value="ESP" />
    </xs:restriction>
  </xs:simpleType>
  <xs:simpleType name="familyType">
    <xs:restriction base="xs:string">
      <xs:enumeration value="AF_INET" />
      <xs:enumeration value="AF_INET6" />
    </xs:restriction>
  </xs:simpleType>
  <xs:simpleType name="tsType">
    <xs:restriction base="xs:string">
      <xs:enumeration value="IPV4_ADDR_RANGE" />
      <xs:enumeration value="IPV4_ADDR_SUBNET" />
      <xs:enumeration value="IPV6_ADDR_RANGE" />
      <xs:enumeration value="IPV6_ADDR_SUBNET" />
```


Confidential, Property of TheGreenBow - Sistech SA - © 2001-2014

```
    </xs:restriction>
  </xs:simpleType>
  <xs:simpleType name="transformType">
    <xs:restriction base="xs:string">
      <xs:enumeration value="ENCR_ALGO" />
      <xs:enumeration value="INTEG" />
      <xs:enumeration value="PRF" />
      <xs:enumeration value="DH_GROUP" />
      <xs:enumeration value="ESN" />
    </xs:restriction>
  </xs:simpleType>
  <xs:simpleType name="eapType">
    <xs:restriction base="xs:string">
      <xs:enumeration value="EAP-MSCHAPV2" />
    </xs:restriction>
  </xs:simpleType>
  <xs:simpleType name="yesnoautoType">
    <xs:restriction base="xs:string">
      <xs:enumeration value="yes" />
      <xs:enumeration value="no" />
      <xs:enumeration value="auto" />
    </xs:restriction>
  </xs:simpleType>
  <xs:simpleType name="dhGroupType">
    <xs:restriction base="xs:string">
      <xs:enumeration value="DH_MODP_768" />
      <xs:enumeration value="DH_MODP_1024" />
      <xs:enumeration value="DH_MODP_1536" />
      <xs:enumeration value="DH_MODP_2048" />
      <xs:enumeration value="DH_MODP_3072" />
      <xs:enumeration value="DH_MODP_4096" />
      <xs:enumeration value="DH_MODP_6144" />
      <xs:enumeration value="DH_MODP_8292" />
    </xs:restriction>
  </xs:simpleType>
  <xs:simpleType name="encryptionAlgoType">
    <xs:restriction base="xs:string">
      <xs:enumeration value="DES" />
      <xs:enumeration value="3DES" />
      <xs:enumeration value="AES_CBC" />
    </xs:restriction>
  </xs:simpleType>
  <xs:simpleType name="authAlgoType">
    <xs:restriction base="xs:string">
      <xs:enumeration value="AUTH_HMAC_MD5_96" />
      <xs:enumeration value="AUTH_HMAC_SHA1_96" />
      <xs:enumeration value="AUTH_HMAC_SHA2_256_128" />
      <xs:enumeration value="AUTH_HMAC_SHA2_384_192" />
      <xs:enumeration value="AUTH_HMAC_SHA2_512_256" />
    </xs:restriction>
  </xs:simpleType>
  <xs:simpleType name="prfAlgoType">
    <xs:restriction base="xs:string">
      <xs:enumeration value="PRF_HMAC_SHA1" />
      <xs:enumeration value="PRF_HMAC_MD5" />
      <xs:enumeration value="PRF_HMAC_SHA2_256" />
      <xs:enumeration value="PRF_HMAC_SHA2_384" />
      <xs:enumeration value="PRF_HMAC_SHA2_512" />
    </xs:restriction>
  </xs:simpleType>
  <xs:simpleType name="esnAlgoType">
    <xs:restriction base="xs:string">
      <xs:enumeration value="NO_EXTENDED_SEQ_NUMBER" />
    </xs:restriction>
  </xs:simpleType>
  <xs:element name="tgbconfig">
    <xs:complexType>
      <xs:sequence>
```


Confidential, Property of TheGreenBow - Sistech SA - © 2001-2014

```
      <xs:element ref="cfg_ikev2" />
    </xs:sequence>
  </xs:complexType>
</xs:element>
<xs:element name="cfg_ikev2">
  <xs:complexType>
    <xs:sequence>
      <xs:element maxOccurs="unbounded" ref="cfg_connectionv2" />
    </xs:sequence>
  </xs:complexType>
</xs:element>
<xs:element name="cfg_connectionv2">
  <xs:complexType>
    <xs:sequence>
      <xs:element ref="cfg_ike_sa" />
      <xs:element maxOccurs="unbounded" ref="cfg_child_sa" />
    </xs:sequence>
    <xs:attribute name="name" use="required" type="xs:NCName" />
  </xs:complexType>
</xs:element>
<xs:element name="cfg_ike_sa">
  <xs:complexType>
    <xs:sequence>
      <xs:element ref="server" />
      <xs:element minOccurs="0" ref="interfacename" />
      <xs:element minOccurs="0" ref="redundant_server" />
      <xs:element ref="port" />
      <xs:element ref="port_nat" />
      <xs:element minOccurs="0" ref="ikeinit_lifetime" />
      <xs:element ref="ikeauth_lifetime" />
      <xs:element ref="retries" />
      <xs:element ref="cfg_dpd" />
      <xs:element ref="cfg_sa" />
      <xs:element minOccurs="2" maxOccurs="2" ref="identity" />
      <xs:element ref="authentication" />
    </xs:sequence>
    <xs:attribute name="family" use="required" type="xs:NCName" fixed="AF_AUTO" />
    <xs:attribute name="name" use="required" type="xs:NCName" />
  </xs:complexType>
</xs:element>
<xs:element name="server" type="xs:NMTOKEN" />
<xs:element name="interfacename" type="xs:NMTOKEN" />
<xs:element name="redundant_server" type="xs:NMTOKEN" />
<xs:element name="port" type="xs:integer" default="500" />
<xs:element name="port_nat" type="xs:integer" default="4500" />
<xs:element name="ikeauth_lifetime" type="xs:integer" default="1800" />
<xs:element name="ikeinit_lifetime" type="xs:integer" default="0" />
<xs:element name="retries" type="xs:integer" default="3" />
<xs:element name="cfg_dpd">
  <xs:complexType>
    <xs:sequence>
      <xs:element ref="interval" />
      <xs:element ref="retrans" />
      <xs:element ref="wait" />
    </xs:sequence>
  </xs:complexType>
</xs:element>
<xs:element name="interval" type="xs:integer" default="30" />
<xs:element name="retrans" type="xs:integer" default="5" />
<xs:element name="wait" type="xs:integer" default="15" />
<xs:element name="cfg_child_sa">
  <xs:complexType>
    <xs:sequence>
      <xs:element ref="childsa_lifetime" />
      <xs:element ref="cfg_sa" />
      <xs:element minOccurs="2" maxOccurs="2" ref="cfg_ts" />
      <xs:element ref="cfg_automation" />
      <xs:element ref="cfg_remotesharing" />
```


Confidential, Property of TheGreenBow - Sistech SA - © 2001-2014

```
      </xs:sequence>
      <xs:attribute name="family" use="required" type="familyType" />
      <xs:attribute name="name" use="required" type="xs:NCName" />
      <xs:attribute name="trafficdetection" type="booleanType" />
    </xs:complexType>
  </xs:element>
  <xs:element name="childsa_lifetime" type="xs:integer" default="1200" />
  <xs:element name="cfg_ts">
    <xs:complexType>
      <xs:sequence>
        <xs:element ref="protocol" />
        <xs:element ref="start_port" />
        <xs:element ref="end_port" />
        <xs:element ref="starting_address" />
        <xs:element ref="ending_address" />
      </xs:sequence>
      <xs:attribute name="location" use="required" type="locationType" />
      <xs:attribute name="type" use="required" type="tsType" />
    </xs:complexType>
  </xs:element>
  <xs:element name="protocol" type="xs:integer" default="0" />
  <xs:element name="start_port" type="xs:integer" default="0" />
  <xs:element name="end_port" type="xs:integer" default="65535" />
  <xs:element name="starting_address" type="xs:NMTOKEN" />
  <xs:element name="ending_address" type="xs:NMTOKEN" />
  <xs:element name="cfg_sa">
    <xs:complexType>
      <xs:sequence>
        <xs:element ref="proposal" />
      </xs:sequence>
    </xs:complexType>
  </xs:element>
  <xs:element name="proposal">
    <xs:complexType>
      <xs:sequence>
        <xs:element maxOccurs="unbounded" ref="transform" />
      </xs:sequence>
      <xs:attribute name="protocol" use="required" type="xs:NCName" />
    </xs:complexType>
  </xs:element>
  <xs:element name="transform">
    <xs:complexType>
      <xs:simpleContent>
        <xs:extension base="xs:NMTOKEN">
          <xs:attribute name="keylength" type="xs:integer" />
          <xs:attribute name="type" use="required" type="transformType" />
        </xs:extension>
      </xs:simpleContent>
    </xs:complexType>
  </xs:element>
  <xs:element name="identity">
    <xs:complexType mixed="true">
      <xs:attribute name="location" type="locationType" />
      <xs:attribute name="type" type="identityType" />
    </xs:complexType>
  </xs:element>
  <xs:element name="authentication">
    <xs:complexType>
      <xs:choice>
        <xs:sequence>
          <xs:element ref="cfg_eap" />
          <xs:element minOccurs="0" maxOccurs="unbounded" ref="certificate" />
        </xs:sequence>
        <xs:element ref="preshared" />
        <xs:element maxOccurs="unbounded" ref="certificate" />
      </xs:choice>
      <xs:attribute name="multipleauth" type="booleanType" />
      <xs:attribute name="sendcertrequest" use="required" type="booleanType" />
```


Confidential, Property of TheGreenBow - Sistech SA - © 2001-2014

```
      <xs:attribute name="type" use="required" type="authenticationType" />
    </xs:complexType>
  </xs:element>
  <xs:element name="cfg_eap">
    <xs:complexType>
      <xs:sequence minOccurs="0">
        <xs:element ref="identity" />
        <xs:element ref="secret" />
      </xs:sequence>
      <xs:attribute name="popup" type="xs:NCName" />
      <xs:attribute name="type" use="required" type="xs:NCName" />
    </xs:complexType>
  </xs:element>
  <xs:element name="secret" type="xs:NMTOKEN" />
  <xs:element name="preshared" type="xs:NMTOKEN" />
  <xs:element name="certificate">
    <xs:complexType>
      <xs:sequence>
        <xs:element ref="public_key" />
        <xs:element minOccurs="0" ref="private_key" />
        <xs:element minOccurs="0" ref="subject" />
      </xs:sequence>
      <xs:attribute name="location" use="required" type="certificateLocation" />
      <xs:attribute name="type" use="required" type="certificateType" />
    </xs:complexType>
  </xs:element>
  <xs:element name="public_key" type="xs:string" />
  <xs:element name="private_key" type="xs:string" />
  <xs:element name="subject" type="xs:string" />
  <xs:element name="cfg_automation">
    <xs:complexType>
      <xs:sequence>
        <xs:choice>
          <xs:element minOccurs="0" ref="ginamode" />
          <xs:sequence>
            <xs:element minOccurs="0" ref="openscriptafterup" />
            <xs:element minOccurs="0" ref="openscriptbeforeup" />
            <xs:element minOccurs="0" ref="openscriptafterdown" />
            <xs:element minOccurs="0" ref="openscriptbeforedown" />
          </xs:sequence>
        </xs:choice>
        <xs:element minOccurs="0" ref="autostart" />
        <xs:element minOccurs="0" ref="usbstart" />
        <xs:element minOccurs="0" ref="trafficdetection" />
      </xs:sequence>
    </xs:complexType>
  </xs:element>
  <xs:element name="openscriptafterup" type="xs:string" />
  <xs:element name="openscriptbeforeup" type="xs:string" />
  <xs:element name="openscriptafterdown" type="xs:string" />
  <xs:element name="openscriptbeforedown" type="xs:string" />
  <xs:element name="autostart" type="booleanType" default="no" />
  <xs:element name="usbstart" type="booleanType" default="no" />
  <xs:element name="trafficdetection" type="booleanType" default="no" />
  <xs:element name="ginamode" type="booleanType" default="no" />
  <xs:element name="cfg_remotesharing">
    <xs:complexType>
      <xs:sequence>
        <xs:element minOccurs="0" maxOccurs="unbounded" ref="remotecomputer" />
      </xs:sequence>
    </xs:complexType>
  </xs:element>
  <xs:element name="remotecomputer">
    <xs:complexType>
      <xs:simpleContent>
        <xs:extension base="xs:NMTOKEN">
          <xs:attribute name="alias" use="required" type="xs:NCName" />
        </xs:extension>
```


Confidential, Property of TheGreenBow - Sistech SA - © 2001-2014

```
      </xs:simpleContent>
    </xs:complexType>
  </xs:element>
</xs:schema>
```


Confidential, Property of TheGreenBow - Sistech SA - © 2001-2014