



Cyberoam Configuration Guide for VPNC Interoperability Testing using DES Encryption Algorithm

Document Version:2.0-12/07/2007

IMPORTANT NOTICE

Elitecore has supplied this Information believing it to be accurate and reliable at the time of printing, but is presented without warranty of any kind, expressed or implied. Users must take full responsibility for their application of any products. Elitecore assumes no responsibility for any errors that may appear in this document. Elitecore reserves the right, without notice to make changes in product design or specifications. Information is subject to change without notice.

USER'S LICENSE

The Appliance described in this document is furnished under the terms of Elitecore's End User license agreement. Please read these terms and conditions carefully before using the Appliance. By using this Appliance, you agree to be bound by the terms and conditions of this license. If you do not agree with the terms of this license, promptly return the unused Appliance and manual (with proof of payment) to the place of purchase for a full refund.

LIMITED WARRANTY

Software: Elitecore warrants for a period of ninety (90) days from the date of shipment from Elitecore: (1) the media on which the Software is furnished will be free of defects in materials and workmanship under normal use; and (2) the Software substantially conforms to its published specifications except for the foregoing, the software is provided AS IS. This limited warranty extends only to the customer as the original licenses. Customers exclusive remedy and the entire liability of Elitecore and its suppliers under this warranty will be, at Elitecore or its service center's option, repair, replacement, or refund of the software if reported (or, upon, request, returned) to the party supplying the software to the customer. In no event does Elitecore warrant that the Software is error free, or that the customer will be able to operate the software without problems or interruptions. Elitecore hereby declares that the anti virus and anti spam modules are powered by Kaspersky Labs and the performance thereof is under warranty provided by Kaspersky Labs. It is specified that Kaspersky Lab does not warrant that the Software identifies all known viruses, nor that the Software will not occasionally erroneously report a virus in a title not infected by that virus.

Hardware: Elitecore warrants that the Hardware portion of the Elitecore Products excluding power supplies, fans and electrical components will be free from material defects in workmanship and materials for a period of One (1) year. Elitecore's sole obligation shall be to repair or replace the defective Hardware at no charge to the original owner. The replacement Hardware need not be new or of an identical make, model or part; Elitecore may, in its discretion, replace the defective Hardware (or any part thereof) with any reconditioned product that Elitecore reasonably determines is substantially equivalent (or superior) in all material respects to the defective Hardware.

DISCLAIMER OF WARRANTY

Except as specified in this warranty, all expressed or implied conditions, representations, and warranties including, without limitation, any implied warranty or merchantability, fitness for a particular purpose, non-infringement or arising from a course of dealing, usage, or trade practice, and hereby excluded to the extent allowed by applicable law.

In no event will Elitecore or its supplier be liable for any lost revenue, profit, or data, or for special, indirect, consequential, incidental, or punitive damages however caused and regardless of the theory of liability arising out of the use of or inability to use the product even if Elitecore or its suppliers have been advised of the possibility of such damages. In the event shall Elitecore's or its supplier's liability to the customer, whether in contract, tort (including negligence) or otherwise, exceed the price paid by the customer. The foregoing limitations shall apply even if the above stated warranty fails of its essential purpose.

In no event shall Elitecore or its supplier be liable for any indirect, special, consequential, or incidental damages, including, without limitation, lost profits or loss or damage to data arising out of the use or inability to use this manual, even if Elitecore or its suppliers have been advised of the possibility of such damages.

RESTRICTED RIGHTS

Copyright 2000 Elitecore Technologies Ltd. All rights reserved. Cyberoam, Cyberoam logo are trademark of Elitecore Technologies Ltd. Information supplies by Elitecore Technologies Ltd. Is believed to be accurate and reliable at the time of printing, but Elitecore Technologies assumes no responsibility for any errors that may appear in this documents. Elitecore Technologies reserves the right, without notice, to make changes in product design or specifications. Information is subject to change without notice

CORPORATE HEADQUARTERS

Elitecore Technologies Ltd.
904 Silicon Tower,
Off. C.G. Road,
Ahmedabad – 380015, INDIA
Phone: +91-79-66065606
Fax: +91-79-26407640
Web site: www.elitecore.com , www.cyberoam.com

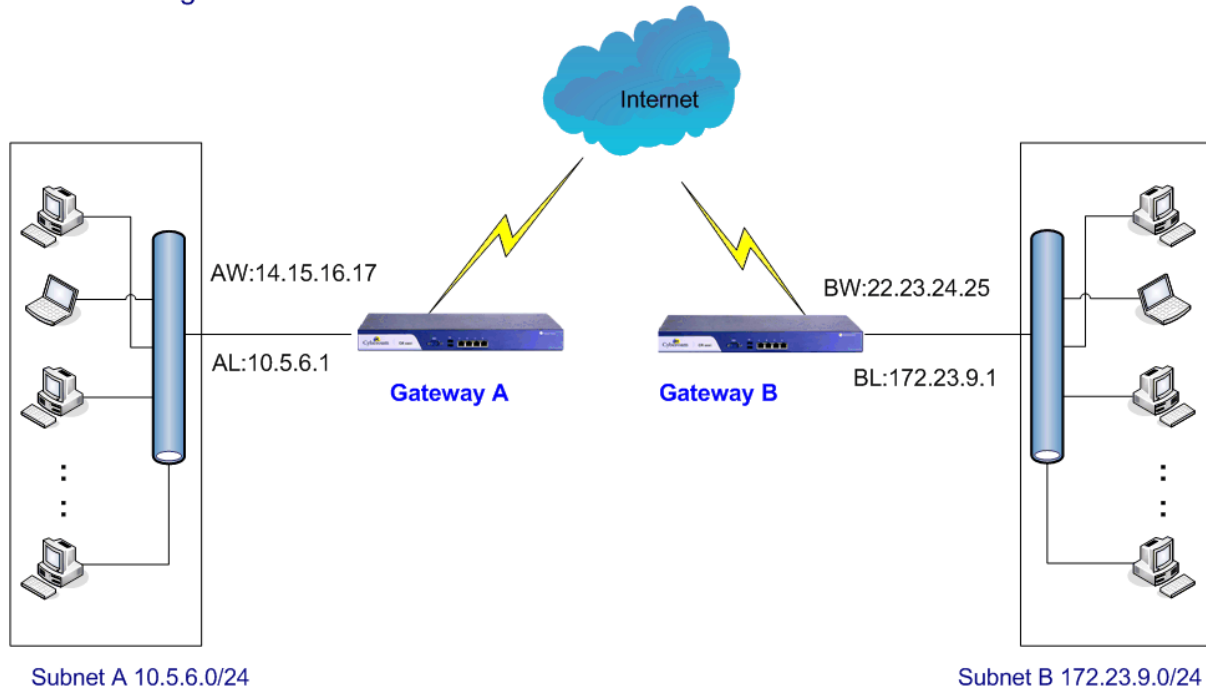
Contents

Scenario 1: Gateway-to-Gateway with preshared secrets	4
Step-by-Step Configuration Gateway A	5
Diagnostics	6
Scenario 2: Gateway-to-Gateway with Digital Certificates.....	7
Case I: Peers are using different CAs i.e. Gateway A and Gateway B are using different CAs....	8
Step-by-Step Configuration of Gateway A	8
Diagnostics	9
Case II: Peers are using trusted third party CA e.g. Verisign, Microsoft	10
Step-by-Step Configuration of Gateway A	10
Diagnostics	11

Scenario 1: Gateway-to-Gateway with preshared secrets

The following is a typical gateway-to-gateway VPN that uses a preshared secret for authentication.

Network diagram



Gateway A connects the internal LAN 10.5.6.0/24 to the Internet. Gateway A's LAN interface has the address 10.5.6.1, and its WAN (Internet) interface has the address 14.15.16.17.

Gateway B connects the internal LAN 172.23.9.0/24 to the Internet. Gateway B's WAN (Internet) interface has the address 22.23.24.25. Gateway B's LAN interface address, 172.23.9.1, can be used for testing IPsec but is not needed for configuring Gateway A.

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

Step-by-Step Configuration Gateway A

Log on to Gateway A using Web Admin Console and follow the steps:

Step 1: Create VPN Policy

Go to VPN → Policy → Create Policy and create VPN policy with following values:

Policy Name: CRA-2-CRB
Using Template: None
Keying Method: Automatic
Allow Re-keying: Yes
Key Negotiation Tries: 3
Pass Data in Compressed Format: No
Perfect Forward Secrecy (PFS): Yes

Phase 1

Encryption Algorithm: 3DES Authentication Algorithm: SHA1
DH Group (Key Group): 2 (DH1024)
Key life: 28800 sec

Phase 2

Encryption Algorithm: 3DES Authentication Algorithm: SHA1
DH Group (Key Group): 2 (DH1024)
Key life: 3600 sec

Step 2: Create IPSec connection

Go to VPN → IPSec Connection → Create Connection and create connection with the following values:

Connection name: n2n_CRB
Policy: CRA-2-CRB
Action on restart: Active
Mode: Tunnel
Connection Type: Net to Net

Authentication Type: Preshared Key
Preshared Key: hr5xb84l6aa9r6


Local server IP address (WAN IP address): 14.15.16.17
Local Internal Network: 10.5.6.0/24

Remote server IP address (WAN IP address): 22.23.24.25
Remote Internal Network: 172.23.9.0/24


User Authentication Mode: Disabled
Protocol: All


Step 3: Activate Connection

Go to VPN → IPSec Connection → Manage Connection and click  against the n2n_CRB connection.

-  Under the Connection status indicates that the connection is successfully activated

Step 4: Establish Connection

To establish connection from Gateway A, go to VPN → IPsec Connection → Manage Connection and click  against the connection

-  under the Connection status indicates that the connection is successfully established.

Diagnostics

If you are not able to establish the connection, check VPN log from Telnet Console.

- Log on to Telnet Console using command:
telnet <Gateway IP address>
- Type 8 in Select Menu number field to go to option “VPN Management”

```

Main Menu
AA. Appliance Activation
00. Cyberoam Configuration Wizard
R. Restart Management Services
1. Network Configuration
2. System Configuration
3. Route Configuration
4. Cyberoam Console
5. Cyberoam Management
6. Upgrade Version
7. Bandwidth Monitor
8. VPN Management
9. Shutdown/Reboot Cyberoam
0. Exit

Select Menu Number [0-9]: 8

```

- Type 3 in Select Menu number field to go to option “View VPN Logs”

```

VPN Management Menu
-----
Main Menu

1. Regenerate RSA Key
2. Restart VPN Service
3. View VPN Logs
4. View Connection Wise VPN Logs
5. Advance VPN Logs
6. PPTP VPN Logs
0. Exit

Select Menu Number [0-6]: 3_

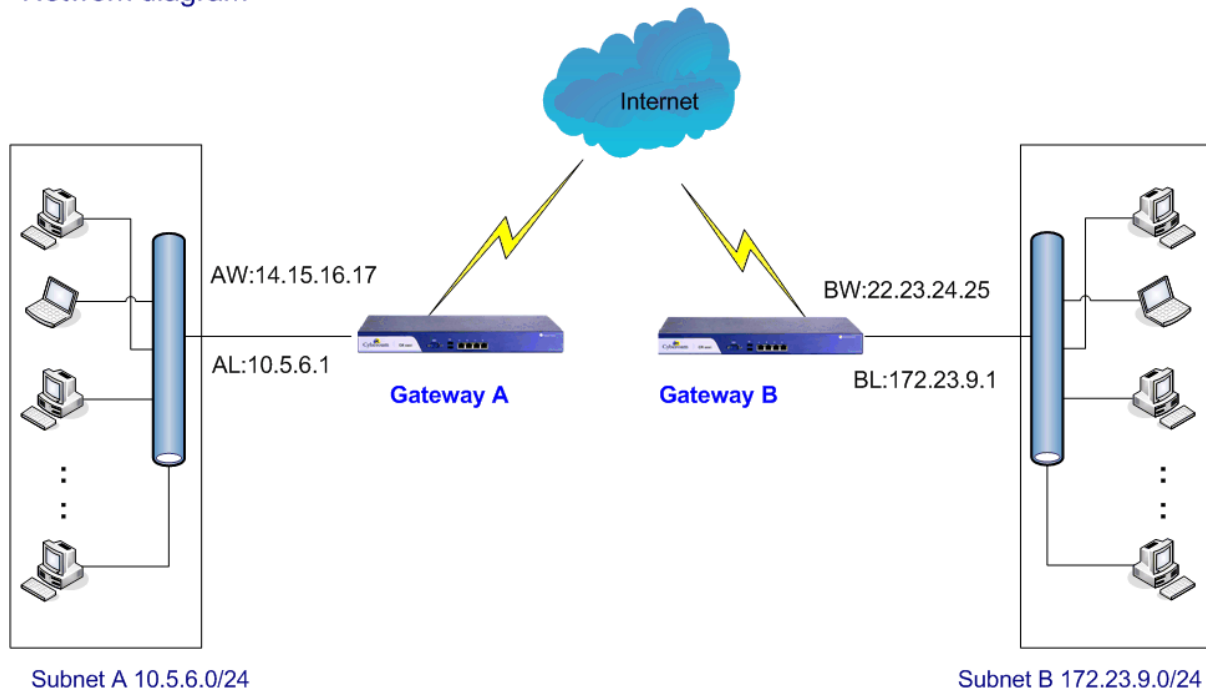
```

Refer to <http://kb.cyberoam.com/default.asp?id=305&Lang=1&SID=> for understanding logs and troubleshooting.

Scenario 2: Gateway-to-Gateway with Digital Certificates

The following is a typical gateway-to-gateway VPN that uses a digital certificate for authentication.

Network diagram



Gateway A connects the internal LAN 10.5.6.0/24 to the Internet. Gateway A's LAN interface has the address 10.5.6.1, and its WAN (Internet) interface has the address 14.15.16.17.

Gateway B connects the internal LAN 172.23.9.0/24 to the Internet. Gateway B's WAN (Internet) interface has the address 22.23.24.25. Gateway B's LAN interface address, 172.23.9.1, can be used for testing IPsec but is not needed for configuring Gateway A.

The IKE Phase 1 parameters used in Scenario 1 are:

- Main mode
- TripleDES
- SHA-1
- MODP group 2 (1024 bits)
- Authentication with signatures authenticated by PKIX certificates; both Gateway A and Gateway B have end-entity certificates that chain to a root authority called "Trusted Root CA"
- 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

Following sections are included:

- [Case I – Peers using different CA](#)
- [Case II – Peers using Same CA](#)

Case I: Peers are using different CAs i.e. Gateway A and Gateway B are using different CAs

Step-by-Step Configuration of Gateway A

Log on to Gateway A using Web Admin Console and follow the steps:

Step 1. Generate CA

Go to VPN → Certificate Authority → Manage Certificate Authority and

Click Default certificate authority. If you are generating CA for the first time, enter complete details as required else modify details if required.

Click Generate/Re-generate

Step 2. Download CA generated in step 1 and forward to the Gateway B.

Go to VPN → Certificate Authority → Manage Certificate Authority

Click Default certificate authority

Click Download. CA is downloaded in tar.gz format. One can unzip the file using winzip or winrar.

This CA is to be uploaded at Gateway B.

Step 3. Obtain and Upload Remote Certificate Authority i.e. CA of Gateway B

Unzip the CA received from the Remote user to extract two files: default.pem and default.der

Go to VPN → Certificate Authority → Upload Certificate Authority

Step 4. Generate Local Certificate

Go to VPN → Certificate → New Certificate and click Self Signed Certificate to create certificate. Create certificate with the following value:

Certificate name: AHMD_cert

Valid upto: Specify as per your requirement

Key length: Specify as per your requirement

Password: Specify as per your requirement

Certificate ID (Email): john@e*****.com

Step 5. Download Default CRL and forward to Gateway B

Go to VPN → Certificate Authority → Manage CRL

Click Download

This CRL is to be uploaded at Gateway B.

Step 6. Obtain and Upload CRL of Gateway B

Go to VPN → Certificate Authority → Upload CRL

CRL Name: Specify as per your requirement

CRL File: Provide file path of the CRL of Gateway B

Step 7. Create IPSec connection

Go to VPN → IPSec Connection → Create Connection and create connection with the following values:

Connection name: n2n_AHMD
 Policy: Default Policy
 Action on restart: Active
 Mode: Tunnel
 Connection Type: Net to Net


Authentication Type: Digital Certificate
 Local Certificate: Select Certificate created in step 4 i.e. AHMD_cert
 Remote Certificate: Select 'External Certificate'. Alternately if certificate DLH_cert used by Gateway B is available on Gateway A, you can select that certificate.

Local server IP address (WAN IP address): 14.15.16.17
 Local Internal Network: 10.5.6.0/24
 Local ID: Automatically displays ID specified in the Local certificate created in step 4 i.e. john@e*****.com

Remote server IP address (WAN IP address): 22.23.24.25
 Remote Internal Network: 172.23.9.0/24
 Remote ID: dean@e*****.com (provided by Gateway B Administrator)

User Authentication Mode: Disabled
 Protocol: All


Step 8. Activate Connection

Go to VPN → IPSec Connection → Manage Connection and click  against the n2n_AHMD connection.



under the Connection status indicates that the connection is successfully activated

Step 9. Establish Connection

To establish connection from Gateway A, go to VPN → IPSec Connection → Manage Connection and click  against the connection



under the Connection status indicates that the connection is successfully established.

Diagnostics

Same as Scenario 1

Case II: Peers are using trusted third party CA e.g. Verisign, Microsoft

Step-by-Step Configuration of Gateway A

Log on to Gateway A using Web Admin Console and follow the steps:

Step 1. Obtain and upload third party CA

Go to VPN → Certificate Authority → Upload Certificate Authority

Certificate Authority Name: Specify as per your requirement

Certificate Format: As provided by third party CA

Certificate: File path of third party CA

Click Upload

Step 2. Obtain and Upload Certificate from third party CA

Go to VPN → Certificate → New Certificate and click Upload Certificate

Certificate name: Specify as per your requirement

Password: Specify as per your requirement

Confirm Password: Same as specified in Password field

Certificate: File path of Certificate

Private Key: File path for Private key

Step 3. Obtain and Upload CRL from third party CA

Go to VPN → Certificate Authority → Upload CRL

CRL Name: Specify as per your requirement

CRL File: File path of the CRL

Step 4. Create IPSec connection

Go to VPN → IPSec Connection → Create Connection and create connection with the following values:

Connection name: n2n_AHMD

Policy: Default Policy

Action on restart: Active

Mode: Tunnel

Connection Type: Net to Net

Authentication Type: Digital Certificate

Local Certificate: Select Certificate uploaded in step 2

Remote Certificate: Select "External Certificate"

Local server IP address (WAN IP address): 14.15.16.17

Local Internal Network: 10.5.6.0/24

Local ID: Automatically displays ID specified in the Local certificate uploaded in step 2 i.e. john@e****.com

Remote server IP address (WAN IP address): 22.23.24.25


Remote Internal Network: 172.23.9.0/24


Remote ID: dean@e*****.com (Provided by Gateway B Administrator)

User Authentication Mode: Disabled


Protocol: All


Step 5. Activate Connection

Go to VPN → IPSec Connection → Manage Connection and click  against the n2n_AHMD connection.

 under the Connection status indicates that the connection is successfully activated

Step 6. Establish Connection

To establish connection from Gateway A, go to VPN → IPSec Connection → Manage Connection and click  against the connection

 under the Connection status indicates that the connection is successfully established.

Diagnostics

Same as Scenario 1