Cyberoam
Unified Threat Management

VPN Management Guide

Version 10

Document version 10.0-1.0-06/03/2010

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 Commtouch respectively and the performance thereof is under warranty provided by Kaspersky Labs and by Commtouch. 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 no 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

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

Technical Support

You may direct all questions, comments, or requests concerning the software you purchased, your registration status, or similar issues to Customer care/service department at the following address:

Corporate Office
eLitecore Technologies Ltd.
904, Silicon Tower
Off C.G. Road
Ahmedabad 380015
Gujarat, India.
Phone: +91-79-66065606
Fax: +91-79-26462200
Web site: www.elitecore.com

Cyberoam contact:
Technical support (Corporate Office): +91-79-26400707
Email: support@cyberoam.com
Web site: www.elitecore.com

Visit www.cyberoam.com for the regional and latest contact information.

Typographic Conventions

Material in this manual is presented in text, screen displays, or command-line notation.

Item	Convention	Example
Server		Machine where Cyberoam Software - Server component is installed
Client		Machine where Cyberoam Software - Client component is installed
User		The end user
Username		Username uniquely identifies the user of the system
Part titles	Bold and shaded font typefaces	**Report**
Topic titles	Shaded font typefaces	Introduction
Subtitles	Bold & Black typefaces	**Notation conventions**
Navigation link	Bold typeface	**Group Management → Groups → Create** it means, to open the required page click on Group management then on Groups and finally click Create tab
Name of a particular parameter / field / command button text	Lowercase italic type	Enter policy name, replace policy name with the specific name of a policy Or Click Name to select where Name denotes command button text which is to be clicked
Cross references	Hyperlink in different color	refer to Customizing User database Clicking on the link will open the particular topic
Notes & points to remember	Bold typeface between the black borders	**Note**
Prerequisites	Bold typefaces between the black borders	Prerequisite • Prerequisite details

Overview

Welcome to the Cyberoam's – VPN Management Guide.

Cyberoam's integrated Internet security solution is purpose-built to meet the unified threat management needs of corporate, government organizations and educational institutions. It also provides assistance in improving Bandwidth management, increasing Employee productivity, and reducing legal liability associated with undesirable Internet content access.

Guide provides a basic introduction to VPN and gives some fundamental information of those technologies that are relevant to the way Cyberoam implements VPN. It outlines how VPN tunnel is actually created and gives a detailed picture of the different settings that can be used to adjust the VPN policies using Cyberoam.

Introduction to VPN

A Virtual Private Network (VPN) is a tunnel that carries private network traffic from one endpoint system to another over a public network such as the Internet without the traffic being aware that there are intermediate hops between the endpoints or the intermediate hops being aware they are carrying the network packets that are traversing the tunnel. The tunnel may optionally compress and/or encrypt the data, providing enhanced performance and some measure of security.

VPN allows you to pretend you are using a leased line or a direct telephone call to communicate between the endpoints.

VPN allow users and telecommuters to connect to their corporate intranets or extranets. VPN is cost-effective because users can connect to the Internet locally and tunnel back to connect to corporate resources. This not only reduces overhead costs associated with traditional remote access methods, but also improves flexibility and scalability.

Cyberoam and VPN

For all business people traveling or working from home, connecting securely to the corporate network is essential. With Cyberoam, setting up a VPN is almost effortless.

The two endpoints in Cyberoam VPN are referred to as:

Local - First endpoint is the local machine itself

Remote - Second endpoint is the remote peer - the machine you are trying to establish a VPN connection to, or the machine which is trying to establish a VPN connection with you.

Cyberoam VPN automatically encrypts the data and sends it to the remote site over the Internet, where it is automatically decrypted and forwarded to the intended destination. By encrypting, the integrity and confidentiality of data is protected even when transmitted over the untrusted public network. Cyberoam uses IPSec standard i.e. IPSec protocol to protect traffic. In IPSec, the identity of communicating users is checked with the user authentication based on digital certificates, public keys or preshared keys.

Cyberoam ensures that all the VPN traffic passing through the VPN tunnels is threat free. All the firewall rules and policies are applicable to the traffic going into the VPN tunnels and coming out of the VPN tunnels. Cyberoam inspects all the traffic going into the VPN tunnels and coming out of the tunnels and makes sure that there are no viruses, worms, spam, and inappropriate content or intrusion attempts in the VPN traffic. As VPN traffic is, by default subjected to the DoS inspection, Cyberoam provides a facility by which one can bypass scanning of traffic coming from certain hosts from VPN zone. The above functionality is achieved by adding one additional zone called VPN zone. VPN traffic passes through VPN zone and firewall rule can be applied to VPN zone.

Cyberoam can be used to establish VPN connection between sites, LAN-to-LAN and Client-to-LAN connection. VPN is the bridge between Local & Remote networks/subnets.

Cyberoam supports following protocols to authenticate and encrypt traffic:

- Internet Protocol Security (IPSec)
- Layer Two Tunneling Protocol (L2TP)
- Point-to-Point Tunneling Protocol (PPTP)

Note

VPN is not supported when Cyberoam is deployed as Bridge. Hence when you change the deployment mode from Gateway to Bridge mode, Cyberoam will delete all the custom and default firewall rules for VPN zone, dynamic hosts and hosts groups, virtual hosts mapped to VPN zone, VPN zone from Local ACL

Policy

Encryption and Authentication method

Authentication of communicating parties and integrity of exchanged data is crucial for the reliable implementation of VPN.

Encryption is used to provide confidentiality of data during the negotiation. Cyberoam supports 3DES encryption algorithm which is extensively tested public algorithm and uses hash functions - message digest MD5 algorithm for Data integrity.

3DES: Triple DES is a symmetric strong encryption algorithm that is compliant with the OpenPGP standard. It is the Application of the DES standard where three keys are used in succession to provide additional security.

AES: Advanced Encryption Standard AES offers the highest standard of security. The effective key lengths that can be used with AES are 128, 192 and 256 Bits.

This security system supports a number of encryption algorithms.

Serpent: Serpent is a 128-bit block cipher i.e. data is encrypted and decrypted in 128-bit chunks variable key length to be 128, 192, or 256 bits. The Serpent algorithm uses 32 rounds, or iterations of the main algorithm.

Serpent is faster than DES and more secure than Triple DES.

Blowfish: Blowfish is a symmetric encryption algorithm which uses the same secret key to both encrypt and decrypt messages. Blowfish is also a block cipher which divides a message into fixed length blocks during encryption and decryption. Blowfish has a 64-bit block size and a key length of anywhere from 32 bits to 448 bits and uses 16 rounds of main algorithm

Twofish: Twofish is a symmetric key block cipher with a block size of 128 bits and key sizes up to 256 bits.

Preshared Key

An authentication mechanism whereby the key is used in encryption is exchanged before hand/prior to negotiation with another system.

Preshared key authentication is the process by which two systems prove their identity to each other where each system encrypts some unpredictable, arbitrary data with a key that has been exchanged beforehand. If they can successfully decrypt the message, it is assumed that the sender is valid.

A single shared key is used for encryption and decryption. The data is encrypted by a key and send to the recipient over the Internet. At the receiving end, the data is decrypted with the exact same key that was used for encryption.

Digital Certificates

Digital Certificates are yet another authentication method employing digital signatures and public key cryptography.

A digital certificate is a document that guarantees the identity of a person or entity and is issued by the trusted third party Certificate Authority (CA). Digital certificate holders have a public or private key pair which can be used to authenticate the sender and decrypt the incoming message ensuring that only the certificate holder can decode the message.

A certificate is used to associate a public/private key pair with a given IP address or host name and issued by CA for a specific period of time. A CA can be in-house CA, run by your own organization, or a public CA. To use certificates for negotiation, both peers have to generate public/private key pairs, request, and receive public key certificates, and are configured to trust the CA that issues the certificates.

Users can download and install certificate from Cyberoam.

Public Key

Public key authentication uses two keys – public key available to anyone and a private key held by only one individual. The sender encrypts the data with the recipient’s public key. Only the recipient can decrypt the data, being the only one who possesses the corresponding private key.

VPN Policy

Policy describes the security parameters that are used for negotiations to establish and maintain a secure tunnel between two peers.

Before you set up your secure tunnels, to make their configuration faster and easier, you can create VPN policies that work on a global level. Rather than configuring the policy parameters for every tunnel you create, you can configure general policies and then later apply them to your secure tunnels.

Authentication mode

To ensure secure communication, there is two phases to every IKE (Internet Key Exchange) negotiation - Phase 1 (Authentication) and Phase 2 (Key exchange).

The Phase 1 negotiation establishes a secure channel between peers and determines a specific set of cryptographic protocols, exchanges shared secret keys and encryption and authentication algorithm that will be used for generating keys.

The Phase 2 negotiation establishes a secure channel between peers to protect data. During Phase 2 negotiation, the protocol security association for the tunnel is established. Either of the peers can initiate Phase 1 or Phase 2 renegotiation at any time. Both can specify intervals after which to negotiate.

Key life

Lifetime of key is specified as Key life.

Once the connection is established after exchanging authenticated and encrypted keys, connection is not dropped till the key life. If the key life of both the peers is not same then negotiation will take place whenever the key life of any one peer is over. This means intruder has to decrypt only one key to break in your system.

Key generation and key rotation are important because the longer the life of the key, the larger the amount of data at risk, and the easier it becomes to intercept more ciphered text for analysis.

Perfect Forward Secrecy (PFS)

It becomes difficult for a network intruder to get the big picture if keys are changing and they have to keep cracking keys for every negotiation. This is achieved by implementing PFS. By selecting PFS, new key will be generated for every negotiation and a new DH key exchange is included. So every time intruder will have to break yet another key even though he already knows the key. This enhances security.

Diffie-Hellman (DH) Group (IKE group)

Diffie-Hellman is a public-key cryptography scheme that allows peers to establish a shared secret over an insecure communications channel. Diffie-Hellman Key Exchange uses a complex algorithm and public and private keys to encrypt and then decrypt the data.

The Diffie-Hellmann group describes the key length used in encryption. Group number also termed as Identifiers.

DH Group	Key length (bits)
1	768
2	1024
5	1536
14	2048
15	3072
16	4096

Negotiation fails if same groups are not specified on each peer. The group cannot be switched during the negotiation.

Re-key Margin

Time before the next key exchange. Time is calculated by subtracting the time elapsed since the last key exchange from the key life. By turning Re-keying ‘Yes’, negotiation process starts automatically without interrupting service before key expiry.

Dead Peer detection settings

Use to check whether Cyberoam is able to connect the IP address or not. Set time interval after which the status of peer is to be checked and what action to take, if peer is not alive.

Tunnel Negotiation

Negotiation process starts to establish the connection when local or remote peer wants to communicate with each other. Depending on the connection parameters defined, the key is generated which is used for negotiations. Lifetime of key is specified as Key life. Once the connection is established, connection is alive/active and data can be transferred up to the specified key life. Connection will be closed/deactivated once the key expires.

If the connection is to be activated again then the entire negotiation process is to be started all over again. Negotiation process can be started again automatically by either local or remote peer only if Allow Re-keying is set to 'Yes'. Set the re-keying time in terms of the remaining key life when negotiation is to be started automatically without interrupting the communication before key expiry. For example, if key life is 8 hours and Re-key margin time is 10 minutes then negotiation process will automatically start after 7 hours 50 minutes of key usage.

Negotiation process will generate new key only if Perfect Forward Secrecy (PFS) is set to 'Yes'. PFS will generate a new key from scratch and there will be no dependency between old and new key.

Re-keying	Result
Yes	Local and remote peer both will be able to initiate request for connection. Depending on PFS, negotiation process will use same key or generate a new key.
No	Only remote peer will be able to initiate request for connection. Depending on PFS, negotiation process will use same key or generate a new key.

Cyberoam provides 5 default policies and you can also create a custom policy to meet your organization's requirement.

To make VPN connection configuration an easy task, following five preconfigured VPN policies are included for the frequently used VPN deployment scenarios:

- Road warrior
- L2TP
- Head office connectivity
- Branch office connectivity
- Default

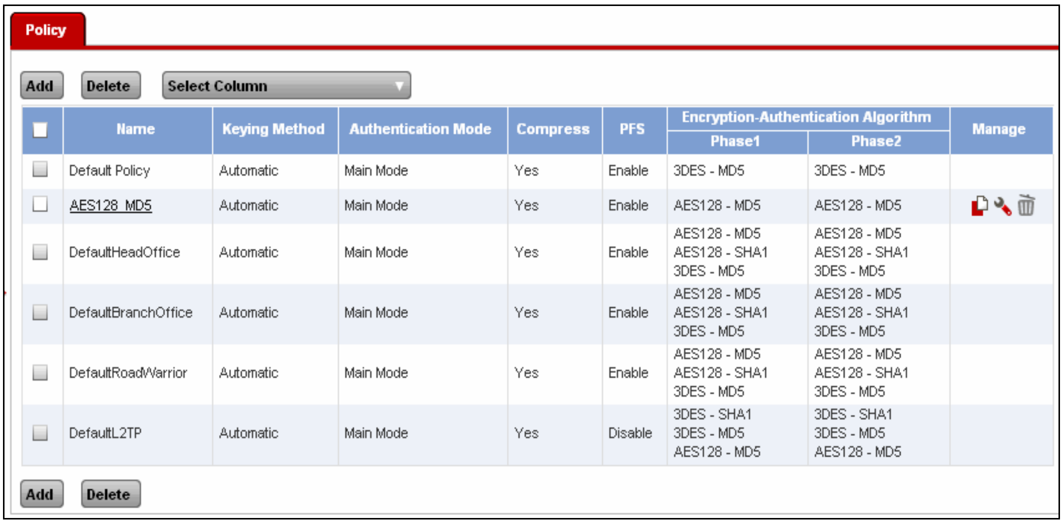
To configure custom VPN Policies, go to **VPN → Policy → Policy**.

- Add
- View
- Edit – Click the Edit icon in the Manage column against the VPN Policy to be modified. Edit VPN Policy window is displayed which has the same parameters as the Add VPN Policy window.
- Duplicate – Click the duplicate icon in the Manage column against the VPN Policy to be duplicated. Add VPN Policy window is displayed which has the same values for parameters as the existing policy. Click OK to add a new policy with modification in values for parameters.

- Customize Display Columns - Click the ‘Select Columns’ list to customize the columns to be displayed. By default, all the columns are selected and visible. You can uncheck the checkbox against the column which is not to be displayed.
- Delete – Click the Delete icon 🗑 in the Manage column against a VPN Policy to be deleted. A dialog box is displayed asking you to confirm the deletion. Click OK to delete the VPN Policy. To delete multiple VPN policies, select them ☑ and click the Delete button.

Manage VPN Policies

To manage custom VPN policies, go to **VPN → Policy → Policy**.



□	Name	Keying Method	Authentication Mode	Compress	PFS	Encryption-Authentication Algorithm		Manage
						Phase1	Phase2	
□	Default Policy	Automatic	Main Mode	Yes	Enable	3DES - MD5	3DES - MD5	
□	AES128_MD5	Automatic	Main Mode	Yes	Enable	AES128 - MD5	AES128 - MD5	🗑
□	DefaultHeadOffice	Automatic	Main Mode	Yes	Enable	AES128 - MD5 AES128 - SHA1 3DES - MD5	AES128 - MD5 AES128 - SHA1 3DES - MD5	
□	DefaultBranchOffice	Automatic	Main Mode	Yes	Enable	AES128 - MD5 AES128 - SHA1 3DES - MD5	AES128 - MD5 AES128 - SHA1 3DES - MD5	
□	DefaultRoadWarrior	Automatic	Main Mode	Yes	Enable	AES128 - MD5 AES128 - SHA1 3DES - MD5	AES128 - MD5 AES128 - SHA1 3DES - MD5	
□	DefaultL2TP	Automatic	Main Mode	Yes	Disable	3DES - SHA1 3DES - MD5 AES128 - MD5	3DES - SHA1 3DES - MD5 AES128 - MD5	

Screen – Manage VPN Policies

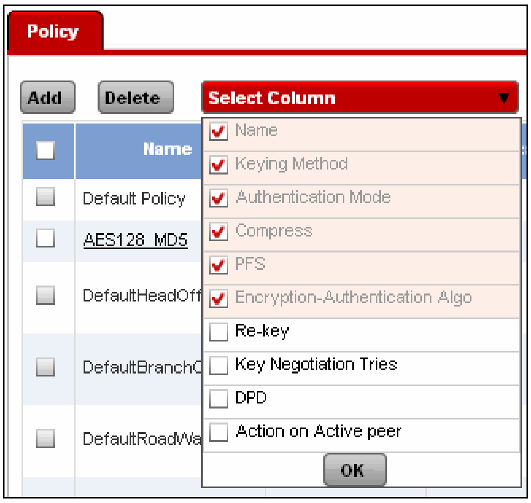
Screen Elements	Description
Add Button	Add a new VPN Policy
Name	Name of the VPN Policy
Keying Method	Automatic or Manual
Authentication Mode	Authentication mode selected: Main or Aggressive mode
Compress	Compression enabled or not
PFS	PFS enabled or not
Encryption-Authentication Algorithm	Encryption and Authentication Algorithm used for Phase1 and Phase2
Re-Key	Re-keying enabled or not
Key Negotiation Tries	Number of times Key Negotiation Tries is allowed
DPD	Dead Peer Detection enabled or not
Action on Active Peer	Action selected when dead peer detection is activated: Hold, Disconnect, Re-initiate
Edit Icon	Edit the VPN Policy
Delete Button	Delete the VPN Policy Alternately, click the delete icon against the policy to be deleted.

Table – Manage VPN Policies screen elements

Customize Display Columns

By default, VPN Policy page displays policy details in the following columns: Name, Keying method, Authentication Mode, Compress, PFS, Encryption-Authentication Algorithm, Re-Key, Key Negotiation Tries, DPD and Action on Active Peer. You can customize the number of columns to be displayed as per your requirement.

Go to **VPN → Policy → Policy** and click on the ‘Select Column’ list to customize the number of columns to be displayed.

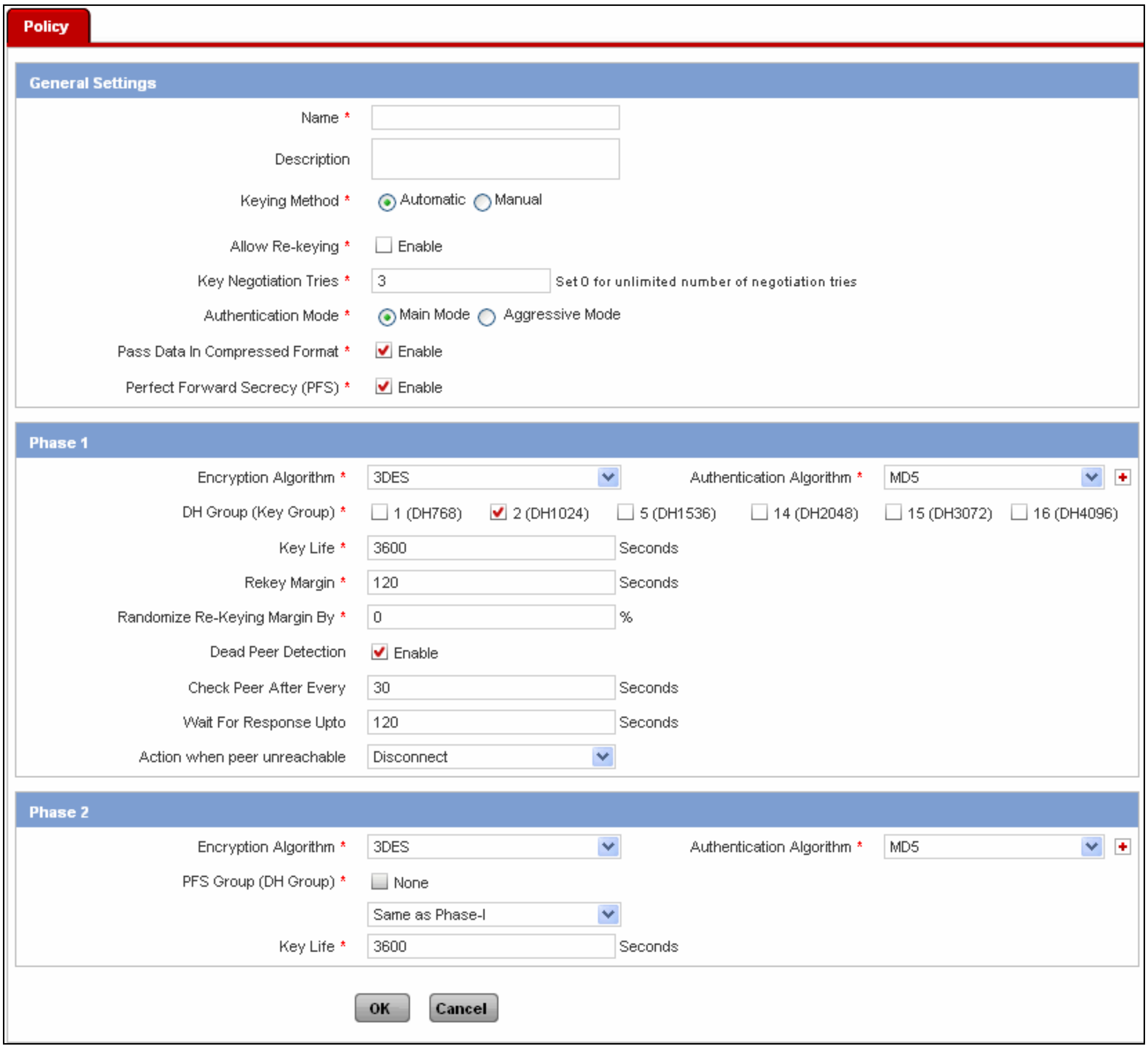


Screen – Customize Display Columns for VPN Policy

Select the columns ☑ to be displayed on the page. You can also select the order in which the columns will be displayed. Drag & drop the column to customize the view in desired order.

VPN Policy Parameters

To add, edit or duplicate policies, go to **VPN → Policy → Policy**. Click Add Button to add a new policy or Edit Icon 🔧 in the Manage column against the policy to be modified.



Policy

General Settings

Name *

Description

Keying Method * ● Automatic ○ Manual

Allow Re-keying * □ Enable

Key Negotiation Tries * 3 Set 0 for unlimited number of negotiation tries

Authentication Mode * ● Main Mode ○ Aggressive Mode

Pass Data In Compressed Format * ☑ Enable

Perfect Forward Secrecy (PFS) * ☑ Enable

Phase 1

Encryption Algorithm * 3DES

Authentication Algorithm * MD5

DH Group (Key Group) * □ 1 (DH768) ☑ 2 (DH1024) □ 5 (DH1536) □ 14 (DH2048) □ 15 (DH3072) □ 16 (DH4096)

Key Life * 3600 Seconds

Rekey Margin * 120 Seconds

Randomize Re-Keying Margin By * 0 %

Dead Peer Detection ☑ Enable

Check Peer After Every 30 Seconds

Wait For Response Upto 120 Seconds

Action when peer unreachable Disconnect

Phase 2

Encryption Algorithm * 3DES

Authentication Algorithm * MD5

PFS Group (DH Group) * □ None

Same as Phase-I

Key Life * 3600 Seconds

Screen – Add VPN Policy

Screen Elements	Description
Name	Name to identify the VPN Policy
Description	VPN Policy Description
Keying Method	Select keying method: Automatic or Manual. Keying method defines how the keys for the connection are to be managed. Manual key exchange is not supported for L2TP connection.
Allow Re-Keying	Enable Re-Keying to start the negotiation process automatically before key expiry. Process will start automatically at the specified time in re-key margin. If enabled, negotiation process can be initiated by both the local or remote peer. Depending on PFS, negotiation process will use same key or generate a new key
Key Negotiation Tries	Specify maximum key negotiation trials allowed. Set 0 for unlimited number of tries.
Authentication Mode	Select Authentication mode. Authentication mode is used for exchanging authentication information. **Available Options**: **Main mode**

	Aggressive mode – With Aggressive mode, tunnel can be established faster then using Main mode as less number of messages are exchanged during authentication and no cryptographic algorithm is used to encrypt the authentication information. Use Aggressive mode when remote peer has dynamic IP addresses. Depending on Authentication mode, the phase 1 parameters are exchanged for authentication purpose. In Main mode, the phase 1 parameters are exchanged in multiple rounds with encrypted authentication information while in aggressive mode phase1 parameters are exchanged in single message without encrypted information
Pass Data in Compressed Format	Enable to pass data in compressed format to increase throughput.
Perfect Forward Secrecy	Enable if new key should be generated for every negotiation on key expiry. Enable to generate new key for every negotiation on key expiry and disable to use same key for every negotiation.
PHASE 1	
Encryption Algorithm	Select encryption algorithm that would be used by communicating parties for integrity of exchanged data for phase 1. Supported Encryption algorithms: DES, 3DES, AES128, AES192, AES256, TwoFish, BlowFish, Serpent **3DES -** Triple DES is a symmetric strong encryption algorithm that is compliant with the OpenPGP standard. It is the application of DES standard where three keys are used in succession to provide additional security. **AES -** Advanced Encryption Standard offers the highest standard of security. The effective key lengths that can be used with AES are 128, 192 and 256 Bits. This security system supports a number of encryption algorithms. **Serpent -** Serpent is a 128-bit block cipher i.e. data is encrypted and decrypted in 128-bit chunks variable key length to be 128, 192, or 256 bits. The Serpent algorithm uses 32 rounds, or iterations of the main algorithm. Serpent is faster than DES and more secure than Triple DES. **Blowfish -** Blowfish is a symmetric encryption algorithm which uses the same secret key to both encrypt and decrypt messages. Blowfish is also a block cipher which divides a message into fixed length blocks during encryption and decryption. Blowfish has a 64-bit block size and a key length of anywhere from 32 bits to 448 bits and uses 16 rounds of main algorithm **Twofish -** Twofish is a symmetric key block cipher with a block size of 128 bits and key sizes up to 256 bits
Authentication Algorithm	Select authentication algorithm that would be used by communicating parties for integrity of exchanged data for phase 1. Supported Authentication algorithms: MD5, SHA1

	Maximum three combination of encryption and authentication algorithm can be selected. The remote peer must be configured to use at least one of the defined combinations. Click + to add more than one combination of encryption and authentication algorithm.
DH Group	Select one Diffie-Hellman group from 1, 2, 5, 14, 15 or 16. DH group specifies the key length used for encryption. DH Group 1 uses 768-bit encryption DH Group 2 uses 1024-bit encryption DH Group 5 uses 1536-bit encryption DH Group 14 uses 2048-bit encryption DH Group 15 uses 3072-bit encryption DH Group 16 uses 4096-bit encryption The remote peer must be configured to use the same group. If mismatched groups are specified on each peer, negotiation fails.
Key Life	Specify keylife in terms of seconds. Key life is the amount of time that will be allowed to pass before the key expires.
Re-key Margin	Specify Re-key margin. Set time in terms of the remaining key life. Re-key margin is the time when the negotiation process should be started automatically without interrupting the communication before the key expiry. For example, if key life is 8 hours and re-key margin is 10 minutes then negotiation process will automatically start after 7 hours 50 minutes usage of key life.
Randomize Re-keying Margin By	Specify Randomize re-keying time For example, if key life is 8 hours, re-key margin is 10 minutes and randomize re-keying time is 20% then the re-key margin will be 8 to 12 minutes and negotiation process will start automatically 8 minutes before the key expiry and will try up to 2 minutes after key expiry.
Dead Peer Detection	Enable DPD for Dead Peer Detection check to check at regular interval whether peer is live or not.
Check Peer After Every	Specify time after which the peer should be checked for its status. (Only if Dead Peer Detection option is ‘Enabled’). Once the connection is established, peer which initiated the connection checks whether another peer is live or not.
Wait For Response Up To	Specify till what time (seconds) initiated peer should wait for the status response. (Only if Dead Peer Detection option is ‘Enabled’). If the response is not received within the specified time, the peer is considered to be inactive.
Action When Peer Unreachable	Specify what action should be taken if peer is not active. (Only if Dead Peer Detection option is ‘Enabled’) Hold – hold the connection Disconnect – close the connection Re-initiate – reestablish the connection
PHASE 2	
Encryption Algorithm	Select encryption algorithm that would be used by communicating parties for integrity of exchanged data for phase 2. Supported Encryption algorithms: DES, 3DES, AES128,

	AES192, AES256, TwoFish, BlowFish, Serpent **3DES -** Triple DES is a symmetric strong encryption algorithm that is compliant with the OpenPGP standard. It is the application of DES standard where three keys are used in succession to provide additional security. **AES -** Advanced Encryption Standard offers the highest standard of security. The effective key lengths that can be used with AES are 128, 192 and 256 Bits. This security system supports a number of encryption algorithms. **Serpent -** Serpent is a 128-bit block cipher i.e. data is encrypted and decrypted in 128-bit chunks variable key length to be 128, 192, or 256 bits. The Serpent algorithm uses 32 rounds, or iterations of the main algorithm. Serpent is faster than DES and more secure than Triple DES. **Blowfish -** Blowfish is a symmetric encryption algorithm which uses the same secret key to both encrypt and decrypt messages. Blowfish is also a block cipher which divides a message into fixed length blocks during encryption and decryption. Blowfish has a 64-bit block size and a key length of anywhere from 32 bits to 448 bits and uses 16 rounds of main algorithm **Twofish -** Twofish is a symmetric key block cipher with a block size of 128 bits and key sizes up to 256 bits.
Authentication Algorithm	Select authentication algorithm that would be used by communicating parties for integrity of exchanged data for phase 2. Supported Authentication algorithms: MD5, SHA1 Maximum three combination of encryption and authentication algorithm can be selected. The remote peer must be configured to use at least one of the defined combinations. Click ✚ to add more than one combination of encryption and authentication algorithm
PFS (DH) Group	Select one Diffie-Hellman group from 1, 2, 5, 14, 15 or 16. DH group specifies the key length used for encryption. DH Group 1 uses 768-bit encryption DH Group 2 uses 1024-bit encryption DH Group 5 uses 1536-bit encryption DH Group 14 uses 2048-bit encryption DH Group 15 uses 3072-bit encryption DH Group 16 uses 4096-bit encryption The remote peer must be configured to use the same group. If mismatched groups are specified on each peer, negotiation fails. If ‘Same as Phase 1’ is selected PFS group specified at connection initiator’s end will be used. If No PFS is selected, this security parameter can not be added for Phase 2
Key Life	Specify keylife in terms of seconds.

	Key life is the amount of time that will be allowed to pass before the key expires. Default time is 3600 seconds

Table – Add VPN Policy screen elements

IPSec

IP Security (IPSec) is a suite of protocols designed for cryptographically secure communication at the IP layer (layer 3).

IPSec protocols:

- **Authentication Header (AH)** - Used for the authentication of packet senders and for ensuring the integrity of packet data. The Authentication Header protocol (AH) checks the authenticity and integrity of packet data. In addition, it checks that the sender and receiver IP addresses have not been changed in transmission. Packets are authenticated using a checksum created using a Hash-based Message Authentication Code (HMAC) in connection with a key.

- **Encapsulating Security Payload (ESP)** - Used for encrypting the entire packet and for the authenticating its contents. In addition to encryption, the ESP offers the ability to authenticate senders and verify packet contents.

IPSec modes:

- **Transport Mode** - the original IP packet is not encapsulated in another packet. The original IP header is retained, and the rest of the packet is sent either in clear text (AH) or encrypted (ESP). Either the complete packet can be authenticated with AH, or the payload can be encrypted and authenticated using ESP. In both cases, the original header is sent over the WAN in clear text.

Use Transport mode where both endpoints understand IPSEC directly. Transport mode is used between peers supporting IPSec, or between a host and a gateway, if the gateway is being treated as a host.

- **Tunnel Mode** - the complete packet – header and payload – is encapsulated in a new IP packet. An IP header is added to the IP packet, with the destination address set to the receiving tunnel endpoint. The IP addresses of the encapsulated packets remain unchanged. The original packet is then authenticated with AH or encrypted and authenticated using ESP.

Tunnel mode is primarily used for interoperability with gateways or end systems that do not support L2TP/IPSec or PPTP VPN site-to-site connections.

IPSec connections types (for Tunnel mode only):

- **Remote Access** - This type of VPN is a user-to-internal network connection via a public or shared network. Many large companies have employees that need to connect to the Internal network from the field. These field agents access the Internal network by using remote computers and laptops without static IP address.
- **Site-to-Site** - A Site-to-Site VPN connects an entire network (such as a LAN or WAN) to a remote network by way of a network-to-network connection. A network-to-network connection requires routers on each side of the connecting networks to transparently process and route information from one node on a LAN to a node on a remote LAN.
- **Host-to-Host** - Host-to-Host VPN connects one desktop or workstation to another by way of a host-to-host connection. This type of connection uses the network to which each host is

connected to create the secure tunnel to each other

IPSec Connection

To configure IPSec connections, go to **VPN → IPSec → Connection**. You can:

- Add
- View
- Edit – Click the Edit icon in the Manage column against the IPSec Connection to be modified. Edit IPSec Connection is displayed in a new window which has the same parameters as the Add IPSec Connection window.
- Customize Display Columns - Click the ‘Select Columns’ list to customize the columns to be displayed. By default, all the columns are selected and visible. You can uncheck the checkbox against the column which is not to be displayed.
- Delete – Click the Delete icon in the Manage column against an IPSec Connection to be deleted. A dialog box is displayed asking you to confirm the deletion. Click OK to delete the IPSec Connection. To delete multiple IPSec Connections, select them ☑ and click the Delete button.

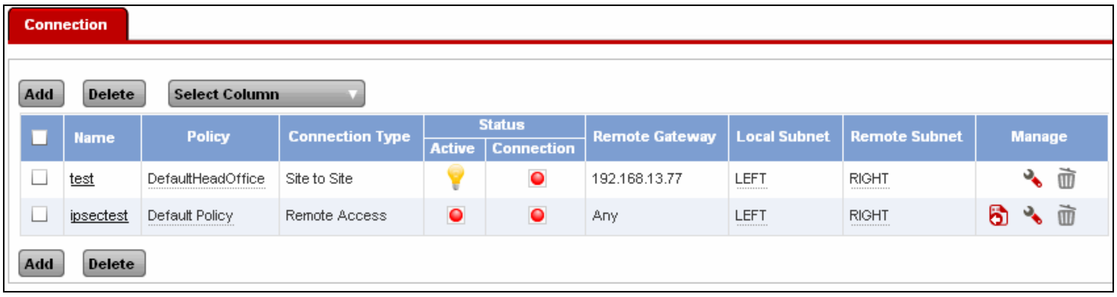
Note

IPSec connection – On deletion of the connection, Cyberoam does not delete hosts and firewall rules related to the connection. One can delete if required.

Remote Access connection – On deletion of the connection, Cyberoam automatically deletes all the automatically created dynamic hosts and firewall rules related to the connection.

Manage IPSec Connections

To manage IPSec connections, go to **VPN → IPSec → Connection**.



□	Name	Policy	Connection Type	Status		Remote Gateway	Local Subnet	Remote Subnet	Manage
				Active	Connection				
□	test	DefaultHeadOffice	Site to Site	💡	●	192.168.13.77	LEFT	RIGHT	
□	ipsectest	Default Policy	Remote Access	●	●	Any	LEFT	RIGHT	

Screen – Manage IPSec Connections

Screen Elements	Description
Add Button	Add a new IPSec Connection
Name	Name of the IPSec Connection
Policy	Name of the VPN Policy selected
Connection Type	Connection type selected: Remote Access, Site-to-Site, Host-to-Host
Status	Status of the Connection

	💡 - Activated connection. Click to deactivate the connection 🔴 - Deactivated connection. Click to activate the connection 🔴 - Activated and Disconnected. Click to initiate the connection. 🟢 - Activated and Connected. Click to disconnect the connection. When you disconnect, connection will be deactivated and to re-establish connection the connection, activate connection. 💡 - Activated but Partially connected. Click to disconnect the connection. When multiple subnets are configured for LAN and/or remote network, Cyberoam creates sub-connection for each subnet. Connection Status in Yellow color indicates that one of the sub-connection is not active.
Remote Gateway	Remote VPN Server IP Address selected as the Remote Gateway
Local Subnet	IP Host selected as Local Subnet
Remote Subnet	IP Host selected as Remote Subnet
Authentication Type	Type of Authentication selected. Authentication of user depends on the connection type. **Available Options**: Preshared Key, Digital Certificate or RSA Key
Action on Initiate	Action to be taken of VPN Restart **Available Options**: Respond Only, Initiate or Disable
Local ID	Value for local ID selected **Available Options**: DNS, IP Address Email Address or DER ASN1 DN (X.509). For preshared key and RSA key, DER ASN1 DN (X.509) is not applicable. In case of Local Certificate, ID and its value is displayed automatically as specified in the Local Certificate.
Remote ID	Value for Remote ID selected **Available Options**: DNS, IP Address Email Address or DER ASN1 DN (X.509). For preshared key and RSA key, DER ASN1 DN (X.509) is not applicable.
Export Icon	Export Icon to export connection configuration file. Export icon is available for Remote Access connection only
Edit Button	Edit the IPSec Connection
Delete Button	Delete the IPSec Connection Alternately, click the delete icon against the connection to be

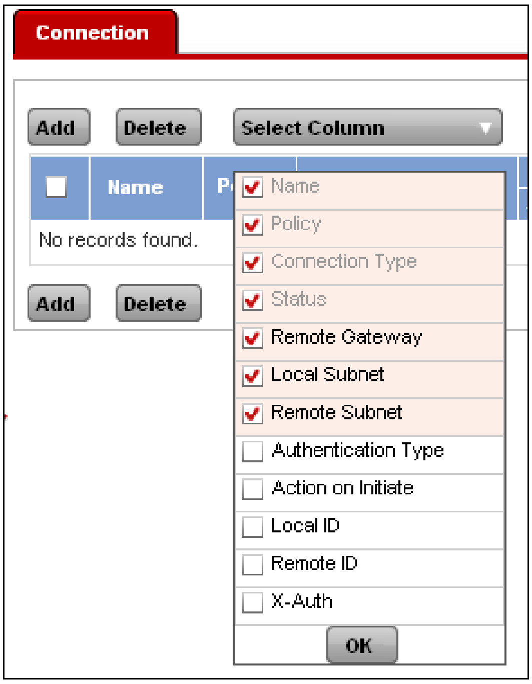
	deleted.

Table – Manage IPSec Connections screen elements

Customize Display Columns

By default, VPN Policy page displays policy details in the following columns: Name, Policy, Connection Type, Status, Remote Gateway, Local Subnet, Remote Subnet, Authentication Type, Action on Initiate Local ID, Remote ID and X-Auth. You can customize the number of columns to be displayed as per your requirement.

Go to **VPN → IPSec → Connection** and click on the ‘Select Column’ list to customize the number of columns to be displayed.



Connection

Add Delete Select Column ▾

□ Name P

No records found.

Add Delete

☑ Name
☑ Policy
☑ Connection Type
☑ Status
☑ Remote Gateway
☑ Local Subnet
☑ Remote Subnet
□ Authentication Type
□ Action on Initiate
□ Local ID
□ Remote ID
□ X-Auth

OK

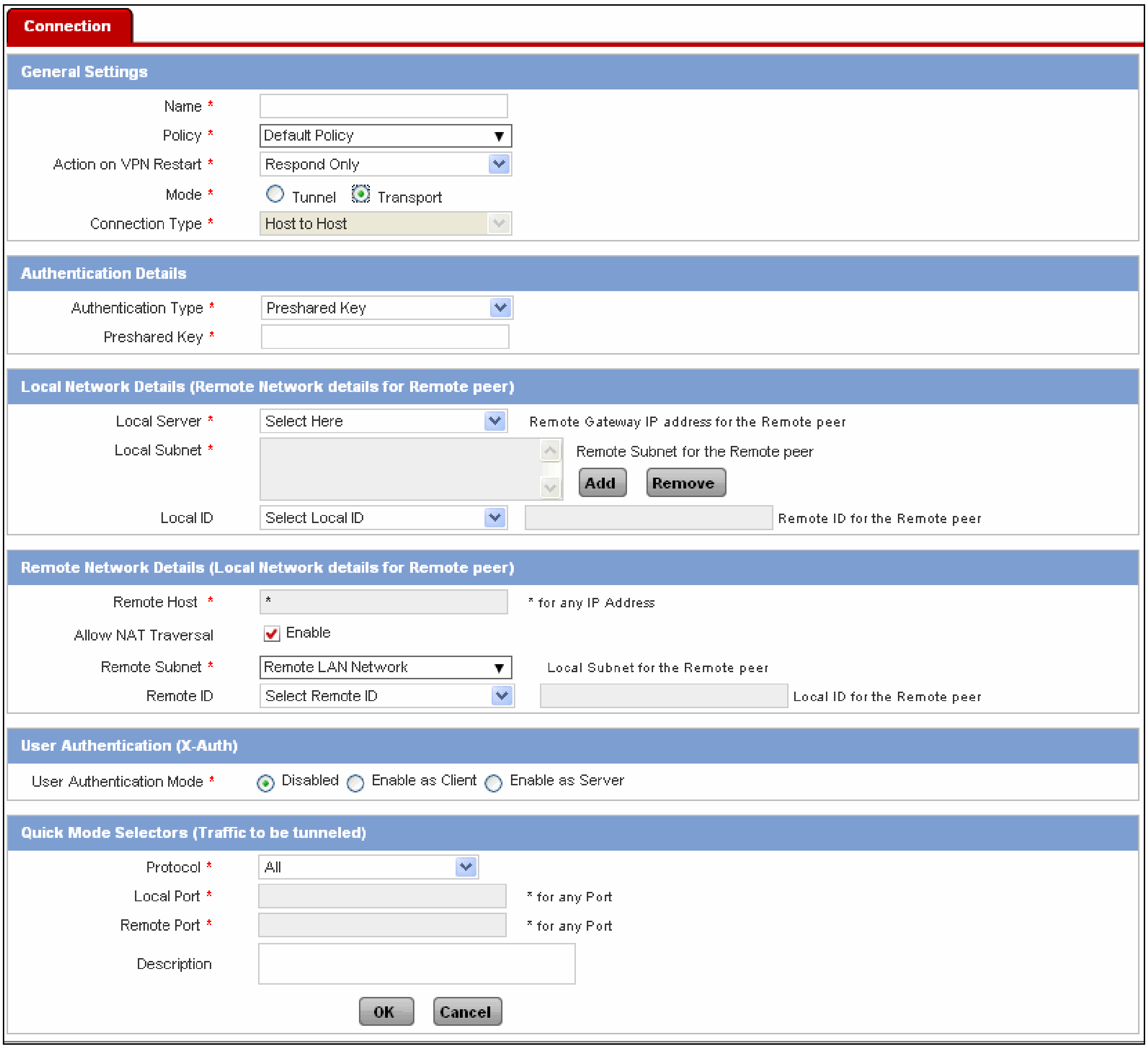
Screen – Customize Display Columns for IPSec Connection

Select the columns ☑ to be displayed on the page. You can also select the order in which the columns will be displayed. Drag & drop the column to customize the view in desired order.

IPSec Connection Parameters

To add or edit VPN connections, go to **VPN → IPSec → Connection**. Click Add Button to add a new connection or Edit Icon 🔧 in the Manage column against the connection to be modified. Following are the VPN connection modes/types in Cyberoam.

Parameters – Transport Mode



General Settings

Name *
Policy * Default Policy
Action on VPN Restart * Respond Only
Mode * ○ Tunnel ● Transport
Connection Type * Host to Host

Authentication Details

Authentication Type * Preshared Key
Preshared Key *

Local Network Details (Remote Network details for Remote peer)

Local Server * Select Here — Remote Gateway IP address for the Remote peer
Local Subnet * — Remote Subnet for the Remote peer

Local ID Select Local ID — Remote ID for the Remote peer

Remote Network Details (Local Network details for Remote peer)

Remote Host * * — * for any IP Address
Allow NAT Traversal ☑ Enable
Remote Subnet * Remote LAN Network — Local Subnet for the Remote peer
Remote ID Select Remote ID — Local ID for the Remote peer

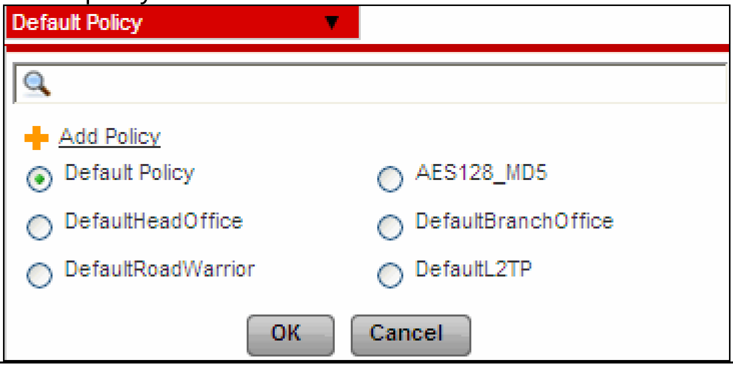
User Authentication (X-Auth)

User Authentication Mode * ● Disabled ○ Enable as Client ○ Enable as Server

Quick Mode Selectors (Traffic to be tunneled)

Protocol * All
Local Port * — * for any Port
Remote Port * — * for any Port
Description

Screen – Add Transport Mode IPSec Connection

Screen Elements	Description
Name	Name to identify the IPSec Connection
Policy	Select policy to be used for connection  Default Policy Add Policy ● Default Policy ○ AES128_MD5 ○ DefaultHeadOffice ○ DefaultBranchOffice ○ DefaultRoadWarrior ○ DefaultL2TP OK Cancel
Action on VPN Restart	Select the action for the connection. **Available options**: • **Respond Only** - Keep connection in disabled till the user responds

	- **Initiate** – Activate connection on system/service start so that the connection can be established whenever required - **Disable -** Keep connection disabled till the user activates
Mode	Select Transport mode
Connection Type	Host-to-Host Connection **Note** In Transport mode, only Host-to-Host connection is supported.
Authentication details	
Authentication Type	Select Authentication Type. Authentication of user depends on the connection type. **Available options**: **Preshared key** authentication is a mechanism whereby a single key is used for encryption and decryption. Both the peers should possess the preshared key. Remote peer uses the preshared key for decryption. Specify the preshared key to be used. This preshared key will have to be shared or communicated to the peer at the remote end. At the remote end, client will have to specify this key for authentication. Refer to VPN Client guide, Phase 1 Configuration. If there is mismatch in the key, user will not be able to establish the connection. **Digital Certificate** authentication is a mechanism whereby sender and receiver both use digital certificate issued by the Certificate Authority. Both sender and receiver must have each other's Certificate Authority. a) Select the local certificate that should be used for authentication by Cyberoam b) Select the remote certificate that should be used for authentication by remote peer **RSA Key** authentication is a mechanism whereby two keys – Local and Remote RSA - are used for encryption and decryption. Local key is known only to the owner and never transmitted over network. Displays automatically generated key, which cannot be modified. Local RSA key can be regenerated from CLI Console. Refer to Console guide for more details.
Local network details (remote network details for remote peer)	
Local Server	Select local server.
Local ID	For preshared key and RSA key, select any type of id and specify its value DER ASN1 DN (X.509) is not applicable. In case of Local Certificate, ID and its value is displayed automatically as specified in the Local Certificate.
Remote network details (local network details for remote peer)	
Remote Host	Specify IP address of remote peer/host. Specify * for any IP

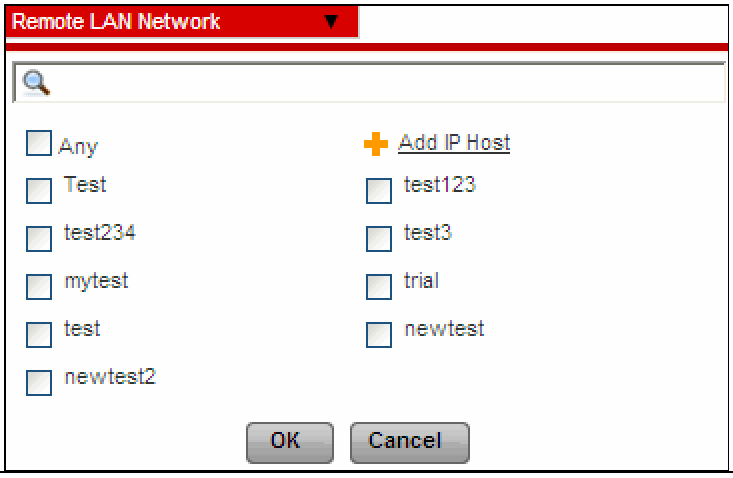
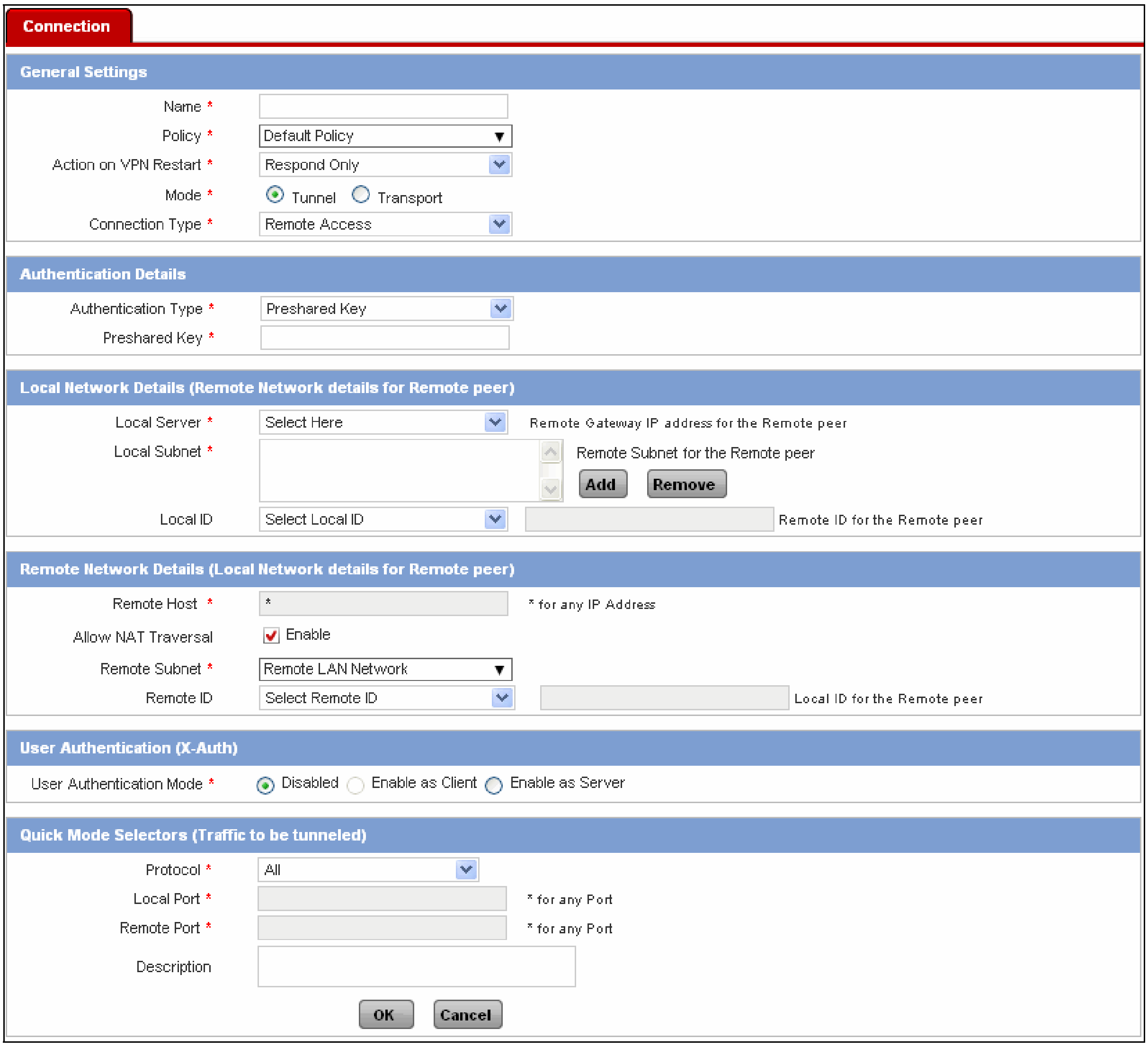
	address.
Allow NAT Traversal	Enable NAT traversal if a NAT device is located between your VPN endpoints i.e. when remote peer has private/non-routable IP address. At a time only one connection can be established behind one NAT-box. By default, it is enabled.
Remote LAN Network	Select IP addresses and netmask of remote network which is allowed to connect to the Cyberoam server through VPN tunnel. Multiple subnets can be specified. Select IP Hosts from the list of IP Hosts available. You can also add a new IP Host and include in the list.  Remote LAN Network □ Any Add IP Host □ Test □ test123 □ test234 □ test3 □ mytest □ trial □ test □ newtest □ newtest2 OK Cancel
Remote ID	For preshared key, select any type of id and specify its value, DER ASN1 DN (X.509) is not applicable
User authentication (x-auth)	
User Authentication mode	Select whether user authentication is required at the time of connection or not Click Disable if user authentication is not required If enabled as client, specify username and password If enabled as server, add all the users which are to be allowed to connect.
Quick mode selectors (traffic to be tunneled)	
Protocol	Select all the protocols that are to be allowed for negotiations. Tunnel will pass only that data which uses the specified protocol.
Local Port	Specify Local Port for TCP or UDP
Remote Port	Specify Remote Port for TCP or UDP
Description	IPSec VPN Connection Description

Table – Add Transport Mode VPN Connection screen elements

Parameters – Remote Access VPN Connection



Connection

General Settings

Name *

Policy * Default Policy

Action on VPN Restart * Respond Only

Mode * ● Tunnel ○ Transport

Connection Type * Remote Access

Authentication Details

Authentication Type * Preshared Key

Preshared Key *

Local Network Details (Remote Network details for Remote peer)

Local Server * Select Here — Remote Gateway IP address for the Remote peer

Local Subnet * — Remote Subnet for the Remote peer

Local ID Select Local ID — Remote ID for the Remote peer

Remote Network Details (Local Network details for Remote peer)

Remote Host * * — * for any IP Address

Allow NAT Traversal ☑ Enable

Remote Subnet * Remote LAN Network

Remote ID Select Remote ID — Local ID for the Remote peer

User Authentication (X-Auth)

User Authentication Mode * ● Disabled ○ Enable as Client ○ Enable as Server

Quick Mode Selectors (Traffic to be tunneled)

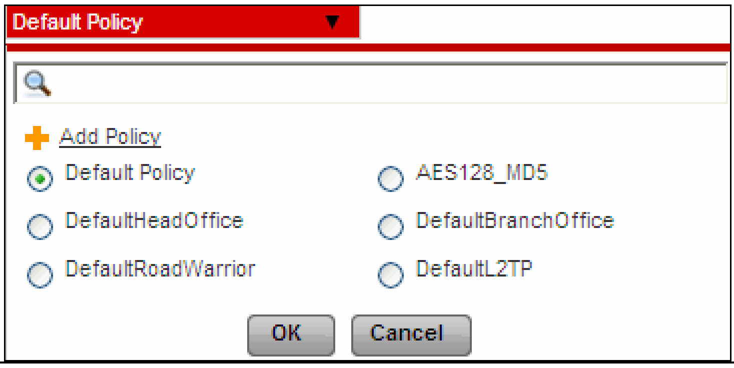
Protocol * All

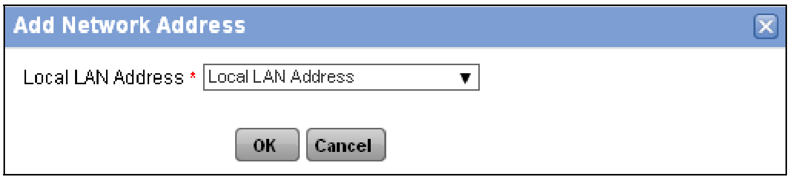
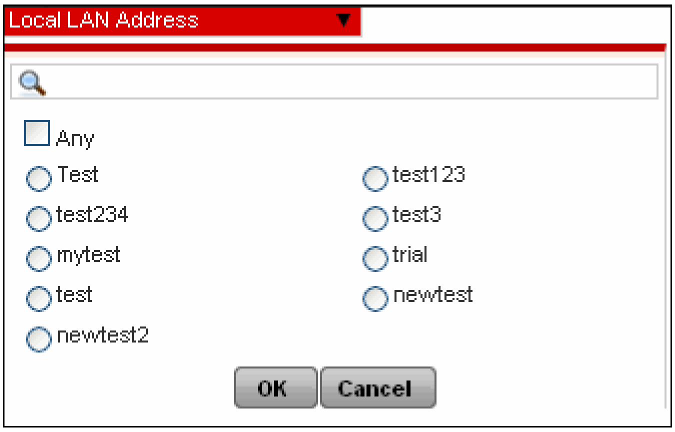
Local Port * — * for any Port

Remote Port * — * for any Port

Description

Screen – Add Remote Access IPSec Connection

Screen Elements	Description
Name	Name to identify the IPSec Connection
Policy	Select policy to be used for connection  Default Policy Add Policy ● Default Policy ○ AES128_MD5 ○ DefaultHeadOffice ○ DefaultBranchOffice ○ DefaultRoadWarrior ○ DefaultL2TP OK Cancel
Action on VPN Restart	Select the action for the connection. **Available options**:

	- **Respond Only** - Keep connection in disabled till the user responds - **Initiate** – Activate connection on system/service start so that the connection can be established whenever required - **Disable** - Keep connection disabled till the user activates
Mode	Select Tunnel mode
Connection Type	Remote Access Connection
Authentication details	
Authentication Type	Select Authentication Type. Authentication of user depends on the connection type. **Available options**: **Preshared key** authentication is a mechanism whereby a single key is used for encryption and decryption. Both the peers should possess the preshared key. Remote peer uses the preshared key for decryption. Specify the preshared key to be used. This preshared key will have to be shared or communicated to the peer at the remote end. At the remote end, client will have to specify this key for authentication. Refer to VPN Client guide, Phase 1 Configuration. If there is mismatch in the key, user will not be able to establish the connection. **Digital Certificate** authentication is a mechanism whereby sender and receiver both use digital certificate issued by the Certificate Authority. Both sender and receiver must have each other's Certificate Authority. a) Select the local certificate that should be used for authentication by Cyberoam b) Select the remote certificate that should be used for authentication by remote peer.
Local network details (remote network details for remote peer)	
Local Server	Select local server.
Local LAN Address	Select Local LAN Address. Add and Remove LAN Address using Add Button and Remove Button  Add Network Address Local LAN Address * Local LAN Address ▼ OK Cancel  Local LAN Address ▼ □ Any ○ Test ○ test123 ○ test234 ○ test3 ○ mytest ○ trial ○ test ○ newtest ○ newtest2 OK Cancel
Local ID	For preshared key and RSA key, select any type of id and specify its

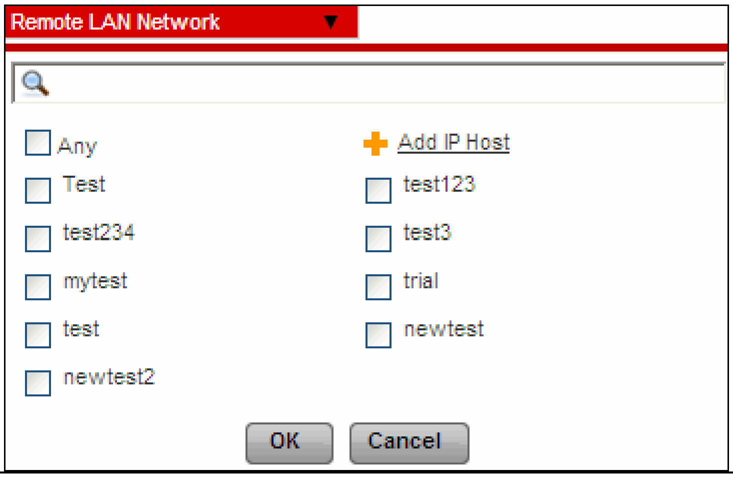
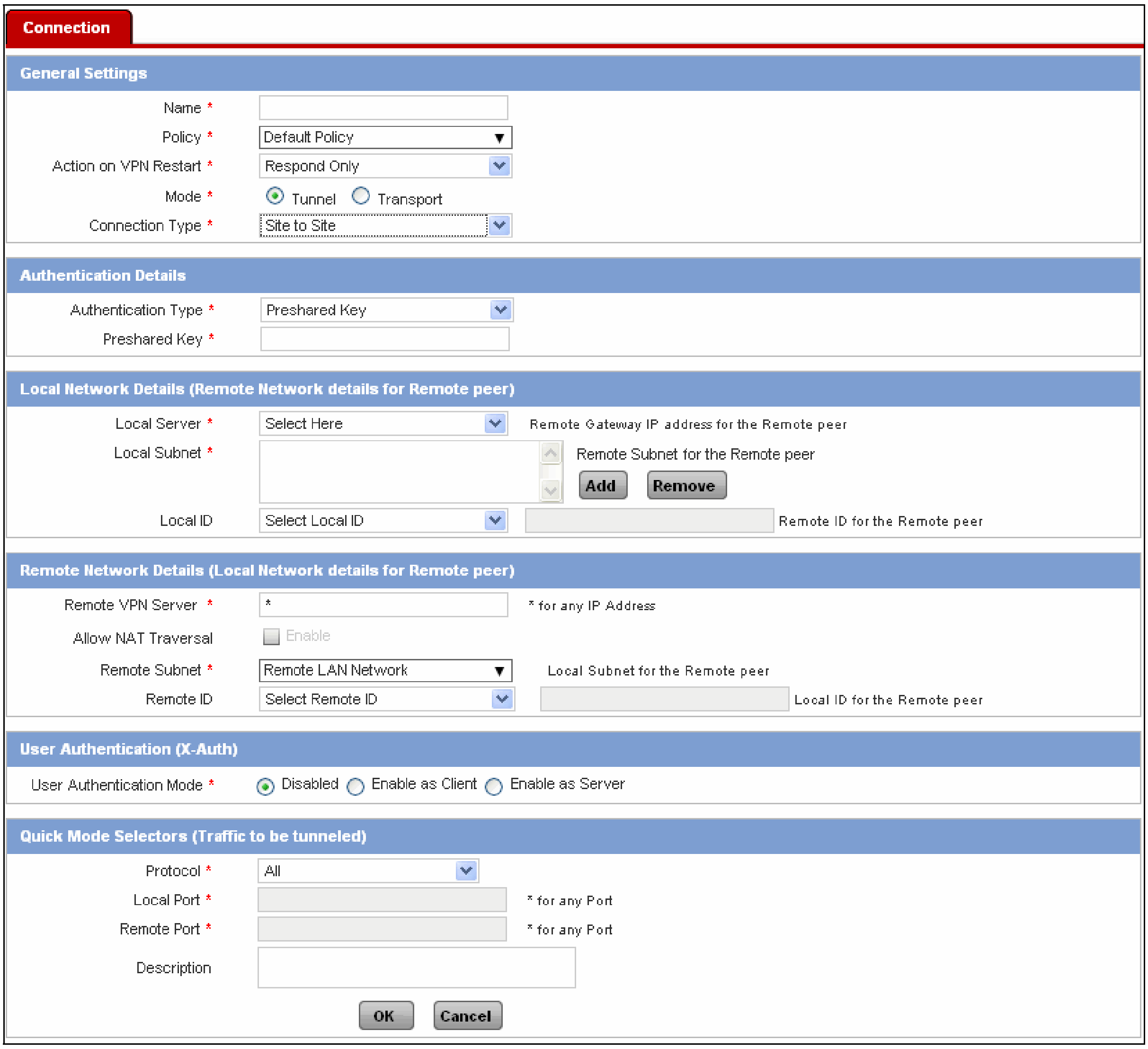
	value DER ASN1 DN (X.509) is not applicable. In case of Local Certificate, ID and its value is displayed automatically as specified in the Local Certificate.
Remote network details (local network details for remote peer)	
Remote Host	Select IP address of remote peer/host. Specify * for any IP Address.
Allow NAT Traversal	Enable NAT traversal if a NAT device is located between your VPN endpoints i.e. when remote peer has private/non-routable IP address. At a time only one connection can be established behind one NAT-box.
Remote LAN Network	Select IP Hosts from the list of IP Hosts available. You can also add a new IP Host and include in the list.  Remote LAN Network ▼ □ Any Add IP Host □ Test □ test123 □ test234 □ test3 □ mytest □ trial □ test □ newtest □ newtest2 OK Cancel
Remote ID	For preshared key, select any type of id and specify its value, DER ASN1 DN (X.509) is not applicable.
User authentication (x-auth)	
User Authentication mode	Select whether user authentication is required at the time of connection or not Click Disable if user authentication is not required If enabled as client, specify username and password If enabled as server, add all the users which are to be allowed to connect.
Quick mode selectors (traffic to be tunneled)	
Protocol	Select all the protocols that are to be allowed for negotiations. Tunnel will pass only that data which uses the specified protocol.
Local Port	Specify Local Port for TCP or UDP
Remote Port	Specify Remote Port for TCP or UDP
Description	IPSec VPN Connection Description

Table – Add Remote Access VPN Connection screen elements

Parameters – Site-to-Site VPN Connection



General Settings

Name *

Policy * Default Policy

Action on VPN Restart * Respond Only

Mode * ● Tunnel ○ Transport

Connection Type * Site to Site

Authentication Details

Authentication Type * Preshared Key

Preshared Key *

Local Network Details (Remote Network details for Remote peer)

Local Server * Select Here — Remote Gateway IP address for the Remote peer

Local Subnet * — Remote Subnet for the Remote peer

Local ID Select Local ID — Remote ID for the Remote peer

Remote Network Details (Local Network details for Remote peer)

Remote VPN Server * * — * for any IP Address

Allow NAT Traversal □ Enable

Remote Subnet * Remote LAN Network — Local Subnet for the Remote peer

Remote ID Select Remote ID — Local ID for the Remote peer

User Authentication (X-Auth)

User Authentication Mode * ● Disabled ○ Enable as Client ○ Enable as Server

Quick Mode Selectors (Traffic to be tunneled)

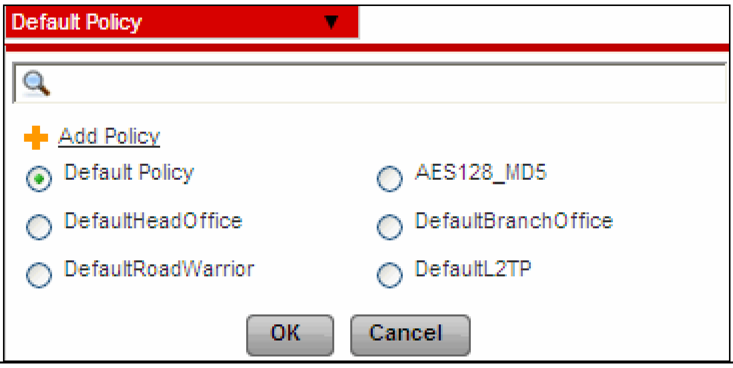
Protocol * All

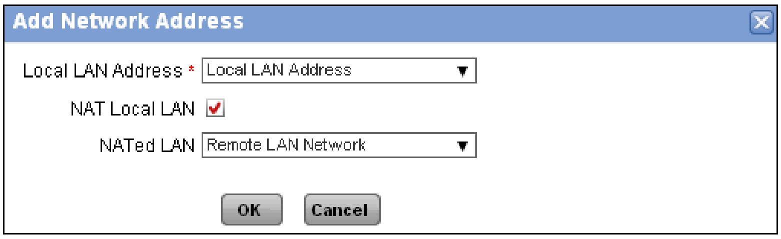
Local Port * — * for any Port

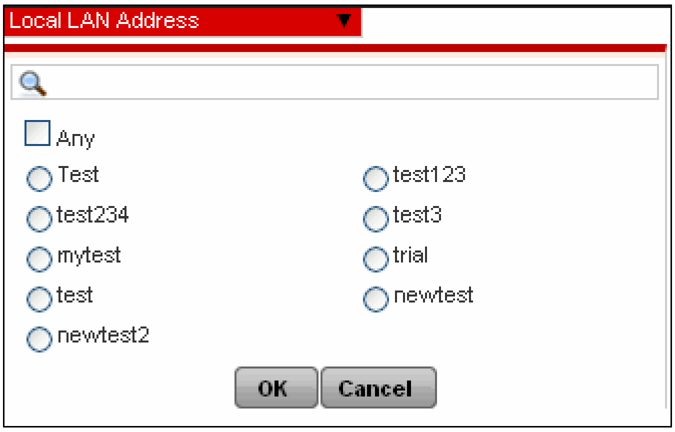
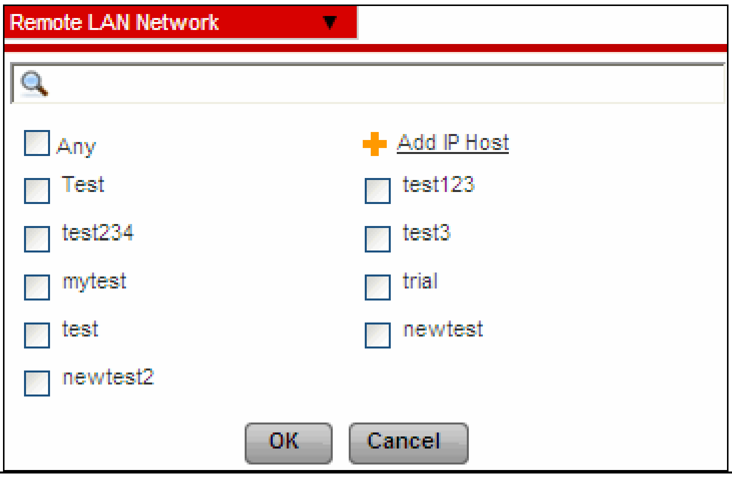
Remote Port * — * for any Port

Description

Screen – Add Site to Site IPSec Connection

Screen Elements	Description
Name	Name to identify the IPSec Connection
Policy	Select policy to be used for connection  Default Policy Add Policy ● Default Policy ○ AES128_MD5 ○ DefaultHeadOffice ○ DefaultBranchOffice ○ DefaultRoadWarrior ○ DefaultL2TP
Action on Activation	Select the action for the connection. **Available options**: **Respond Only** - Keep connection in disabled till the user responds

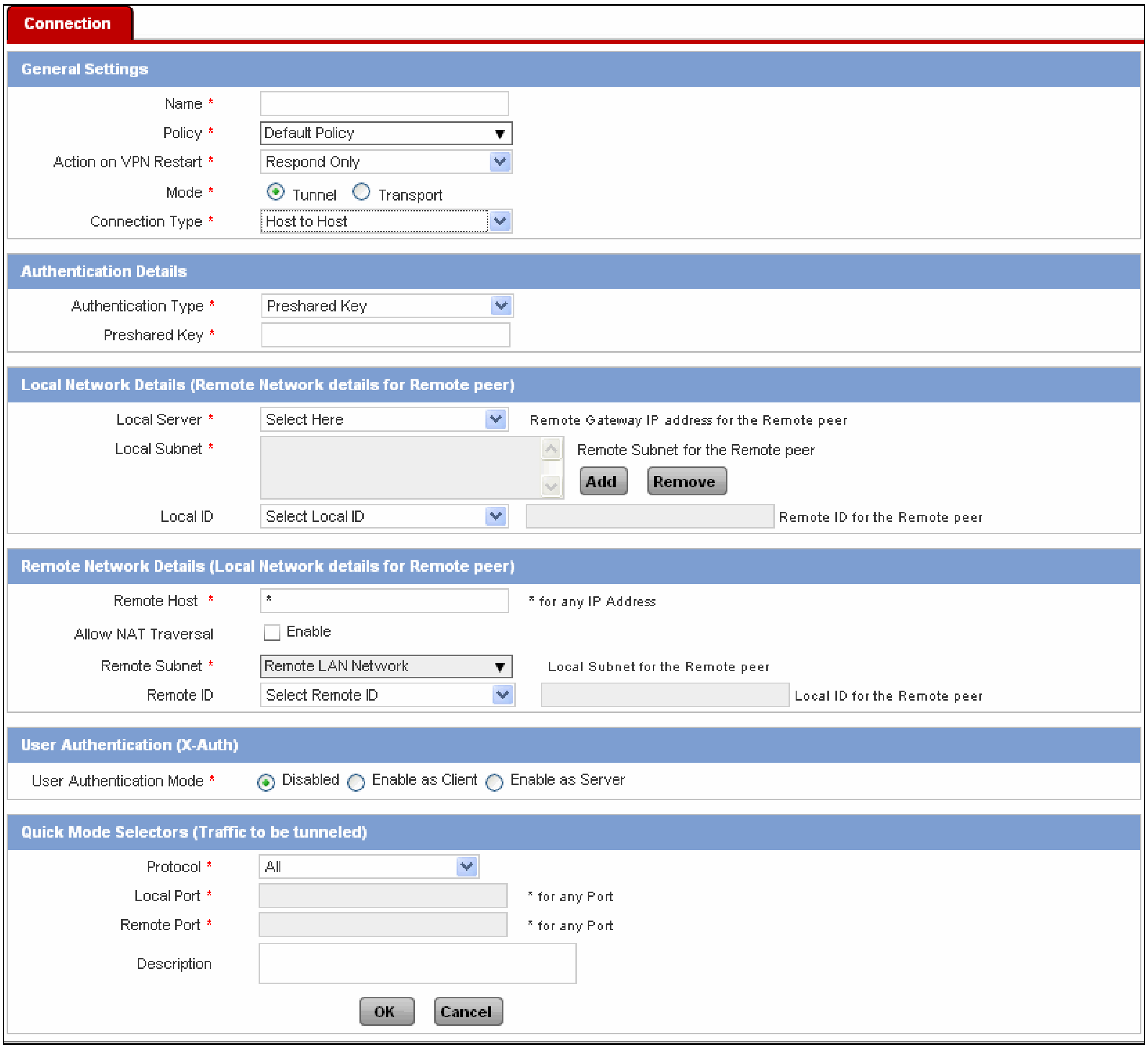
	Initiate – Activate connection on system/service start so that the connection can be established whenever required **Disable -** Keep connection disabled till the user activates
Mode	Select Tunnel mode
Connection Type	Site-to-Site Connection
Authentication details	
Authentication Type	Select Authentication Type. Authentication of user depends on the connection type. **Available options**: **Preshared key** authentication is a mechanism whereby a single key is used for encryption and decryption. Both the peers should possess the preshared key. Remote peer uses the preshared key for decryption. Specify the preshared key to be used. This preshared key will have to be shared or communicated to the peer at the remote end. At the remote end, client will have to specify this key for authentication. Refer to VPN Client guide, Phase 1 Configuration. If there is mismatch in the key, user will not be able to establish the connection. **Digital Certificate** authentication is a mechanism whereby sender and receiver both use digital certificate issued by the Certificate Authority. Both sender and receiver must have each other's Certificate Authority. a) Select the local certificate that should be used for authentication by Cyberoam b) Select the remote certificate that should be used for authentication by remote peer **RSA Key** authentication is a mechanism whereby two keys – Local and Remote RSA - are used for encryption and decryption. Local key is known only to the owner and never transmitted over network. Displays automatically generated key which cannot be modified. Local RSA key can be regenerated from CLI Console. Refer to Console guide for more details.
Local network details (remote network details for remote peer)	
Local Server	Select local server.
Local LAN Address	Select Local LAN Address. Add and Remove LAN Address using Add Button and Remove Button  Add Network Address Local LAN Address * Local LAN Address ▼ NAT Local LAN ☑ NATed LAN Remote LAN Network ▼ OK Cancel

	 Local LAN Address ▼ □ Any ○ Test ○ test123 ○ test234 ○ test3 ○ mytest ○ trial ○ test ○ newtest ○ newtest2 OK Cancel
Local ID	For preshared key and RSA key, select any type of id and specify its value DER ASN1 DN (X.509) is not applicable. In case of Local Certificate, ID and its value is displayed automatically as specified in the Local Certificate.
Remote network details (local network details for remote peer)	
Remote Host	Specify IP address of remote peer/host. Specify * for any IP address.
Remote LAN Network	Select IP addresses and netmask of remote network which is allowed to connect to the Cyberoam server through VPN tunnel. Multiple subnets can be specified. Select IP Hosts from the list of IP Hosts available. You can also add a new IP Host and include in the list.  Remote LAN Network ▼ □ Any Add IP Host □ Test □ test123 □ test234 □ test3 □ mytest □ trial □ test □ newtest □ newtest2 OK Cancel
Remote ID	For preshared key, select any type of id and specify its value, DER ASN1 DN (X.509) is not applicable. **Note** In a single connection, same subnet for LAN and Remote network cannot be configured.
User authentication (x-auth)	
User Authentication mode	Select whether user authentication is required at the time of connection or not Click Disable if user authentication is not required If enabled as client, specify username and password

	If enabled as server, add all the users which are to be allowed to connect.
Quick mode selectors (traffic to be tunneled)	
Protocol	Select all the protocols that are to be allowed for negotiations. Tunnel will pass only that data which uses the specified protocol.
Local Port	Specify Local Port for TCP or UDP
Remote Port	Specify Remote Port for TCP or UDP
Description	IPSec VPN Connection Description

Table – Add Site to Site VPN Connection screen elements

Parameters – Host-to-Host VPN Connection



Connection

General Settings

Name *

Policy * Default Policy

Action on VPN Restart * Respond Only

Mode * ● Tunnel ○ Transport

Connection Type * Host to Host

Authentication Details

Authentication Type * Preshared Key

Preshared Key *

Local Network Details (Remote Network details for Remote peer)

Local Server * Select Here — Remote Gateway IP address for the Remote peer

Local Subnet * — Remote Subnet for the Remote peer

Add Remove

Local ID Select Local ID — Remote ID for the Remote peer

Remote Network Details (Local Network details for Remote peer)

Remote Host * * — * for any IP Address

Allow NAT Traversal □ Enable

Remote Subnet * Remote LAN Network — Local Subnet for the Remote peer

Remote ID Select Remote ID — Local ID for the Remote peer

User Authentication (X-Auth)

User Authentication Mode * ● Disabled ○ Enable as Client ○ Enable as Server

Quick Mode Selectors (Traffic to be tunneled)

Protocol * All

Local Port * — * for any Port

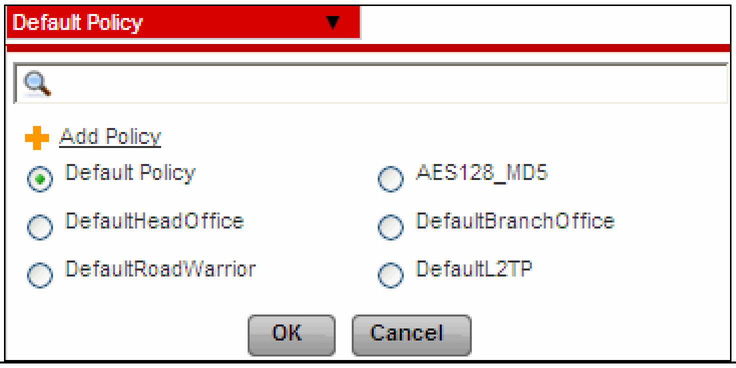
Remote Port * — * for any Port

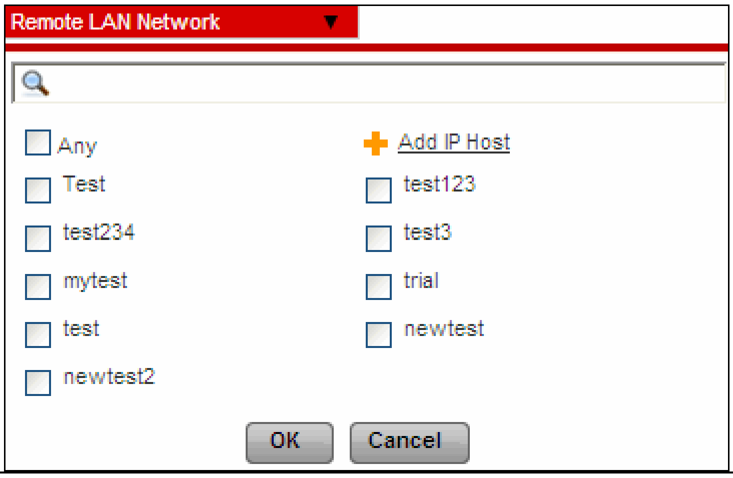
Description

OK Cancel

Screen – Add Host-to-Host IPSec Connection

Screen Elements	Description
Name	Name to identify the IPSec Connection
Policy	Select policy to be used for connection

	 Default Policy ▼ Add Policy ● Default Policy ○ AES128_MD5 ○ DefaultHeadOffice ○ DefaultBranchOffice ○ DefaultRoadWarrior ○ DefaultL2TP OK Cancel
Action on Activation	Select the action for the connection. **Available options**: **Respond Only** - Keep connection in disabled till the user responds **Initiate** – Activate connection on system/service start so that the connection can be established whenever required **Disable** - Keep connection disabled till the user activates
Mode	Select Tunnel mode
Connection Type	Host-to-Host Connection
Authentication details	
Mode	Select Tunnel mode
Connection Type	Host-to-Host Connection
Authentication Type	Select Authentication Type. Authentication of user depends on the connection type. **Available options**: **Preshared key** authentication is a mechanism whereby a single key is used for encryption and decryption. Both the peers should possess the preshared key. Remote peer uses the preshared key for decryption. Specify the preshared key to be used. This preshared key will have to be shared or communicated to the peer at the remote end. At the remote end, client will have to specify this key for authentication. Refer to VPN Client guide, Phase 1 Configuration. If there is mismatch in the key, user will not be able to establish the connection. **Digital Certificate** authentication is a mechanism whereby sender and receiver both use digital certificate issued by the Certificate Authority. Both sender and receiver must have each other's Certificate Authority. a) Select the local certificate that should be used for authentication by Cyberoam b) Select the remote certificate that should be used for authentication by remote peer **RSA Key** authentication is a mechanism whereby two keys – Local and Remote RSA - are used for encryption and decryption. Local key is known only to the owner and never transmitted over network. Displays automatically generated key which cannot be modified.

	Local RSA key can be regenerated from CLI Console. Refer to Console guide for more details.
Local network details (remote network details for remote peer)	
Local Server	Select local server.
Local ID	For preshared key and RSA key, select any type of id and specify its value DER ASN1 DN (X.509) is not applicable. In case of Local Certificate, ID and its value is displayed automatically as specified in the Local Certificate.
Remote network details (local network details for remote peer)	
Remote Host	Specify IP address of remote peer/host. Specify * for any IP address.
Allow NAT Traversal	Enable NAT traversal if a NAT device is located between your VPN endpoints i.e. when remote peer has private/non-routable IP address. At a time only one connection can be established behind one NAT-box. By default, it is enabled.
Remote LAN Network	Select IP addresses and netmask of remote network which is allowed to connect to the Cyberoam server through VPN tunnel. Multiple subnets can be specified. Select IP Hosts from the list of IP Hosts available. You can also add a new IP Host.  Remote LAN Network ▼ □ Any + Add IP Host □ Test □ test123 □ test234 □ test3 □ mytest □ trial □ test □ newtest □ newtest2 OK Cancel
Remote ID	For preshared key, select any type of id and specify its value, DER ASN1 DN (X.509) is not applicable.
User authentication (x-auth)	
User Authentication mode	Select whether user authentication is required at the time of connection or not Click Disable if user authentication is not required. If enabled as client, specify username and password. If enabled as server, add all the users, which are to be allowed to connect.
Quick mode selectors (traffic to be tunneled)	
Protocol	Select all the protocols that are to be allowed for negotiations. Tunnel will pass only that data which uses the specified protocol.

Local Port	Specify Local Port for TCP or UDP
Remote Port	Specify Remote Port for TCP or UDP
Description	IPSec VPN Connection Description

Table – Add Host-to-Host VPN Connection screen elements

L2TP

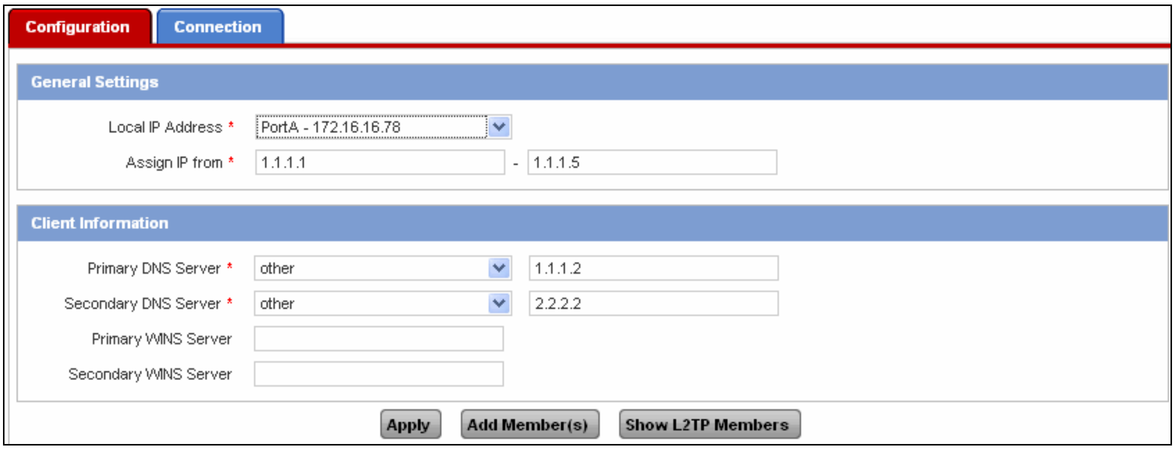
You can use Layer 2 Tunneling Protocol (L2TP) to create VPN tunnel over public networks such as the Internet. For authentication, currently Cyberoam supports only Password Authentication Protocol (PAP) algorithm.

Configuration

To manage L2TP configuration, go to **VPN → L2TP → Configuration**. You can,

- Configure
- Add L2TP Members
- View L2TP Members

L2TP Configuration



General Settings

Local IP Address * PortA - 172.16.16.78

Assign IP from * 1.1.1.1 - 1.1.1.5

Client Information

Primary DNS Server * other 1.1.1.2

Secondary DNS Server * other 2.2.2.2

Primary WINS Server

Secondary WINS Server

Screen – Configure L2TP

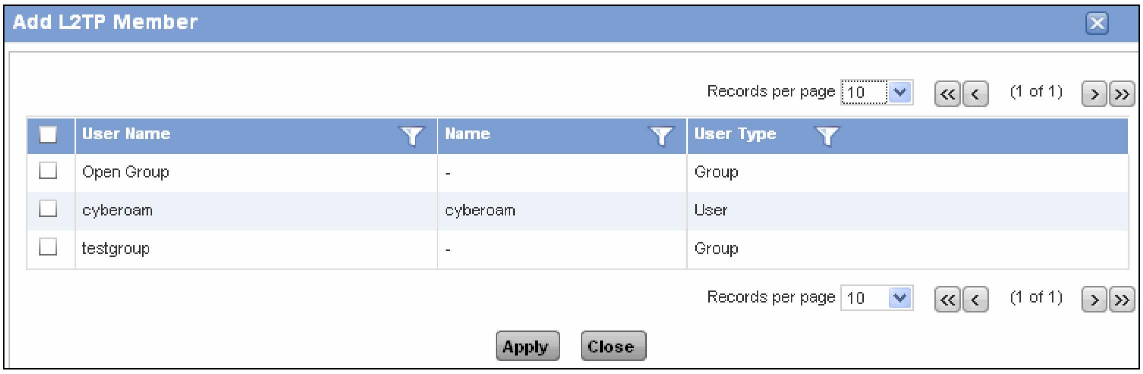
Screen Elements	Description
Local IP Address	Displays local IP address that will be assigned to L2TP server.
Assign IP From	Specify IP address range if L2TP server has to lease IP Addresses.
Client information	
Primary DNS Server	Select Primary DNS Server from the list. Alternately, you can also specify DNS Server by choosing 'Other' from the list.
Secondary DNS Server	Specify Secondary DNS server Alternately, you can also specify DNS Server by choosing 'Other' from the list.

Primary WINS Server	Specify WINS Server
Secondary WINS Server	Specify Alternate WINS Server

Table – Configure L2TP screen elements

Add L2TP Members

Click ‘Add Members’ button to add user or user groups to L2TP members list. A pop-up window is displayed to select the users. You can also select multiple users or user groups.



□	User Name	Name	User Type
□	Open Group	-	Group
□	cyberoam	cyberoam	User
□	testgroup	-	Group

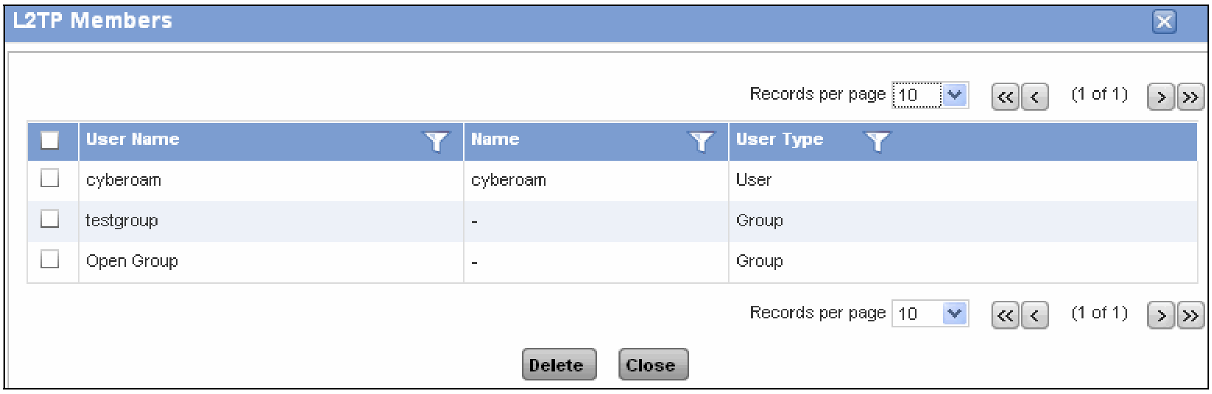
Screen – Add L2TP Members

Select Users or user groups who are to be allowed access through L2TP connection. Click ‘Apply’ button to add these users and user groups to the L2TP members list.

You can also search for users or user groups to be added to the Members list.

View L2TP Members

Click ‘Show L2TP Members’ button to view user or user groups that are in L2TP members list. A pop-up window is displayed to view the users. You can also select multiple users or user groups and delete them.



□	User Name	Name	User Type
□	cyberoam	cyberoam	User
□	testgroup	-	Group
□	Open Group	-	Group

Screen – View L2TP Members

The page displays the list of L2TP members who are allowed access through L2TP connection. To delete users, select ☑ the users to be deleted and click Delete button.

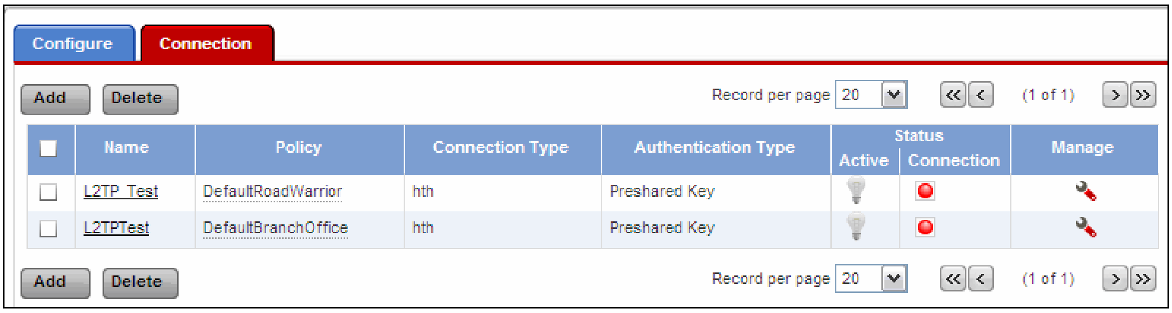
You can also search for users or user groups to be deleted from the Members list.

Connection

To manage L2TP connections, go to **VPN** → **L2TP** → **Connection**.

- Add
- View
- Edit – Click the Edit icon in the Manage column against the L2TP Connection to be modified. Edit L2TP Connection is displayed in a new window which has the same parameters as the Add L2TP Connection window.
- Delete – Click the Delete icon in the Manage column against a L2TP Connection to be deleted. A dialog box is displayed asking you to confirm the deletion. Click OK to delete the L2TP Connection. To delete multiple L2TP Connections, select them ☑ and click the Delete button.

Manage L2TP VPN Connections



□	Name	Policy	Connection Type	Authentication Type	Status		Manage
					Active	Connection	
□	L2TP_Test	DefaultRoadWarrior	hth	Preshared Key	💡	●	🔧
□	L2TPTest	DefaultBranchOffice	hth	Preshared Key	💡	●	🔧

Screen – Manage L2TP Connection

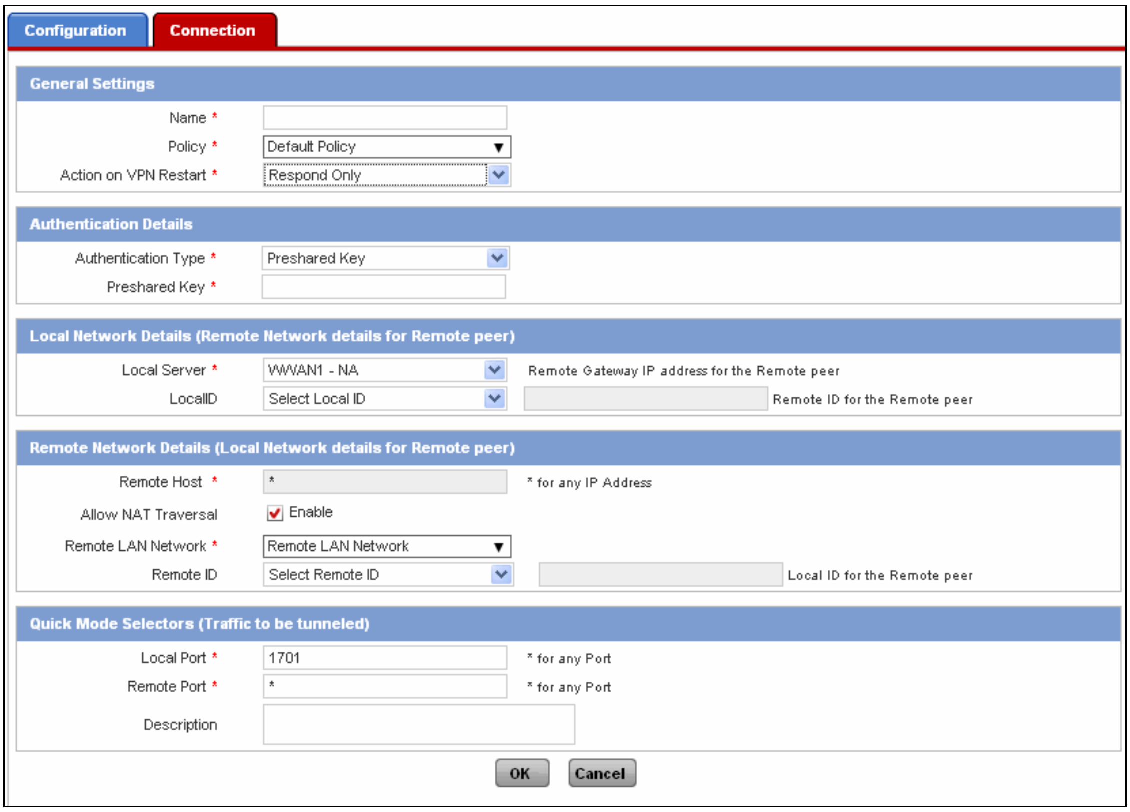
Screen Elements	Description
Add Button	Add a new L2TP Connection
Name	Name of the L2TP Connection
Policy	Name of the VPN Policy selected
Authentication Type	Type of Authentication selected: Preshared Key or Digital Certificate.
Status	Status of the Connection 💡 - Activated connection. Click to deactivate the connection 💡 - Deactivated connection. Click to activate the connection 🔴 - Activated and Disconnected. Click to initiate the connection. 🟢 - Activated and Connected. Click to disconnect the connection. When you disconnect, connection will be deactivated and to re-establish connection the connection, activate connection. 💡 - Activated but Partially connected. Click to disconnect the connection. When multiple subnets are configured for LAN and/or remote network, Cyberoam creates sub-connection for each subnet. Connection Status in Yellow color indicates that one of the sub-connection is not active.
Edit Button	Edit the L2TP VPN Connection

Delete Button	Delete the L2TP VPN Connection Alternately, click the delete icon against the connection to be deleted.

Table – Manage L2TP Connections screen elements

L2TP Connection Parameters

To add or edit L2TP connections, go to **VPN** → **L2TP** → **Connection**. Click Add Button to add a new connection or Edit Icon to modify the details of the connection.



General Settings

Name *

Policy * Default Policy

Action on VPN Restart * Respond Only

Authentication Details

Authentication Type * Preshared Key

Preshared Key *

Local Network Details (Remote Network details for Remote peer)

Local Server * WAN1 - NA   Remote Gateway IP address for the Remote peer

LocalID Select Local ID   Remote ID for the Remote peer

Remote Network Details (Local Network details for Remote peer)

Remote Host * *   * for any IP Address

Allow NAT Traversal ☑ Enable

Remote LAN Network * Remote LAN Network

Remote ID Select Remote ID   Local ID for the Remote peer

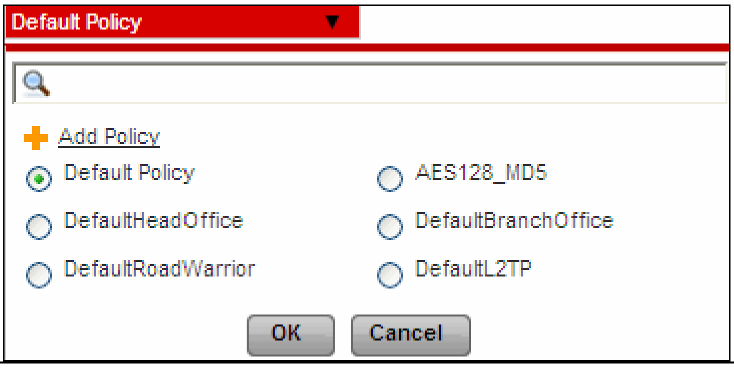
Quick Mode Selectors (Traffic to be tunneled)

Local Port * 1701   * for any Port

Remote Port * *   * for any Port

Description

Screen – Add a L2TP Connection

Screen Elements	Description
Name	Name to identify the L2TP Connection
Policy	Select policy to be used for L2TP connection  Default Policy ▼ Add Policy ● Default Policy ○ AES128_MD5 ○ DefaultHeadOffice ○ DefaultBranchOffice ○ DefaultRoadWarrior ○ DefaultL2TP OK Cancel
Action on VPN Restart	Select the action for the connection.

	Available options: **Respond Only** - Keep connection in disabled till the user responds **Initiate** – Activate connection on system/service start so that the connection can be established whenever required **Disable** - Keep connection disabled till the user activates
Authentication details	
Authentication Type	Select Authentication Type. Authentication of user depends on the connection type. **Available options**: **Preshared key** authentication is a mechanism whereby a single key is used for encryption and decryption. Both the peers should possess the preshared key. Remote peer uses the preshared key for decryption. Specify the preshared key to be used. This preshared key will have to be shared or communicated to the peer at the remote end. At the remote end, client will have to specify this key for authentication. Refer to VPN Client guide, Phase 1 Configuration. If there is mismatch in the key, user will not be able to establish the connection. **Digital Certificate** authentication is a mechanism whereby sender and receiver both use digital certificate issued by the Certificate Authority. Both sender and receiver must have each other’s Certificate Authority. Select the local certificate that should be used for authentication by Cyberoam.
Local network details (remote network details for remote peer)	
Local Server	Select local server.
Local ID	For preshared key and RSA key, select any type of id and specify its value DER ASN1 DN (X.509) is not applicable. In case of Local Certificate, ID and its value is displayed automatically as specified in the Local Certificate.
Remote network details (local network details for remote peer)	
Remote Host	Specify IP address of remote peer/host. Specify * for any IP address.
Allow NAT Traversal	Enable NAT traversal if a NAT device is located between your VPN endpoints i.e. when remote peer has private/non-routable IP address. At a time only one connection can be established behind one NAT-box. By default, it is enabled.
Remote LAN Network	Select IP addresses and netmask of remote network which is allowed to connect to the Cyberoam server through VPN tunnel. Multiple subnets can be specified. Select IP Hosts from the list of IP Hosts available. You can also add a new IP Host and include in the list.

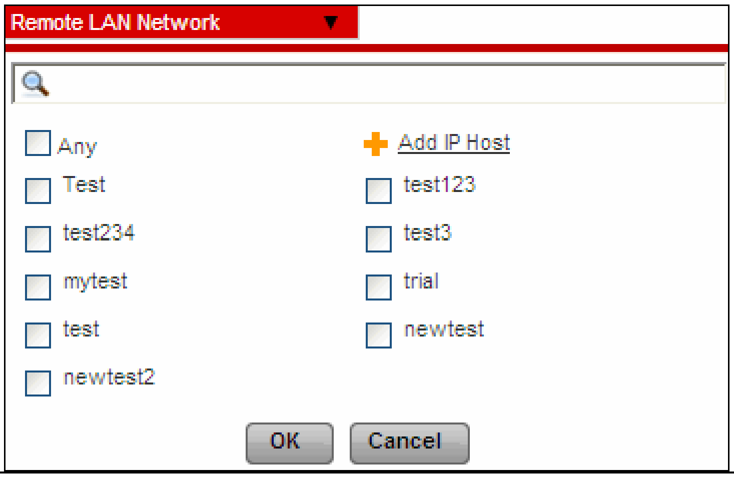
	 Remote LAN Network ▼ □ Any Add IP Host □ Test □ test123 □ test234 □ test3 □ mytest □ trial □ test □ newtest □ newtest2 OK Cancel
Remote ID	For preshared key, select any type of id and specify its value, DER ASN1 DN (X.509) is not applicable.
Quick mode selectors (traffic to be tunneled)	
Local Port	Specify Local Port for TCP or UDP
Remote Port	Specify Remote Port for TCP or UDP
Description	L2TP VPN Connection Description

Table – Add L2TP Connections screen elements

PPTP

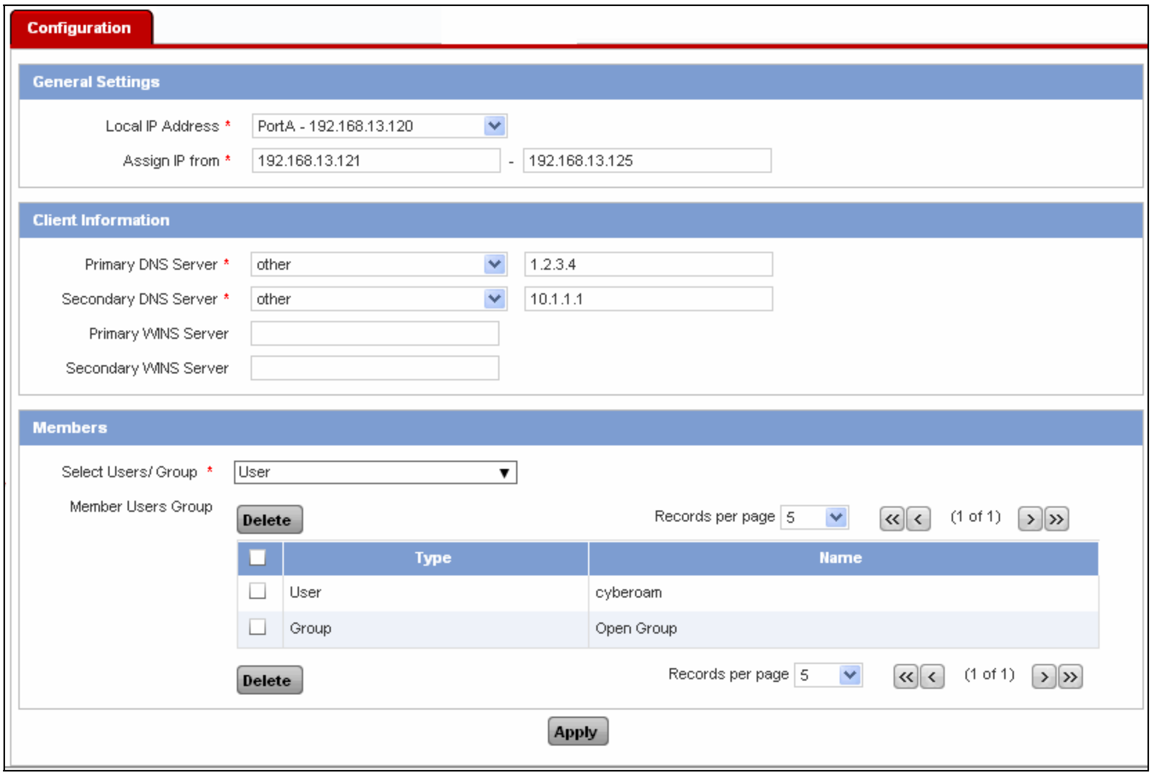
Cyberoam support PPTP to tunnel PPP traffic between two VPN peers. Windows or Linux PPTP clients can establish a PPTP tunnel with a Cyberoam Appliance that has been configured to act as a PPTP server.

PPTP Connection

To manage PPTP configuration,, go to **VPN** → **PPTP** → **Configuration**. You can,

- Configure
- Add PPTP Members
- View PPTP Members

PPTP Configuration



General Settings

Local IP Address * PortA - 192.168.13.120

Assign IP from * 192.168.13.121 - 192.168.13.125

Client Information

Primary DNS Server * other 1.2.3.4

Secondary DNS Server * other 10.1.1.1

Primary WINS Server

Secondary WINS Server

Members

Select Users/ Group * User

Member Users Group

☐	Type	Name
☐	User	cyberoam
☐	Group	Open Group

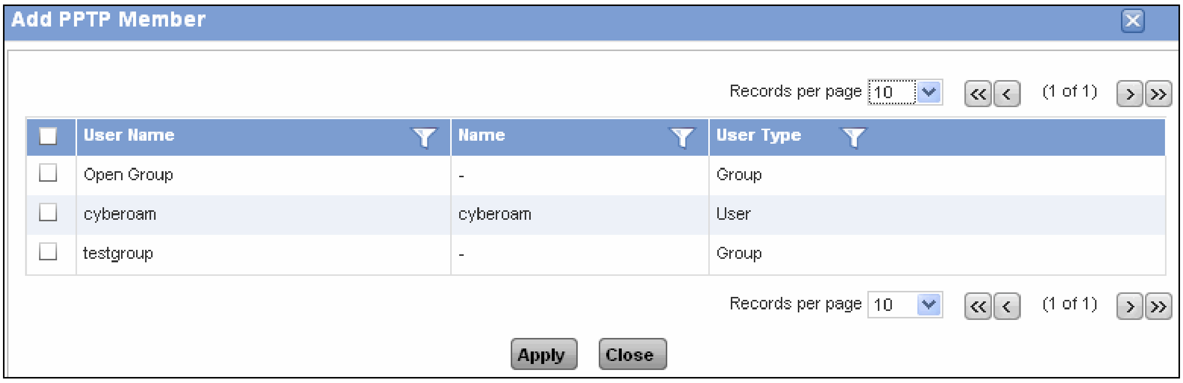
Screen – Configure PPTP

Screen Elements	Description
Local IP Address	Displays local IP address that will be used for PPTP server.
Assign IP From	Specify IP address range. PPTP server will lease IP address to the PPTP client from the specified IP address range. The PPTP client uses the assigned IP address as its source address for the duration of the connection. Do not specify the same IP address range in L2TP configuration and PPTP configuration.
Client information	
Primary DNS Server	Specify DNS Server to be used at the client end
Secondary DNS Server	Specify Alternate DNS server to be used at the client end
Primary WINS Server	Specify WINS Server to be used at the client end
Secondary WINS Server	Specify Alternate WINS Server to be used at the client end

Table – Configure PPTP screen elements

Add PPTP Members

Click ‘Add Members’ button to add user or user groups to PPTP members list. A pop-up window is displayed to select the users. You can also select multiple users or user groups.



Add PPTP Member

☐	User Name	Name	User Type
☐	Open Group	-	Group
☐	cyberoam	cyberoam	User
☐	testgroup	-	Group

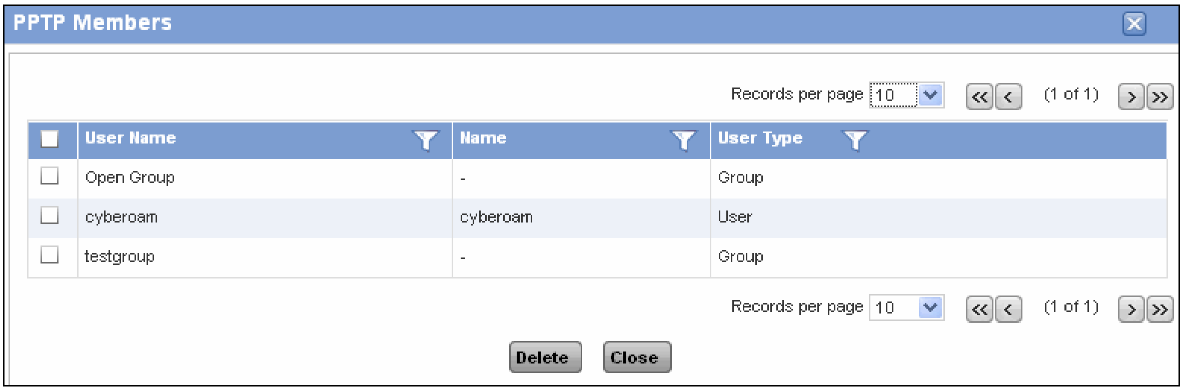
Screen – Add PPTP Members

Select users or user groups who are to be allowed access through PPTP connection. Click 'Apply' button to add these users and user groups to the PPTP members list.

You can also search for users or user groups to be added to the Members list.

View PPTP Members

Click 'Show PPTP Members' button to view user or user groups that are in PPTP members list. A pop-up window is displayed to view the users. You can also select multiple users or user groups and delete them.



PPTP Members

☐	User Name	Name	User Type
☐	Open Group	-	Group
☐	cyberoam	cyberoam	User
☐	testgroup	-	Group

Screen – View PPTP Members

The page displays a list of PPTP members who are allowed access through PPTP connection. To delete users, select ☑ the users to be deleted and click Delete button.

You can also search for users or user groups to be deleted from the Members list.

Failover

Connection Failover is a feature that enables to provide an automatic backup connection for VPN traffic and provide "Always ON" VPN connectivity for IPSec and L2TP connections. If the primary connection fails, the subsequent connection in the Group will take over without manual intervention and keep traffic moving. The entire process is transparent to users.

To configure connection failover, you have to:

- Create Connection Group. Connection Group is the grouping of all the connections that are to be used for failover. The order of connections in the Group defines fail over priority of the connection.

- Define Fail over condition

A VPN group is a set of VPN tunnel configurations i.e. IPSec connections. The Phase 1 and Phase 2 security parameters for each connection in a group can be different or identical except for the IP address of the remote gateway. The order of connections in the Group defines fail over priority of the connection.

Connection included in the Group must be activated and manually connected for the first time before participating in the failover. Connection will not failover to the subsequent connection if it is manually disconnected.

When the primary connection fails, the subsequent active connection in the Group takes over without manual intervention and keep traffic moving. The entire process is transparent to users. For example if the connection established using 4th Connection in the Group is lost then 5th Connections will take over.

Cyberoam considers connection as failed connection if:

- Remote peer does not reply - for Net to Net and Host to Host connection
- Local Gateway fails – for Remote Access connection

Connections that are not the part of the Connection Group will not participate in failover and such connections will not be re-established automatically if lost.

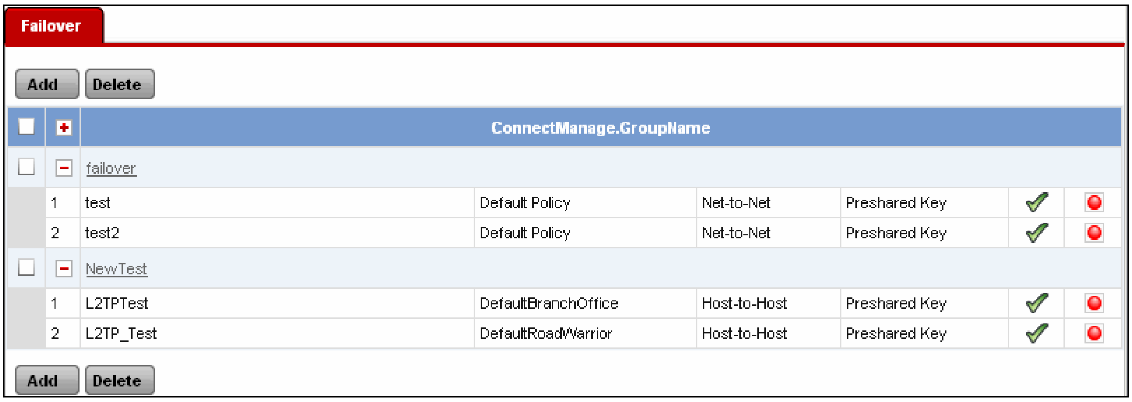
Prerequisites

- Packets of the protocol specified in failover condition must be allowed from local server to remote server and its reply on both Local and Remote server
- One connection can be included in one Group only
- Connection must be ACTIVE to participate in failover

To configure Failover condition for the connection groups, go to **VPN → Failover → Failover**

- Add
- View
- Delete – Click the Delete icon 🗑 in the Manage column against a Connection group to be deleted. A dialog box is displayed asking you to confirm the deletion. Click OK to delete the Connection group. To delete multiple Connection groups, select them ☑ and click the Delete button.

Manage Connection Groups



☐	⊞	ConnectManage.GroupName					
☐	⊟	failover					
	1	test	Default Policy	Net-to-Net	Preshared Key	✓	🔴
	2	test2	Default Policy	Net-to-Net	Preshared Key	✓	🔴
☐	⊟	NewTest					
	1	L2TPTest	DefaultBranchOffice	Host-to-Host	Preshared Key	✓	🔴
	2	L2TP_Test	DefaultRoadWarrior	Host-to-Host	Preshared Key	✓	🔴

Screen – Manage Connection Failover Group

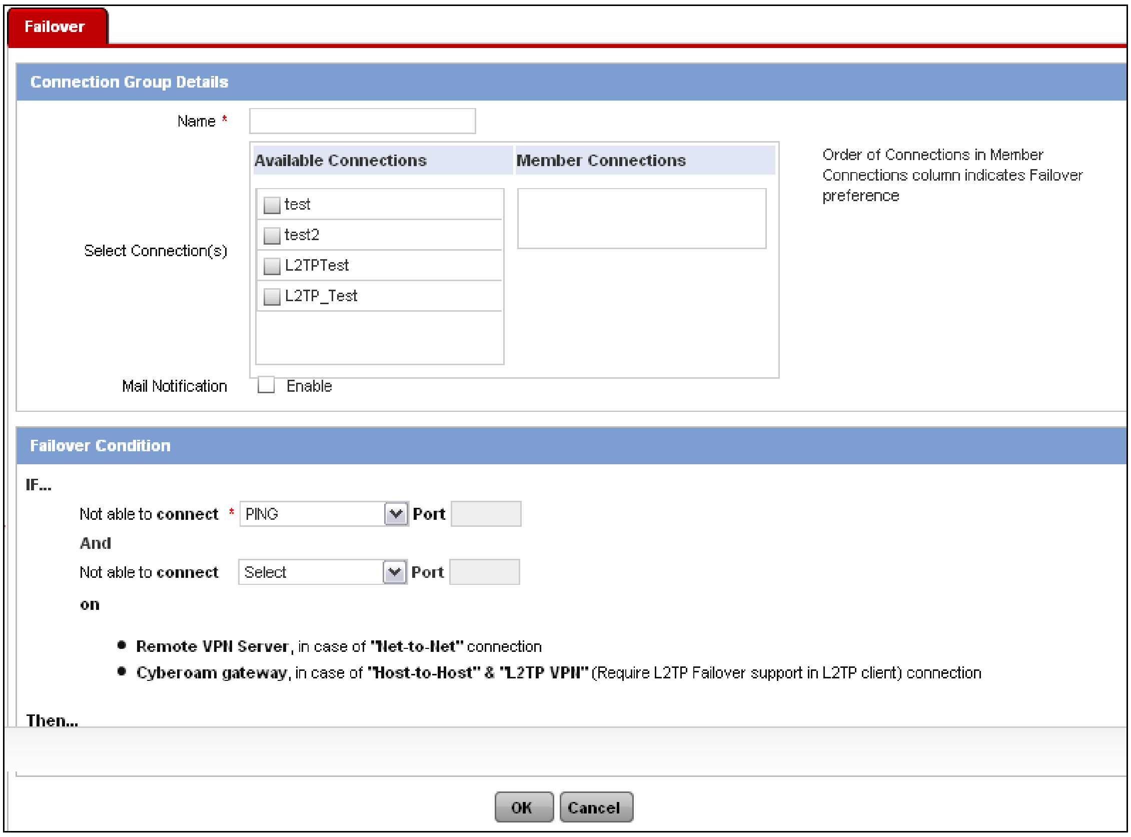
Screen Elements	Description
Add Button	Add a new connection group
Connection Group Name	Name to identify the Connection Group
Member Connections	Selected Connections for Failover
Member Connection Status	Status of the Connection ✓ - Activated connection ✗- Deactivated connection 🔴- Activated and Disconnected 🟢- Activated and Connected 🟠 - Activated but partially connected
Delete Button	Delete the connection group Alternately, click the delete icon against the group to be deleted.

Table – Manage Connection Failover Groups screen elements

Click drop down ⊞ icon against the Connection Group name to view the list of Connections in the Group.

Failover Connection Group Parameters

To add connection groups and failover conditions, go to **VPN → Failover → Failover**. Click Add Button to add a new connection. Failover Connection Group Parameters are given below.



Failover

Connection Group Details

Name *

Select Connection(s)

Available Connections	Member Connections
□ test □ test2 □ L2TPTest □ L2TP_Test	

Order of Connections in Member Connections column indicates Failover preference

Mail Notification □ Enable

Failover Condition

IF...

Not able to connect * PING Port

And

Not able to connect Select Port

on

- **Remote VPN Server**, in case of **"Net-to-Net"** connection
- **Cyberoam gateway**, in case of **"Host-to-Host" & "L2TP VPN"** (Require L2TP Failover support in L2TP client) connection

Then...

Screen – Add a Connection Failover Group

Screen Elements	Description
Name	Specify a name for connection group
Select Connections	'Available Connections' list displays the list of connections that can be added to the failover group. Click on the connections to be added to Member connections list. Cyberoam will select the subsequent active connection from Member Connections list if primary connection fails. Top down order of connections in the Member Connections list specifies the failover preference i.e. if primary connection fails, the very next connection in the list will be used by Cyberoam to keep the VPN traffic moving. Use Move Up and Move Down to change the order. Once the connection is included in any Group, it will not be displayed in 'Available Connection' list. Remote Access connections will not be listed in 'Available Connections' list. You need to define minimum 2 member connections in a Group.
Mail Notification	Enable Mail Notification to receive Connection failure notification incase connection fails. Notification is mailed on the email address configured in Email Settings from the Network Configuration Wizard.
Failover Condition	
IF	Specify Failover condition. Cyberoam checks for the connection failure after every 30 seconds and if failure is detected, VPN traffic is transferred through the subsequent connection

	specified in the Connection Group. Cyberoam considers connection as failed connection if: **Remote server does not reply** - for Site-to-Site connection **Cyberoam Gateway fails** – for Host-to-Host, L2TP VPN, Remote Access connection Specify communication Protocol i.e. TCP, UDP, PING. Select the protocol depending on the service to be tested on the remote server or local gateway depending on type of connection A request on the specified port is send and if it is not responded, Cyberoam considers the Connection as failed and shift the traffic to the subsequent connection. Fail over condition is not applicable if: Connection is manually disconnected from either of the ends. Connection not included in any Group.

Table – Add Connection Failover Group screen elements

Live Connections

View the list of all the connected IPSec tunnels from **VPN → Live Connections → IPSec Connections**.

Page displays important parameters like Name, Local Server, Local Subnet, User Name, Remote Server / Host and Remote Subnet.

Page allows administrator to disconnect any of the IPSec connection. Click the ‘Disconnect’ button to disconnect live connections.