CHAPTER 14

VPN Global Settings

These help topics describe the VPN Global Settings windows.

VPN Global Settings

This window displays the VPN global settings for the router.

Edit Button

Click the Edit button to add or change VPN global settings.

Enable IKE

The value is True if IKE is enabled; it is False if IKE is disabled.

Note

If IKE is disabled, VPN configurations will not operate.

Enable Aggressive Mode

The value is True if Aggressive Mode is enabled; it is False if Aggressive Mode is disabled. The Aggressive Mode feature allows you to specify RADIUS tunnel attributes for an IPSec peer and to initiate an IKE aggressive mode negotiation with the tunnel attributes.
XAuth Timeout

The number of seconds the router is to wait for a system to respond to the XAuth challenge.

IKE Identity

Either the host name of the router or the IP address that the router will use to identify itself in IKE negotiations.

Dead Peer Detection

Dead Peer Detection (DPD) enables a router to detect a dead peer and, if detected, delete the IPSec and IKE security associations with that peer.

IKE Keepalive (Sec)

The value is the number of seconds that the router waits between sending IKE keepalive packets.

IKE Retry (Sec)

The value is the number of seconds that the router waits between attempts to establish an IKE connection with the remote peer. By default, “2” seconds is displayed.

DPD Type

Either On Demand or Periodic.

If set to On Demand, DPD messages are sent on the basis of traffic patterns. For example, if a router has to send outbound traffic and the liveliness of the peer is questionable, the router sends a DPD message to query the status of the peer. If a router has no traffic to send, it never sends a DPD message.

If set to Periodic, the router sends DPD messages at the interval specified by the IKE Keepalive value.

IPSec Security Association (SA) Lifetime (Sec)

The amount of time after which IPSec security associations (SAs) will expire and be regenerated. The default is 3600 seconds (1 hour).
IPSec Security Association (SA) Lifetime (Kilobytes)

The number of kilobytes that the router can send over the VPN connection before the IPSec SA expires. The SA will be renewed after the shortest lifetimes is reached.

VPN Global Settings: IKE

This window lets you specify global settings for IKE and IPSEC.

Enable IKE

Leave this box checked if you want to use VPN.

⚠️ Caution
If IKE is disabled, VPN configurations will not work.

Enable Aggressive mode

The Aggressive Mode feature allows you to specify RADIUS tunnel attributes for an IPSec peer and to initiate an IKE aggressive mode negotiation with the tunnel attributes.

Identity (of this router)

This field specifies the way the router will identify itself. Select either IP address or host name.

XAuth Timeout

The number of seconds the router is to wait for a response from a system requiring XAuth authentication.

Enable Dead Peer Detection (DPD)

Dead Peer Detection (DPD) enables a router to detect a dead peer and, if detected, delete the IPSec and IKE security associations with that peer.

The Enable Dead Peer Detection checkbox is disabled when the Cisco IOS image that the router is using does not support DPD.
Keepalive
Specify the number of seconds that the router should maintain a connection when it is not being used.

Retry
Specify the number of seconds that the router should wait between attempts to establish an IKE connection with a peer. The default value is ‘2’ seconds.

DPD Type
Select On Demand or Periodic.
If set to On Demand, DPD messages are sent on the basis of traffic patterns. For example, if a router has to send outbound traffic and the liveliness of the peer is questionable, the router sends a DPD message to query the status of the peer. If a router has no traffic to send, it never sends a DPD message.
If set to Periodic, the router sends DPD messages at the interval specified by the IKE Keepalive value.

VPN Global Settings: IPSec
Edit global IPSec settings in this window.

Authenticate and Generate new key after every
Check this box and specify the time interval at which the router should authenticate and generate a new key. If you do not specify a value, the router will authenticate and generate a new key every hour.

Generate new key after the current key encrypts a volume of
Check this box and specify the number of kilobytes that should be encrypted by the current key before the router authenticates and generates a new one. If you do not specify a value, the router will authenticate and generate a new key after the current key has encrypted 4,608,000 kilobytes.
VPN Key Encryption Settings

The VPN Key Encryption Settings window appears if the Cisco IOS image on your router supports Type 6 encryption, also referred to as *VPN key encryption*. You can use this window to specify a master key to use when encrypting VPN keys, such as pre-shared keys, Easy VPN keys, and XAuth keys. When encrypted, these keys will not be readable by someone viewing the router’s configuration file.

Enable VPN Keys Encryption

Check to enable encryption of these keys.

Current Master Key

This field contains asterisks (*) when a master key has been configured.

New Master Key

Enter a new master key in this field. Master keys must be at least 8 characters long and can be as long as 128 characters.

Confirm Master Key

Reenter the master key in this field for confirmation. If the values in this field and in the New Master Key field do not match, Cisco SDM prompts you to reenter the key.