Configuring VPN

This chapter provides conceptual information about Virtual Private Networks (VPN) configuration and management on the Cisco 910 Industrial Routers (*hereafter* referred to as the router).

Understanding VPN Connection Types

As a machine-to machine (M2M) gateway, the router collects the information reported by every sensor. The reported information should be protected when it is transfered through Internet. In a typical deployment scenario of the router, the main purpose of VPN is to provide a security path for transporting sensor data to admin.

The following VPN connection types are supported on the router:

PPTP

Point-to-Point Tunneling Protocol (PPTP) is a Layer 2 tunneling protocol which allows a remote client to use a public IP network in order to communicate securely with servers at a private corporate network. PPTP tunnels the IP.

IPsec

Internet Protocol Security (IPsec) is a protocol suite for securing Internet Protocol (IP) communications by authenticating and encrypting each IP packet of a communication session. IPsec includes protocols for establishing mutual authentication between agents at the beginning of the session and negotiation of cryptographic keys to be used during the session. IPsec can be used in protecting data flows between a pair of hosts (host-to-host), between a pair of security gateways (site-to-site), or between a security gateway and a host (remote-access).

IPsec uses cryptographic security services to protect communications over Internet Protocol (IP) networks. IPsec supports network-level peer authentication, data origin authentication, data integrity, data confidentiality (encryption), and replay protection.

IPsec is an end-to-end security scheme operating in the Internet Layer of the Internet Protocol Suite, while some other Internet security systems in widespread use, such as Transport Layer Security (TLS) and Secure Shell (SSH), operate in the upper layers at Application layer. Hence, only IPsec protects any application traffics over an IP network. Applications can be automatically secured by its IPsec at the IP layer. Without IPsec, the protocols of TLS/SSL must be inserted under each of applications for protection.

L2TP

Layer 2 Tunneling Protocol (L2TP) is a tunneling protocol used to support VPNs or as part of the delivery of services by ISPs. It does not provide any encryption or confidentiality by itself. Rather, it relies on an encryption protocol that it passes within the tunnel to provide privacy.

L2TP with IPsec

Because of the lack of confidentiality inherent in the L2TP protocol, it is often implemented along with IPsec. By using L2TP with IPsec, L2TP packets between the endpoints are encapsulated by IPsec.

The configuration of L2TP with IPsec supports certificates using the preshared keys or RSA signature methods.

Configuring PPTP

Beginning in privileged EXEC mode, follow these steps to configure PPTP on the router:

	Command	Purpose
Step 1	**configure terminal**	Enter global configuration mode.
Step 2	**crypto vpn {l2tp | ipsec | pptp | l2tp_ipsec}** *profile-name*	Connect to the VPN service. Choose one of the following types: l2tp, ipsec, pptp, or l2tp_ipsec. For *profile-name*: enter the target tunnel profile or name. **Note** The command should be activated again if the profile configuration is changed. **Note** Use “no crypto vpn” to disconnect from a VPN tunnel.
Step 3	**vpdn-group** *name*	Associates a VPDN group with a customer or VPDN profile.
Step 4	**request dialin**	Create a request dial-in VPDN subgroup that configures the router to request the establishment of a dial-in tunnel to a tunnel server, and enters VPDN request-dialin group configuration mode.
Step 5	**protocol pptp**	Specifies the tunneling protocol that a VPDN subgroup will use.
Step 6	**initiate-to** *ip-address*	Specifies the IP address (VPN server) that will be tunneled to.
Step 7	**interface dialer** *number*	Create a Dialer interface. The interface number will fall within the scope of 0~255

	Command	Purpose
Step 8	**ip address negotiated**	Specify that the IP address for a particular interface is obtained via PPP/IPCP address negotiation.
Step 9	**dialer-group** *number*	Assign the dialer interface to a dialer group. This command applies the interesting traffic definition to the interface.
Step 10	**ppp authentication chap**	Set the PPP authentication method to Challenge Handshake Authentication Protocol (CHAP)
Step 11	**ppp chap hostname** *username*	Define an interface-specific CHAP hostname.
Step 12	**ppp chap password** *password*	Define an interface-specific CHAP password.
Step 13	**ppp encrypt mppe auto**	Enable Microsoft Point-to-Point Encryption (MPPE) on the virtual template.
Step 14	**exit**	Return to global configuration mode.
Step 15	**show interface Dialer** *interface-number*	(Optional) Show interface statistics.
Step 16	**show vpdn tunnel pptp**	(Optional) Display details about PPTP active VPDN tunnel.
Step 17	**show vpdn session pptp**	(Optional) Display details about PPTP active VPDN session.
Step 18	**copy running-config startup-config**	(Optional) Save your entries in the configuration file.

The following example shows how to configure PPTP client on the router:

```
Router# configure terminal
Router(config)# vpdn-group 2
Router(config-vpdn)# request-dialin
Router(config-vpdn-req-in)# protocol pptp
Router(config-vpdn-req-in)# exit
Router(config-vpdn)# initiate-to 172.19.66.181
Router(config-vpdn)# exit
Router(config)# interface Dialer 2
Router(config-if)# ip address negotiated
Router(config-if)# dialer-group 2
Router(config-if)# ppp encrypt mppe auto
Router(config-if)# ppp authentication ms-chap-v2
Router(config-if)# ppp chap hostname vpn
Router(config-if)# ppp chap password cisco123
Router(config-if)# exit
```

The following example shows a sample output of the **show interface Dialer** command:

```
Router# show interface dialer 2
Dialer2 Link encap:Point-to-Point Protocol
          inet addr:192.168.3.148  P-t-P:192.168.3.148  Mask:255.255.255.255
          UP POINTOPOINT RUNNING NOARP MULTICAST  MTU:1396  Metric:1
          RX packets:12 errors:0 dropped:0 overruns:0 frame:0
          TX packets:9 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:3
          RX bytes:210 (210.0 B)  TX bytes:102 (102.0 B)
```

The following example shows a sample output of the **show vpdn tunnel pptp** command:

```
Router# show vpdn tunnel pptp
PPTP Tunnel Information Total tunnels 1 Sessions 1
  Remote Address    Port    Sessions    State
    192.168.1.2    1723    1    established
```

The following example shows a sample output of the **show vpdn session pptp** command:

```
Router# show vpdn session pptp
PPTP Tunnel Information Total tunnels 1 Sessions 1
```

```
Interface    Local Address    Username    State
Dialer20    192.168.1.6    cisco_client    established
```

Configuring IPsec

Beginning in privileged EXEC mode, follow these steps to configure IPsec on the router:

	Command	Purpose
Step 1	**configure terminal**	Enter global configuration mode.
Step 2	**crypto vpn {l2tp | ipsec | pptp | l2tp_ipsec}** *profile-name*	Connect to the VPN service. Choose one of the following types: l2tp, ipsec, pptp, or l2tp_ipsec. For *profile-name*: enter the target tunnel profile or name. **Note** The command should be activated again if the profile configuration is changed. **Note** Use "no crypto vpn" to disconnect from a VPN tunnel.
Step 3	**crypto isakmp profile** *name*	Set IPsec VPN profile.
Step 4	**set peer** {**address** *ip-address* | **host** *fqdn-hostname*}	Set peer VPN ip address.
Step 5	**self-identity** {**address** *ip-address* | **user-fqdn** *fqdn-hostname*}	(Optional) To define the ISAKMP identity used by the router when participating in the Internet Key Exchange (IKE) protocol. Default value is the WAN IP address of the router. For *ip-address*: set the ISAKMP identity to the IP address of the interface that is used to communicate to the remote peer during IKE negotiations. For *fqdn-hostname*: set the ISAKMP identity to the host name concatenated with the domain name (for example, myhost.example.com). **Note** Self-identity is not supported in main mode.
Step 6	**match identity** {**address** *ip-address* | **user-fqdn** *fqdn-hostname*}	(Optional) To define the ISAKMP identity used by the peer server when participating in the Internet Key Exchange (IKE) protocol. Default value is the WAN IP address of the peer server. For *ip-address*: set the ISAKMP identity to the IP address of the interface that is used to communicate to the remote peer during IKE negotiations. For *fqdn-hostname*: set the ISAKMP identity to the host name concatenated with the domain name (for example, myhost.example.com). **Note** Self-identity is not supported in main mode.
Step 7	**match address** {**remote-access** | **site-to-site** *local-subnet local-netmask peer-subnet peer-netmask*}	(Optional) Define the VPN type. If the option is not set, default value is host-to-host.
Step 8	**initiate mode** {**aggressive** | **main**}	(Optional) Define the ISAKMP operation mode. Default value is main mode.
Step 9	**keepalive** *seconds*	(Optional) Set the number of seconds between DPD messages. The range is from 10 to 3600 seconds. The connection would be dropped after 5 messages. Default value is 30s.

	Command	Purpose
Step 10	**xauth-identity** *name* **xauth-password** *password*	(Optional) Set Xauth identity name and password. If the option is set, xauth would be enabled. **Note** Xauth is not supported for site-to-site type.
Step 11	**policy authentication** {**pre-share** | **rsa-sig**}	Set authentication for ISAKMP to pre-shared key or certificate authentication. **Note** Certificate is not supported for aggressive mode. It works only for the main mode.
Step 12	**passphrase** *password-phrase*	(Optional) Set rsa-sig private key pass phrase.
Step 13	**pre-share-key** *keystring*	(Optional) Set pre-share key value.
Step 14	**exit**	Return to global configuration mode.
Step 15	**show crypto isakmp sa**	(Optional) Display details about ISAKMP SA.
Step 16	**show crypto ipsec sa**	(Optional) Display details about IPsec SA.
Step 17	**copy running-config startup-config**	(Optional) Save your entries in the configuration file.

Table 18-1shows the limitations of the IPsec configuration.

Table 18-1 Limitations of the IPsec Configuration

	main	aggressive	main and Xauth	aggressive and Xauth
remote-access-psk	No	Yes	Yes	Yes
remote-access-rsa	No	No	Yes	No
site-to-site-psk	Yes	Yes	No	No
site-to-site-rsa	Yes	No	No	No

The following example shows how to configure IPsec remote-access type with RSA authentication on the router:

```
Router# configure terminal
Router(config)# crypto isakmp profile remote-access-cert
Router(config-ipsec-pf)# set peer address 10.0.1.200
Router(config-ipsec-pf)# match address remote-access
Router(config-ipsec-pf)# xauth-identity justin xauth-password cisco123
Router(config-ipsec-pf)# policy authentication rsa-sig
Router(config-ipsec-pf)# passphrase 123456
Router(config-ipsec-pf)# exit
Router(config)#
```

The following example shows how to configure IPsec remote-access type with PSK authentication on the router:

```
Router# configure terminal
Router(config)# crypto isakmp profile remote-access-psk
Router(config-ipsec-pf)# set peer address 10.0.1.200
Router(config-ipsec-pf)# self-identity user-fqdn access
Router(config-ipsec-pf)# initiate mode aggressive
Router(config-ipsec-pf)# match address remote-access
Router(config-ipsec-pf)# policy authentication pre-share
Router(config-ipsec-pf)# pre-share-key cisco123
Router(config-ipsec-pf)# xauth-identity justin xauth-password cisco123
Router(config-ipsec-pf)# exit
```

```
Router(config)#
```

The following example shows how to configure IPsec site-to-site type with RSA authentication on the router:

```
Router# configure terminal
Router(config)# crypto isakmp profile site2site-cert
Router(config-ipsec-pf)# set peer address 10.0.1.200
Router(config-ipsec-pf)# match address site-to-site 192.168.30.0 255.255.255.0
192.168.20.0 255.255.255.0
Router(config-ipsec-pf)# initiate mode main
Router(config-ipsec-pf)# policy authentication rsa-sig
Router(config-ipsec-pf)# passphrase 123456
Router(config-ipsec-pf)# exit
Router(config)#
```

The following example shows how to configure IPsec site-to-site type with PSK authentication on the router:

```
Router# configure terminal
Router(config)# crypto isakmp profile site2site-psk
Router(config-ipsec-pf)# set peer address 10.0.1.200
Router(config-ipsec-pf)# match address site-to-site 192.168.30.0 255.255.255.0
192.168.20.0 255.255.255.0
Router(config-ipsec-pf)# initiate mode main
Router(config-ipsec-pf)# policy authentication pre-share
Router(config-ipsec-pf)# pre-share-key cisco123
Router(config-ipsec-pf)# exit
Router(config)#
```

Configuring L2TP

Beginning in privileged EXEC mode, follow these steps to configure L2TP on the router:

	Command	Purpose
Step 1	**configure terminal**	Enter global configuration mode.
Step 2	**crypto vpn {l2tp | ipsec | pptp | l2tp_ipsec}** *profile-name*	Connect to the VPN service. Choose one of the following types: l2tp, ipsec, pptp, or l2tp_ipsec. For *profile-name*: enter the target tunnel profile or name. **Note** The command should be activated again if the profile configuration is changed. **Note** Use “no crypto vpn” to disconnect from a VPN tunnel.
Step 3	**vpdn-group** *name*	Associates a VPDN group with a customer or VPDN profile.
Step 4	**request dialin**	Create a request dial-in VPDN subgroup that configures the router to request the establishment of a dial-in tunnel to a tunnel server, and enters VPDN request-dialin group configuration mode.
Step 5	**protocol l2tp**	Specifies the tunneling protocol that a VPDN subgroup will use.
Step 6	**initiate-to** *ip-address*	Specify the IP address (VPN server) that will be tunneled to.

	Command	Purpose
Step 7	**l2tp security crypto-profile** *profile-name*	Configure IP Security (IPsec) protection of Layer 2 Tunnel Protocol (L2TP). For *profile-name*, specify the name of the crypto profile to be used for IPsec protection of tunneled PPP sessions.
Step 8	**interface dialer** *number*	Create a Dialer interface. The interface number will fall within the scope of 0~255
Step 9	**ip address negotiated**	Specify that the IP address for a particular interface is obtained via PPP/IPCP address negotiation.
Step 10	**dialer-group** *number*	Assign the dialer interface to a dialer group. This command applies the interesting traffic definition to the interface.
Step 11	**ppp authentication chap**	Set the PPP authentication method to Challenge Handshake Authentication Protocol (CHAP)
Step 12	**ppp chap hostname** *username*	Define an interface-specific CHAP hostname.
Step 13	**ppp chap password** *password*	Define an interface-specific CHAP password.
Step 14	**exit**	Return to global configuration mode.
Step 15	**show interface Dialer** *interface-number*	(Optional) Show interface statistics.
Step 16	**show vpdn tunnel l2tp**	(Optional) Display details about L2TP active VPDN tunnel.
Step 17	**copy running-config startup-config**	(Optional) Save your entries in the configuration file.

The following example shows how to configure L2TP with IPsec on the router:

```
Router# configure terminal
Router(config)# vpdn-group 2
Router(config-vpdn)# request-dialin
Router(config-vpdn-req-in)# protocol l2tp
Router(config-vpdn-req-in)# exit
Router(config-vpdn)# initiate-to 172.19.66.213
Router(config-vpdn)# l2tp security crypto-profile ipsec1
Router(config-vpdn)# exit
Router(config)# interface Dialer 2
Router(config-if)# ip address negotiated
Router(config-if)# dialer-group 1
Router(config-if)# ppp encrypt mppe auto
Router(config-if)# ppp authentication ms-chap-v2
Router(config-if)# ppp chap hostname test
Router(config-if)# ppp chap password test
Router(config-if)# exit
```

The following example shows a sample output of the **show interface Dialer** command:

```
Router# show interface dialer 0
Link encap:Point-to-Point Protocol
inet addr:192.168.1.128  P-t-P:192.168.1.99  Mask:255.255.255.255
UP POINTOPOINT RUNNING NOARP MULTICAST  MTU:1410  Metric:1
RX packets:5 errors:0 dropped:0 overruns:0 frame:0
TX packets:5 errors:0 dropped:0 overruns:0 carrier:0
collisions:0 txqueuelen:3
RX bytes:234 (234.0 b)  TX bytes:240 (240.0 b)
```

The following example shows a sample output of the **show vpdn tunnel l2tp** command:

```
Router# show vpdn tunnel l2tp
L2TP Tunnel Information Total tunnels 1
  Remote Address    Port    State
  192.168.1.99      1701    established
```