

Establish IPsec VPN between Cisco and IR900

Configure Cisco Router

Current configuration : 1603 bytes

```

!
crypto isakmp policy 1                                //define IKE Policy
  encr 3des                                           //define 3des cryptographic algorithm
  hash md5                                           //define md5 hashing algorithm
  authentication pre-share                           //define to pre-shared key authentication mode
  group 2                                             //define Diffie-Hellman identifier
crypto isakmp key abc123 address 0.0.0.0 0.0.0.0    //configure pre-shared key to abc123 (according to your need),
                                                    the other side of VPN is 0.0.0.0 (because InRouter's IP is always dynamic IP)
!
!
crypto ipsec transform-set ESP-3DES-MD5 esp-3des esp-md5-hmac //create mapping ensemble esp-3des esp-md5-hmac,
                                                    "ESP-3DES-MD5" is the name of mapping
                                                    ensemble.
!
!
!
crypto dynamic-map DYNMAP 100                        //create dynamic security map DYNMAP 100
  set transform-set ESP-3DES-MD5                    //use the mapping ensemble mentioned above
  ESP-3DES-MD5
  match address 100                                  //quoted the access-list to determine the flow of protected
!
!
crypto map OUTSIDE_MAP 10000 ipsec-isakmp dynamic DYNMAP //put dynamic map into formal map
                                                    "OUTSIDE_MAP" is the name of formal map
!
!
!
!
interface FastEthernet0/0
  ip address 219.239.xxx.xxx 255.255.255.240
  ip nat outside
  duplex auto
  speed auto
  crypto map OUTSIDE_MAP                            //apply confidentiality map to FastEthernet0/0
!

interface FastEthernet0/1
    
```

```

ip address 192.168.1.1 255.255.255.0
ip nat inside
duplex auto
speed auto
!
ip nat inside source list 101 interface FastEthernet0/0 overload //configure NAT, the access from 192.168.1.0/24 to
192.168.2.0/24 is not translated , other access will be translated to IP address on
FastEthernet0/0
ip route 0.0.0.0 0.0.0.0 219.239.xxx.xxx //configure RIP
!
no ip http server
no ip http secure-server
!
access-list 100 permit ip 192.168.1.0 0.0.0.255 192.168.2.0 0.0.0.255 //define VPN protected flow
access-list 101 deny ip 192.168.1.0 0.0.0.255 192.168.2.0 0.0.0.255 //define NAT regulated access-list
access-list 101 permit ip 192.168.1.0 0.0.0.255 any
!
end

```

Configure IR900

1. Click “Wizard” to create a new IPsec Tunnel:

The screenshot shows the InHand network management interface. On the left is a navigation menu with categories: Administration, Layer2 Switch, Network, Link Backup, Routing, Firewall, QoS, VPN, Industrial, Tools, and Wizards. The 'Wizards' menu item is highlighted with a red box. The main content area is titled 'Wizards >> New IPsec Tunnel' and has two tabs: 'Status' and 'Basic Setup'. The 'Status' tab is active, displaying 'System Status' information for a Router (IR915P). Below the status information is a list of configuration options, with 'New IPsec Tunnel' highlighted by a red box. Other options include 'New LAN', 'New WAN', 'New Cellular', and 'IPsec Expert Config'. A 'Sync Time' button is visible next to the system status information.

System Status	
Name	Router
Model	IR915P
Serial Number	RP9151406232931
MAC Address	0018.0505.9bb1
	0018.0505.9bb2
Current Version	1.0.0.r8618
Current Bootloader Version	2011.09.r5656
Router Time	2016-11-15 11:19:31
	2016-11-15 11:18:15
	0 day, 00:01:16
	0.19 / 0.08 / 0.03
	120.18MB / 71.45MB (59.46%)

- Administration
- Layer2 Switch
- Network
- Link Backup
- Routing
- Firewall
- QoS
- VPN
- Industrial
- Tools
- Wizards

Save Configuration

Copyright ©2001-2016
InHand Networks Co., Ltd.
All rights reserved.

Wizards >> New IPsec Tunnel

New IPsec Tunnel

Basic Parameters

Tunnel ID: 1

Map Interface: cellular 1

Destination Address: 203.86.63.238

Negotiation Mode: Main Mode

Local Subnet: 192.168.2.1

Local Netmask: 255.255.255.0

Remote Subnet: 192.168.11.1

Remote Netmask: 255.255.255.0

Phase 1 Parameters

IKE Policy: 3DES-MD5-DH2

IKE Lifetime: 86400 s

Local ID Type: IP Address

Local ID:

Remote ID Type: IP Address

Remote ID:

Authentication Type: Shared Key

Key:

Phase 2 Parameters

IPSec Policy: 3DES-MD5-96

IPSec Lifetime: 3600 s

Basic Parameters: set basic parameters of IPSec tunnel.

Destination Address: set to VPN server IP/domain, e.g.: server IP address is 203.86.63.238

Startup Modes: select Auto Activated.

Negotiation Mode: optional between Main Mode and Aggressive Mode. Generally, select Main Mode.t

Local Subnet: IPSec local subnet protected. E.g.: 192.168.2.1. *It's the InRouter subnet, you can set InRouter LAN address*

Local Net Mask: IPSec local Net Mask protected. E.g.: 255.255.255.0.

Remote Subnet: IPSec remote subnet protected. E.g.: 192.168.11.1. *It's the ZyXel firewall intranet, you can set the subnet which your business server is in.*

Remote Net Mask: IPSec remote Net Mask protected. E.g.: 255.255.0.0.

Phase 1 Parameters: configure parameters during the Phase 1 of IPSec negotiation.

IKE Policy: optional between 3DES-MD5-96 and AES-MD5-96, suggest selecting 3DES-MD5-96.

IKE Lifetime: the default is 86400 seconds.

Local ID Type: optional among FQDN, USERFQDN, IP address, suggest selecting IP address.

Remote ID Type: optional among FQDN, USERFQDN, IP address, suggest selecting IP address.

Authentication Type: optional between Shared Key and Certificate, generally choose Shared Key.

Key: set IPsec VPN negotiating key.

Phase 2 Parameters: configure parameters during the Phase 2 of IPsec negotiation.

IPsec Policy: optional between 3DES-MD5-96 and AES-MD5-96, suggest selecting 3DES-MD5-96.

IPsec Lifetime: the default is 3600 seconds.

2. Click “Apply” to finish adding IPsec Tunnel:

The screenshot shows the InHand Networks configuration interface for VPN >> IPsec. It includes a sidebar with navigation options like Administration, Layer2 Switch, Network, Link Backup, Routing, Firewall, QoS, VPN, Industrial, Tools, and Wizards. The main content area has tabs for Status, IPsec Setting, and IPsec Extern Setting. Under IPsec Setting, there are three sections: IKEv2 Policy, IPsec Policy, and IPsec Tunnels. The IPsec Tunnels section is highlighted with a red box and contains a table with the following data:

Name	Status	Local Subnets	Remote Subnets	Interface	IKE Version
IPsec2_203.86.63.238	Disconnected	192.168.2.0/255.255.255.0	192.168.11.0/255.255.255.0	fastethernet 0/1	IKEv1

Below the table are buttons for Add, Modify, and Delete. The bottom left corner of the interface shows the copyright notice: Copyright ©2001-2016 InHand Networks Co., Ltd. All rights reserved.

You can check the basic information about this IPsec VPN tunnel as the above picture shows.

InHand Networks

3900 Jermantown Rd., Suite 150

Fairfax, VA 22030

USA

T: +1-703-348-2988

F: +1-703-348-2988

info@inhandnetworks.com

www.inhandnetworks.com

