



IPsec VPN using CTM-200

Model	CTM-200
Revision:	Rev 1.3

Revision Control

Description	Revision	Date
Customer Release	Rev 1.0	Mar. 24, 2011
Added step of setting pre-shared key in web page steps	Rev 1.3	Apr. 25, 2011
Included full tunnel and dynamic IP configurations	Rev 1.2	Jul. 26 2013
Removed WebIF portion for CTM200R2. Updated content	Rev 1.3	Nov 28 2015

Contents

Revision Control	1
1. Overview	2
1.1 Requirements.....	4
1.1.1 IPsec Parameters.....	4
1.2 IPsec Operation.....	4
2. IPsec Configuration between Two Chameleon Modems.....	5
2.1 Initiator (Split tunnel).....	6
2.2 Initiator (Split tunnel, Dynamic IP).....	6
2.3 Responder (Split tunnel)	7
2.4 Initiator or Responder (Full tunnel)	7
3. IPsec Configuration between a Chameleon Modem and a Corporate VPN Router	8
3.1 Supported Equipment.....	8
4. Test IPsec Tunnel Functionality.....	8

I. Overview

A VPN can be used to provide a secure, routable connection between a remote wireless device (modem) on the public Internet with a static IP and a remote server. The data being transmitted and received by the modem is secure within a protected VPN tunnel.

Internet Protocol Security (IPsec) is a protocol suite that enables devices to secure communication at the Internet Protocol (IP), or network layer. IPsec provides security in the following ways:

- **Data confidentiality:** Data communicated across the tunnel is encrypted to prevent the deciphering of data if intercepted
- **Origin authentication:** The identity of each peer in the tunnel is validated to prevent the impersonation of devices
- **Integrity Validation:** Data communicated across the tunnel is validated to prevent data tampering

The Cypress Chameleon series of industrial wireless data routers/modems support IPsec VPN communications through a **split tunnel** (section 2.1 and 2.2) or **full tunnel** (section 2.4):

- A split tunnel will route outgoing traffic for the specified remote subnet through the tunnel, and all other outgoing data will be sent over the unencrypted Internet.
- A full tunnel will route ALL outgoing traffic through the tunnel

This application note provides steps on setting up a VPN using the IPsec tools available on the Chameleon modems for the following cases:

- site-to-site IPsec VPN between two Chameleon modems (figure 1)
- site-to-site IPsec VPN between a Chameleon modem and a corporate IPsec VPN router (figure 2)

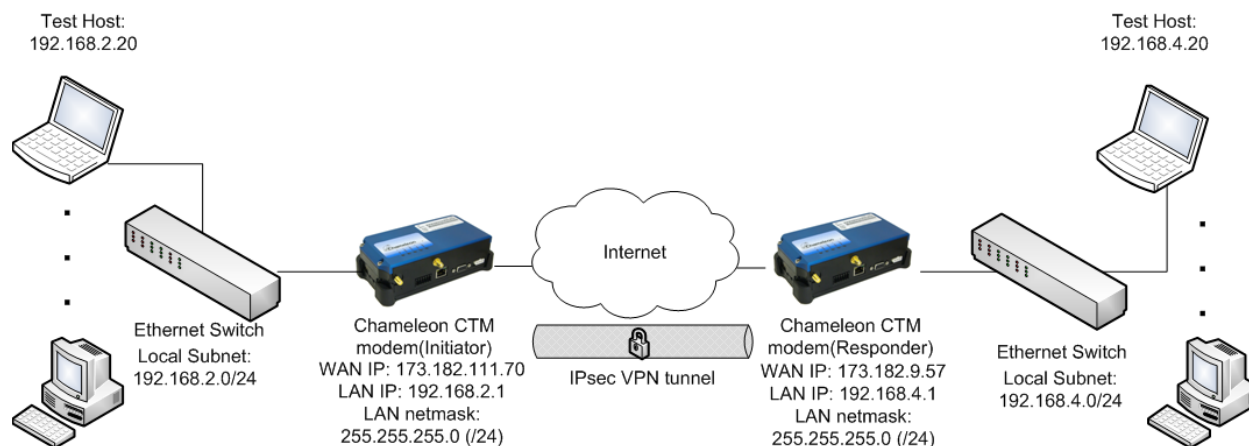


Figure 1: Site-to-site IPsec VPN between two Chameleon modems

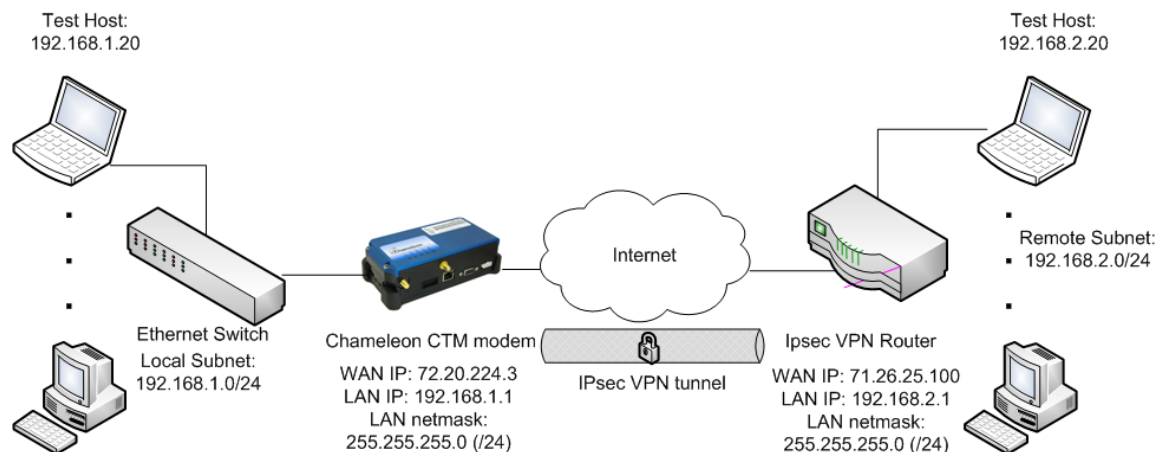


Figure 2: Site-to-site IPsec VPN between a Chameleon modem and a corporate IPsec VPN router

A site-to-site VPN is used to connect two remote networks together via a VPN tunnel. In technical terms, a site-to-site VPN connects the remote subnets located behind the LAN side of each IPsec peer.

The target audience of this application note is IT personnel involved with the configuration of Chameleon modems for an application requiring an IPsec VPN. Some understanding of IPsec setup and configuration is required to properly configure modems.

1.1 Requirements

1.1.1 IPsec Parameters

The CTM modem supports the establishment of IPsec VPN tunnels using the encapsulating security payload (ESP) protocol and tunnel mode.

- ESP protocol ensures data confidentiality, origin authentication, and integrity validation
- Tunnel mode allows a VPN tunnel to be set up

To successfully set up an IPsec communication tunnel between a CTM modem and other VPN hardware a variety of settings must be configured.

Remote Node Configuration:

- Peer (Server) IP Address
- IKE exchange mode: aggressive, main
- Initial Contact: On/Off
- Passive: On (Server), Off (Client)
- Generate Policy: On/Off
- IKE Phase 1 Lifetime
- NAT Traversal
- IKE Encryption algorithm e.g. AES256, DES, 3DES
- IKE hash algorithm e.g. MD5, SHA1
- IKE Diffie-Hellman Group e.g. 3DES with Group 2 (1024-bit prime)
- Pre-shared key for IPsec

Security Association (SA) Specifications:

- PFS Group
- IPsec-SA Lifetime
- SA Encryption Algorithm: e.g. AES256, AES, DES, 3DES
- SA Authentication Algorithm: e.g. hmac_md5, hmac_sha1
- Server LAN IP subnet(s)/ netmask(s) (up to 10)

1.2 IPsec Operation

To establish an IPsec VPN tunnel, the IPsec VPN client and server use the Internet Key Exchange (IKE) protocol to generate a shared key used for encryption of security parameters. The IKE protocol is based on ISAKMP (Internet Security and Key Management Protocol), a framework for establishing secure connections, or security associations (SAs) used for negotiating security and encryption key parameters.

To establish an IPsec VPN tunnel the client and server perform the following steps:

1. IKE Phase 1: Establish a secure connection over which IPsec security parameters can be communicated, i.e. a secure tunnel to exchange IPsec parameters
2. ISAKMP Phase 2: Establish a secure connection over which IP data can be communicated, i.e. the effective IPsec VPN tunnel between the peers

As a result of negotiations in each phase, a shared key is securely generated at each IPsec peer. Using a symmetric encryption algorithm, a shared key is used for encrypting IPsec security parameters (Phase 1) and a shared key is used for encrypting IP data (Phase 2).

Phase 1 and 2 negotiations are repeated periodically, as configured via IKE Phase 1 lifetime and IPsec-SA lifetime parameters, respectively. This increases the security of the IPsec VPN tunnel since the shared keys will be changing periodically.

2. IPsec Configuration between Two Chameleon Modems

When setting up two devices to communicate over an IPsec tunnel, the following **MUST** be considered:

1. Both Chameleon modems must use identical algorithms (ie. identical hash, encryption algorithms).
2. One modem must be specified as the Initiator and the other must be specified as the Responder.
3. Both modems must have different local tunnel subnets specified (e.g. If CTM1 has a Local IP address of 192.168.1.0/24, then CTM2 must **NOT** use 192.168.1.0/24. CTM2 **COULD** use 192.168.2.0/24 for example.
4. The following sections will show an example of the IPsec setup between the Initiator Modem and the Responder Modem. This purpose of this example is to setup a very basic IPsec tunnel between two Chameleon modems.
5. See link to the CTM200 command reference for more details on any commands:
http://www.cypress.bc.ca/documents/Command_Ref/CTM200/

2.1 Initiator (Split tunnel)

Below is an example of how to configure IPsec on a CTM200 as the initiator. This initiator configuration would work well with the responder example in section 2.3:

```
cmd lanip 0 192.168.2.1 255.255.255.0      # Configure LAN0 IP
cmd lanip 1 192.168.3.1 255.255.255.0    # Configure LAN1 IP
cmd ipsec enable 1                        # Enable IPsec
cmd ipsec remgw 173.182.9.57              # Remote gateway IP
cmd ipsec ikepeerid address 173.182.9.57  # Remote peer address
cmd ipsec remnet 1 192.168.4.0 24         # IPsec remote subnet
cmd ipsec psk Cypress                     # Pre shared key
cmd save                                  # Save configuration
cmd pwr mode 2                             # Power cycle gateway
```

2.2 Initiator (Split tunnel, Dynamic IP)

Below is an example of how to configure IPsec on a CTM200 as the initiator if the CTM200 has a dynamic IP address (opposed to a static IP address). The difference between this example and the previous is that now we are using different identifiers for the CTM200 and the remote peer to compensate for the dynamic IP address.

```
cmd lanip 0 192.168.2.1 255.255.255.0    # Configure LAN0 IP
cmd lanip 1 192.168.3.1 255.255.255.0    # Configure LAN1 IP
cmd ipsec enable 1                        # Enable IPsec
cmd ipsec ikeexchange aggressive          # Set IKE exchange mode to aggressive
cmd ipsec remgw 173.182.9.57              # Remote gateway IP
cmd ipsec ikemyid user_fqdn client@test.com # IPsec local identifier (FQDN)
cmd ipsec ikepeerid user_fqdn server@test.com # IPsec remote identifier (FQDN)
cmd ipsec ikeverifyid 1                   # Verify peer identifier
cmd ipsec natt 2                           # Always use NAT traversal
cmd ipsec remnet 1 192.168.4.0 24         # IPsec remote subnet
cmd ipsec psk Cypress                     # IPsec pre shared key
cmd save                                  # Save configuration
cmd pwr mode 2                             # Power cycle gateway
```

Note the **ikemyid** and **ikepeerid** commands above. Since this CTM200 has a dynamic IP address assigned to its SIM card, we must identify the local ID and remote ID as a non-IP address so we use FQDN instead.

Since FQDN names are used instead, the CTM200 and remote peer can identify each other using arbitrary names instead of IP identifiers.

2.3 Responder (Split tunnel)

Below is an example of how to configure IPsec on a CTM200 as the responder. This responder configuration would work well with the initiator example in section 2.1:

```
cmd lanip 0 192.168.4.1 255.255.255.0      # Configure LAN0 IP
cmd lanip 1 192.168.5.1 255.255.255.0    # Configure LAN1 IP
cmd ipsec enable 1                        # Enable IPsec
cmd ipsec ikeinitial 0                    # Disable IPsec initiation
cmd ipsec ikepassive 1                    # Enable IPsec responder
cmd ipsec remgw 173.182.111.70            # Remote gateway IP
cmd ipsec ikepeerid address 173.182.111.70 # Remote peer address
cmd ipsec remnet 1 192.168.2.0 24         # IPsec remote subnet
cmd ipsec psk Cypress                     # IPsec pre shared key
cmd save                                  # Save configuration
cmd pwr mode 2                            # Power cycle gateway
```

2.4 Initiator or Responder (Full tunnel)

Full Tunnel Notes:

- To set up a full tunnel, you must be on firmware **2.0.5.3034** or above.
- When split-tunnel is disabled, ALL outgoing traffic from the CTM-200 will be routed through the IPsec tunnel.
- When split-tunnel is disabled, **ONLY ONE** remote subnet should be defined. ie. cmd ipsec remnet 2..10 should all be **0.0.0.0**.
- When split-tunnel is disabled A PC on the remote side of the tunnel will not be able to access PC/devices on the LAN side of the CTM-200.

The full tunnel setup will incorporate **everything** used in the split tunnel setup, except one adjustment must be made:


```
cmd ipsec split 0          # enable full tunnel
cmd save                  # save configuration
cmd pwr mode 2           # power cycle gateway
```

3. IPsec Configuration between a Chameleon Modem and a Corporate VPN Router

3.1 Supported Equipment

IPsec supported VPN hardware:

- Checkpoint VPN-1.
- Cisco PIX firewalls, VPN concentrators and routers running IOS.
- Enterasys routers with VPN capabilities.
- IBM/ISS Proventia UTM
- Intoto
- Juniper E-series and Netscreen series.
- Nokia
- Nortel VPN Routers
- SonicWALL Firewall/VPN Appliances

(Note: not all of the hardware listed above has been tested with the Chameleon CTM modem)

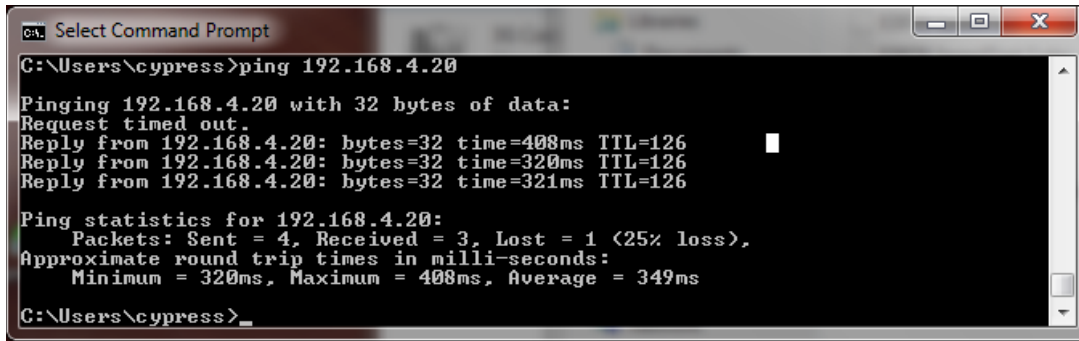
Refer to Section 2 (IPsec Configuration between Two Chameleon Modems). When configuring IPsec between a Chameleon Modem and a corporate router (Cisco ASA etc.) you can substitute the corporate router as either the Initiator or Responder Chameleon Modem used in Section 2.

4. Test IPsec Tunnel Functionality

Refer to the topology shown in the beginning of this application note for IP addresses used in these examples.

After both modems have been configured for either a split tunnel or a full tunnel, you can test by pinging from the hosts located behind the Chameleon modems to the host on the other side of the tunnel.

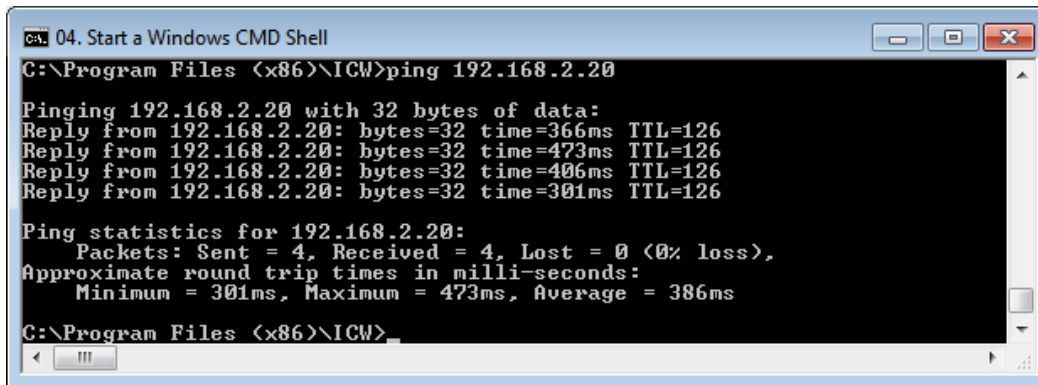
Ex. Ping from host 192.168.2.20 to 192.168.4.20, at the same time ping from host 192.168.4.20 to 192.168.2.20. Both pings should go through.



```
ca. Select Command Prompt
C:\Users\cypress>ping 192.168.4.20
Pinging 192.168.4.20 with 32 bytes of data:
Request timed out.
Reply from 192.168.4.20: bytes=32 time=408ms TTL=126
Reply from 192.168.4.20: bytes=32 time=320ms TTL=126
Reply from 192.168.4.20: bytes=32 time=321ms TTL=126

Ping statistics for 192.168.4.20:
    Packets: Sent = 4, Received = 3, Lost = 1 (25% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 320ms, Maximum = 408ms, Average = 349ms
C:\Users\cypress>_
```

(Ping from 192.168.2.20 to 192.168.4.20)



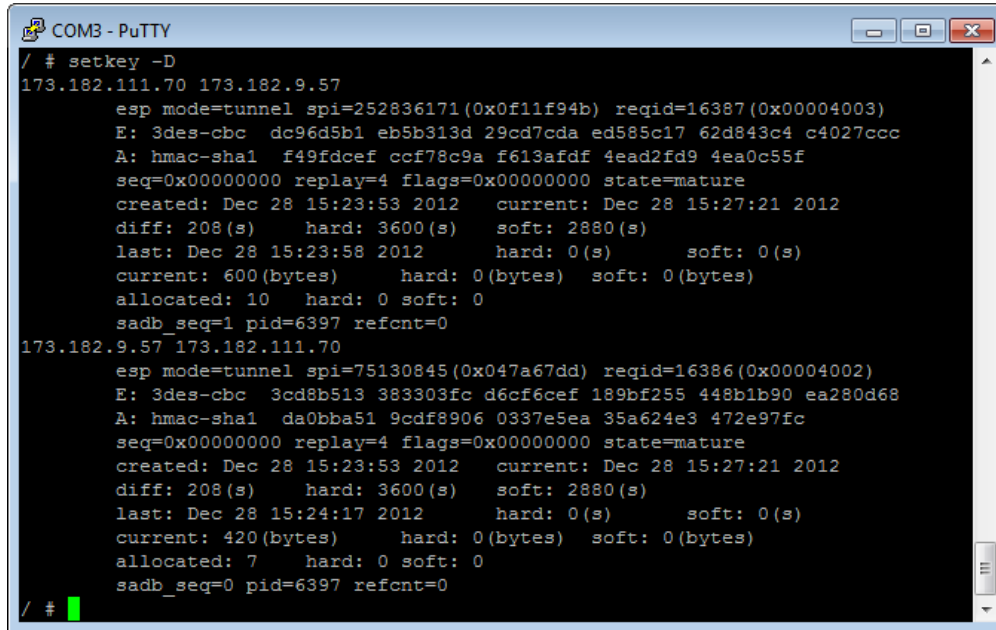
```
ca. 04. Start a Windows CMD Shell
C:\Program Files (x86)\ICW>ping 192.168.2.20
Pinging 192.168.2.20 with 32 bytes of data:
Reply from 192.168.2.20: bytes=32 time=366ms TTL=126
Reply from 192.168.2.20: bytes=32 time=473ms TTL=126
Reply from 192.168.2.20: bytes=32 time=406ms TTL=126
Reply from 192.168.2.20: bytes=32 time=301ms TTL=126

Ping statistics for 192.168.2.20:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 301ms, Maximum = 473ms, Average = 386ms
C:\Program Files (x86)\ICW>_
```

(Ping from 192.168.4.20 to 192.168.2.20)

To see if the tunnel is up (both IPsec Phase 1 and IPsec Phase 2 established), enter the following in a Telnet/SSH/Serial session:

setkey -D



```

COM3 - PuTTY
/ # setkey -D
173.182.111.70 173.182.9.57
  esp mode=tunnel spi=252836171(0x0f11f94b) reqid=16387(0x00004003)
  E: 3des-cbc dc96d5b1 eb5b313d 29cd7cda ed585c17 62d843c4 c4027ccc
  A: hmac-sha1 f49fdcef ccf78c9a f613afdf 4ead2fd9 4ea0c55f
  seq=0x00000000 replay=4 flags=0x00000000 state=mature
  created: Dec 28 15:23:53 2012    current: Dec 28 15:27:21 2012
  diff: 208(s)    hard: 3600(s)    soft: 2880(s)
  last: Dec 28 15:23:58 2012    hard: 0(s)    soft: 0(s)
  current: 600(bytes)    hard: 0(bytes)    soft: 0(bytes)
  allocated: 10    hard: 0    soft: 0
  sadb_seq=1 pid=6397 refcnt=0
173.182.9.57 173.182.111.70
  esp mode=tunnel spi=75130845(0x047a67dd) reqid=16386(0x00004002)
  E: 3des-cbc 3cd8b513 383303fc d6cf6cef 189bf255 448b1b90 ea280d68
  A: hmac-sha1 da0bba51 9cdf8906 0337e5ea 35a624e3 472e97fc
  seq=0x00000000 replay=4 flags=0x00000000 state=mature
  created: Dec 28 15:23:53 2012    current: Dec 28 15:27:21 2012
  diff: 208(s)    hard: 3600(s)    soft: 2880(s)
  last: Dec 28 15:24:17 2012    hard: 0(s)    soft: 0(s)
  current: 420(bytes)    hard: 0(bytes)    soft: 0(bytes)
  allocated: 7    hard: 0    soft: 0
  sadb_seq=0 pid=6397 refcnt=0
/ #

```

Technical Support

**Cypress Solutions Service
Support Group**
1.844.462.9773 or 778.372.4603
9.00am to 5.00pm PST
support@cypress.bc.ca