Cisco Tunnel Control Protocol on Cisco EasyVPN

This document highlights the steps to configure the Cisco® Tunnel Control Protocol (cTCP) feature on Cisco IOS® Easy VPN Servers, Easy VPN Remotes, and Cisco VPN Clients. With this feature enabled, VPN users will be able to establish VPN tunnels from the client/remote to the Easy VPN Server through a third-party Network Address Transport (NAT) device or firewall.

Challenge

There are many situations where customers require a VPN client to operate in an environment where standard ESP (Protocol 50) or UDP 500 (IKE) can either not function, or not function transparently (without modification to existing firewall rules).

Situations where standard ESP or UDP 500 are not permitted include:

- Small/home office router performing Network/Port Address Translation (NAT/PAT). This router sits between the EasyVPN Remote/Client and the Server and usually supports both TCP and UDP translation by default with no restrictions, but ESP might not be permitted.
- PAT-provided IP address behind a large corporation. This could exist if a service provider provides non-public addresses to clients and then performs PAT. This scenario is identical to that documented above. However, in the corporation scenario, it is common that only predefined TCP applications are permitted (TCP 80, TCP 443, etc.) for added network protection. These devices include Cisco PIX® security appliances, large Cisco IOS Software-based routers, Checkpoint firewalls, etc. A hotel providing private address space to guests could fall under this category, or the first.
- Non-NAT Firewall (Packet Filtering or Stateful). This scenario is common at companies that wish to use routable address space on their internal networks. Often in this environment, only particular TCP applications will function, but UDP outbound is not permitted because it is considered to be a potential corporate security hole. Our customers are sometimes consultants or employees located at these networks, trying to tunnel back into another corporation from behind an existing firewall. These devices include Cisco IOS routers and Cisco PIX firewalls, either operating as a stateful firewall or a stateless packet filter.
- Proxy server. If a proxy server is smart enough to look at each packet to confirm that the activity occurring is the defined activity, our solution may not work. However, for proxy servers that simply proxy TCP service ports (such as Borderware firewalls) our solution should work in this situation.

Solution

To solve this problem without modifying the rules configured in the firewall, Cisco has come up with a protocol called Cisco Tunneling Control Protocol. When cTCP is enabled on client and headend device, IKE and ESP traffic will be encapsulated in the TCP header, so that the firewalls in between the client and the headend device would simply permit this traffic, considering it as TCP traffic.

cTCP is also called TCP over IPsec, or TCP traversal.

Network Setup

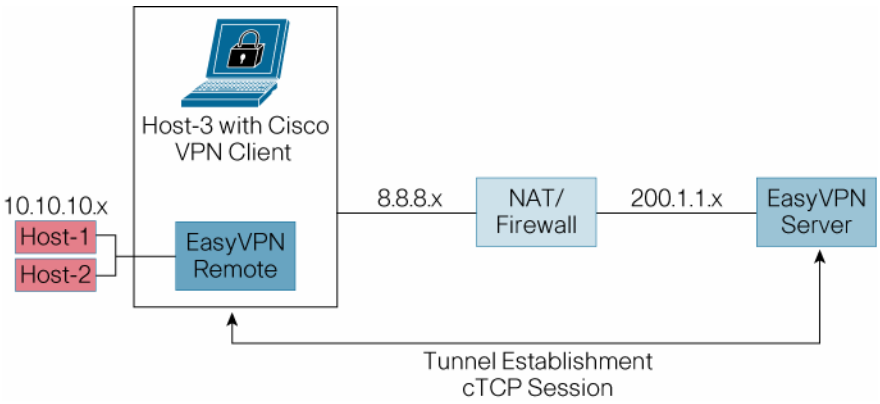
Components Used

The information in this document is based on the following software and hardware versions:

- Cisco 2821 Router with Cisco IOS Software Release 12.4(11)T as EasyVPN Server
- Cisco 871w Router with Cisco IOS Software Release 12.4(11)T as EasyVPN Remote
- Cisco VPN Client Version 4.0.5
- Cisco 1811 Router as firewall

This document uses the network setup shown in Figure 1.

Figure 1. Network Setup



After the topology is set, make sure Host-1, Host-2, and Host-3 are able to reach the server.

A few things to remember when deploying cTCP:

- The client initiates a cTCP connection using a random, unused (unused at the time of selecting the port) TCP port number as the source port. Any application that later uses that port may not work.
- Session setup and teardown: cTCP session initiation follows a fixed number of retransmissions (that is not configurable) before declaring failure. Just like the server, the client does not react to a TCP RST received on the source port (for the same reasons of anyone being able to generate such a packet). It will close the session only when the VPN session on top of the cTCP session is closed, and will then send a TCP RST (that the server ignores).
- Keepalive: cTCP client needs to send periodic keepalives to keep NAT/firewall sessions alive. To this end, cTCP client sends a TCP ACK ack'ing the last sequence number received from the hub. The keepalive interval defaults to 5 seconds; however, it can be configured.

Configure cTCP on Cisco Easy VPN

Server

- Configure a typical EasyVPN server tunnel setup, using either crypto map or DVTI.
- Enable ctcp option on the server. Configure up to 10 ports on the server to listen to. (e.g., crypto ctcp port <port number1> … <port number10>)

Remote

- Configure ezvpn profile on the remote router (e.g., crypto ipsec client ezvpn easy)
- Enable ctcp option under the ezvpn profile on the remote router (e.g., ctcp enable <port number>)
- Configure the interface on remote that is connected to host-1, as Easyvpn **'inside interface'**.
- Configure the interface on remote that is connected to firewall, as Easyvpn **'outside interface'**.

NAT/Firewall

- Configure ip inspect rule on the middle router that acts as firewall (e.g., ip inspect name <name> tcp). Apply this rule on the interface that is connected to ctcp-client to inspect the incoming tcp requests (e.g., ip inspect <name> in).
- Configure the access-list policy on the firewall (e.g., ip access-list extended <name>). Apply this policy on the interface that is connected to server (e.g., ip access-group <name> in).

Sample Configuration and Troubleshooting Output

Server Configuration Using Virtual Tunnel Interface

```
version 12.4
!
hostname easyvpn-2821
!
aaa new-model
!
aaa authentication login USERAUTH local
aaa authorization network branch local
!
aaa session-id common
!
resource policy
!
ip subnet-zero
ip cef
!
!
username newuser password 0 cisco123
username 871-ctcp password 0 cisco123
!
!!! Enabling ctcp on server
 crypto ctcp port  10001 10002 10003
```

```
!!! The following is a typical EasyVPN configuration
crypto isakmp policy 1
     encr 3des
     authentication pre-share
     group 2
crypto isakmp key cisco123 address 0.0.0.0 0.0.0.0
crypto isakmp keepalive 60
!

crypto isakmp client configuration group branch
 key ciscocisco
 dns 172.19.217.95
 domain cisco.com
 pool dynpool
 save-password
!
crypto isakmp profile vi
   match identity group branch
   client authentication list USERAUTH
   isakmp authorization list branch
   client configuration address respond
   virtual-template 1
!
!
crypto ipsec transform-set transform-1 esp-3des esp-sha-hmac
!
crypto ipsec profile ipsec-vi
 set transform-set transform-1
 set isakmp-profile vi
!
interface Loopback1
 description Anchor for VTI
 ip address 30.30.30.1 255.255.255.0
!
interface GigabitEthernet0/0
 description $ETH-LAN$$ETH-SW-LAUNCH$$INTF-INFO-GE 0/0$$FW_OUTSIDE$
 ip address 200.1.1.100 255.255.255.0
 duplex auto
 speed auto
!
interface GigabitEthernet0/1
 description $ES_LAN$$FW_INSIDE$
 ip address 172.19.217.96 255.255.255.0
 duplex auto
 speed auto
!
interface Virtual-Template1 type tunnel
 description $FW_INSIDE$
 ip unnumbered Loopback1
```

```
 tunnel mode ipsec ipv4
 tunnel protection ipsec profile ipsec-vi
!
!
ip local pool dynpool 30.30.30.10 30.30.30.20
ip route 0.0.0.0 0.0.0.0 GigabitEthernet0/0
end
```

Spoke Router with DVTI Configuration

```
version 12.4
!
hostname ctcp-remote
!
no aaa new-model
!
ip subnet-zero
!
ip cef
no ip dhcp use vrf connected
ip dhcp excluded-address 10.10.10.1
!
ip dhcp pool sdm-pool
   import all
   network 10.10.10.0 255.255.255.248
   default-router 10.10.10.1
   lease 0 2
!
crypto ctcp keepalive 60
!
username cisco privilege 15 password 0 cisco
!
crypto ipsec client ezvpn branch
 connect manual
 ctcp enable 10001
 group branch key ciscocisco
 mode client
 peer 200.1.1.100
 virtual-interface 1
 username 871-ctcp password cisco123
 xauth userid mode local
!
interface FastEthernet0
 no cdp enable
!
interface FastEthernet1
 no cdp enable
!
interface FastEthernet2
 no cdp enable
!
```

```
interface FastEthernet3
 no cdp enable
!
interface FastEthernet4
 ip address  8.8.8.11 255.255.255.0
 duplex auto
 speed auto
 no cdp enable
 crypto ipsec client ezvpn branch
!
interface Virtual-Template1 type tunnel
no ip address
tunnel mode ipsec ipv4
!
interface Vlan1
 description $ETH-SW-LAUNCH$$INTF-INFO-HWIC 4ESW$
 ip address 10.10.10.1 255.255.255.248
 ip tcp adjust-mss 1452
 crypto ipsec client ezvpn branch inside
!
ip route 0.0.0.0 0.0.0.0 FastEthernet4
!
end
```

Server Configuration Using Crypto Map

```
version 12.4
!
hostname easyvpn-2821
!
aaa new-model
!
aaa authentication login USERAUTH local
aaa authorization network branch local
!
aaa session-id common
!
resource policy
!
ip subnet-zero
ip cef
!
!
username newuser password 0 cisco123
username 871-ctcp password 0 cisco123
!
!!! Enabling ctcp on server
 crypto ctcp port  10001 10002 10003

!!! The following is a typical EasyVPN configuration
crypto isakmp policy 1
```

```
     encr 3des
     authentication pre-share
     group 2
crypto isakmp key cisco123 address 0.0.0.0 0.0.0.0
crypto isakmp keepalive 60
!
crypto isakmp client configuration group branch
 key ciscocisco
 dns 172.19.217.95
 domain cisco.com
 pool dynpool
 save-password
!
!
crypto ipsec transform-set transform-1 esp-3des esp-sha-hmac
!
!!!Configuring dynamic map
crypto dynamic-map dynmap 1
   set transform-set transform-1
   reverse-route
!
!!!Configuring crypto-map
crypto map clientmap client authentication list USERAUTH
crypto map clientmap isakmp authorization list branch
crypto map clientmap client configuration address respond
crypto map clientmap 1 ipsec-isakmp dynamic dynmap
!
!!!Applying crypto map on the outside (firewall-server) interface of
server
interface GigabitEthernet0/0
 description $ETH-LAN$$ETH-SW-LAUNCH$$INTF-INFO-GE 0/0$$FW_OUTSIDE$
 ip address 200.1.1.100 255.255.255.0
 crypto map clientmap
 duplex auto
 speed auto
!
interface GigabitEthernet0/1
 description $ES_LAN$$FW_INSIDE$
 ip address 172.19.217.96 255.255.255.0
 duplex auto
 speed auto
!
!
ip local pool dynpool 30.30.30.10 30.30.30.20
ip route 0.0.0.0 0.0.0.0 GigabitEthernet0/0
end
```

Remote Configured with Crypto Map

```
version 12.4
!
```

```
hostname ctcp-remote
!
no aaa new-model
!
ip subnet-zero
!
ip cef
no ip dhcp use vrf connected
ip dhcp excluded-address 10.10.10.1
!
ip dhcp pool sdm-pool
   import all
   network 10.10.10.0 255.255.255.248
   default-router 10.10.10.1
   lease 0 2
!
crypto ctcp keepalive 60
!
username cisco privilege 15 password 0 cisco
!
!!! Enabling ezvpn profile with ctcp
crypto ipsec client ezvpn branch
 connect manual
 ctcp enable 10001
 group branch key ciscocisco
 mode client
 peer 200.1.1.100
username 871-ctcp password cisco123
 xauth userid mode local
!
interface FastEthernet0
 no cdp enable
!
interface FastEthernet1
 no cdp enable
!
interface FastEthernet2
 no cdp enable
!
interface FastEthernet3
 no cdp enable
!
interface FastEthernet4
 ip address  8.8.8.11 255.255.255.0
 duplex auto
 speed auto
 no cdp enable
 crypto ipsec client ezvpn branch
!
!
```

```
interface Vlan1
 description $ETH-SW-LAUNCH$$INTF-INFO-HWIC 4ESW$
 ip address 10.10.10.1 255.255.255.248
 ip tcp adjust-mss 1452
 crypto ipsec client ezvpn branch inside
!
ip route 0.0.0.0 0.0.0.0 FastEthernet4
!
end
```

Firewall Configuration

```
version 12.4
hostname C1811
!
no aaa new-model
!
resource policy
!
ip subnet-zero
!
ip cef
no ip dhcp use vrf connected
!
!
!!! Configuring ip inspect rule
ip inspect name myfw tcp timeout 500
ip inspect name myfw udp timeout 100
no ip ips deny-action ips-interface
!
!!! Applying inspect rule to the inside interface (client-firewall) of
the firewall
interface FastEthernet0
 ip address 8.8.8.8 255.255.255.0
 ip nat inside
 ip inspect myfw in
 ip virtual-reassembly
 duplex auto
 speed auto
!
!!!  Applying access-group to outside (firewall-server) interface of
the firewall
interface FastEthernet1
 ip address 200.1.1.201 255.255.255.0
 ip access-group fw_acl in
 ip nat outside
 ip virtual-reassembly
 duplex auto
 speed auto
!
ip nat inside source list 7 interface FastEthernet1 overload
```

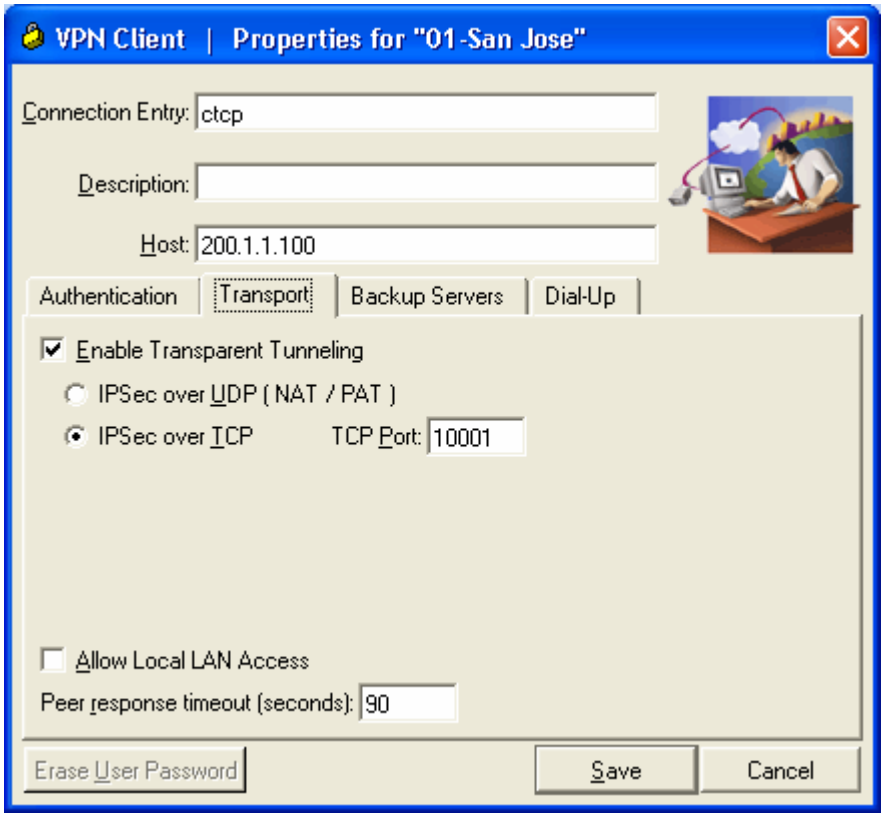
```
!
!!!Configuring access-list
ip access-list extended fw_acl
 deny   tcp any any
 deny   udp any any
 permit icmp any any
 permit ip any any
!
access-list 7 permit 8.8.8.0 0.0.0.255
access-list 7 permit any
!
end
```

Cisco VPN Client

- Transport tab: Choose IPsec over TCP.
- TCP port: 10000 (or any port configured on the EasyVPN server)

The screen shot is shown in Figure 2.

Figure 2. cTCP Configuration on Cisco VPN Client



Troubleshooting

Verify Server

Sample Output on Server Configured with DVTI

```
easyvpn-2821#debug crypto ctcp
```

```
002735: *Mar 16 01:26:52.234 UTC: cTCP: Connection[481F772C]
200.1.1.201:62339 200.1.1.100:10001: created

002736: *Mar 16 01:26:52.234 UTC: cTCP: SYN from 200.1.1.201:62339

002737: *Mar 16 01:26:52.234 UTC: cTCP: Sending
SYN(4729A37D)ACK(33683097) to 200.1.1.201:62339

002738: *Mar 16 01:26:52.238 UTC: cTCP: Connection[481F772C]
200.1.1.201:62339 200.1.1.100:10001:  found

002739: *Mar 16 01:26:52.238 UTC: cTCP: ACK from 200.1.1.201:62339

002740: *Mar 16 01:26:52.238 UTC: cTCP: Connection[481F772C]
200.1.1.201:62339 200.1.1.100:10001:  found

002741: *Mar 16 01:26:52.242 UTC: cTCP: updating PEER Seq number to
33683520

002742: *Mar 16 01:26:52.242 UTC: cTCP: Pak with contiguous buffer

002743: *Mar 16 01:26:52.242 UTC: cTCP: mangling IKE packet from peer:
200.1.1.201:500->62339 200.1.1.10

0:500->500

002744: *Mar 16 01:26:52.242 UTC: cTCP: Connection[481F772C]
200.1.1.201:62339 200.1.1.100:10001:  found

002745: *Mar 16 01:26:52.274 UTC: cTCP: demangling outbound IKE
packet: 200.1.1.100:500->500 200.1.1.201

:62339->500

002746: *Mar 16 01:26:52.274 UTC: cTCP: encapsulating IKE packet

002747: *Mar 16 01:26:52.274 UTC: cTCP: updating LOCAL Seq number to
4729A4F2

002748: *Mar 16 01:26:52.322 UTC: cTCP: Connection[481F772C]
200.1.1.201:62339 200.1.1.100:10001:  found

002749: *Mar 16 01:26:52.322 UTC: cTCP: updating PEER Seq number to
3368358C

002750: *Mar 16 01:26:52.322 UTC: cTCP: Pak with contiguous buffer

002751: *Mar 16 01:26:52.322 UTC: cTCP: mangling IKE packet from peer:
200.1.1.201:500->62339 200.1.1.10

0:500->500

002752: *Mar 16 01:26:52.326 UTC: cTCP: demangling outbound IKE
packet: 200.1.1.100:500->500 200.1.1.201

:62339->500

002753: *Mar 16 01:26:52.326 UTC: cTCP: encapsulating IKE packet

002754: *Mar 16 01:26:52.326 UTC: cTCP: updating LOCAL Seq number to
4729A56E

002755: *Mar 16 01:26:52.326 UTC: cTCP: demangling outbound IKE
packet: 200.1.1.100:500->500 200.1.1.201

:62339->500

002756: *Mar 16 01:26:52.326 UTC: cTCP: encapsulating IKE packet

002757: *Mar 16 01:26:52.326 UTC: cTCP: updating LOCAL Seq number to
4729A5D2

002758: *Mar 16 01:26:52.334 UTC: cTCP: Connection[481F772C]
200.1.1.201:62339 200.1.1.100:10001:  found

002759: *Mar 16 01:26:52.334 UTC: cTCP: updating PEER Seq number to
33683600

002760: *Mar 16 01:26:52.334 UTC: cTCP: Pak with contiguous buffer

002761: *Mar 16 01:26:52.334 UTC: cTCP: mangling IKE packet from peer:
200.1.1.201:500->62339 200.1.1.10

0:500->500

002762: *Mar 16 01:26:52.338 UTC: %CRYPTO-6-VPN_TUNNEL_STATUS:
(Server)  Authentication PASSED  User=871-ctcp  Group=branch
Client_public_addr=200.1.1.201  Server_public_addr=200.1.1.100
```

```
002763: *Mar 16 01:26:52.338 UTC: cTCP: demangling outbound IKE
packet: 200.1.1.100:500->500 200.1.1.201

:62339->500

002764: *Mar 16 01:26:52.338 UTC: cTCP: encapsulating IKE packet

002765: *Mar 16 01:26:52.338 UTC: cTCP: updating LOCAL Seq number to
4729A62E

002766: *Mar 16 01:26:52.342 UTC: cTCP: Connection[481F772C]
200.1.1.201:62339 200.1.1.100:10001:  found

002767: *Mar 16 01:26:52.342 UTC: cTCP: updating PEER Seq number to
3368365C

002768: *Mar 16 01:26:52.342 UTC: cTCP: Pak with contiguous buffer

002769: *Mar 16 01:26:52.342 UTC: cTCP: mangling IKE packet from peer:
200.1.1.201:500->62339 200.1.1.10

0:500->500

002770: *Mar 16 01:26:52.346 UTC: cTCP: Connection[481F772C]
200.1.1.201:62339 200.1.1.100:10001:  found

002771: *Mar 16 01:26:52.346 UTC: cTCP: updating PEER Seq number to
336837E0

002772: *Mar 16 01:26:52.346 UTC: cTCP: Pak with contiguous buffer

002773: *Mar 16 01:26:52.346 UTC: cTCP: mangling IKE packet from peer:
200.1.1.201:500->62339 200.1.1.10

0:500->500

002774: *Mar 16 01:26:52.354 UTC: %CRYPTO-6-VPN_TUNNEL_STATUS:
(Server)  Save password feature ON  User=871-ctcp  Group=branch
Client_public_addr=200.1.1.201  Server_public_addr=200.1.1.100

002775: *Mar 16 01:26:52.354 UTC: cTCP: demangling outbound IKE
packet: 200.1.1.100:500->500 200.1.1.201

:62339->500

002776: *Mar 16 01:26:52.354 UTC: cTCP: encapsulating IKE packet

002777: *Mar 16 01:26:52.354 UTC: cTCP: updating LOCAL Seq number to
4729A7A2

002778: *Mar 16 01:26:52.366 UTC: cTCP: Connection[481F772C]
200.1.1.201:62339 200.1.1.100:10001:  found

002779: *Mar 16 01:26:52.366 UTC: cTCP: updating PEER Seq number to
33683844

002780: *Mar 16 01:26:52.366 UTC: cTCP: Pak with contiguous buffer

002781: *Mar 16 01:26:52.366 UTC: cTCP: mangling IKE packet from peer:
200.1.1.201:500->62339 200.1.1.10

0:500->500

002782: *Mar 16 01:26:52.366 UTC: cTCP: demangling outbound IKE
packet: 200.1.1.100:500->500 200.1.1.201

:62339->500

002783: *Mar 16 01:26:52.366 UTC: cTCP: encapsulating IKE packet

002784: *Mar 16 01:26:52.366 UTC: cTCP: updating LOCAL Seq number to
4729A806

002785: *Mar 16 01:26:52.402 UTC: cTCP: Connection[481F772C]
200.1.1.201:62339 200.1.1.100:10001:  found

002786: *Mar 16 01:26:52.402 UTC: cTCP: updating PEER Seq number to
33683EF8

002787: *Mar 16 01:26:52.402 UTC: cTCP: Pak with contiguous buffer

002788: *Mar 16 01:26:52.402 UTC: cTCP: mangling IKE packet from peer:
200.1.1.201:500->62339 200.1.1.10

0:500->500

002789: *Mar 16 01:26:52.406 UTC: cTCP: demangling outbound IKE
packet: 200.1.1.100:500->500 200.1.1.201

:62339->500
```

```
002790: *Mar 16 01:26:52.406 UTC: cTCP: encapsulating IKE packet
002791: *Mar 16 01:26:52.406 UTC: cTCP: updating LOCAL Seq number to
4729A8EA
002792: *Mar 16 01:26:52.410 UTC: %LINEPROTO-5-UPDOWN: Line protocol
on Interface Virtual-Access3, chang
ed state to up
002793: *Mar 16 01:26:52.410 UTC: %CRYPTO-6-EZVPN_CONNECTION_UP:
(Server)  Mode=CLIENT_OR_NEM_PLUS  Clie
nt_type=CISCO_IOS  User=871-ctcp  Group=branch
Client_public_addr=200.1.1.201  Server_public_addr=200.1
.1.100  Assigned_client_addr=30.30.30.13
002794: *Mar 16 01:26:52.414 UTC: cTCP: Connection[481F772C]
200.1.1.201:62339 200.1.1.100:10001:  found
002795: *Mar 16 01:26:52.414 UTC: cTCP: updating PEER Seq number to
33683F4C
002796: *Mar 16 01:26:52.414 UTC: cTCP: Pak with contiguous buffer
002797: *Mar 16 01:26:52.414 UTC: cTCP: mangling IKE packet from peer:
200.1.1.201:500->62339 200.1.1.10
0:500->500


easyvpn-2821#xinl-gateway#sh cryp ctcp
        Remote                                  Local              VRF
Status

200.1.1.201:52597       200.1.1.100:10001
CTCP_ACK_R

Easyvpn-2821#sh crypto sess detail
Crypto session current status

Code: C - IKE Configuration mode, D - Dead Peer Detection
K - Keepalives, N - NAT-traversal, T - cTCP encapsulation
X - IKE Extended Authentication

Interface: Virtual-Access3
Username: 871-ctcp
Profile: vi
Group: branch
Assigned address: 30.30.30.20
Uptime: 00:28:14
Session status: UP-ACTIVE
Peer: 200.1.1.201 port 52597 fvrf: (none) ivrf: (none)
      Phase1_id: branch
      Desc: (none)
  IKE SA: local 200.1.1.100/500 remote 200.1.1.201/52597 Active
          Capabilities:CDXT connid:1039 lifetime:23:31:45
  IPSEC FLOW: permit ip 0.0.0.0/0.0.0.0 0.0.0.0/0.0.0.0
        Active SAs: 2, origin: crypto map
        Inbound:  #pkts dec'ed 0 drop 0 life (KB/Sec) 4465673/1905
        Outbound: #pkts enc'ed 0 drop 0 life (KB/Sec) 4465673/1905
```

Verify Remote

```
ctcp-remote#debug crypto ctcp
*Mar  9 23:33:36.682: cTCP: initiating a new connection:
*Mar  9 23:33:36.682: cTCP: Connection[84017C98] 200.1.1.100:10001
8.8.8.11:25690: created
*Mar  9 23:33:36.682: cTCP: Sending SYN(B9B5EDB1) to 200.1.1.100:10001
*Mar  9 23:33:36.686: cTCP: Connection[84017C98] 200.1.1.100:10001
8.8.8.11:25690:  found
*Mar  9 23:33:36.686: cTCP: Connection[84017C98] 200.1.1.100:10001
8.8.8.11:25690:  found
*Mar  9 23:33:36.686: cTCP: Connection[84017C98] 200.1.1.100:10001
8.8.8.11:25690:  found
*Mar  9 23:33:36.686: cTCP: Connection[84017C98] 200.1.1.100:10001
8.8.8.11:25690:  found
*Mar  9 23:33:36.686: cTCP: Connection[84017C98] 200.1.1.100:10001
8.8.8.11:25690:  found
*Mar  9 23:33:36.686: cTCP: SYN/ACK from 200.1.1.100:10001
*Mar  9 23:33:36.686: cTCP: Sending (B9B5EDB2)ACK(147D25B8) to
200.1.1.100:10001
*Mar  9 23:33:36.690: cTCP: encapsulating IKE packet
*Mar  9 23:33:36.690: cTCP: updating LOCAL Seq number to B9B5F23C
*Mar  9 23:33:36.726: cTCP: Connection[84017C98] 200.1.1.100:10001
8.8.8.11:25690:  found
*Mar  9 23:33:36.726: cTCP: Connection[84017C98] 200.1.1.100:10001
8.8.8.11:25690:  found
*Mar  9 23:33:36.726: cTCP: Connection[84017C98] 200.1.1.100:10001
8.8.8.11:25690:  found
*Mar  9 23:33:36.726: cTCP: Connection[84017C98] 200.1.1.100:10001
8.8.8.11:25690:  found
*Mar  9 23:33:36.726: cTCP: updating PEER Seq number to 147D272B
*Mar  9 23:33:36.726: cTCP: Pak with contiguous buffer
*Mar  9 23:33:36.774: cTCP: encapsulating IKE packet
*Mar  9 23:33:36.774: cTCP: updating LOCAL Seq number to B9B5F2A8
*Mar  9 23:33:36.778: cTCP: Connection[84017C98] 200.1.1.100:10001
8.8.8.11:25690:  found
*Mar  9 23:33:36.778: cTCP: Connection[84017C98] 200.1.1.100:10001
8.8.8.11:25690:  found
*Mar  9 23:33:36.778: cTCP: Connection[84017C98] 200.1.1.100:10001
8.8.8.11:25690:  found
*Mar  9 23:33:36.778: cTCP: Connection[84017C98] 200.1.1.100:10001
8.8.8.11:25690:  found
*Mar  9 23:33:36.778: cTCP: Connection[84017C98] 200.1.1.100:10001
8.8.8.11:25690:  found
*Mar  9 23:33:36.778: cTCP: updating PEER Seq number to 147D27A7
*Mar  9 23:33:36.778: cTCP: Pak with contiguous buffer
*Mar  9 23:33:36.778: cTCP: Connection[84017C98] 200.1.1.100:10001
8.8.8.11:25690:  found
*Mar  9 23:33:36.778: cTCP: Connection[84017C98] 200.1.1.100:10001
8.8.8.11:25690:  found
*Mar  9 23:33:36.778: cTCP: updating PEER Seq number to 147D280B
*Mar  9 23:33:36.778: cTCP: Pak with contiguous buffer
*Mar  9 23:33:36.786: cTCP: encapsulating IKE packet
*Mar  9 23:33:36.786: cTCP: updating LOCAL Seq number to B9B5F31C
```

```
*Mar  9 23:33:36.790: cTCP: Connection[84017C98] 200.1.1.100:10001
8.8.8.11:25690:  found
*Mar  9 23:33:36.790: cTCP: Connection[84017C98] 200.1.1.100:10001
8.8.8.11:25690:  found
*Mar  9 23:33:36.790: cTCP: Connection[84017C98] 200.1.1.100:10001
8.8.8.11:25690:  found
*Mar  9 23:33:36.790: cTCP: Connection[84017C98] 200.1.1.100:10001
8.8.8.11:25690:  found
*Mar  9 23:33:36.790: cTCP: updating PEER Seq number to 147D2867
*Mar  9 23:33:36.790: cTCP: Pak with contiguous buffer
*Mar  9 23:33:36.790: cTCP: encapsulating IKE packet
*Mar  9 23:33:36.790: cTCP: updating LOCAL Seq number to B9B5F378
*Mar  9 23:33:36.794: cTCP: encapsulating IKE packet
*Mar  9 23:33:36.794: cTCP: updating LOCAL Seq number to B9B5F4FC
*Mar  9 23:33:36.806: cTCP: Connection[84017C98] 200.1.1.100:10001
8.8.8.11:25690:  found
*Mar  9 23:33:36.806: cTCP: Connection[84017C98] 200.1.1.100:10001
8.8.8.11:25690:  found
*Mar  9 23:33:36.806: cTCP: Connection[84017C98] 200.1.1.100:10001
8.8.8.11:25690:  found
*Mar  9 23:33:36.806: cTCP: Connection[84017C98] 200.1.1.100:10001
8.8.8.11:25690:  found
*Mar  9 23:33:36.806: cTCP: updating PEER Seq number to 147D29DB
*Mar  9 23:33:36.806: cTCP: Pak with contiguous buffer
*Mar  9 23:33:36.814: cTCP: encapsulating IKE packet
*Mar  9 23:33:36.814: cTCP: updating LOCAL Seq number to B9B5F560
*Mar  9 23:33:36.818: cTCP: Connection[84017C98] 200.1.1.100:10001
8.8.8.11:25690:  found
*Mar  9 23:33:36.818: cTCP: Connection[84017C98] 200.1.1.100:10001
8.8.8.11:25690:  found
*Mar  9 23:33:36.818: cTCP: Connection[84017C98] 200.1.1.100:10001
8.8.8.11:25690:  found
*Mar  9 23:33:36.818: cTCP: Connection[84017C98] 200.1.1.100:10001
8.8.8.11:25690:  found
*Mar  9 23:33:36.818: cTCP: updating PEER Seq number to 147D2A3F
*Mar  9 23:33:36.818: cTCP: Pak with contiguous buffer
*Mar  9 23:33:36.850: cTCP: encapsulating IKE packet
*Mar  9 23:33:36.850: cTCP: updating LOCAL Seq number to B9B5FC14
*Mar  9 23:33:36.858: cTCP: Connection[84017C98] 200.1.1.100:10001
8.8.8.11:25690:  found
*Mar  9 23:33:36.858: cTCP: Connection[84017C98] 200.1.1.100:10001
8.8.8.11:25690:  found
*Mar  9 23:33:36.858: cTCP: Connection[84017C98] 200.1.1.100:10001
8.8.8.11:25690:  found
*Mar  9 23:33:36.858: cTCP: Connection[84017C98] 200.1.1.100:10001
8.8.8.11:25690:  found
*Mar  9 23:33:36.858: cTCP: updating PEER Seq number to 147D2B23
*Mar  9 23:33:36.858: cTCP: Pak with contiguous buffer
*Mar  9 23:33:36.862: cTCP: encapsulating IKE packet
*Mar  9 23:33:36.862: cTCP: updating LOCAL Seq number to B9B5FC68
*Mar  9 23:33:36.866: %CRYPTO-6-EZVPN_CONNECTION_UP: (Client)
User=871-ctcp  Group=branch  Server_public_addr=200.1.1.100
Assigned_client_addr=30.30.30.10
*Mar  9 23:33:37.450: cTCP: encapsulating IKE packet
*Mar  9 23:33:37.450: cTCP: updating LOCAL Seq number to B9B5FD4C
```

```
*Mar  9 23:33:38.822: %LINK-3-UPDOWN: Interface Loopback0, changed
state to up
*Mar  9 23:33:39.822: %LINEPROTO-5-UPDOWN: Line protocol on Interface
Loopback0, changed state to up


ctcp-remote#sh cry ctcp
        Remote                          Local              VRF
Status


200.1.1.100:10001          8.8.8.11:25690
CTCP_ACK_S


ctcp-remote#sh crypto ipsec clie ezvpn
Easy VPN Remote Phase: 8

Tunnel name : branch
Inside interface list: Vlan1
Outside interface: Virtual-Access2 (bound to FastEthernet4)
Current State: IPSEC_ACTIVE
Last Event: MTU_CHANGED
Address: 30.30.30.10
Mask: 255.255.255.255
DNS Primary: 172.19.217.95
Default Domain: cisco.com
Save Password: Allowed
Configuration URL [version]:  [0]
Config status: not applied, Last successfully applied version: 0
Current EzVPN Peer: 200.1.1.100 (cTCP encapped)

ctcp-remote#sh crypto sess detail
Crypto session current status

Code: C - IKE Configuration mode, D - Dead Peer Detection
K - Keepalives, N - NAT-traversal, T - cTCP encapsulation
X - IKE Extended Authentication

Interface: FastEthernet4
Uptime: 00:07:52
Session status: UP-ACTIVE
Peer: 200.1.1.100 port 500 fvrf: (none) ivrf: (none)
      Phase1_id: 200.1.1.100
      Desc: (none)
  IKE SA: local 8.8.8.11/500 remote 200.1.1.100/500 Active
          Capabilities:CXT connid:2005 lifetime:23:51:41
  IPSEC FLOW: permit ip 0.0.0.0/0.0.0.0 0.0.0.0/0.0.0.0
        Active SAs: 2, origin: crypto map
        Inbound:  #pkts dec'ed 0 drop 0 life (KB/Sec) 4524266/3117
        Outbound: #pkts enc'ed 3 drop 0 life (KB/Sec) 4524265/3117
```

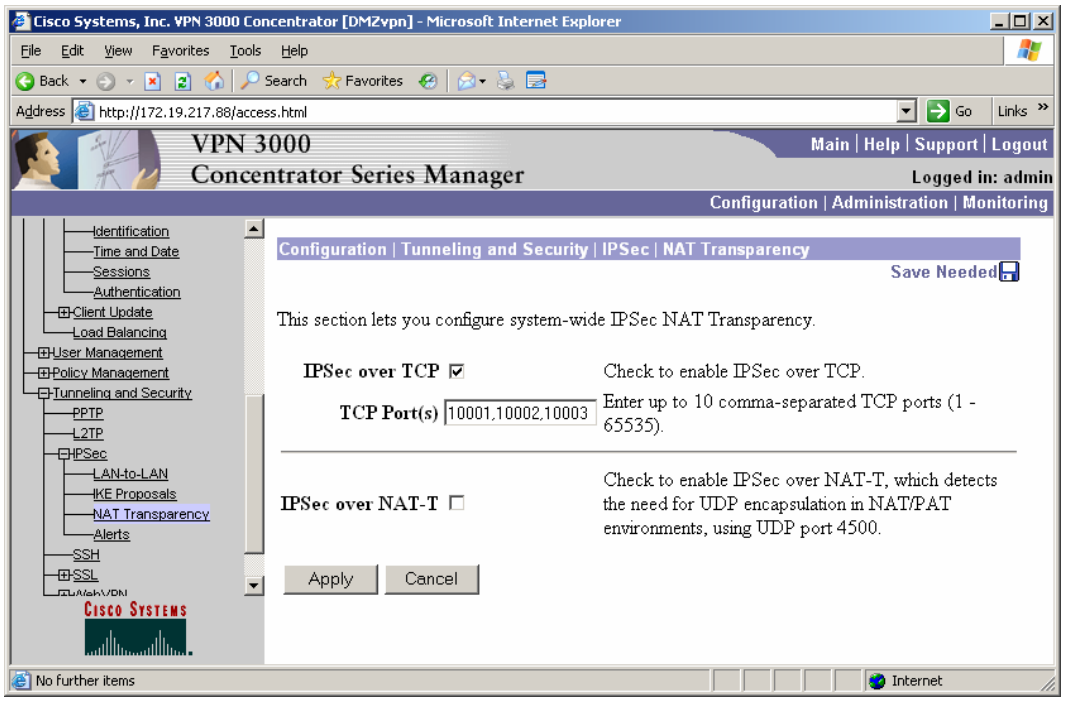
Interoperability

cTCP is available for all EasyVPN Servers and Remotes, including Cisco integrated services routers, VPN 3000 concentrators, and adaptive security appliances. Cross testing has been done between the Cisco IOS Router headend and the Cisco VPN 3002 hardware client, Cisco VPN 3000 headend and Cisco IOS Remote, and Cisco ASA headend and Cisco IOS Remote.

Cisco VPN 3000

Figure 3 shows the cTCP configuration on the VPN 3000 concentrator. It enables IPsec over TCP and specifies the TCP ports for the concentrator to listen to.

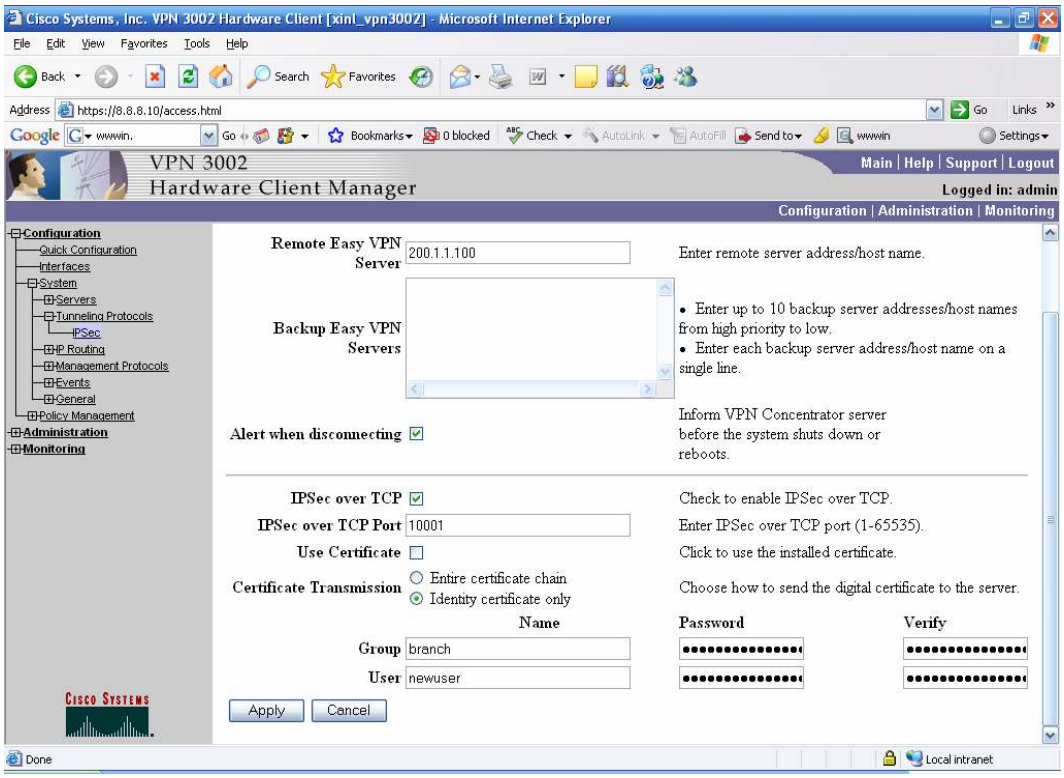
Figure 3. cTCP on Cisco VPN 3000 Concentrator



To learn more about configuring a Cisco VPN 3000 concentrator as an EasyVPN Server, visit http://www.cisco.com/en/US/tech/tk583/tk372/technologies_configuration_example09186a00800945cf.shtml.

Figure 4 shows the cTCP configuration on a VPN 3002 hardware client. It enables IPsec over TCP and specifies one of the TCP ports the server listens to.

Figure 4. cTCP on VPN 3002 Hardware Client



Cisco ASA Appliance

Enable cTCP on the Cisco ASA appliance by configuring **"crypto isakmp ipsec-over-tcp port 10000"**. For more information about configuring the adaptive security appliance as an EasyVPN Server, visit http://www.cisco.com/en/US/products/ps6635/products_white_paper09186a008063e37a.shtml.

Americas Headquarters
Cisco Systems, Inc.
170 West Tasman Drive
San Jose, CA 95134-1706
USA
www.cisco.com
Tel: 408 526-4000
800 553-NETS (6387)
Fax: 408 527-0883

Asia Pacific Headquarters
Cisco Systems, Inc.
168 Robinson Road
#28-01 Capital Tower
Singapore 068912
www.cisco.com
Tel: +65 6317 7777
Fax: +65 6317 7799

Europe Headquarters
Cisco Systems International BV
Haarlerbergpark
Haarlerbergweg 13-19
1101 CH Amsterdam
The Netherlands
www-europe.cisco.com
Tel: +31 0 800 020 0791
Fax: +31 0 20 357 1100

Cisco has more than 200 offices worldwide. Addresses, phone numbers, and fax numbers are listed on the Cisco Website at www.cisco.com/go/offices.

Printed in USA

C07-402269-01 4/07