Utility name:
CTCLIENT.EXE version 1.3.0
CTSERVER.EXE version 1.3.0

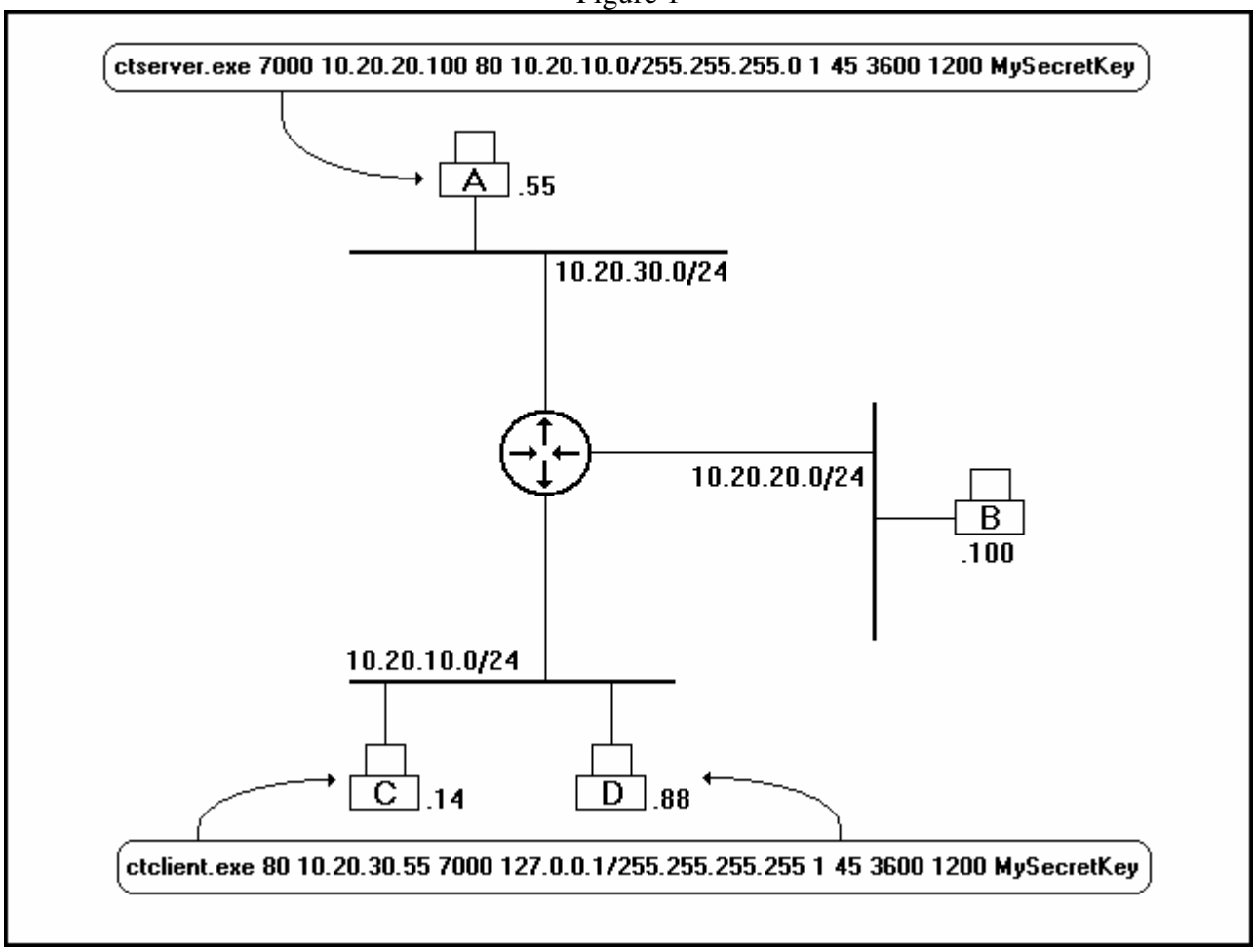
Purpose:
Establishes an encrypted point to point tunnel between a server and one or more clients using a proprietary 256-bit symmetric stream cipher. TCP traffic is encrypted as it is bidirectionally marshaled through the tunnel between CTCLIENT and CTSERVER and is converted back to the original unencrypted traffic, which is then delivered to the destination hosts. For proper operation, the client and server executables must be matched versions.

Author:
Bill Chaison, BC.Soft@yahoo.com, http://chaison.freewebpage.org

Development environment:
MS Visual C++ 6.0, console application, Winsock 2, multithreaded, 1163 lines of code per utility.

Example applications:
Point to multi-point tunneling, host-based secure channel, secure network traffic path exception, etc.

Figure 1



The scenario in figure 1 illustrates how hosts (C) and (D), which do not have direct access to host (B), can access the web server on host (B) through an encrypted tunnel with host (A). All traffic between (C) and (A) and between (D) and (A) that passes through the tunnel is encrypted using per-session read-write keying. Host (A) then sends the normal unencrypted traffic to host (B). The parameters used with ctserver.exe in this example indicate that host (A) will listen on TCP port 7000 for encrypted sessions then decrypt and relay all of the received data to host (B) over destination TCP port 80. The ACL used by ctserver.exe in this example restricts access to just hosts (C) and (D). The example application in figure 1 also indicates that incomplete TCP connection attempts to host (B) will be dropped after 1 second, completed TCP sessions to host (B) that have been idle for more than 45 seconds will also be dropped, and all instances of ctserver.exe and ctclient.exe will terminate after 1 hour from the time they were launched. Some additional considerations – if host (B) must be called by name as "http://www.mysite.net" then hosts (C) and (D) may need a "hosts" file entry or some other name resolution provision to ensure that "www.mysite.net" resolves to the loopback address, 127.0.0.1, instead of the address for host (B). All traffic being processed through the tunnel must be initiated by hosts (C) and (D). This pair of utilities does not provide transparent forwarding. All traffic marshaled by host (A) will use the IP address of host (A). For instance, the HTTP logs of host (B) will show the IP address of host (A) for web requests made by hosts (C) and (D).

To get additional help with the command line arguments, open a shell and execute each program without parameters.