6.6 VPN Tools Command Reference

This section describes all commands that can be called when using vpncmd in Use VPN Tools Command (for example, certificate generating tools or traffic speed test tool) mode.

6.6.1 "About": Display the version information

Command Name	**About**
Purpose	Display the version information
Description	This displays the version information of this command line management utility. Included in the version information are the vpncmd version number, build number and build information.
Command-line	*About*
Arguments for "About":	
No arguments are required.	

6.6.2 "MakeCert": Create New X.509 Certificate and Private Key

Command Name	**MakeCert**
Purpose	Create New X.509 Certificate and Private Key
Description	Use this to create a new X.509 certificate and private key and save it as a file. The algorithm used to create the public key and private key of the certificate is RSA 1024 bit. You can choose to create a root certificate (self-signed certificate) or a certificate signed by another certificate. To create a certificate that is signed by another certificate, you require a private key file (base 64 encoded) that is compatible with the certificate that uses the signature (X.509 format file). When creating a certificate, you can specify the following: Name (CN), Organization (O), Organization Unit (OU), Country (C), State (ST), Locale (L), Serial Number, and Expiration Date. The created certificate will be saved as an X.509 format file and the private key file will be saved in a Base 64 encoded RSA 1024 bit format file. The MakeCert command is a tool that provides the most rudimentary function for creating certificates. If you want to create a more

	substantial certificate, we recommend that you use either free software such as OpenSSL, or commercial CA (certificate authority) software. Note: This command can be called from the SoftEther VPN Command Line Management Utility. You can also execute this command while connected to the current VPN Server or VPN Client in Administration Mode but, what actually performs the RSA computation, generates the certificate data and saves it to file is the computer on which the command is running, and all this is executed in a context that has absolutely no relationship to the computer that is the destination of the Administration Mode connection.
Command-line	*MakeCert [/CN:cn] [/O:o] [/OU:ou] [/C:c] [/ST:st] [/L:l] [/SERIAL:serial] [/EXPIRES:expires] [/SIGNCERT:signcert] [/SIGNKEY:signkey] [/SAVECERT:savecert] [/SAVEKEY:savekey]*
Arguments for "MakeCert":	
/CN	Specify the Name (CN) item of the certificate to create. You can specify "none".
/O	Specify the Organization (O) item of the certificate to create. You can specify "none".
/OU	Specify the Organization Unit (OU) item of the certificate to create. You can specify "none".
/C	Specify the Country (C) item of the certificate to create. You can specify "none".
/ST	Specify the State (ST) item of the certificate to create. You can specify "none".
/L	Specify the Locale (L) item of the certificate to create. You can specify "none".
/SERIAL	Specify the Serial Number item of the certificate to create. Specify using hexadecimal values. You can specify "none".
/EXPIRES	Specify the Expiration Date item of the certificate to create. If you specify "none" or "0", 3650 days (approx. 10 years) will be used. You can specify a maximum of 10950 days (about 30 years).
/SIGNCERT	For cases when the certificate to be created is signed by an existing certificate, specify the X.509 format certificate file name to be used to sign the signature. When this parameter is omitted, such signature signing is not performed and the new certificate is created as a root certificate.
/SIGNKEY	Specify a private key (RSA, base-64 encoded) that is compatible with the certificate specified by /SIGNCERT.
/SAVECERT	Specify the file name to save the certificate you created. The certificate is saved as an X.509 file that includes a public key that is RSA format 1024 bit.

/SAVEKEY	Specify the file name to save private key that is compatible with the certificate you created. The private key will be saved as an RSA-format 1024-bit private key file.

6.6.3 "TrafficClient": Run Network Traffic Speed Test Tool in Client Mode

Command Name	**TrafficClient**
Purpose	Run Network Traffic Speed Test Tool in Client Mode
Description	Use this to execute the communication throughput measurement tool's client program. Two commands, TrafficClient and TrafficServer, are used for the communication throughput measurement tool to enable the measurement of communication throughput that can be transferred between two computers connected by IP network. The TrafficServer command is used first on another computer which puts the communication throughput measurement tool server in a listening condition. Then the TrafficClient command is used to connect to that server by specifying its host name or IP address and port number, which makes it possible to measure the communication speed. Measurement of the communication speed is carried out by concurrently establishing multiple TCP connections and calculating the actual number of bits of data that can be transferred within a specified time based on the respective results of transferring the maximum stream data on each connection and then using that to calculate the average value (bps) of communication throughput. Normally when there is one TCP connection, it is common to only be able to achieve communication speeds slower than the actual net throughput because of limitations related to the TCP algorithm. We therefore recommend the establishment of multiple concurrent TCP connections when measuring communication results. Because the throughput that is measured using this measurement method is calculated from the bit length of the data that arrives on the receiver side as a stream by TCP, the packet loss that occurs during transfer and the packets with corrupted data are not included in the packets that actually arrive, which means it is possible to calculate a genuine value that is close to the maximum possible communication bandwidth of the network. Using the measurement results, i.e. the stream size transferred by TCP, the approximate value of data volume that actually passed through the network is calculated and this is divided by time to calculate the bits per sec (bps). The calculation assumes the type of

	the physical network is Ethernet (IEEE802.3) and the MAC frame payload size is 1,500 bytes (TCP MSS is 1,460 bytes). By specifying the /RAW option, the calculation will not make corrections for the TCP/IP header and MAC header data volume. Note: This command can be called from the SoftEther VPN Command Line Management Utility. You can also execute this command while connected to the current VPN Server or VPN Client in Administration Mode but, what actually conducts communication and measures the throughput is the computer on which the command is running, and all this is executed in a context that has absolutely no relationship to the computer that is the destination of the Administration Mode connection.
Command-line	*TrafficClient [host:port] [/NUMTCP:numtcp] [/TYPE:download|upload|full] [/SPAN:span] [/DOUBLE:yes|no] [/RAW:yes|no]*
Arguments for "TrafficClient":	
host:port	Specify the host name or IP address and port number that the communication throughput measurement tool server (TrafficServer) is listening for. If the port number is omitted, 9821 will be used.
/NUMTCP	Specify the number of TCP connections to be concurrently established between the client and the server for data transfer. If omitted, 32 will be used.
/TYPE	Specify the direction of data flow when throughput measurement is performed. Specify one of the following options: "download", "upload" or "full". By specifying "download" the data will be transmitted from the server side to the client side. By specifying "upload" the data will be transmitted from the client side to the server side. By specifying "full", the data will be transferred in both directions. When "full" is specified, the NUMTCP value must be an even number of two or more (half the number will be used for concurrent TCP connections in the download direction and the other half will be used in the upload direction). If this parameter is omitted, "full" will be used.
/SPAN	Specify, using seconds, the time span to conduct data transfer for the measurement of throughput. If this parameter is omitted, "15" will be used.
/DOUBLE	When "yes" is specified, the throughput of the measured result will be doubled and then displayed. This option is used for cases when a network device etc. is somewhere on the data route and the total throughput capability that is input and output by this network device is being measured.

/RAW	By specifying "yes", the calculation will not make corrections for the TCP/IP header and MAC header data volume.

6.6.4 "TrafficServer": Run Network Traffic Speed Test Tool in Server Mode

Command Name	**TrafficServer**
Purpose	Run Network Traffic Speed Test Tool in Server Mode
Description	Use this to execute the communication throughput measurement tool's server program. Two commands, TrafficClient and TrafficServer, are used for the communication throughput measurement tool to enable the measurement of communication throughput that can be transferred between two computers connected by IP network. To set the TCP port of this computer to the Listen status to listen for the connection from the TrafficClient of another computer, specify the port number and start the server program using the TrafficServer command. You can display more detailed information on the communication throughput measurement tool by inputting "TrafficClient /?". Note: This command can be called from the SoftEther VPN Command Line Management Utility. You can also execute this command while connected to the current VPN Server or VPN Client in Administration Mode but, what actually conducts communication and measures the throughput is the computer on which the command is running, and all this is executed in a context that has absolutely no relationship to the computer that is the destination of the Administration Mode connection.
Command-line	*TrafficServer [port]*
Arguments for "TrafficServer":	
port	Specify, using an integer, the port number at which to listen for the connection. If the specified port is already being used by another program, or if the port cannot be opened, an error will occur.

6.6.5 "Check": Check whether SoftEther VPN Operation is Possible

Command Name	**Check**
Purpose	Check whether SoftEther VPN Operation is Possible

Description	Use this to check if the current computer that is running vpncmd is a suitable operation platform for SoftEther VPN Server / Bridge. If this check passes on a system, it is highly likely that SoftEther VPN software will operate correctly on that system. Also, if this check does not pass on a system, then this indicates that some type of trouble may arise if SoftEther VPN software is used on that system.
Command-line	*Check*
Arguments for "Check":	
No arguments are required.	