3.7 Virtual NAT & Virtual DHCP Servers

The SoftEther VPN Server and SoftEther VPN Bridge Virtual Hubs feature SecureNAT functionality. This section will explain SecureNAT concepts, methods for setting them and precautions.

3.7.1 What is SecureNAT?

SecureNAT Overview

The SecureNAT function is a hitherto unknown innovative proprietary technology developed for the SoftEther VPN, the use of which enables the creation of a more secure network.

The SecureNAT function is broadly divided into two parts: the virtual NAT function and the virtual DHCP server function. The Virtual Hub Administrator can enable either or both the virtual NAT and virtual DHCP server when SecureNAT is enabled.

Please refer to 10.11 Exploit SecureNAT for Remote Access into Firewall without Any Permission for details on how to set up the SecureNAT function.

The SecureNAT function is oriented towards System Administrators and those with a detailed knowledge of networks. Proper use of the SecureNAT function enables the realization of safe remote access via the VPN. However, its erroneous use may place the entire network at risk. Please do not enable the SecureNAT function without such a knowledge of networks and the permission of the Network Administrator.

Virtualizing the Broadband Router Function

Many general broadband routers developed and commercialized for business and consumer applications integrate the NAT function and the DHCP server function, and connecting a computer internally to a broadband router enables access via NAT to global IP networks (such as the Internet) in addition to the automatic assignment of a private IP address to that computer.

The SoftEther VPN SecureNAT function virtualizes the NAT and DHCP server functions equipped in typical broadband routers and, by carrying out all processing just in user mode, enables the use of functions equivalent to a broadband router between a virtual and a physical LAN.

3-7-1.png

SecureNAT function.

SecureNAT Virtual Interface

The SecureNAT function can be set and enabled/ disabled for each Virtual Hub. Unlike the local bridge function, all settings of the SecureNAT function can be set by the Virtual Hub Administrators. Enabling the SecureNAT function creates a virtual VPN session called a SecureNAT session within the Virtual Hub and creates a virtual network interface (VNI) as if there were a single network adapter within that VPN session. This is called a virtual host network interface.

A virtual host network interface is layer 2 direct connected to the Virtual Hub. As such, from the perspective of other VPN client computers connected to the Virtual Hub and the perspective of cascaded or bridging destination computers when the Virtual Hub is cascaded or locally bridged to other Virtual Hubs or physical LANs, the SecureNAT function's virtual host network interface is recognized as being equivalent to a single computer. The virtual host network interface can also assign IP addresses.

Using SecureNAT with General User Authority

The SecureNAT function and virtual NAT / virtual DHCP server all run as user mode programs. In order to realize a complicated mechanism such as the one present in the virtual NAT in particular, it is usually necessary to use the kernel module within the operating system.

In order to realize the virtual NAT, the SoftEther VPN requires absolutely no special processing in the operating system's kernel mode nor the use of the kernel mode's NAT function. Accordingly, all SecureNAT functions including the virtual NAT function can be freely executed with general user authority.

This feature means that no System Administrator authority is required to use the SecureNAT function. Please refer to 3.2 Operating Modes for details on how to launch the VPN Server / VPN Bridge as a general user.

When general users with permission from the Network Administrator or System Administrator but without a System Administrator account use the SecureNAT function, it becomes possible to realize VPN communication typically not within general user authority. Please refer to 10.11 Exploit SecureNAT for Remote Access into Firewall without Any Permission for specific methods of use.

In addition, System Administrators can use SecureNAT as safe NAT software. Typical NAT programs run as kernel modules. If there is vulnerability such as a buffer overrun in part of the NAT program, it may lead to system invasion and kernel authority theft by a black hat or an entire system crash due to a bug. In contrast, the SoftEther VPN SecureNAT program can be run completely in user space without the need for special system authority. Even if a failure occurs in the SecureNAT program, the effect is limited to the user space which launched the VPN Server / VPN Bridge, thus eliminating the risk of effects to other users and the system overall.

Aims of SecureNAT Use

The SecureNAT function can be use for the following objectives.

- **Use as a Simple Network Gateway**
  Even setting up the VPN Server and Virtual Hub and remotely connecting to that hub only results in closed communication within the Virtual Hub, so it is possible to communicate with the physical network connected to the computer running the VPN Server. Using local bridging in this case commonly involves a layer 2 connection between the Virtual Hub and the physical network, but using the SecureNAT function enables communication with the network connected to the computer operating the VPN Server via the Virtual Hub's virtual host network interface. Therefore, it is possible to make use of SecureNAT's virtual NAT function when preferring not to use the local bridging function, or unable to use it due to not possessing the computer's System Administrator authority or due to use of a UNIX OS version of the VPN Server or VPN Bridge other than Windows, Linux or Solaris.
- **As a DHCP Server**
  Of the SecureNAT functions, it is possible to enable only the DHCP server. In other words, it is possible to use only the DHCP server function operating within the Virtual Hub Ethernet segment. This allows VPN Clients and local bridge destination client computers remotely accessing the Virtual Hub to receive IP addresses assigned by the virtual DHCP server.
  Normally, using DHCP automatic IP address assignment requires locally bridging that Virtual Hub to a separate network of the DHCP server or

connecting to the Virtual Hub from the DHCP server with the VPN Client using the Virtual Network Adapter, but the SecureNAT function's Virtual DHCP server function eliminates this need.

- **As a Simple Gateway to Remotely Access Remote Sites**
  Remote access VPN to a remote site (for instance, sites on which equipment maintenance is to be carried out via the network) using the SoftEther VPN typically involves installing the VPN Server and VPN Bridge on that remote site's computer and connecting to it with a VPN Client or setting up a continuous cascade connection from that site to a VPN Server set up in a separate location, thus enabling communication with a computer node on that remote site using the SoftEther VPN. However, the SecureNAT function can be used as an alternative when a local bridge cannot be set up on a remote site's computer for security or costs limitations or when the OS does not support the SoftEther VPN local bridging function. Please refer to 10.11 Exploit SecureNAT for Remote Access into Firewall without Any Permission for details on these methods of use.

Enabling the SecureNAT Function

This function is disabled in default mode. To enable the SecureNAT function, click on [Virtual NAT & Virtual DHCP Server (SecureNAT)] button in the VPN Server Manager and display the [Virtual NAT and Virtual DHCP Server function (SecureNAT) Setting] window (all subsequent explanations relating to SecureNAT assume that this window is open). Next click on [Enable SecureNAT].

In the vpncmd utility, SecureNAT commands all begin with **"SecureNAT", "Nat"** and **"Dhcp"**. To enable the SecureNAT function for example, use the **[SecureNATEnable]** command.

3-7-2.png

Virtual NAT and Virtual DHCP Server function (SecureNAT) Setting window.

Neither the virtual NAT function or the virtual DHCP server function operate when the SecureNAT function of which they are a part is disabled. Therefore, ensure that the SecureNAT function is enabled before using either of these functions.

3.7.2 Setting the Virtual Host Network Interface

The SecureNAT function enables setting of information relating to the VNI of the virtual node (virtual host) created inside the Virtual Hub.

Click on [SecureNAT Configuration] in the VPN Server Manager and enter the relevant details in the [Virtual Host Network Interface Setting] entry. A list of the entries and default values which can be set is as follows.

Entry	Description	Default Values

MAC Address	The virtual host network interface is a Virtual Network Adapter which supports Ethernet standards like typical computer network adapters and Virtual Network Adapters, so one MAC address can be used. Designate the MAC address to be used.	Total of 6 bytes of random data starting with "00:AC".
IP Address	Designate the IP address of the virtual host network interface.	192.168.30.1
Subnet Mask	Designate the subnet mask of the IP network to which the designated IP address belongs.	255.255.255.0

3-7-3.png

Virtual host administration window.

3.7.3 Virtual NAT

Virtual NAT Function Settings

Set the [Use Virtual NAT Function] checkbox to enable status in the VPN Server Manager to use the SecureNAT's virtual NAT function. Contrarily, select disabled status when not using the function. When starting SecureNAT, the virtual NAT function is enabled by default.

A list of the entries and default values which can be set is as follows.

To set each option, use the VPN Server Manager to make the relevant entries in the [Virtual NAT Setting] box inside [SecureNAT Setting]. In the vpncmd utility, use the **[NatSet]** command.

Entry	Description	Default Values
MTU	Designates the MTU value used by the virtual NAT function on the VNI side. This value designates the maximum length of the Ethernet frame payload size (length excluding the MAC header).	1500 bytes

TCP Session Timeout	Sets whether a TCP/IP session among the entries of the NAT session established via the virtual NAT function is regarded as timed out after a certain number of seconds have elapsed without any communication.	7,200 seconds
UDP Session Timeout	Sets whether a UDP/IP session among the entries of the NAT session established via the virtual NAT function is regarded as timed out after a certain number of seconds have elapsed without any communication.	600 seconds

3-7-4.png

Virtual NAT function administration window.

Using the Virtual NAT Function

TCP/IP and UDP/IP communication using the virtual NAT function is used as follows.

1. Make the appropriate settings and enable the SecureNAT and the virtual NAT function in the Virtual Hub. In particular, match the virtual host's IP address & subnet mask with the IP network address and subnet mask used in that Virtual Hub.
2. In the TCP/IP settings on a separate client computer on the Virtual Hub side (it does not matter whether this is connected by a physical local bridge and cascade connection or via the VPN Client), set the IP address of the SecureNAT virtual host running on the Virtual Hub as the default gateway (combining with the virtual DHCP server function described below also enables automatic settings).
3. When the client computer attempts to perform TCP/IP or UDP/IP communication, the virtual NAT operates entirely as a single router with NAT functionality enabling access to a physical network's host via the computer running the Virtual Hub using that computer's existing network interface. A new session is registered on the virtual NAT function's NAT session table at that time. To display the NAT session table, click on the [Virtual NAT Router Status] button in the VPN Server Manager. In the vpncmd utility, use the **[NatTable]** command.

Operating Principles of the Virtual NAT Function

The virtual NAT function realizes IP routing and NAT (IP masquerade) processing, typically carried out in kernel mode, in user mode.

The hierarchical relationship of the network protocol stack on a system with NAT functionality in kernel mode is shown in the figure below.

3-7-5.png

Stack diagram of network modules in combined normal kernel mode NAT & SoftEther VPN NAT.

The area in red in the diagram above denotes those operating in kernel mode. Achieving functions equivalent to these areas typically required kernel mode programming. However, the likelihood of increased fatal vulnerability in terms of security when executing programs in kernel mode and the possibility of entire system instability due to a program bug suggests that all processing should be carried out in User Mode wherever possible.

To enable these processes in user mode, SoftEther VPN Project developed a proprietary TCP/IP stack for exclusive use with the SecureNAT function and succeeded in implementing it in user mode. SecureNAT's virtual NAT function receives TCP/IP and UDP/IP packets from the virtual network as a router and administers those packets to each session, interpreting them properly in the layers up to the transport layer. For TCP/IP protocol, the TCP/IP stream is reconfigured based on the sequence number within that connection. These reconfigured payload data are forwarded to the target host as fast as possible using the socket API of the operating system running the VPN Server VPN Bridge, in addition to being internally stored in the FIFO buffer. Data received from the destination host also travels this route but in the opposite direction, returning to the Virtual Hub's virtual network. The TCP/IP stack running in user mode is also used at this time, and the data is automatically put into datagram format by recovery and flow control algorithms conforming to TCP/IP protocol standards. SecureNAT's virtual NAT function is realized by way of this extremely complicated processing, although general users do not have to be aware of these operating principles.

3-7-6.png

Stack diagram of network modules in SecureNAT's virtual NAT function.

3.7.4 Points to Note when using Virtual NAT Function

While virtual NAT is a very convenient function, the following precautions should be taken when using it.

- **Using Virtual NAT**
  The use of virtual NAT is recommended for environments running the VPN Server / VPN Bridge without System Administrator authority or OS support for local bridging, i.e. when a computer in the Virtual Hub's layer 2 segment is unable to use the local bridge function and needs to access a physical network host via the physical network interface of the computer actually running the Virtual Hub (particularly where the uses given in 10.11 Exploit SecureNAT for Remote Access into Firewall without Any Permission are applicable).
  Where local bridging can be used to connect a Virtual Hub and a physical network and in the absence of security issues, it is not necessary to connect a virtual network to a physical network using the virtual NAT function.
- **Preventing Connections causing Infinite Looping of Packets**
  Where a computer with VPN Client installed connects to a virtual NAT-enabled Virtual Hub either from the Virtual Network Adapter of its own Virtual Hub or by local bridging to said hub from a physical Network Adapter, and where the default gateways for those Network Adapters designate IP addresses assigned by the Virtual HUB?fs SecureNAT virtual host network interface, communication attempting to connect to an arbitrary IP address tries to use the Virtual Hub's Virtual NAT, which in turn tries to communicate with the destination IP address by calling the operating system's network communication API, resulting in the connection packet falling into an infinite loop. The virtual NAT function is not typically used at the same time as local bridge connections and VPN connections to localhost using the VPN Client. If these types of connections are being made then there is a likelihood that the network design is incorrect.
- **Precautions relating to Performance**
  By possessing an internal virtual TCP/IP stack, SecureNAT performs the highly advanced process of reassembling the TCP/IP stream packetized once by the TCP/IP stack and further TCP/IP packetizing via the operating system. The overhead resulting from these processes is large, such that throughput via the virtual NAT is considerably decreased when compared to physical maximum throughput, even when using a computer with sufficiently high speed. That is why virtual NAT should not be used for performance-centric applications. As previously stated, virtual NAT is a function which can be used as an alternative when the local bridge function cannot be used for security or technical reasons. Where high-speed methods such as local bridging are available, those methods should be used.
- **Handling ICMP Packets**
  When virtual NAT is enabled, sending ICMP packets via IP addresses assigned by a virtual host network interface as routers, and further sending said packets to

a separate host results in the virtual NAT returning dummy ICMP echo response packets to all ICMP echo request packets. This is a specification of the SoftEther VPN whereby this operation becomes inevitable because most operating systems do not allow the transmission of arbitrary ICMP packets in network APIs which can be called up with user authority. When using Virtual NAT it is therefore impossible to confirm the existence of a host on the other side of a Virtual NAT router using ICMP packets.

- **DNS Redirect**
  When Virtual NAT is enabled, UDP 53 port destination packets (DNS packets) to the IP address of the virtual host network interface are automatically forwarded to the DNS server being used as the DNS Server by the computer running the Virtual Hub. This is the same operation carried out by typical broadband routers.
- **Unsupported Functions**
  The User Mode TCP/IP stack used internally by Virtual NAT is not equipped with some sophisticated TCP/IP functions such as the Window Scale option, Selective ACKs and Nagle algorithms. In addition, the nature of Virtual NAT means that IP routing and NAT between virtual networks is not supported. The virtual layer 3 switch function should be used for inter-virtual network IP routing.

3.7.5 Virtual DHCP Server

The Virtual DHCP Server Function

The Virtual DHCP Server function can be used in SecureNAT. Depending on the method of use, there is also no problem in using the DHCP Server without using SecureNAT. The DHCP Server enables a computer connected to a Virtual Hub layer segment to receive an IP address distributed from the DHCP Server and temporarily use that IP address.

The Virtual DHCP Server allocates IP addresses in much the same way as a physical computer DHCP server program. However, it does not offer detailed functions to set numerous options like those included in the Windows Server versions.

The Virtual DHCP Server enables simple DHCP address allocation rather than being a fully fledged DHCP server. The function is most suitable when setting up a Virtual Hub and seeking to automate IP address assignment to that Virtual Hub's computer using the DHCP protocol, but being prevented from doing so due to the effort required to run the DHCP server software on the same segment as the Virtual Hub.

While the DHCP Server function is simplistic, it is able to set IP address expiration dates, administer lease tables and allocate several essential options without problems.

3-7-7.png

Virtual DHCP Server function.

Virtual DHCP Server Function Settings

Set the [Use Virtual DHCP Server Functions] checkbox to enabled status in the VPN Server Manager to use the SecureNAT's Virtual DHCP Server function. Contrarily, select disabled status when not using the function. When starting SecureNAT, the Virtual DHCP Server function is enabled by default.

A list of the entries and default values which can be set is as follows.

To set each option, use the VPN Server Manager to make the relevant entries in the [Virtual DHCP Server Setting] box inside [SecureNAT Setting]. In the vpncmd utility, use the **[DhcpSet]** command.

Entry	Description	Default Values
Distribution IP Address Range	Designates the range of IP addresses allocated by the Virtual DHCP Server to the client.	From 192.168.30.10 to 192.168.30.200
Subnet Mask	Designates the subnet mask value assigned to the client together with the IP address.	255.255.255.0
Lease Limit	Designates the expiration date of the leased IP address.	7,200 seconds
Default Gateway Address Assigned to Client	Designates the setting value of the default gateway address directed to the client. While concurrent use with the Virtual NAT function is assumed in default, it is also possible to change to a different	192.168.30.1

	value. It is also possible not to designate any value.	
DNS Server Address Assigned to Client	Designates the setting value of the DNS server address directed to the client. While concurrent use with the Virtual NAT function is assumed in default, it is also possible to change to a different value. It is also possible not to designate any value.	192.168.30.1
Domain Name Assigned to Client	Designates the setting value of the DNS domain suffix directed to the client. It is also possible not to designate any value.	Domain name attached to computer running Virtual Hub

3-7-8.png

Virtual DHCP Server function administration window.

Obtaining IP Address Lease Table

A list of the IP addresses assigned by the Virtual DHCP Server (IP Address Lease Table) can be displayed at any time. To display the IP Address Lease Table, click on the [Virtual

DHCP Server Status] button in the VPN Server Manager. In the vpncmd utility, use the **[DhcpTable]** command.

3-7-9.png

Virtual DHCP Server IP Address Lease Table display window.

3.7.6 Points to Note when using the Virtual DHCP Server

While Virtual DHCP Server is a convenient function, the following precautions should be taken when using it.

- **Using the Virtual DHCP Server**
  The Virtual DHCP Server provides simple DHCP server functions, and does not require System Administrator Authority to operate. The use of authentic UNIX or Windows DHCP server software is recommended where the Virtual DHCP Server functions are insufficient.

- **Effective Range of DHCP Scope**
  The scope (range) within which IP addresses allocated by the Virtual DHCP Server can be received is limited by the layer 2 segment of the Virtual Hub on which the SecureNAT is operating. Accordingly, where there is no connection to a physical LAN by local bridging in particular, it is possible to limit the range affected by that DHCP server to within the Virtual Hub and to enable only the computer VPN-connected to the Virtual Hub to receive the IP address from the Virtual DHCP Server. The LAN connected to the computer actually running the

Virtual Hub is not affected (this does not apply in the case of local bridging). Needless to say, the entire layer segment is subject to IP address assignment from the DHCP server in the case of cascading between Virtual Hubs or bridging with a separate site.

- **Note on Initial Settings**
  The Virtual DHCP Server function's default settings assign the address space 192.168.30.0/24 to the client computer, and attempt to set the default gateway and DNS server address under the assumption that the Virtual NAT function is to be used concurrently. Not using the Virtual NAT function renders the default gateway and DNS server address default settings meaningless, so be sure to modify them.

- **Allocating IP Addresses only without Allocating Default Gateway & DNS Server Addresses**
  When wishing to use the Virtual DHCP Server to simply allocate an IP address to the client computer without allocating client default gateway and DNS server settings, leave the [Default gateway address] and [DNS server address] boxes in the client-assigned options blank. In this case, the client computer to which the IP address is assigned does not modify the router or DNS server it uses.
  Please note that there have been reports of a problem for client computers using Windows, wherein the options relating to the default gateway and DNS server received upon the previous assignment from the DHCP server are cached, and when these values are left blank on the subsequent connection, these previous ones are applied. While this appears to be a Windows OS specification, we recommend trying to connect to a separate DHCP server once in an attempt to overcome it.

3.7.7 SecureNAT Sessions

When the SecureNAT function is operating on the Virtual Hub, a special virtual session called a SecureNAT session is registered on the Virtual Hub session list. The SecureNAT-operated virtual host VNI is virtually (software-wise) internally connected to this session.

The Virtual Hub Administrator can obtain information on this session in the same way as a normal session.

3.7.8 Logging SecureNAT Status

The entire status of SecureNAT's Virtual NAT and Virtual DHCP Server functions are saved in the Virtual Hub's security log. Below is an example of a saved log.

2012-12-06 15:44:52.557 SecureNAT: The DHCP entry 1 was created. MAC address: 00-AC-85-40-B5-50, IP address: 192.168.30.10, host name: NT4, expiration date: 7200 seconds
The TCP session 1 was created. Connection source 192.168.30.10:1079, Connection destination 207.46.0.166:1863
2012-12-06 15:45:08.104 SecureNAT: The TCP session 1 was created. Connection source 192.168.30.10:1079, Connection destination 207.46.0.166:1863
2012-12-06 15:45:08.401 SecureNAT: The connection to TCP session 1: Host "baym-sb26.msgr.hotmail.com (207.46.0.166)", Port 1863 was successful.
2012-12-06 15:45:08.666 SecureNAT: The TCP session 1 was deleted.
2012-12-06 15:45:14.604 SecureNAT: The UDP session 2 was created. Connection source 192.168.30.10:1048, Connection destination 192.168.30.1:53
2012-12-06 15:45:14.760 SecureNAT: The TCP session 3 was created. Connection source 192.168.30.10:1080, Connection destination 65.54.239.140:1863
2012-12-06 15:45:15.479 SecureNAT: The TCP session 4 was created. Connection source 192.168.30.10:1081, Connection destination 61.197.235.212:143
2012-12-06 15:45:15.494 SecureNAT: The connection to TCP session 4: Host "us.softether.co.jp (61.197.235.212)", Port 143 was successful.