# Version History (ChangeLog)

The revision history of each SoftEther VPN build is here.1

**Download the latest binaries**

Download the source code

- **SoftEther VPN 4.44 Build 9807 RTM (April 16, 2025)**
  - (1) We have implemented the new "TunnelCrack Protection Function" in the VPN Client, which enhances security when using potentially untrusted public wireless Wi-Fi connections. For details, please refer to: https://ja.softether.org/9-about/news/905-TunnelCrack/
    TunnelCrack is a security attack method pointed out in the paper “Bypassing Tunnels: Leaking VPN Client Traffic by Abusing Routing Tables,” presented on August 11, 2023, at the international conference USENIX Security ’23.
    The TunnelCrack attack method poses an issue when using a malicious, untrusted public wireless LAN. Various common VPN client software may be affected by TunnelCrack, and countermeasures on the VPN client software side are necessary.
    Therefore, we have added TunnelCrack protection to the VPN Client. This TunnelCrack protection feature can be enabled easily from the settings screen. When the TunnelCrack protection feature is enabled, TCP and UDP connections over the physical local network are blocked while the VPN connection is active. This strengthens protection when using untrusted public wireless LANs.
    The TunnelCrack protection feature of SoftEther VPN Client supports both “LocalNet Attack” and “ServerIP Attack.”
    Note that, when TunnelCrack protection is enabled, TCP and UDP connections to the physical local LAN are blocked while the VPN connection is active. This protection is beneficial when using untrusted public Wi-Fi. On the other hand, if you enable TunnelCrack protection on a trusted LAN such as a corporate intranet, you will not be able to access servers on the local LAN and the remote VPN destination at the same time (though you can continue to communicate with the remote VPN server until you disconnect the VPN, you will be unable to communicate with local servers). Please keep this in mind.
    When the TunnelCrack protection feature becomes active, any TCP connections already established before activation will be maintained without disconnection. Any new TCP or UDP connections initiated after

activation will be blocked.

- (2) We have added AEAD cipher support for OpenVPN in the VPN Server. This function was backported from the Developer Edition of the SoftEther VPN open-source version. However, since there are various versions of client implementations for the OpenVPN AEAD protocol, there is a possibility that this function may not work properly depending on the client version. If you encounter specific version-related issues, please send us a detailed report, and we will work to improve it.

- (3) In the automatic configuration file generation feature for OpenVPN client apps, we have now included the "data-ciphers" parameter (supported by recent versions of the OpenVPN client). Since older versions of OpenVPN clients still read the "cipher" parameter, we embed both the "data-ciphers" and "cipher" parameters into the configuration file. Note that some quite old versions of the OpenVPN client may not recognize the "data-ciphers" parameter and produce an error. If that happens, simply commenting out the "data-ciphers" parameter will prevent the error.

- (4) We have added a message authentication feature to the RADIUS client function in the VPN Server. If there is a vulnerable network between the VPN Server and the RADIUS server that could allow a third party to tamper with communications, this feature helps prevent such tampering. To enable message authentication, set the "RadiusRequireMessageAuthenticator" item (bool type) to "true" under the virtual HUB settings in the VPN Server's configuration file.
  This message authentication feature was realized by source code donated by Mr. "Atsushi Saito, Aryeh inc." We would like to express our sincere gratitude.

- (5) We removed the explanatory text stating that the multiple login count limitation policy does not apply in bridge mode.

- (6) We fixed an issue in the InRpcEnumLink RPC function, where the non-existent item "LinkHubName" was read as "HubName."

- (7) We fixed a problem with the specification of TCP packet states among the entry parameters for the access list (packet filter) feature in the vpncmd command-line management utility, where the interpretation of the strings "Established" and "Unestablished" was reversed.

- (8) We have improved the following issue, which Amazon Web Services, Inc. (AWS) requested that we fix via their engineer, phillibert. When the IPsec function of VPN Server is enabled and a communication

request packet specifying an SPI for a non-existent IKE_SA arrives, the server processes an error response packet (IKE_NOTICE_ERROR_INVALID_SPI) indicating that the specified SPI does not exist. In doing so, it returns one error packet per incoming UDP packet. Because the size of the error packet can be larger than the size of the incoming packet — up to about 2.75 times the original — this can theoretically be used as a form of UDP amplification. Practically speaking, however, it is believed to be inefficient for an attacker, and thus it is unlikely to be used in an actual UDP amplification attack. Nevertheless, the upload bandwidth of the host running the VPN Server would still be wasted. Customers using a cloud service like AWS, where outgoing bandwidth usage incurs high per-Mbps fees, might lodge complaints to AWS, creating difficulties (and higher support costs) for the cloud provider. That is presumably the background behind AWS's request to fix this issue.
Under SoftEther VPN, if the server does not respond with an error packet (IKE_NOTICE_ERROR_INVALID_SPI) indicating that a specified SPI does not exist, then the IPsec VPN client side may not become aware that an error has occurred. Thus, returning an error response packet was considered useful and, in some cases, necessary. Changing the behavior not to respond with that error packet thus entails certain risks.
However, we tested a version in the Developer Edition of SoftEther VPN (open-source) starting in June 2024 in which the server does not send back such error responses. Even after about ten months, there were no reports from IPsec VPN clients of any particular problems caused by omitting the error response. Based on that, we judged that omitting the response in the stable version of SoftEther VPN is more rational than continuing to send it, in line with AWS's request.
We would like to thank Amazon Web Services, Inc. (AWS) and their engineer, phillibert, for providing technical information on this topic. In connection with this fix, we have assigned vulnerability numbers CVE-2024-38520, GHSA-j35p-p8pj-vqxq ("SoftEther VPN with L2TP - 2.75x Amplification"). Since failing to apply this patch does not lead to any unauthorized intrusions or other security breaches, there is no urgent need to apply it.

- (9) We fixed a code issue in the packet processing for the DeleteIPv6DefaultRouterInRA function of the VPN Server's virtual HUB. This issue could theoretically lead to a NULL reference exception and crash the vpnserver process if (i) the physical communication path (outside the VPN tunnel) uses IPv6, (ii) the inside of the VPN tunnel also uses IPv6, (iii) IPv6 ICMP RA packets are transmitted, and (iv) the packet is malformed.

This issue was reported by "catenacyber" as "NULL dereference in DeleteIPv6DefaultRouterInRA" (CVE-2025-32787, GHSA-xw53-587j-mqh6). We appreciate the thorough reading of our C language source code. However, we currently do not consider this code issue to be an actual "vulnerability."
Technically, the bug arises from calling ParsePacket() on a copy of the packet within the StorePacket() function in Hub.c. If the packet structure is corrupted and ParsePacket() returns NULL, the subsequent code fails to check for NULL, potentially triggering a NULL access exception. However, to reach StorePacket(), the packet must already have been parsed successfully once by ParsePacket() (otherwise it would have been discarded before StorePacket() was called). In other words, a truly malformed packet that causes ParsePacket() to return NULL would never even make it as far as StorePacket().
Hence, although this is a bug in code, it appears on a path that should never occur in practice, and thus does not constitute a security vulnerability. Nonetheless, from the standpoint of improving code quality, the report of such a missing NULL check is extremely valuable. Additionally, it can occasionally be beneficial to have it appear as if there were more frequent "vulnerabilities," since that attracts more active development and usage, enhancing the perceived value of the SoftEther VPN software, while also raising the reporter's reputation. For these reasons, we deliberately obtained a CVE number, and we will keep the GitHub vulnerability entry, effectively treating this as a "vulnerability."

- (10) We fixed a bug in the vpncmd command-line management utility whereby, if the administrator entered an extremely long string in a field expecting a numeric value, it could cause an array overrun and crash the vpncmd program. The cause was the lack of length checking inside the "UniToStrForSingleChars" function.
  This issue occurs only when the administrator intentionally inputs a long string in a local UI input field of the vpncmd command-line management tool. It does not affect the SoftEther VPN Server, Client, or Bridge daemon programs (none of these VPN processing components use that function). This bug only affects the local UI program (vpncmd) and is not a vulnerability in the VPN functionality.
  Among the vpncmd commands using "UniToStrForSingleChars" internally are the certificate creation commands "PtMakeCert" and "PtMakeCert2048." If, for example, you are asked to enter "100" to create a certificate valid for 100 days but instead deliberately type a very long string of characters like "AAAAA...A," vpncmd would crash.
  The discoverer "lzydry" assigned the vulnerability number CVE-2025-25565 to this issue. However, as stated above, it is fundamentally just a UI bug in a local console application and does not affect the core VPN server or client functionality.

Note also that "lzydry" acquired multiple CVE numbers (CVE-2025-25565, CVE-2025-25566, CVE-2025-25567) for the same "UniToStrForSingleChars" bug and assigned a "CVSS v3 score of 9.8 (CRITICAL)" to it. Anyone can request a CVE number, and it is issued without substantial review. The person requesting the number can arbitrarily set the "vulnerability score," so merely having a CVE assigned does not automatically validate the seriousness of the claimed vulnerability.
We would like to thank "lzydry" for his detailed reading of the C code and discovering a bug that had been in the code for years.

  - (11) We have resolved a longstanding issue in the multi-threaded portion of the "Check" command within the vpncmd command-line management utility, in which a crash would rarely occur. The root cause was that the thread-creation code passed a pointer to the stack of the thread-creation caller as the parameter for the newly created thread. Depending on timing — specifically, which thread started running first — this would sometimes result in a crash.
    This bug has existed since around 2004, manifesting very rarely. When installing SoftEther VPN, the vpncmd "Check" command is often used to verify that the OS networking features are functioning correctly. Installing software is supposed to be a pleasant act, but a crash during "Check" can be disappointing. This bug's cause remained a mystery for years, but recently "lzydry" reported that there was a code bug involving stack usage, clarifying the cause. We have now fixed the code by moving the parameter onto the heap (allocated by the caller thread and freed by the created thread), which resolved the problem.
    However, there is no actual security impact here at all; it is not a "vulnerability." In the general definition, a vulnerability is "a weakness of an asset or control that one or more threats can exploit" (ISO 27000). Since a malicious actor cannot exploit this bug to break any security controls, it does not meet the definition of a vulnerability.
    Despite that, "lzydry" has again labeled this issue a "vulnerability," obtained a CVE number (CVE-2025-25568), and assigned it a "CVSS v3 score of 9.8 (CRITICAL)."
    This bug is not actually a vulnerability, and the CVSS v3 attributes assigned are completely unrelated to the technical details of the issue.
    We would like to thank "lzydry" for his detailed reading of the C code and discovering a bug that had been in the code for years.

- **SoftEther VPN 4.43 Build 9799 Beta (August 31, 2023)**
  - TunnelCrack protection implemented in SoftEther VPN Client
- **SoftEther VPN 4.42 Build 9798 RTM (June 30, 2023)**
  - As a result of a high-level code review and technical cooperation by Cisco Systems, Inc. of the United States, six vulnerabilities, including

    CVE-2023-27395, have been fixed. The risk of exploitation of any of the fixed vulnerabilities is relatively low under normal usage and environment, and actual attacks are not easy to conduct, We recommend that you update your software as much as possible.
  - Updated OpenSSL version to 3.0.9.
  - Resolved the problem that older versions of SoftEther VPN Client could not connect with RC4-MD5 when TLS 1.0 - 1.2 is enabled.
  - A potential inconsistency existed in some places due to incomplete locking of CapsCacheLock in the multi-threaded exclusion control for the VPN Server's internal data structure called Caps.
  - Resolved a problem that caused rare crashes due to insufficient multithread locking for a data structure called the IP address table inside the VPN Server's virtual HUB.
  - Removed display of IP address from response error messages in VPN Server's behavior as an HTTPS Web server.
  - DoS attack prevention function is implemented in SoftEther VPN Server.
  - Heap area protection of memory has been enhanced. When memory is released and reallocated, a random security value called a canary is written to the before/after area of memory, and if the value has been modified, the process is terminated (restarted) for safety, assuming it is a buffer overflow of the memory area. This feature may effectively prevent confidentiality or integrity violations in the event that some heap area overflow vulnerability is discovered in this system in the future.
  - The lock acquisition function called RW Lock (reader/writer lock) used inside the OpenSSL library used by this program calls the lock function provided by the OS (libc, pthread, kernel), but it is not supported in recent Linux distributions. However, there is a bug in the RW Lock of pthreads included in recent Linux distributions that, when handling thousands of sessions on a single server, would cause all CPUs to suddenly enter a spinlock interactive wait state, consuming an extremely long amount of CPU time, making VPN communication sessions difficult to communicate with, and causing VPN sessions to disconnect due to timeouts. This problem was caused by a glitch on the OS side. This problem was an OS-side defect and only occurred on at least Ubuntu 20.04 or later Linux distributions and the x64 version. Since this is an OS-side problem that is difficult to fix, we have rewritten the user mode program to use only the normal Mutex Lock instead of the RW Lock to work around this problem. This problem has been avoided.

- **SoftEther VPN 4.41 Build 9787 RTM (March 14, 2023)**
  - All cumulative updates bellow are included.
  - Limit key usage of server certificates when creating X.509 certificates.

- **SoftEther VPN 4.41 Build 9782 Beta (November 17, 2022)**

  - Updated OpenSSL version to 3.0.7.
  - Fixed a problem VPN Client. Now automatic retry will be stopped after specified number of retries even if there is an authentication error when connecting.
  - Fixed a problem that it does not start on Windows XP (occurred on Build 9772).
  - OpenSSL version is now displayed in various places.
  - Fixed a shortcut key error in VPN Client Manager.
  - Fixed a taskbar bug with Windows 11.
  - Sanitized the HTTP version in HttpSendNotImplemented.
  - Added PKCS#11 DLL names (SafeNet, OpenSC, SHALO AUTH).

- **SoftEther VPN 4.39 Build 9772 Beta (April 26, 2022)**
  - Updated OpenSSL version to 3.0.2.
  - Windows 11 support. We have confirmed the operation on Windows 11. Please note that since Windows 11 is a newer product compared to Windows 10, there is a possibility that there may be problems or incomplete behavior caused by the OS, which may affect the use of the VPN.
  - Fixed a problem that prevented new drivers supporting the NetAdapterCx standard from being enumerated properly on Windows 11.
  - Fixed configuration file revision incrementing even when password is changed from the client.
    Sanitize Method in HttpSendNotImplemented.
  - Added support for V_ASN1_GENERALIZEDTIME notation for certificate expiration dates.

- **SoftEther VPN 4.38 Build 9760 RTM (August 17, 2021)**
  - Improve the stability of IPsec function with reducing consuming CPU time / network bandwidth / memory consumption even if your server receive a large number of IPsec packets from indiscriminate attack attempts (brute force attacks, reflection attacks, etc.) targeting generic IPsec VPN devices, which have been occurring frequently on the Internet recently.
  - This RTM build includes all changes from the previously released Beta versions, Build 9754 and Build 9758.
  - If you are using the system with L2TP/IPsec, EtherIP/IPsec or L2TPv3/IPsec features enabled, we recommend that you apply the update. In addition, if you have been receiving indiscriminate attack attempt packets targeting IPsec VPN devices, which have been occurring frequently on the Internet since around August 2021, and have been experiencing reduced communication speed or failed VPN connections for legitimate users, we recommend that you apply the update.

- **SoftEther VPN 4.37 Build 9758 Beta (August 16, 2021)**
    - The frequency of notification of disconnected tunnel identification numbers via IPsec Informational Exchange packets is now limited, reducing the occurrence of nonsensical packet ping-pong between attackers targeting IPsec VPN devices with a wide range of global IP addresses.
    - Recently, we have observed a brute-force cyber attack that originates from several IP addresses of cloud services and indiscriminately attempts to penetrate the network via IPsec VPN against a wide range of global IP addresses of the victim. Based on the behavior of the packets, it is believed that this cyber attack uses a dictionary attack to identify the pre-shared key of the IPsec VPN when a guessable word is used in the pre-shared key, and then establishes an IPsec VPN tunnel to break into various corporate networks. This cyber attack is considered to be an attempt to establish an IPsec VPN tunnel to infiltrate various corporate networks. This cyber attack does not target SoftEther VPN, and there is no possibility that SoftEther VPN will be affected directly at present.
    - However, if you have enabled the L2TP/IPsec, EtherIP/IPsec, or L2TPv3/IPsec features of SoftEther VPN and have not changed the recommended pre-shared key to "vpn" (the default value of three characters), such an attack will establish an IPsec layer tunnel with the attacker's host. In an environment where the pre-shared key has not been changed (strongly not recommended dangerous usage), such an attack will establish an IPsec layer tunnel with the attacker's host. Since L2TP authentication, etc. is not actually established afterwards, even if the attacker does not break into the network, resources such as CPU, memory, and network bandwidth of the host used as the VPN server may be wasted as a result. Especially, SoftEther VPN disconnects the IPsec tunnel established with the attacker when there is no communication for a certain period of time. When SoftEther VPN receives a packet addressed to the identification number of the tunnel that has already been disconnected, it sends a notification to the source IPsec client that the tunnel has been disconnected. This is called an IPsec Informational Exchange packet. The implementation behavior of a bad source IPsec client (the program written by the attacker) is that when the IPsec Informational Exchange packet arrives, the attack host resends another ESP frame to the VPN server. This results in ping-pong between the attacker's program and the IPsec module of the VPN server of SoftEther VPN, which is completely unintended by the attacker, resulting in completely useless consumption of each other's CPU, memory, and network bandwidth. From the point of view of the VPN server administrator, while the attacker is sending IPsec packets in rapid succession, VPN communication by legitimate L2TP/IPsec users will be slowed down or fail to establish VPN communication. The attacker is at a disadvantage.

    - The above notification mechanism of the disconnected tunnel identification number by IPsec Informational Exchange packets is not a bug of SoftEther VPN, but the original intended behavior. However, if the above ping-pong phenomenon occurs and consumes CPU, memory and network bandwidth, it will affect legitimate users. Therefore, in the new build Ver 4.37 Build 9758 released on 08/15/2021, we have implemented a rate limit on the process of sending back IPsec Informational Exchange packets. Specifically, for communications from a particular IPsec client host, we have limited the number of IPsec Informational Exchange packets that can be sent back to the client host to a maximum of 20 per second, after which no further responses will be made.
    - With this new build, even if an attacker establishes an aggressive IPsec VPN session in an environment where the recommended pre-shared key has not been changed to "vpn" (the default value of three characters, dangerous and not recommended), the consumption of CPU, memory and network bandwidth will be reduced.
    - Regardless of the above measures, if you have not changed the recommended pre-shared key to "vpn" (the default value of 3 characters), it is not recommended to use the pre-shared key with the default value of "vpn", so it is recommended to change it to a more complex string of 8 characters or more, as per the guidance message in the VPN server configuration tool, regardless of the presence of this phenomenon.

- **SoftEther VPN 4.36 Build 9754 Beta (June 07, 2021)**
    - Add Linux ARM 64bit CPU support. (now works on ARM 64bit CPUs such as Raspberry Pi 4.)
    - Updated OpenSSL version to 1.1.1k.
    - Fixed the same directory DLL loading problem in the installer (vpnsetup).
    - Japanese government's public personal authentication JPKI 64bit support
    - Support for older SH4 CPUs has been removed.
    - Fixed an issue that caused malformed packets to be generated when the DHCP option exceeded 255 bytes, such as when the static route push feature of the Virtual DHCP Server feature configured more than 28 routes.

- **SoftEther VPN 4.34 Build 9745 RTM (June 24, 2020)**
    - All cumulative updates bellow are included.
    - **Build 9745 beta** is determined to be stable enough and is remarked as RTM.
    - The contents of the packages are exactly the same as **Build 9745 beta**.

- **SoftEther VPN 4.34 Build 9745 Beta (April 5, 2020)**

    - Fix security issue: Fix the security of JSON-API. If the administrator password of the Virtual Hub is empty, JSON-API (which was added in 4.30 Build 9696 Beta) will not be able to access to the virtual hub with a empty password since this release. Because there are relatively many cases in which administrator password is empty for a virtual hub, being able to manage a virtual hub without a password using JSON-API was a security problem. In this release, this behavior has been changed so that JSON-API cannot be accessed in the Virtual Hub management mode until it is configured with non-empty password.
      Acknowledgments: falms

- **SoftEther VPN 4.34 Build 9744 Beta (March 21, 2020)**
    - Bug fix: In VPN Server, you could not connect from older SoftEther VPN (version 3.0 or earlier) due to the specification change of OpenSSL.
    - Bug fix: The Simple Mode checkbox change was not reflected in the Simple Installer Creation Wizard.
    - Feature added: The Tls_Disable1_3 option has been added to the VPN Server. You can disable TLS 1.3 by setting this option to true.
    - Feature added: It is now possible to get a log list of all cluster member servers from the cluster controller.

- **SoftEther VPN 4.32 Build 9731 Beta (January 1, 2020)**
    - Bugfix: Fix the SecureNAT connection problem with ignoring TCP ECN bit enabled packets
    - Bugfix: Imperfect Virtual Hub FDB lock may cause process crush.
    - Bugfix: OpenVPN Certificate Authentication may cause process crush.
    - Improvement: Add a space character between URL and other tokens in the packet log format.

- **SoftEther VPN 4.31 Build 9727 Beta (November 18, 2019)**
    - **Added the new function to reserve and each Virtual MAC address and IP address for each user of L2TP/IPsec, SSTP and OpenVPN L3.**
        - Since SoftEther VPN Ver 4.31 Build 9727, we added the new function to make each L3 VPN users to use the reserved virtual MAC address and the virtual IP address. This function allows the DHCP server in the remote-access destination network to identify the connected user and to assign reserved IP addresses to each of users respectfully. (Figure 1)

figure1.png

Figure 1

- L3 VPN protocols, such as L2TP/IPsec, SSTP and OpenVPN L3, creates virtual L2/L3 layer-transformation adapter for each of VPN connections which are established to the Virtual Hub on SoftEther VPN Server. A virtual L2/L3 layer-transformation adapter has a virtual MAC address. In the previous versions of SoftEther VPN, virtual MAC addresses are randomly assigned each time when users connect to the VPN Server. There were no solution to assign fixed MAC addresses and IP addresses to each of users.
- SoftEther VPN Ver 4.31 Build 9727 and later supports the function to fix virtual MAC addresses of every L3 VPN users. To fix virtual MAC addresses, you have to do the following configuration:
    - 1. When the user object is using the standard user authentication, you need to write the arbitrary virtual MAC address on the "Note" field on the user object. For example, the "Note" field will have the MAC address format which starts with "MAC:" followed by a 6-bytes ASCII-encoded HEX string, such like "MAC:ae:00:00:00:00:01". We recommend to use the "ae" on the first byte of the MAC address. (Figure 2, Figure 3)

      figure2.png

      Figure 2

figure3.png

Figure 3

    - 2. When the user object is using the RADIUS authentication, you need to configure your RADIUS server to reply the "Framed-Interface-Id" (Attribute Number: 96) RADIUS Attribute as the MAC addesses which you want to assign to the user. The reply string must be a 6-bytes ASCII-encoded HEX string, such like "AE0000000001" or "AE-00-00-00-00-01". The string may have "-" or ":" as delimiter.

      Note 1: The RADIUS server can identify if the client is L2 VPN client or L3 VPN client by checking whether the RADIUS Attribute "Proxy-State" (Attribute Number: 33) starts with "L3:" or not. This helps you to realize the solution on the RADIUS server to accept only L3 VPN clients, and deny connections from L2 VPN clients.

      Note 2: Do not assign to the same single MAC address to multiple VPN clients. When two or more VPN sessions have the duplicated MAC address at the same time, the communication will be unstable.

- You can fix each L3 VPN user's virtual MAC address with the above solution. Therefore you can fix the user's IP address by configuring the static IP address reserve list hosted by the existing DHCP server (e.g. Linux dhcpd or Windows DHCP Service) on the target local-area network which the Virtual Hub is connected with the Local Bridge function. To fix the IP addresses assignment by the DHCP server you need to configure the "Static IP address reserve list" function (the function name may vary on each DHCP server product). You need to refer the document of your DHCP Server to configure the static IP address reserve list.
  The following example is Linux dhcpd (isc-dhcp-server)'s setting file to realize the static IP address reserve list configuration.
-
  ```
  The example contents of /etc/dhcp/dhcpd.conf:
  ---
  authoritative;
  ```

```
subnet 10.111.0.0 netmask 255.255.255.0 {
    range 10.111.0.101 10.111.0.199;
    option subnet-mask 255.255.255.0;
    option broadcast-address 10.111.0.255;
    default-lease-time 3600;
    max-lease-time 3600;
}

host ip1 {
   hardware ethernet ae:00:00:00:00:01;
   fixed-address 10.111.0.201;
}

host ip2 {
   hardware ethernet ae:00:00:00:00:02;
   fixed-address 10.111.0.202;
}
---
```

  - **Added the "<CA>" field on the auto-generated OpenVPN configuration file.**
  - **Added the code to use the optimized OpenSSL's implementation to compute the AEAD_CHACHA20POLY1305 algorithm if available.**
  - **Added the function to hide "index.html" by setting "bool DisableJsonRpcWebApi true" on the configuration file.**
  - **Upgraded the OpenSSL version to 1.1.1d.**
  - **Added the DisableIPsecAggressiveMode option. You can set "bool DisableIPsecAggressiveMode true" to disable the IPsec Aggressive Mode to moderate CVE-2002-1623.**

- **SoftEther VPN 4.30 Build 9696 Beta (July 8, 2019)**
  1. **Added the SoftEther VPN Server JSON-RPC API Suite implementation.** The API Suite allows you to easily develop your original SoftEther VPN Server management application to control the VPN Server (e.g. creating users, adding Virtual Hubs, disconnecting a specified VPN sessions). The API document is published on the following GitHub URL. We published the RPC client sample codes for JavaScript, TypeScript and C#.
     1. SoftEther VPN Server JSON-RPC API Suite Document (GitHub)

2. **Added the Embedded HTML5-based Modern Admin Console.** This is currently very limited, under construction. Access to the **"https://<server IP address>/admin/"** from your favorite web browser. Note: Your HTML5 development contribution is very appreciated. The current HTML5 pages are written by Daiyuu Nobori (the core developer of SoftEther VPN). He is obviously lack of HTML5 development ability. Please kindly consider to contribute for SoftEther VPN's development on GitHub. Your code will help every people running SoftEther VPN Server. Contributing to the HTML5 web administration console doesn't require any programming skills of C/C++ languages for developing the VPN Server program.

   html5.jpg

   - **Note: You can disable the SoftEther VPN Server JSON-RPC API Suite and the HTML5-based Modern Admin Console by setting the "DisableJsonRpcWebApi" option to "true" in the configuration file.**
3. Fixed the problem occurs when RPC messages between Cluster Members exceed 64Kbytes.
4. Fixed the RADIUS PEAP client to use the standard TLS versioning.
5. **Fix the vulnerability.** Added the user buffer address verification code on some I/O control codes of the NDIS 5.x legacy Local Bridge driver to fix **SE201901: SoftEther VPN Server NDIS 5.x Windows Local Bridge Driver Local Privilege Escalation Vulnerability**. Acknowledgments: This fix is based on a report by DownWithUp.
6. Added the support of ChaCha20-Poly1305-IETF AEAD for RUDP.
7. Added the function to display the protocol details about the VPN session.
8. Fixed the bug that the language switching function was disabled. (Build 9695 -> Build 9696)

- **SoftEther VPN 4.29 Build 9680 RTM (February 28, 2019)**
  - Switched the license of SoftEther VPN from GPLv2 to Apache License 2.0. Text messages on source codes and UIs have been modified.
  - Supports 4-digit expiration date on X.509 certificates.
  - Replaced SHA-0 implementation.
  - Improved integrity and security of C source codes. Fixed several buffer overflows and integer overflows. Enforced NULL pointer checks. Fixed problems on the size of malloc() and Zero Memory functions. These problems include a vulnerability that a malformed packet will cause the buffer overflow at the receive path. This vulnerability may occur abnormal process exit with the buffer security check mechanism built-in with SoftEther VPN binary. Although this buffer overflow can theoretically bypass the security check in theory, in the actual binary it is detected by the buffer security check inserted by the C compiler and the

    process is forcibly terminated. Therefore, as a result, it can be abused by a DoS attacker. Acknowledgments: The last problems is discovered and reported by Fabrizio Steiner.
    - Modified the behavior at the executing of the ethtool command to call just the command name instead of the full path.
    - Fixed a single code on the SecureNAT function that SYN and ACK were reverse.
    - Fixed the bug on the creating of SingleInstance objects that the temporary file will remain as a garbage after the file lock will fail on UNIX operating systems.
    - Fixed the problem that the full path of the home directory will be sometimes obtained as wrong value on UNIX operating systems.
    - Fixed the problem that processing the system datetime values which are before 1970-01-01.

- **SoftEther VPN 4.28 Build 9669 Beta (September 11, 2018)**
  Fix a VPN Server problem with IPsec IKE MD5 digest algorithm which is used by Windows XP or earlier.
  Fix a VPN Server functional problem that Windows XP or earlier version cannot distinguish the SHA-256 Authenticode binary signature.
  Improvement of SecureNAT TCP/IP connection stability.
  Improvement of VPN Client user interface.
  For Linux x86 and x64 versions, the Makefile is changed to try "-no-pie" option at first in order to hide warning messages on Ubuntu 18.04 systems.

- **SoftEther VPN 4.27 Build 9668 Beta (May 29, 2018)**
  Fixed the "-fPIC" error at the make command on Ubuntu Linux.

- **SoftEther VPN 4.27 Build 9666 Beta (April 21, 2018)**
  Fixed an issue that the VPN Client Virtual Network Driver fails to communicate when LTE or 3G wireless modems are used to connect to the internet by the computer running Windows 10 Spring Creators Update (version 1803). Please be careful that It is necessary to reinstall the device driver of the Virtual Network Adapter after upgrading the VPN client to build 9666 or later in order to solve the problem.
  When reinstalling the device driver of the Virtual Network Driver card, we changed the behavior as to cleanup the older driver before installing the newer driver.
  When installing a new device driver of the Virtual Network Driver card, we changed the initial random MAC address from 00-AC-xx-xx-xx-xx to 5E-xx-xx-xx-xx-xx. This realizes the compliance with the local address bit of the MAC address rule.
  There was one vulnerability on SoftEther VPN for Windows. When loading the DLL file by the LoadLibrary() function in Windows VPN programs, we changed the behavior not to search the current directory. Based on this improvement, even

if there are untrusted DLL files in the current directory, it is now safe to avoid the problem of unexpected security problem caused by the default loading behavior of Windows. Acknowledgments: This is based on a report by Herman Groeneveld, aka Sh4d0wman.

- **SoftEther VPN 4.25 Build 9656 RTM (January 15, 2018)**
  There are 11 vulnerabilities on SoftEther VPN. There vulnerabilities are found by the source code audit process conducted by Max Planck Institute for Molecular Genetics and Mr. Guido Vranken in late 2017. This build fixes all of these vulnerabilities.

  7 missing memory boundaries checks and similar memory problems. There are no risk of arbitrary code execution or intrusion on these bugs in my analysis. However, these problems may lead to crash the running server process. So these bugs must be fixed.

  - Buffer overread in ParseL2TPPacket()
  - Memory corruption in IcmpParseResult
  - Missing bounds check in ParseUDP() can lead to invalid memory access
  - Out-of-bounds read in IPsec_PPP.c (unterminated string buffer)
  - Overlapping parameters to memcpy() via StrToIp6()
  - PACK ReadValue() crash vulnerability
  - Potential use of uninitialized memory via IPToInAddr6()

  4 memory leaks. While the amount of leakage is very small per time, these bugs can finally cause process crash by out of memory. So these bugs must be fixed.

  - Memory leak in NnReadDnsRecord
  - Memory leak in RadiusLogin()
  - Memory leak via ParsePacketIPv4WithDummyMacHeader
  - Remote memory leak in OpenVPN server code

  1 coding improvement. This is not a bug, however, I fixed the code to avoid furture misunderstanding.

  - RecvAll can return success on failure (leading to use of uninitialized memory)

  **Contributors for this bugfix:**
  - Max Planck Institute for Molecular Genetics
  - Mr. Guido Vranken

  Also, this build has the following improvements:
  - Fix a bug in the Win32EnumDirExW() function.
  - Add the Alternative subject name field on the new X.509 certificate creation.

- **SoftEther VPN 4.24 Build 9652 Beta** **(December 21, 2017)**
  Fixed the bug which occurs the L2TP/IPsec connection error with Android Oreo on the Build 9647 and 9651.
  Added the function to save the DNS query log on the packet logs.

- **SoftEther VPN 4.24 Build 9651 Beta** **(October 23, 2017)**
  Fixed the bug on the OpenVPN Server function in Build 9647.

- **SoftEther VPN 4.23 Build 9647 Beta** **(October 18, 2017)**
  Upgraded OpenSSL to 1.0.2l.
  Source code is now compatible with OpenSSL 1.1.x. Supports DHE-RSA-CHACHA 20-POLY 1305 and ECDHE-RSA-CHACHA 20-POLY 1305, which are new encryption methods of TLS 1.2. (In order to use this new function, you need to recompile yourself using OpenSSL 1.1.x.)
  TrafficServer / TrafficClient function (The traffic throughput measurement function) is now multithreaded and compatible with about 10 Gbps using NIC with the RSS feature.
  Changed the default algorithm for SSL from RC4-MD5 to AES128-SHA.
  Fixed a bug that occurr wrong checksum recalculation in special case of the TCP-MSS clamp processing.
  Fixed the calculation interval of update interval of DHCP client packet issued by kernel mode virtual NAT function of SecureNAT function.
  Driver upgrade and DLL name change with Crypto ID support of USB security token.
  Fixed a problem that CPU sleep processing was not performed when the wait time of the Select() function was INFINITE on Mac OS X.
  Added the StrictSyslogDatetimeFormat flag onto the ServerConfiguration section on the VPN Server configuration file, which sets Syslog date format to RFC3339.
  Fixed wrong English in the UI.
  Using client parameter in function CtConnect
  Remove blank line at the start from init file (Debian)
  Stop Radius Delay from counting to next_resend
  Add DH groups 2048,3072,4096 to IPSec_IKE
  Add HMAC SHA2-256, HMAC SHA2-384, HMAC SHA2-512 support
  Openvpn extend ciphers
  Fixed RSA key bits wrong calculation for certain x509 certificate
  Added support for RuToken USB key PKCS#11
  OpenSSL 1.1 Port

- **SoftEther VPN 4.22 Build 9634 Beta** **(November 27, 2016)**
  Added the support for TLS 1.2. Added TLS 1.2-based cipher sets: AES128-GCM-SHA256, AES128-SHA256, AES256-GCM-SHA384, AES256-SHA256, DHE-RSA-AES128-GCM-SHA256, DHE-RSA-AES128-SHA256, DHE-RSA-AES256-GCM-SHA384, DHE-RSA-

AES256-SHA256, ECDHE-RSA-AES128-GCM-SHA256, ECDHE-RSA-AES128-SHA256, ECDHE-RSA-AES256-GCM-SHA384 and ECDHE-RSA-AES256-SHA384.
Added the function to allow to configure specific TLS versions to accept / deny. In the VPN Server configuration file you can set Tls_Disable1_0, Tls_Disable1_1 and Tls_Disable1_2 flags to true to disable these TLS versions individually.
Added the support for TLS 1.2 on the OpenVPN protocol.
Updated the version of OpenSSL to 1.0.2j.
Added the support for Windows Server 2016.
Fixed the 2038-year problem.
Added the support for recording HTTPS destination hostnames, using SNI attributes, on the packet logging function.
Added the function to append the name of Virtual Hub into the "Called-Station-ID (30)" attribute value in the RADIUS authentication request packet.
Improved the behavior of Virtual Layer-3 switches. The interval of ARP request is set to 1 second.
Fixed the problem of the slow startup of VPN Server in Windows 10.
Added the support for 4096 bits RSA authentication with smart cards.
Added the support for the CryptoID USB token.
Fixed the UI string resource in English.
Fix that ParseTcpOption doesn't work correctly
Add LSB header
Support Debian package build on aarch64 architecture
Support Debian package build on ARMv7l architecture
cppcheck issues
Default to TLS connections only
Allow specific SSL/TLS versions to be disabled
Adding Radius AVP Called-Station-Id
Fixed typo
Update CentOS makefiles and spec file
Systemd service configuration files for SoftEther
Fix set initialization, set.OnlyCapsuleModeIsInvalid could be garbage
Fixed OSX CPU utilization by replacing broken kevent() with select()
Add the possibility to send the Virtual Hub Name to an external DHCP server
Added armv5tel for debian/rules and made pushed routes work correct with OpenVPN
fix LogFileGet won't save to SAVEPATH
Fix for Debian Package
Try to autodetect OS and CPU instead of requiring user input
Support For Radius Realm

- **SoftEther VPN 4.21 Build 9613 Beta (April 24, 2016)**
  Added SoftEther VPN Server Manager for Mac OS X.
  Now you can manage your SoftEther VPN Server, running remotely, from your

Mac in local.

- **SoftEther VPN 4.20 Build 9608 RTM (April 18, 2016)**
All cumulative updates below are included.
Fixed a minor English typo.

- **SoftEther VPN 4.19 Build 9605 Beta (March 3, 2016)**
The version of OpenSSL is updated to 1.0.2g to fix the vulnerability which was published in March 2016. SSLv2 is now disabled completely.
Fixed a multi-byte character problem in the certificate generating tool.
Enable the cache of the destination IP address of the additional TCP connection for a VPN session.

- **SoftEther VPN 4.19 Build 9599 Beta (October 19, 2015)**
Fixed the problem that an unnecessary "Insert disk" dialog box appears when installing VPN Server or VPN Bridge on Windows 10.
Added the "/NOHUP" parameter in the "TrafficServer" command of vpncmd.
Added the "/REDIRECTURL" parameter in some access list commands of vpncmd.
Added the virtual address check routines in kernel-mode drivers to prevent blue screen or invalid memory access. Previous versions of kernel-mode drivers did not check the virtual addresses from the user-mode. (NOTE: All kernel-mode drivers are protected by ACL to avoid privilege escalation in all previous versions. Only users with Administrator privileges were able to cause blue screen or invalid memory access by passing invalid addresses from the user-mode. Therefore this was not a security flaw.) Appreciate Meysam Firozi's contribution to report the similar problem in the Win10Pcap driver.

- **SoftEther VPN 4.19 Build 9582 Beta (October 6, 2015)**
Dramatically improvement of the performance of the Virtual NAT function of SecureNAT in Linux. In the previous versions of SoftEther VPN, the SecureNAT performance was very slow in the specific situation that the Linux Virtual Machine (VM) is running with virtual Ethernet interfaces which are prohibited to enable the promiscuous mode (this problem has been frequently appeared on cloud servers such like Amazon EC2/AWS or Windows Azure). In such a situation, SecureNAT must use the user-mode TCP/IP stack simulation and it was very slow and had high latency. This version of SoftEther VPN Server adds the new "RAW IP Mode" in the SecureNAT function. The RAW IP Mode is enabled by default, and is effective only if the VPN Server process is running in the root privileges. In the RAW IP Mode, the SecureNAT function realizes to transmit and receive TCP, UDP and ICMP packets which headers are modified. This behavior realizes drastically improved performance than legacy user-mode SecureNAT in the previous versions. In order to avoid the misunderstanding of receiving packets which are towards to the Virtual NAT function, some packet filter rules are automatically added to the iptables chain list. You can disable the

RAW IP Mode by setting the "DisableIpRawModeSecureNAT" value to "1" on the Virtual Hub Extending Options.

Improved the performance of the Kernel-mode SecureNAT.

Improved the stability of the L2TP VPN sessions on the network with heavy packet-losses.

Added the compatibility with Cisco 800 series routers (e.g. Cisco 841M) on the L2TPv3 over IPsec protocol. These new Cisco routers have modified L2TPv3 header interpreter. Therefore SoftEther VPN Server needed to add new codes to support these new Cisco routers.

Added the support the compatibility to YAMAHA RTX series routers on the L2TPv3 over IPsec protocol.

Added the support for EAP and PEAP. SoftEther VPN Server can now speak RFC3579 (EAP) or Protected EAP (PEAP) to request user authentications to the RADIUS server with the MS-CHAPv2 mechanism. If this function is enabled, all requests from L2TP VPN clients which contain MS-CHAPv2 authentication data will be converted automatically to EAP or PEAP when it is transferred to the RADIUS server. You must enable this function manually for each of Virtual Hubs. To enable the function converting from MS-CHAPv2 to EAP, set the "RadiusConvertAllMsChapv2AuthRequestToEap" value to "true" in the vpn_server.config. To enable the functin converting from MS-CHAPv2 to PEAP, set both "RadiusConvertAllMsChapv2AuthRequestToEap" and "RadiusUsePeapInsteadOfEap" options to "true".

- **SoftEther VPN 4.19 Build 9578 Beta (September 15, 2015)**
  Solved the problem that kernel mode drivers do not pass the general tests of "Driver Verifier Manager" in Windows 10.

- **SoftEther VPN 4.18 Build 9570 RTM (July 26, 2015)**
  Compabible with Windows 10.
  Solved the problem that the customized language setting on the "lang.config" file.
  config sometimes corrupts in the rare condition.

- **SoftEther VPN 4.17 Build 9566 Beta (July 16, 2015)**
  Improved stability with Windows 10 Beta.
  Updated the OpenSSL library to 1.0.2d.

- **SoftEther VPN 4.17 Build 9562 Beta (May 30, 2015)**
  Added supports for Windows 10 Technical Preview Build 10130.
  Increased the maximum Ethernet frame size from 1560 bytes to 1600 bytes.

Fixed the compiler error while building the source code of SoftEther VPN on Windows.
Added memory tags on the memory allocation function calls in kernel-mode device drivers.
Fixed the freeze problem of the VPN Client that the computer enters to suspend or hibernation state while the VPN Client is connected to the VPN Server.
Windows-version executable and driver files are now signed by the SHA-256 digital code-sign certificate.

- **SoftEther VPN 4.15 Build 9546 Beta (April 5, 2015)**
  Fixed the problem that the Local Bridge function does not work correctly on Windows 10 Technical Preview Build 10049.

- **SoftEther VPN 4.15 Build 9539 Beta (April 4, 2015)**
  Add the code to instruct the VPN Client to disconnect the VPN session automatically when Windows is being suspending or hibernating.

- **SoftEther VPN 4.15 Build 9538 Beta (March 27, 2015)**
  Fixed the dialog-box size problem on Windows 10 Technical Preview Build 10041.

- **SoftEther VPN 4.15 Build 9537 Beta (March 26, 2015)**
  Upgraded built-in OpenSSL from 0.9.8za to 1.0.2a. Please note that this change has not been well-tested. This upgrading of OpenSSL might cause problems. In that case, please post the bug report.

- **SoftEther VPN 4.14 Build 9529 Beta (February 2, 2015)**
  **We are very sorry.** The previous version 4.13 (beta) has a problem to accept L2TP connections due to the session-state quota-limitation code by the minor change between Build 9514 and 9524. The problem is fixed on this build. Please update to this build if you are facing to the L2TP problem on version 4.13.
  Added the function to record underlying source IP addresses of VPN clients on every packet log lines. This function can be disabled by set the "NoPhysicalIPOnPacketLog" flag in the Virtual Hub Extended Option to "1".

- **SoftEther VPN 4.13 Build 9524 Beta (January 31, 2015)**
  Modified the behavior of the Local Bridge function in the VPN Server on Linux. In the previous versions, if several Local Bridge creation operations will be made, then the operations to disable the offloading function on the target Ethernet devices will be conducted as many as same. After this version, the operation to disable the offloading function will be called only once for each device if several Local Bridge creation operations will be made on the same Ethernet device.
  Added the "SecureNAT_RandomizeAssignIp" Virtual Hub Extended Option. If you set this option to non-zero value, then the Virtual DHCP Server of the

SecureNAT function will choose an unused IP address randomly from the DHCP pool while the default behavior is to choose the first unused IP address.
Added the "DetectDormantSessionInterval" Virtual Hub Extended Option. If you set this option to non-zero value, then the Virtual Hub will treat the VPN sessions, which have transmitted no packets for the last specified intervals (in seconds), as Dormant Sessions. The Virtual Hub will not flood packets, which should be flood, to any Dormant Sessions.
Added the implementation of the SHA() function in the source code. This made the building process easier on the low-memory embedded hardware which has its OpenSSL implementation without the SHA () function.
Improved the behavior on Windows 10 Technical Preview to show the OS version information correctly.

- **SoftEther VPN 4.12 Build 9514 Beta (November 17, 2014)**
  Added the VLAN ID dynamic assignment function by RADIUS. It is very useful when the layer-2 Ethernet segment with aggregated IEEE802.1Q tagged VLANs is bridged to your Virtual Hub. Each VPN session will be assigned its own VLAN ID by the RADIUS attribute value when the user is authenticated by the external RADIUS server unless the user object has a VLAN ID security policy. The RADIUS attribute with the name "Tunnel-Pvt-Group-ID" (ID = 81) will be used as the VLAN ID. The data type must be STRING. This function is disabled by default. You have to set the "AssignVLanIdByRadiusAttribute" value to "1" in the Virtual Hub Extended Options in advance.
  Added the OpenVPNDefaultClientOption option in the vpn_server.config. The specified option string will be used alternatively when the connecting OpenVPN Client does not provide the connection string. Some incomplete OpenVPN Clients with the --enable-small compiling option always forget to specify this connection string. This option can make VPN Server allow such OpenVPN Clients.
  Improved the DHCP option parser to allow the external DHCP server pushes the classless routing table which exceeds 255 bytes.
  Added the support for "hair-pin connection" on the NAT Traversal function.
  Fixed the performance problem when the server computer has the wrong resolv.conf setting file on Linux.
  Fixed the VPN Client configuration backup folder name which the setup wizard automatically creates.
  Fixed the UDP checksum value of the beacon packets which are sent by the Virtual Layer 3 Switch function.

- **SoftEther VPN 4.11 Build 9506 Beta (October 22, 2014)**
  As a response to the SSLv3 POODLE problem we added the "AcceptOnlyTls" configuration flag on the vpn_server.config for SoftEther VPN Server. Please set this flag is you want to completely disable the SSLv3 function in SoftEther VPN Server.
  Added the perfect forward security (PFS) support on SSL/TLS. SoftEther VPN

Server can now accept connections with DHE-RSA-AES128-SHA or DHE-RSA-AES256-SHA ciphers.

- **SoftEther VPN 4.10 Build 9505 Beta (October 3, 2014)**
  Implemented the hash table algorithm for the MAC address database of Virtual Hubs. It improves the performance when there are a large number of MAC addresses registered on the database.
  Improved the performance on slow-CPU hardware (e.g. embedded Linux boxes).
  Added the DoNotDisableOffloading flag on Local Bridge settings. This flag will disable the automated disabling operation for hardware offloading on the specified Ethernet interface on Linux.
  Supports the kernel-supported IEEE802.1Q tagged VLAN on Windows and Linux. It will enable tagged-VLAN support on the Local Bridge function with some specific network interface drivers.
  Added the FloodingSendQueueBufferQuota option.
  Sets the lower priority value on the oom_adj process parameter for Linux.
  Randomized the reconnection interval in Cascade Connection.
  Increased the memory usage limit on 64-bit systems.
  Modified the behavior of the ConfigGet command and the /CSV option in vpncmd for Windows to work around for the Windows console API bug.
  Added the DisableSessionReconnect option on VPN Server and VPN Bridge. It makes Cascade Connection client sessions to disconnect immediately from the destination VPN Server when the based TCP connection is disconnected.
  Makes it enable to use the PrivacyFilterMode security policy on Cascade server VPN sessions.
  Added the GlobalParams configuration option on VPN Server and VPN Bridge. It allows administrators to modify and optimize the performance parameters of VPN Server and VPN Bridge.
  Reduced the processor time of looking up the ACL entries when storing and forwarding packets across a Virtual Hub.
  Reduced the usage of the memory on embedded Linux environments.
  Fixed a minor bug on the GUI setting screen of the SecureNAT routing table pushing option.
  Added the ServerLogSwitchType and the LoggerMaxLogSize option on VPN Server and VPN Bridge. They can change the logging behavior of VPN Server and VPN Bridge.
  Implemented the config template file. The template filename is "vpn_server_template.config" for VPN Server, and "vpn_server_template.config" for VPN Bridge. The VPN Server and VPN Bridge loads the template file as the initial configuration state when the configuration file does not exists.

- **SoftEther VPN 4.10 Build 9473 Beta (July 12, 2014)**

Added the "SuppressClientUpdateNotification" option in the Virtual Hub Extended Option list. This option will push the flag to the VPN Client to suppress the update notification screen on the VPN Client manager. To push this flag, set "1" to the "SuppressClientUpdateNotification" option in your Virtual Hub.
Added the warning message when the background service process is run by a non-root user (only in UNIX).
Fixed the deadlock bug when UNIX versions of SoftEther VPN Server process is shutting down.
Added supports for third-party PKCS#11 DLLs: ePass 1000 ND / ePass 2000 / ePass 2003 / ePass 3000.
Fixed typo.
The expression of the disclaimer statement for exporting / importing has been modified.
Fixed the VPN Azure connection problem on Version 4.09 Build 9451 Beta.
Fixed the problem that VPN Server Manager and VPN Client Manager sometimes become slow when the update check server is unreachable from the computer.
Removed space characters in every URLs of all download files on the SoftEther VPN Download Center web site to avoid the downloading problem in some HTTP clients.
A github patch which was posted by a contributor has been applied: "update debian packaging, install init script".

- **SoftEther VPN 4.09 Build 9451 Beta (June 9, 2014)**
  Improves User-mode SecureNAT performance by modifying the processing of TCP_FIN packets. It should improve the performance of the FTP protocol.

- **SoftEther VPN 4.08 Build 9449 (June 8, 2014)**
  **Add a new command to generate a RSA 2048 bit certificate.**
  The vpncmd command-line utility has MakeCert command to generate a 1024 bit self-signed RSA certificate. However, in recent years it is recommended to use 2048 bit RSA certificates. Therefore, on this version a new command MakeCert2048 has been added. Use this command to generate a 2048 bit self-signed RSA certificate.

  **Workaround for the NAT traversal problem.**
  Adjusted the priority between TCP/IP Direct Connection and UDP-based NAT-Traversal. On this version (Ver 4.08), NAT-Traversal will always be used if the client program detects that the specified TCP destination port on the destination server is occupied by non-SoftEther VPN Server. Anyone who faces to the connection problem on the VPN Server which is behind the NAT-box should install this update.

In the previous version (Ver 4.07), when the VPN Client attempts to connect to the VPN Server, the client firstly establish the connection via the TCP/IP direct protocol. If the TCP connection establishes successfully (in the layer-3) but the TCP port returns non-VPN protocol data (in the layer-7), the protocol error occurs immediately even if the NAT-Traversal connection attempt is still pending. This phenomenon often occurs when the VPN Server is behind the NAT-box, and the NAT-box has a listening TCP-443 port by itself. In that condition, the VPN Client attempts to connect to that TCP-443 port firstly, and the protocol error occurs immediately NAT-box returns non-VPN protocol (e.g. HTML-based administration page).

In order to work around that, this version (Ver 4.08) of VPN Client changed the behavior. On this version, if the VPN Client detects that the destination TCP Port is occupied by a non-VPN program, then the client will always use NAT-Traversal socket. This minor change will fix the connection problem to VPN servers behind the NATs.

Note: The built-in NAT-Traversal function on SoftEther VPN is for temporary use only. It is not recommended to keep using UDP-based NAT-Traversal connection to beyond the NAT-box when the VPN Server is behind the NAT-box, for long-term use. It is reported that some cheap NAT-boxes disconnect UDP session in regular period (a few minutes) after NAT-Traversal connection has been made. The strongly recommended method to run VPN Server behind the NAT is to make a TCP port mapping on the NAT-box to transfer incoming VPN connection packets (e.g. TCP port 443) to the private IP address of the VPN Server.

- **SoftEther VPN 4.07 Build 9448 (June 6, 2014)**
  **We updated the internal OpenSSL to 0.9.8za.**
  This fixes the latest OpenSSL vulnerability which has unfold on June 05.
  This vulnerability does not affect on SoftEther VPN. However, we updated the SoftEther VPN build with OpenSSL 0.9.8za. The new build also includes additional improvements.
  More details about this OpenVPN vulnerability is described at http://www.openssl.org/news/secadv_20140605.txt.

  **Other updates on this build are as followings:**
  The problem with OpenVPN Connect for Android 1.1.14 has been fixed. In the previous versions, OpenVPN Connect for Android 1.1.14 reports "PolarSSL Error" when it connects to the SoftEther VPN Server, if the server SSL certificate is self-signed root certificate. This X.509 certificate parsing problem is OpenVPN Connect's bug, however we performed work around for this OpenVPN Connect's bug. Please mind that you need to regenerate your self-

signed root certificate in order to comply with OpenVPN Connect at once after upgrading the VPN Server to this version. To regenerate the certificate, use the GUI tool on VPN Server Manager, or execute the "ServerCertRegenerate" command on vpncmd.

The automated root certificate and intermediate certificates downloading function has been implemented. It is very helpful when you use a commercial certificate which has been issued by a commercial CA (Certificate Authority), including VeriSign, GlobalSign or RapidSSL. In previous versions, you had to install the root certificate and intermediate certificates manually into the "chain_certs" directory. On this version, you do not need any longer to do such a manual installation of chained certs.

The OpenVPN configuration file generating function identifies the root certificate correctly, in order to embed it as the "<ca>" inline directive in the auto-generated OpenVPN configuration file. It is very helpful if you are using a commercial certificate which has been issued by a commercial CA (Certificate Authority), including VeriSign, GlobalSign or RapidSSL. (In previous versions, you had to perform the editing task for the OpenVPN configuration file manually.)

UI typos have been fixed, and some minor bugs have been fixed.

- **SoftEther VPN 4.06 Build 9435 (Beta) (March 26, 2014)**
  Previous versions of VPN Client have a port-confliction problem of the TCP port (TCP 9930) for RPC (Remote Procedure Call) on the VPN Client service for Windows, if the same port is occupied by another service. This version has solved the confliction problem.

- **SoftEther VPN 4.06 Build 9433 (Beta) (March 21, 2014)**
  **Fixed a crashing bug on NAT-Traversal connections.**
  We sincerely apologize that the SoftEther VPN Server of the last build (Build 9432) has a serious crashing bug if a VPN client connects to the VPN Server in the NAT Traversal mode, in UNIX system. This serious bug was caused by the problem of the processing of Unicode string (which is used by a warning message for NAT Traversal connections). We fixed the serious bug by this Build 9433. If you are using SoftEther VPN Server Build 9430 or 9432 in UNIX, please update it to Build 9433 as soon as possible.

- **SoftEther VPN 4.06 Build 9432 (Beta) (March 20, 2014)**
  We apologize that the previous build (Build 9430) has a problem that the RSA certificate authentication doesn't work.

This build has been fixed the problem. Please use Build 9432 if you are intending to use the RSA certificate authentication function.

- **SoftEther VPN 4.06 Build 9430 (Beta) (March 20, 2014)**

  **Thank you for waiting!**

  Added the following five advanced functions into SoftEther VPN Server (experimental):
  - RADIUS / NT Domain user authentication function
  - RSA certificate user authentication function
  - Deep-inspect packet logging function
  - Source IP address control list function
  - syslog transfer function

  Added the split-tunneling function (experimental):
  - Split tunneling is the function for enterprises to allow users communicate only to the specified IPv4 subnets through a VPN tunnel.
  - You can set up either SecureNAT Virtual DHCP Server or any external DHCP server to push static routing tables to all VPN clients.
  - The Virtual DHCP Server function in SecureNAT now supports classless static routing table pushing option (RFC 3442).
  - All types of VPN clients (SoftEther VPN Client, OpenVPN Client, L2TP/IPsec client and MS-SSTP client) can receive the static routing table pushed.

  Added the function which allows the VPN server administrator to obtain the DDNS private key on the DDNS setup dialog-box.
  Improved the behavior of the Privacy Filter Mode security policy. In the previous versions, a VPN session which is enabled the Privacy Filter Mode option cannot transmit any packets toward other Privacy Filter Mode enabled VPN sessions, except broadcast packets and ARP packets. On or after this version, both broadcast packets and ARP packets will also be blocked by the Privacy Filter Mode policy to eliminate the broadcast traffics. For the backward compatibility, this behavior can be changed by the "DropBroadcastsInPrivacyFilterMode" and "DropArpInPrivacyFilterMode" bool options on the Virtual Hub Extended Options.
  Added the generating function of X.509 v3 certificates with the SHA-2 (SHA-256) hashing algorithm to improve the security.
  According to the users reports, on very minor Linux environment, the "vpnserver stop" shutdown operation sometimes hangs up. The SoftEther VPN Project hasn't reproduce the issue yet. However, we added the fail-safe code to run "killall -KILL vpnserver" after the process shutdown operation times out (90 seconds).
  Added the option to disable the NAT Traversal tunneling function on the connection settings screen in VPN Client and Cascade Connection.
  Added Several Fixes for OS X.

Added Improved Simplified Chinese UI resources.
Added Workaround for when vpnserver hangs on stop on minor Linux environments.
On VPN Servers in People's Republic of China, the above five functions are currently disabled by default, under the orders from Beijing. Although Chinese users can enable these functions manually, Enterprise users in People's Republic of China are recommended to use these enterprise functions with PacketiX VPN Server 4.0 Chinese Edition.

- **SoftEther VPN 4.05 Build 9423 (Beta) (February 18, 2014)**
  Added Files for building CentOS/RHEL RPM.
  Set the "VPN over DNS" and "VPN over ICMP" functions disabled by default on VPN Server / VPN Bridge.

- **SoftEther VPN 4.05 Build 9422 (Beta) (February 17, 2014)**
  Added the supporting of /hostname and /password command-line arguments on VPN Client.
  Added the NSDI 6.x Lightweight Helper Kernel-mode Module for the local-bridge function. This kernel-mode driver runs only on Windows 8.1 / Windows Server 2012 R2 or later.

- **SoftEther VPN 4.05 Build 9416 (Beta) (February 6, 2014)**
  Added the support for OpenBSD on the source code.
  Added the debian packaging on the source code.
  Added the adminip.txt CIDR support.
  Added the supporting VLAN for Mac OS X using TunTapOSX.
  Added the .zip package with vpnsmgr.exe and vpncmd.exe for system administrators.

- **SoftEther VPN 4.04 Build 9412 (January 15, 2014)**
  Whole English UI texts are checked and corrected by a native speaker of English. Fixed typos.

- **SoftEther VPN 4.03 Build 9411 (January 7, 2014)**
  Modified the source-code tree. In the build 9408, some C# build-utility source codes were missing. In this build, full set of all source codes including the BuildUtil program are appended. No functional differences between this build and the last build.

- **SoftEther VPN 4.03 Build 9408 (Jaunary 4, 2014)**
  SoftEther VPN became open source software from this build. More details on this page. Note that the major version 3.xx was skipped for internal reason of our project. So this open-sourced new version starts with major version 4.xx.

- **SoftEther VPN 2.00 Build 9387 (September 16, 2013)**

This build realizes the compatibility with Microsoft Windows 8.1 and Windows Server 2012 R2 (RTM). This build supports Windows 8.1 and Windows Server 2012 R2 officially. This build fixes the former problem when the user upgrades from Windows 8 to Windows 8.1 by upgrade installation.
The major version number of SoftEther VPN was incremented on this build.

- **SoftEther VPN 1.01 Build 9379 RTM (August 18, 2013)**
  **This security update is to strengthen the security of SoftEther VPN 1.0 (Server and Bridge).**
  There is a remote administration function on SoftEther VPN 1.0. The function is to allow administrators to connect to the VPN server remotely to manage the server. In older versions, a third person can login to the VPN Server in the Virtual Hub Administration Mode if the administrator has forgot to set the administrator's password on a Virtual Hub. Older versions are also safe if any strong password is set on the Virtual Hub. However we suppose that there are some administrators who have forgot to set passwords for Virtual Hubs. In order to protect such potential vulnerable servers, this security update strengthens the VPN server program to deny all empty (not set) passwords on the Virtual Hub Administration Mode. Your VPN server has been safe also in older versions if you set any passwords for Virtual Hubs. However, we strongly recommend to apply this update program to all VPN server administrators who might have potential empty passwords on Virtual Hubs.

- **SoftEther VPN 1.00 Build 9376, 9377 RTM (August 3, 2013)**
  This is a minor fix.
  Improvement Stability of NAT Traversal.
  Add HTTP User-Agent Indication Behavior when using VPN Gate Client.

- **SoftEther VPN 1.00 Build 9371 RTM (July 25, 2013)**
  This is the RTM version of SoftEther VPN 1.0. It is not a BETA version.
  We have fixed a lot of bugs in former builds. This RTM build is a stable build for everyone.
  We will continue to improve features and performances on SoftEther VPN hereafter.

- **SoftEther VPN 1.00 Build 9367 RC4 (July 21, 2013)**
  This should be the final beta release before the RTM version of SoftEther VPN 1.0.

- **SoftEther VPN 1.00 Build 9091 RC3 (May 19, 2013)**

We released RC3 with the following improvements. RC3 should be the final release candidate before the GA (Generally Available) build.
- Fixed a crush bug which might occurred during the shutdown of vpnserver process with using L2TPv3 or EtherIP over IPsec.
- The statistics of cumulative transferred-bytes and packets-counter are appended on the list of Visual Hubs and on the list of User Objects on each Virtual Hub, on VPN Server Manager and vpncmd.
- On the list of User Objects enumeration in both VPN Server Manager and vpncmd, the expire-date of each User Object are appended on the displayed list.
- Improvements of stability of Dynamic DNS Function and NAT-Traversal Function.

- **SoftEther VPN 1.00 Build 9079 RC2 Fix17 (May 5, 2013)**
  Fixed a typo. Fixed a wrong bitmap image on the installer.

- **SoftEther VPN 1.00 Build 9078 RC2 Fix16 (April 28, 2013)**
  A security fix. The previous versions have ignored the "deny_empty_password" option in the Virtual Hub Administration Options List. This build fixed this security bug.
  Fixed some minor bugs.
  Improvement of the respond-time on IPv6 DNS name resolver.

- **SoftEther VPN 1.00 Build 9074 RC2 Fix15 (April 24, 2013)**
  Minor improvement around the Dynamic DNS Client function.

- **SoftEther VPN 1.00 Build 9071 RC2 Fix14 (April 20, 2013)**
  Fixed a minor timeout bug.

- **SoftEther VPN 1.00 Build 9070 RC2 Fix13 (April 18, 2013)**
  Enabled advanced security check routines for butter overflow (Win32 binaries only.)
  File sizes have been increased a little, but the performance wasn't affected.

- **SoftEther VPN 1.00 Build 9069 RC2 Fix12 (April 17, 2013)**
  Fixed a minor bug on SSL packet processing.
  Fixed a miror bug on TCP listener. (very rare crash)

- **SoftEther VPN 1.00 Build 9053 RC2 Fix11 (April 8, 2013)**
  Fixed a minor bug on UDP packet processing.
  Added a new feature: IKE and OpenVPN (in UDP packets) Packet Logging Function.

- **SoftEther VPN 1.00 Build 9045 RC2 Fix10 (April 2, 2013)**
  Fixed a minor bug, and improved the stability.

- **SoftEther VPN 1.00 Build 9043 RC2 Fix9 (April 1, 2013)**
  Fixed a critical bug was in the HTTP packet parser.
  Improvement of the stability of UDP-based communication.
  Fixed a problem: SecureNAT's connectivity polling packet interval was too short.

- **SoftEther VPN 1.00 Build 9035 RC2 Fix8 (March 26, 2013)**
  Fixed a crash bug: While you are changeing the X.509 server certificate, if a new SSL-VPN connection is being made, the new connection attempt will cause the crash because lack of critical section locking. However this bug was very rare. We found it in the heavy stress test.

- **SoftEther VPN 1.00 Build 9033 RC2 Fix7 (March 22, 2013)**
  Fixed a minor bug.

- **SoftEther VPN 1.00 Build 9030 RC2 Fix6 (March 21, 2013)**
  Fixed a bug: A logged error message around the L2TP/SSTP/OpenVPN user-authentication was incorrect.

- **SoftEther VPN 1.00 Build 9029 RC2 Fix5 (March 17, 2013)**
  Fixed a minor bug and typo.

- **SoftEther VPN 1.00 Build 9027 RC2 Fix4 (March 12, 2013)**
  Fixed a minor bug.

- **SoftEther VPN 1.00 Build 9026 RC2 Fix3 (March 10, 2013)**
  Fixed a bug: the timeout to the DDNS server was too small.

- **SoftEther VPN 1.00 Build 9024 RC2 Fix2 (March 09, 2013)**
  Fixed a bug: On Windows, VPN over DNS could not be enabled.

- **SoftEther VPN 1.00 Build 9023 RC2 Fix1 (March 08, 2013)**
  Fixed a minor bug.

- **SoftEther VPN 1.00 Build 9022 RC2 (March 08, 2013)**
  The initial release.