WIKIPEDIA

Secure Socket Tunneling Protocol

Secure Socket Tunneling Protocol (**SSTP**) is a form of virtual private network (VPN) tunnel that provides a mechanism to transport PPP traffic through an SSL/TLS channel. SSL/TLS provides transport-level security with key negotiation, encryption and traffic integrity checking. The use of SSL/TLS over TCP port 443 allows SSTP to pass through virtually all firewalls and proxy servers except for authenticated web proxies.[1]

SSTP servers must be authenticated during the SSL/TLS phase. SSTP clients can optionally be authenticated during the SSL/TLS phase and must be authenticated in the PPP phase. The use of PPP allows support for common authentication methods, such as EAP-TLS and MS-CHAP.

SSTP is available for Linux, BSD, and Windows.[2]

SoftEther VPN Server, a cross-platform open-source VPN server, also supports SSTP as one of its multi-protocol capability.

Similar functionality can be obtained by using open-source solutions like OpenVPN, however on Windows a third-party client software must be installed due to the lack of native built-in VPN client.

For Windows, SSTP is available on Windows Vista SP1 and later, in RouterOS, and in SEIL since its firmware version 3.50. It is fully integrated with the RRAS architecture in these operating systems, allowing its use with Winlogon or smart-card authentication, remote-access policies and the Windows VPN client.[3] The protocol is also used by Windows Azure for Point-to-Site Virtual Network.[4]

SSTP was intended only for remote client access, it generally does not support site-to-site VPN tunnels.[5]

SSTP suffers from the same performance limitations as any other IP-over-TCP tunnel. In general, performance will be acceptable only as long as there is sufficient excess bandwidth on the un-tunneled network link to guarantee that the tunneled TCP timers do not expire. If this becomes untrue, performance falls off dramatically. This is known as the "TCP meltdown problem".[6][7]

SSTP supports user authentication only; it does not support device authentication or computer authentication.

Contents

Packet structure

The following header structure is common to all types of SSTP packets:[8]

SSTP header

Bit offset	Bits 0–7	8–14	15	16–31
0	Version	Reserved	C	Length
32+	Data			

- Version (8 bits) – communicates and negotiates the version of SSTP that is used.
- Reserved (7 bits) – reserved for future use.
- C (1 bit) – control bit indicating whether the SSTP packet represents an SSTP control packet or an SSTP data packet. This bit is set if the SSTP packet is a control packet.
- Length (16 bits) – packet length field, composed of two values: a Reserved portion and a Length portion.
  - Reserved (4 bits) – reserved for future use.
  - Length (12 bits) – contains the length of the entire SSTP packet, including the SSTP header.
- Data (variable) – when control bit C is set, this field contains an SSTP control message. Otherwise, the data field would contain a higher-level protocol. At the moment, this can only be PPP.

Control message

The data field of the SSTP header contains an SSTP control message only when the header's Control bit C is set.

SSTP control message

Bit offset	Bits 0–15	16–31
0	Message type	Attributes count
32+	Attributes	

- Message type (16 bits) – specifies the type of SSTP control message being communicated. This dictates the number and types of attributes that can be carried in the SSTP control packet.
- Attributes count (16 bits) – specifies the number of attributes appended to the SSTP control message.
- Attributes (variable) – contains a list of attributes associated with the SSTP control message. The number of attributes is specified by the Attributes count field.

See also

- AuthIP
- L2TP/IPsec
- HTTPS

- OpenVPN
- OpenConnect VPN
- PPTP
- SoftEther VPN, an open-source VPN server program which supports SSTP-VPN protocol.

References

1. Jain, Samir (2007-01-17). "SSTP FAQ - Part 2: Client Specific" (http://blogs.technet.com/b/rrasblog/archive/2007/01/17/sstp-faq-part-2-client-specific.aspx). Microsoft TechNet. Retrieved 2015-10-17.
2. "SSTP-Client" (http://sstp-client.sourceforge.net/). 2011-09-17. Retrieved 2015-10-17.
3. Tulloch, Mitch (2008-01-22). "SSTP Makes Secure Remote Access Easier" (http://www.biztechmagazine.com/article/2008/01/sstp-makes-secure-remote-access-easier). Retrieved 2015-10-17.
4. McGuire, Cheryl (2015-08-11). "Configure a point-to-site VPN connection to an Azure Virtual Network" (https://azure.microsoft.com/en-us/documentation/articles/vpn-gateway-point-to-site-create/). Retrieved 2015-10-17.
5. Jain, Samir (2007-01-10). "SSTP FAQ - Part 1: Generic" (http://blogs.technet.com/b/rrasblog/archive/2007/01/10/sstp-faq-part-1-generic.aspx). Retrieved 2015-10-17.
6. Titz, Olaf (2001-04-23). "Why TCP Over TCP Is A Bad Idea" (http://sites.inka.de/bigred/devel/tcp-tcp.html). Retrieved 2015-10-17.
7. Honda, Osamu; Ohsaki, Hiroyuki; Imase, Makoto; Ishizuka, Mika; Murayama, Junichi (October 2005). "Understanding TCP over TCP: effects of TCP tunneling on end-to-end throughput and latency" (http://adsabs.harvard.edu/abs/2005SPIE.6011..138H). doi:10.1117/12.630496 (https://doi.org/10.1117%2F12.630496). Retrieved 2015-10-17.
8. "MS-SSTP: Secure Socket Tunneling Protocol (SSTP)" (https://technet.microsoft.com/en-us/subscriptions/cc247338.aspx). Microsoft TechNet. 2015-10-16. Retrieved 2015-10-17.

External links

- [MS-SSTP]: Secure Socket Tunneling Protocol (SSTP) (https://msdn.microsoft.com/en-us/library/cc247338.aspx) by Microsoft Open Specification Promise
- RRAS Technet Blog (http://blogs.technet.com/rrasblog/archive/tags/SSTP/default.aspx)
- Microsoft develops new tunneling protocol (http://www.techworld.com/networking/news/index.cfm?newsID=7814&pagtype=all)
- How SSTP based VPN connection works (http://blogs.technet.com/rrasblog/archive/2007/01/10/how-sstp-based-vpn-connection-works.aspx)
- HSC's SSTP Client for Linux (http://www.hsc.fr/ressources/outils/sstoper/index.html.en)
- SSTP Client for Linux (http://sstp-client.sourceforge.net/)

Retrieved from "https://en.wikipedia.org/w/index.php?title=Secure_Socket_Tunneling_Protocol&oldid=804760982"

This page was last edited on 11 October 2017, at 00:03.