|  |
| --- |
| **SSTP Server** |

|  |
| --- |
| SSTP is a form of 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. |

|  |
| --- |
| SSTP is available for Linux, BSD, and Windows. |

|  |
| --- |
| VyOS utilizes accel-ppp to provide SSTP server functionality. We support both local and |

|  |
| --- |
| RADIUS authentication. |

|  |
| --- |
| As SSTP provides PPP via a SSL/TLS channel the use of either publically signed |

certificates as well as a private PKI is required.

|  |
| --- |
| **Note** |
| All certificates should be stored on VyOS under /config/auth . If certificates are not stored   |  | | --- | |  | |

in the /config directory they will not be migrated during a software update. **Certificates**

**Self Signed CA**

To generate the CA, the server private key and certificates the following commands can be used.

|  |
| --- |
| vyos@vyos:~$ mkdir -p /config/user-data/sstp  vyos@vyos:~$ openssl req -newkey rsa:4096 -new -nodes -x509 -days 3650 -keyout /config/user-data/sstp/server.key -out /config/user-data/sstp/server.crt |

|  |
| --- |
| Generating a 4096 bit RSA private key  .........................++  ...............................................................++  writing new private key to 'server.key'  [...]  Country Name (2 letter code) [AU]:  State or Province Name (full name) [Some-State]:  Locality Name (eg, city) []:  Organization Name (eg, company) [Internet Widgits Pty Ltd]: Organizational Unit Name (eg, section) []:  Common Name (e.g. server FQDN or YOUR name) []:  Email Address []: |

|  |
| --- |
| vyos@vyos:~$ openssl req -new -x509 -key /config/user-data/sstp/server.key -out /config/user-data/sstp/ca.crt  [...]  Country Name (2 letter code) [AU]:  State or Province Name (full name) [Some-State]:  Locality Name (eg, city) []:  Organization Name (eg, company) [Internet Widgits Pty Ltd]:  Organizational Unit Name (eg, section) []:  Common Name (e.g. server FQDN or YOUR name) []:  Email Address []: |

**Configuration**

|  |
| --- |
| **set vpn sstp authentication local-users username <user> password <pass>** |

Create *<user>* for local authentication on this system. The users password will be set to *<pass>*.

|  |
| --- |
| **set vpn sstp authentication local-users username <user> disable** |

Disable *<user>* account.

|  |
| --- |
| **set vpn sstp authentication local-users username <user> static-ip <address>** |

Assign static IP address to *<user>* account.

|  |
| --- |
| **set vpn sstp authentication local-users username <user> rate-limit download <bandwidth>** |

Download bandwidth limit in kbit/s for *<user>*.

|  |
| --- |
| **set vpn sstp authentication local-users username <user> rate-limit upload <bandwidth>** |

Upload bandwidth limit in kbit/s for *<user>*.

|  |
| --- |
| **set vpn sstp authentication protocols <pap | chap | mschap | mschap-v2>** |

Require the peer to authenticate itself using one of the following protocols: pap, chap, mschap, mschap-v2.

|  |
| --- |
| **set vpn sstp authentication mode <local | radius>** |

Set authentication backend. The configured authentication backend is used for all queries.

|  |  |
| --- | --- |
|  | **radius**: All authentication queries are handled by a configured RADIUS server. |
|  | **local**: All authentication queries are handled locally. |
| **set vpn sstp gateway-address <gateway>** | |

Specifies single *<gateway>* IP address to be used as local address of PPP interfaces.

|  |
| --- |
| **set vpn sstp port <port>** |

Specifies the port *<port>* that the SSTP port will listen on (default 443).

|  |
| --- |
| **set vpn sstp client-ip-pool subnet <subnet>** |

Use *<subnet>* as the IP pool for all connecting clients.

|  |
| --- |
| **set vpn sstp client-ipv6-pool prefix <address> mask <number-of-bits>** |

Use this comand to set the IPv6 address pool from which an SSTP client will get an IPv6 prefix of your defined length (mask) to terminate the SSTP endpoint at their side. The mask length can be set from 48 to 128 bit long, the default value is 64.

|  |
| --- |
| **set vpn sstp client-ipv6-pool delegate <address> delegation-prefix <number-of-bits>** |

Use this command to configure DHCPv6 Prefix Delegation (RFC3633) on SSTP. You will have to set your IPv6 pool and the length of the delegation prefix. From the defined IPv6 pool you will be handing out networks of the defined length (delegation-prefix). The length of the delegation prefix can be set from 32 to 64 bit long.

|  |
| --- |
| **set vpn sstp name-server <address>** |

Connected client should use *<address>* as their DNS server. This command accepts both IPv4 and IPv6 addresses. Up to two nameservers can be configured for IPv4, up to three for IPv6.

Maximum number of IPv4 nameservers

**SSL Certificates**

|  |
| --- |
| **set vpn sstp ssl ca-cert-file <file>** |

Path to *<file>* pointing to the certificate authority certificate.

|  |
| --- |
| **set vpn sstp ssl cert-file <file>** |

Path to *<file>* pointing to the servers certificate (public portion).

**PPP Settings**

|  |
| --- |
| **set vpn sstp ppp-options lcp-echo-failure <number>** |

Defines the maximum *<number>* of unanswered echo requests. Upon reaching the value *<number>*, the session will be reset.

|  |
| --- |
| **set vpn sstp ppp-options lcp-echo-interval <interval>** |

If this option is specified and is greater than 0, then the PPP module will send LCP pings of the echo request every *<interval>* seconds.

|  |
| --- |
| **set vpn sstp ppp-options lcp-echo-timeout** |

Specifies timeout in seconds to wait for any peer activity. If this option specified it turns on adaptive lcp echo functionality and “lcp-echo-failure” is not used.

|  |
| --- |
| **set vpn sstp ppp-options mppe <require | prefer | deny>** |

Specifies MPPE negotioation preference.

 **require** - ask client for mppe, if it rejects drop connection

 **prefer** - ask client for mppe, if it rejects don’t fail

 **deny** - deny mppe   
Default behavior - don’t ask client for mppe, but allow it if client wants. Please note that RADIUS may override this option by MS-MPPE-Encryption-Policy attribute.

**RADIUS**

**Server**

|  |
| --- |
| **set vpn sstp authentication radius server <server> port <port>** |

Configure RADIUS *<server>* and its required port for authentication requests.

|  |
| --- |
| **set vpn sstp authentication radius server <server> key <secret>** |

Configure RADIUS *<server>* and its required shared *<secret>* for communicating with the RADIUS server.

|  |
| --- |
| **set vpn sstp authentication radius server <server> fail-time <time>** |

Mark RADIUS server as offline for this given *<time>* in seconds.

|  |
| --- |
| **set vpn sstp authentication radius server <server> disable** |

Temporary disable this RADIUS server.

**Options**

|  |
| --- |
| **set vpn sstp authentication radius acct-timeout <timeout>** |

Timeout to wait reply for Interim-Update packets. (default 3 seconds)

|  |
| --- |
| **set vpn sstp authentication radius dynamic-author server <address>** |

Specifies IP address for Dynamic Authorization Extension server (DM/CoA)

|  |
| --- |
| **set vpn sstp authentication radius dynamic-author port <port>** |

Port for Dynamic Authorization Extension server (DM/CoA)

|  |
| --- |
| **set vpn sstp authentication radius dynamic-author key <secret>** |

Secret for Dynamic Authorization Extension server (DM/CoA)

|  |
| --- |
| **set vpn sstp authentication radius max-try <number>** |

Maximum number of tries to send Access-Request/Accounting-Request queries

|  |
| --- |
| **set vpn sstp authentication radius timeout <timeout>** |

Timeout to wait response from server (seconds)

|  |
| --- |
| **set vpn sstp authentication radius nas-identifier <identifier>** |

Value to send to RADIUS server in NAS-Identifier attribute and to be matched in DM/CoA requests.

|  |
| --- |
| **set vpn sstp authentication radius nas-ip-address <address>** |

Value to send to RADIUS server in NAS-IP-Address attribute and to be matched in DM/CoA requests. Also DM/CoA server will bind to that address.

|  |
| --- |
| **set vpn sstp authentication radius source-address <address>** |

Source IPv4 address used in all RADIUS server queires.

|  |
| --- |
| **set vpn sstp authentication radius rate-limit attribute <attribute>** |

Specifies which RADIUS server attribute contains the rate limit information. The default attribute is *Filter-Id*.

|  |
| --- |
| **set vpn sstp authentication radius rate-limit enable** |

Enables bandwidth shaping via RADIUS.

|  |
| --- |
| **set vpn sstp authentication radius rate-limit vendor** |

Specifies the vendor dictionary, dictionary needs to be in /usr/share/accel-ppp/radius.

**Example**

 Use local user *foo* with password *bar*

|  |  |
| --- | --- |
|  | Client IP addresses will be provided from pool *192.0.2.0/25* |
| set vpn sstp authentication local-users username vyos password vyos set vpn sstp authentication mode local  set vpn sstp gateway-address 192.0.2.254  set vpn sstp client-ip-pool subnet 192.0.2.0/25  set vpn sstp name-server 10.0.0.1  set vpn sstp name-server 10.0.0.2  set vpn sstp ssl ca-cert-file /config/auth/ca.crt  set vpn sstp ssl cert-file /config/auth/server.crt  set vpn sstp ssl key-file /config/auth/server.key | |
| **Testing SSTP** | |

Once you have setup your SSTP server there comes the time to do some basic testing. The Linux client used for testing is called sstpc. sstpc requires a PPP configuration/peer file.

The following PPP configuration tests MSCHAP-v2:

|  |
| --- |
| $ cat /etc/ppp/peers/vyos  usepeerdns  #require-mppe  #require-pap  require-mschap-v2  noauth  lock  refuse-pap  refuse-eap  refuse-chap  refuse-mschap  #refuse-mschap-v2  nobsdcomp  nodeflate  debug |
| You can now “dial” the peer with the follwoing command: sstpc --log-level 4 --log-stderr --   |  | | --- | |  | |

|  |
| --- |
| user vyos --password vyos vpn.example.com -- call vyos . |

A connection attempt will be shown as:

|  |
| --- |
| $ sstpc --log-level 4 --log-stderr --user vyos --password vyos vpn.example.com -- call vyos |

|  |
| --- |
| Mar 22 13:29:12 sstpc[12344]: Resolved vpn.example.com to 192.0.2.1 Mar 22 13:29:12 sstpc[12344]: Connected to vpn.example.com  Mar 22 13:29:12 sstpc[12344]: Sending Connect-Request Message Mar 22 13:29:12 sstpc[12344]: SEND SSTP CRTL PKT(14)  Mar 22 13:29:12 sstpc[12344]: TYPE(1): CONNECT REQUEST, ATTR(1): Mar 22 13:29:12 sstpc[12344]: ENCAP PROTO(1): 6  Mar 22 13:29:12 sstpc[12344]: RECV SSTP CRTL PKT(48)  Mar 22 13:29:12 sstpc[12344]: TYPE(2): CONNECT ACK, ATTR(1): Mar 22 13:29:12 sstpc[12344]: CRYPTO BIND REQ(4): 40  Mar 22 13:29:12 sstpc[12344]: Started PPP Link Negotiation  Mar 22 13:29:15 sstpc[12344]: Sending Connected Message  Mar 22 13:29:15 sstpc[12344]: SEND SSTP CRTL PKT(112)  Mar 22 13:29:15 sstpc[12344]: TYPE(4): CONNECTED, ATTR(1): |

|  |
| --- |
| Mar 22 13:29:15 sstpc[12344]: CRYPTO BIND(3): 104 Mar 22 13:29:15 sstpc[12344]: Connection Established |

|  |
| --- |
| $ ip addr show ppp0  164: ppp0: <POINTOPOINT,MULTICAST,NOARP,UP,LOWER\_UP> mtu 1452 qdisc fq\_codel state UNKNOWN group default qlen 3  link/ppp promiscuity 0  inet 100.64.2.2 peer 100.64.1.1/32 scope global ppp0  valid\_lft forever preferred\_lft forever |