|  |
| --- |
| **OpenConnect** |

|  |
| --- |
| OpenConnect-compatible server feature is available from this release. Openconnect |

VPN supports SSL connection and offers full network access. SSL VPN network

extension connects the end-user system to the corporate network with access controls

based only on network layer information, such as destination IP address and port

number. So, it provides safe communication for all types of device traffic across public

|  |
| --- |
| networks and private networks, also encrypts the traffic with SSL protocol. |

|  |
| --- |
| The remote user will use the openconnect client to connect to the router and will |

|  |
| --- |
| receive an IP address from a VPN pool, allowing full access to the network. |

|  |
| --- |
| **Configuration** |

|  |
| --- |
| **SSL Certificates** |

|  |
| --- |
| We need to generate the certificate which authenticates users who attempt to access |

the network resource through the SSL VPN tunnels. The following commands will create

a self signed certificates and will be stored in configuration:

|  |
| --- |
| run generate pki ca install <CA name>  run generate pki certificate sign <CA name> install <Server name> |

|  |
| --- |
| We can also create the certificates using Cerbort which is an easy-to-use client that |

|  |
| --- |
| fetches a certificate from Let’s Encrypt an open certificate authority launched by the |

|  |
| --- |
| EFF, Mozilla, and others and deploys it to a web server. |

|  |
| --- |
| sudo certbot certonly --standalone --preferred-challenges http -d <domain name> |

|  |
| --- |
| **Server Configuration** |

|  |
| --- |
| set vpn openconnect authentication local-users username <user> password <pass> set vpn openconnect authentication mode <local password|radius>  set vpn openconnect network-settings client-ip-settings subnet <subnet>  set vpn openconnect network-settings name-server <address>  set vpn openconnect network-settings name-server <address>  set vpn openconnect ssl ca-certificate <pki-ca-name>  set vpn openconnect ssl certificate <pki-cert-name>  set vpn openconnect ssl passphrase <pki-password> |

|  |
| --- |
| **2FA OTP support** |

|  |
| --- |
| Instead of password only authentication, 2FA password authentication + OTP key can |

|  |
| --- |
| be used. Alternatively, OTP authentication only, without a password, can be used. To do |

|  |
| --- |
| this, an OTP configuration must be added to the configuration above: |

|  |
| --- |
| set vpn openconnect authentication mode local <password-otp|otp>  set vpn openconnect authentication local-users username <user> otp <key>  set vpn openconnect authentication local-users username <user> interval <interval (optional)> set vpn openconnect authentication local-users username <user> otp-length <otp-length (optional)> set vpn openconnect authentication local-users username <user> token-type <token-type (optional)> |

|  |
| --- |
| For generating an OTP key in VyOS, you can use the CLI command (operational mode): |

|  |
| --- |
| generate openconnect username <user> otp-key hotp-time |
| **Verification** |

|  |
| --- |
| vyos@vyos:~$ sh openconnect-server sessions  interface username ip remote IP RX TX state uptime----------- ---------- ------------- ----------- ------- --------- --------- -------- sslvpn0 tst 172.20.20.198 192.168.6.1 0 bytes 152 bytes connected 3s |

|  |
| --- |
| **Note** |

|  |
| --- |
| It is compatible with Cisco (R) AnyConnect (R) clients. |
| **Example** |

|  |
| --- |
| **SSL Certificates generation** |

|  |
| --- |
| Follow the instructions to generate CA cert (in configuration mode): |

|  |
| --- |
| vyos@vyos# run generate pki ca install ca-ocserv  Enter private key type: [rsa, dsa, ec] (Default: rsa)  Enter private key bits: (Default: 2048)  Enter country code: (Default: GB) US  Enter state: (Default: Some-State) Delaware  Enter locality: (Default: Some-City) Mycity  Enter organization name: (Default: VyOS) MyORG  Enter common name: (Default: vyos.io) oc-ca  Enter how many days certificate will be valid: (Default: 1825) 3650  Note: If you plan to use the generated key on this router, do not encrypt the private key.  Do you want to encrypt the private key with a passphrase? [y/N] N  2 value(s) installed. Use "compare" to see the pending changes, and "commit" to apply.  [edit] |

|  |
| --- |
| Follow the instructions to generate server cert (in configuration mode): |

|  |
| --- |
| vyos@vyos# run generate pki certificate sign ca-ocserv install srv-ocserv Do you already have a certificate request? [y/N] N  Enter private key type: [rsa, dsa, ec] (Default: rsa)  Enter private key bits: (Default: 2048)  Enter country code: (Default: GB) US  Enter state: (Default: Some-State) Delaware |

|  |
| --- |
| Enter locality: (Default: Some-City) Mycity  Enter organization name: (Default: VyOS) MyORG  Enter common name: (Default: vyos.io) oc-srv  Do you want to configure Subject Alternative Names? [y/N] N  Enter how many days certificate will be valid: (Default: 365) 1830  Enter certificate type: (client, server) (Default: server)  Note: If you plan to use the generated key on this router, do not encrypt the private key.  Do you want to encrypt the private key with a passphrase? [y/N] N  2 value(s) installed. Use "compare" to see the pending changes, and "commit" to apply.  [edit] |

Each of the install command should be applied to the configuration and commited before

using under the openconnect configuration:

|  |
| --- |
| vyos@vyos# commit  [edit]  vyos@vyos# save  Saving configuration to '/config/config.boot'...  Done  [edit] |

|  |
| --- |
| **Openconnect Configuration** |

|  |
| --- |
| Simple setup with one user added and password authentication: |

|  |
| --- |
| set vpn openconnect authentication local-users username tst password 'OC\_bad\_Secret' set vpn openconnect authentication mode local password  set vpn openconnect network-settings client-ip-settings subnet '172.20.20.0/24' set vpn openconnect network-settings name-server '10.1.1.1'  set vpn openconnect network-settings name-server '10.1.1.2'  set vpn openconnect ssl ca-certificate 'ca-ocserv'  set vpn openconnect ssl certificate 'srv-ocserv' |

|  |
| --- |
| **Adding a 2FA with an OTP-key** |

|  |
| --- |
| First the OTP keys must be generated and sent to the user and to the configuration: |

|  |
| --- |
| vyos@vyos:~$ generate openconnect username tst otp-key hotp-time # You can share it with the user, he just needs to scan the QR in his OTP app # username: tst  # OTP KEY: 5PA4SGYTQSGOBO3H3EQSSNCUNZAYAPH2  # OTP URL: otpauth://totp/tst@vyos?  secret=5PA4SGYTQSGOBO3H3EQSSNCUNZAYAPH2&digits=6&period=30█████████████████████████████████████████ █████████████████████████████████████████ ████ ▄▄▄▄▄ █▀ ██▄▀ ▄█▄▀▀▄▄▄▄██ ▄▄▄▄▄ ████ ████ █ █ █▀ █▄▄▀▀▀▄█ ▄▄▀▄ █ █ █ ████ ████ █▄▄▄█ █▀█▀▄▄▀ ▄▀ █▀ ▀▄██ █▄▄▄█ ████ ████▄▄▄▄▄▄▄█▄█▄▀ ▀▄█ ▀ ▀ ▀ █▄█▄▄▄▄▄▄▄████ ████ ▄▄▄▀▄▄ ▄███▀▄▀█▄██▀ ▀▄ ▀▄█ ▀ ▀████ ████ ▀▀ ▀ ▄█▄ ▀ ▀▄ ▄█▀ ▄█ ▄▀▀▄██ █████ ████▄ █▄▀▀▄█▀ ▀█▄█▄▄▄▄ ▄▀█▀▀█ ▀ ▄ ▀█▀████ █████ ▀█▀▄▄ █ ▀▄▄ ▄█▄ ▀█▀▀ █▀ ▄█████ ████▀██▀█▄▄ ▀▀▀▀█▄▀ ▀█▄▄▀▀▀ ▀ ▀█▄██▀▀████ ████▄ ▄ ▄▀▄██▀█ ▄ ▀▄██ ▄▄ ▀▀▄█▄██ ▄█████ ████▀▀ ▄▀ ▄ ▀█▀█▀█ █▀█▄▄▀█▀█▄██▄▄█ ▀████ |

|  |
| --- |
| ████ █ ▀█▄▄█▄ ▀ ▄▄▀▀ ▀ █▄█▀████ █▀ ▀████ ████▄██▄██▄█▀ ▄▀ ▄▄▀▄ ▄▀█ ▄ ▄▄▄ ▀█▄ ████ ████ ▄▄▄▄▄ █▄ ▀█▄█ ▄ ▀ ▄ ▄ █▄█ ▄▀▄█████ ████ █ █ █ ▀▄██▄▄▀█▄▀▄██▄▀ ▄ ▀██▀████ ████ █▄▄▄█ █ ██▀▄▄ ▀▄▄▀█▀ ▀█ ▄▀█ ▀██████ ████▄▄▄▄▄▄▄█▄███▄███▄█▄▄▄▄█▄▄█▄██▄█▄█████ █████████████████████████████████████████ █████████████████████████████████████████ # To add this OTP key to configuration, run the following commands: set vpn openconnect authentication local-users username tst otp key 'ebc1c91b13848ce0bb67d9212934546e41803cfa' |

|  |
| --- |
| Next it is necessary to configure 2FA for OpenConnect: |

|  |
| --- |
| set vpn openconnect authentication mode local password-otp  set vpn openconnect authentication local-users username tst otp key 'ebc1c91b13848ce0bb67d9212934546e41803cfa' |

|  |
| --- |
| Now when connecting the user will first be asked for the password and then the OTP |

|  |
| --- |
| key. |

|  |
| --- |
| **Warning** |

|  |
| --- |
| When using Time-based one-time password (TOTP) (OTP HOTP-time), be sure that the |

|  |
| --- |
| time on the server and the OTP token generator are synchronized by NTP |

|  |
| --- |
| To display the configured OTP user settings, use the command: |

|  |
| --- |
| show openconnect-server user <username> otp <full|key-b32|key-hex|qrcode|uri> |

|  |
| --- |
| **Identity Based Configuration** |

|  |
| --- |
| OpenConnect supports a subset of it’s configuration options to be applied on a per |

|  |
| --- |
| user/group basis, for configuration purposes we refer to this functionality as “Identity |

|  |
| --- |
| based config”. The following OpenConnect Server Manual outlines the set of |

|  |
| --- |
| configuration options that are allowed. This can be leveraged to apply different sets of |

|  |
| --- |
| configs to different users or groups of users. |

|  |
| --- |
| sudo mkdir -p /config/auth/ocserv/config-per-user  sudo touch /config/auth/ocserv/default-user.conf |

|  |
| --- |
| set vpn set vpn openconnect authentication identity-based-config mode user  set vpn openconnect authentication identity-based-config directory /config/auth/ocserv/config-per-user set vpn openconnect authentication identity-based-config default-config /config/auth/ocserv/default-user.conf |

|  |
| --- |
| **Warning** |

|  |
| --- |
| The above directory and default-config must be a child directory of /config/auth, since |

|  |
| --- |
| files outside this directory are not persisted after an image upgrade. |

|  |
| --- |
| Once you commit the above changes you can create a config file in the |

|  |
| --- |
| /config/auth/ocserv/config-per-user directory that matches a username of a user you |

|  |
| --- |
| have created e.g. “tst”. Now when logging in with the “tst” user the config options you |

|  |
| --- |
| set in this file will be loaded. |

|  |
| --- |
| Be sure to set a sane default config in the default config file, this will be loaded in the |

|  |
| --- |
| case that a user is authenticated and no file is found in the configured directory matching |

|  |
| --- |
| the users username/group. |

|  |
| --- |
| sudo nano /config/auth/ocserv/config-per-user/tst |

|  |
| --- |
| The same configuration options apply when Identity based config is configured in group |

|  |
| --- |
| mode except that group mode can only be used with RADIUS authentication. |

|  |
| --- |
| **Warning** |

|  |
| --- |
| OpenConnect server matches the filename in a case sensitive manner, make sure the |

|  |
| --- |
| username/group name you configure matches the filename exactly. |
| **Configuring RADIUS accounting** |

|  |
| --- |
| OpenConnect can be configured to send accounting information to a RADIUS server to |

|  |
| --- |
| capture user session data such as time of connect/disconnect, data transferred, and so |

|  |
| --- |
| on. |

|  |
| --- |
| Configure an accounting server and enable accounting with: |

|  |
| --- |
| set vpn openconnect accounting mode radius  set vpn openconnect accounting radius server 172.20.20.10  set vpn openconnect accounting radius server 172.20.20.10 port 1813  set vpn openconnect accounting radius server 172.20.20.10 key your\_radius\_secret |

|  |
| --- |
| **Warning** |

|  |
| --- |
| The RADIUS accounting feature must be used with the OpenConnect authentication |

|  |
| --- |
| mode RADIUS. It cannot be used with local authentication. You must configure the |

|  |
| --- |
| OpenConnect authentication mode to “radius”. |

|  |
| --- |
| An example of the data captured by a FREERADIUS server with sql accounting: |

|  |
| --- |
| mysql> SELECT username, nasipaddress, acctstarttime, acctstoptime, acctinputoctets,  acctoutputoctets, callingstationid, framedipaddress, connectinfo\_start FROM radacct;  +----------+---------------+---------------------+---------------------+-----------------+------------------+-------------------+-----------------+-----------------------------------+  | username | nasipaddress | acctstarttime | acctstoptime | acctinputoctets | acctoutputoctets | callingstationid | framedipaddress | connectinfo\_start | |

|  |
| --- |
| +----------+---------------+---------------------+---------------------+-----------------+------------------+-------------------+-----------------+-----------------------------------+  | test | 198.51.100.15 | 2023-01-13 00:59:15 | 2023-01-13 00:59:21 | 10606 | 152 | 192.168.6.1 | 172.20.20.198 | Open AnyConnect VPN Agent v8.05-1 |  +----------+---------------+---------------------+---------------------+-----------------+------------------+-------------------+-----------------+-----------------------------------+ |

Previous Next