|  |
| --- |
| **RSA-Keys**[](https://docs.vyos.io/en/latest/configuration/vpn/rsa-keys.html#rsa-keys) |

|  |
| --- |
| RSA can be used for services such as key exchanges and for encryption purposes. To |

|  |
| --- |
| make IPSec work with dynamic address on one/both sides, we will have to use RSA keys |

|  |
| --- |
| for authentication. They are very fast and easy to setup. |

|  |
| --- |
| First, on both routers run the operational command “generate pki key-pair install <key- |

|  |
| --- |
| pair nam>>”. You may choose different length than 2048 of course. |

|  |
| --- |
| vyos@left# run generate pki key-pair install ipsec-LEFT  Enter private key type: [rsa, dsa, ec] (Default: rsa)  Enter private key bits: (Default: 2048)  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 Configure mode commands to install key pair:  Do you want to install the public key? [Y/n] Y  set pki key-pair ipsec-LEFT public key 'MIIBIjANBgkqh...'  Do you want to install the private key? [Y/n] Y  set pki key-pair ipsec-LEFT private key 'MIIEvgIBADAN...'  [edit] |

|  |
| --- |
| Configuration commands will display. Note the command with the public key (set pki |

|  |
| --- |
| key-pair ipsec-LEFT public key ‘MIIBIjANBgkqh…’). Then do the same on the opposite |

|  |
| --- |
| router: |

|  |
| --- |
| vyos@left# run generate pki key-pair install ipsec-RIGHT |

|  |
| --- |
| Note the command with the public key (set pki key-pair ipsec-RIGHT public key |

|  |
| --- |
| ‘FAAOCAQ8AMII…’). |

|  |
| --- |
| The noted public keys should be entered on the opposite routers. |

|  |
| --- |
| On the LEFT: |

|  |
| --- |
| set pki key-pair ipsec-RIGHT public key 'FAAOCAQ8AMII...' |

|  |
| --- |
| On the RIGHT: |

|  |
| --- |
| set pki key-pair ipsec-LEFT public key 'MIIBIjANBgkqh...' |

|  |
| --- |
| Now you are ready to setup IPsec. The key points: |

|  |
| --- |
| 1. Since both routers do not know their effective public addresses, we set the |

|  |
| --- |
| local-address of the peer to “any”. |

|  |
| --- |
| 2. On the initiator, we set the peer address to its public address, but on the |

|  |
| --- |
| responder we only set the id. |

|  |
| --- |
| 3. On the initiator, we need to set the remote-id option so that it can identify IKE |

|  |
| --- |
| traffic from the responder correctly. |

|  |
| --- |
| 4. On the responder, we need to set the local id so that initiator can know who’s |

|  |
| --- |
| talking to it for the point #3 to work. |

|  |
| --- |
| On the LEFT (static address): |

set vpn ipsec interface eth0

|  |
| --- |
| set vpn ipsec esp-group MyESPGroup proposal 1 encryption aes128 set vpn ipsec esp-group MyESPGroup proposal 1 hash sha1 |

|  |
| --- |
| set vpn ipsec ike-group MyIKEGroup proposal 1 dh-group 2  set vpn ipsec ike-group MyIKEGroup proposal 1 encryption aes128 set vpn ipsec ike-group MyIKEGroup proposal 1 hash sha1 |

|  |
| --- |
| set vpn ipsec site-to-site peer @RIGHT authentication id LEFT  set vpn ipsec site-to-site peer @RIGHT authentication mode rsa  set vpn ipsec site-to-site peer @RIGHT authentication rsa local-key ipsec-LEFT  set vpn ipsec site-to-site peer @RIGHT authentication rsa remote-key ipsec-RIGHT  set vpn ipsec site-to-site peer @RIGHT authentication remote-id RIGHT  set vpn ipsec site-to-site peer @RIGHT default-esp-group MyESPGroup  set vpn ipsec site-to-site peer @RIGHT ike-group MyIKEGroup  set vpn ipsec site-to-site peer @RIGHT local-address 192.0.2.10  set vpn ipsec site-to-site peer @RIGHT connection-type respond  set vpn ipsec site-to-site peer @RIGHT tunnel 1 local prefix 192.168.99.1/32 # Additional loopback address on the local  set vpn ipsec site-to-site peer @RIGHT tunnel 1 remote prefix 192.168.99.2/32 # Additional loopback address on the remote |

|  |
| --- |
| On the RIGHT (dynamic address): |

set vpn ipsec interface eth0

|  |
| --- |
| set vpn ipsec esp-group MyESPGroup proposal 1 encryption aes128 set vpn ipsec esp-group MyESPGroup proposal 1 hash sha1 |

|  |
| --- |
| set vpn ipsec ike-group MyIKEGroup proposal 1 dh-group 2  set vpn ipsec ike-group MyIKEGroup proposal 1 encryption aes128 set vpn ipsec ike-group MyIKEGroup proposal 1 hash sha1 |

|  |
| --- |
| set vpn ipsec site-to-site peer 192.0.2.10 authentication id RIGHT  set vpn ipsec site-to-site peer 192.0.2.10 authentication mode rsa  set vpn ipsec site-to-site peer 192.0.2.10 authentication rsa local-key ipsec-RIGHT  set vpn ipsec site-to-site peer 192.0.2.10 authentication rsa remote-key ipsec-LEFT  set vpn ipsec site-to-site peer 192.0.2.10 authentication remote-id LEFT  set vpn ipsec site-to-site peer 192.0.2.10 connection-type initiate  set vpn ipsec site-to-site peer 192.0.2.10 default-esp-group MyESPGroup  set vpn ipsec site-to-site peer 192.0.2.10 ike-group MyIKEGroup  set vpn ipsec site-to-site peer 192.0.2.10 local-address any  set vpn ipsec site-to-site peer 192.0.2.10 tunnel 1 local prefix 192.168.99.2/32 # Additional loopback address on the local  set vpn ipsec site-to-site peer 192.0.2.10 tunnel 1 remote prefix 192.168.99.1/32 # Additional loopback address on the remote |