goodNETnick_VyOS_KB

Release 0.1

goodNETnick

Sep 18, 2022

CONTENTS

Note: This project is under not so active development.

CHAPTER

ONE

CONTENTS

1.1 IPSec Authentication using x509 certificates (VyOS 1.4)

1.1.1 Task

Create an IPsec VPN tunnel using X.509 certificates in VyOS 1.4.

1.1.2 Introduction

To accomplish this, we need a pair of keys (public & private) and the appropriate X.509 certificate for each IPsec peer. We also need a self-signed Root CA certificate to validate the peer certificates.

Proper use of certificates involves creating a PKI infrastructure with root and intermediate CAs, certificate revocation validation, and other elements.

In this example, we will use a simplified PKI infrastructure consisting only of Root CAs. A VyOS router will be used as the Root CA.

1.1.3 Configuration

So. There are two VyOS routers (R1 & R2). We need to connect them using IPsec with X.509 certificate authentication.

First step. Choose R1 as Root CA. Generate a key pair for the Root CA

Use Operational Mode commands, not Configuration Mode:

```
vyos@R1:~$ generate pki ca install CA
Enter private key type: [rsa, dsa, ec] (Default: rsa)
Enter private key bits: (Default: 2048)
Enter country code: (Default: GB)
Enter state: (Default: Some-State)
Enter locality: (Default: Some-City)
Enter organization name: (Default: VyOS)
Enter common name: (Default: vyos.io) CA
Enter how many days certificate will be valid: (Default: 1825)
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:
```

(continues on next page)

(continued from previous page)

```
set pki ca CA certificate 'MIIDnTCCAo........='
set pki ca CA private key 'MIIEvwIBAD........='
```

This will give you the encryption key pair. Copy the lines with the keys and commands to set them (after the output lines "Configure mode commands to install"):

```
set pki ca CA certificate 'MIIDnTCCAo........='
set pki ca CA private key 'MIIEvwIBAD........='
```

paste these commands into configuration mode on R1 (CA):

```
vyos@R1:~$ configure
vyos@R1# set pki ca CA certificate 'MIIDnTCCAo........='
vyos@R1# set pki ca CA private key 'MIIEvwIBAD........='
vyos@R1# commit
vyos@R1# save
```

We still need the Root CA certificate command for Router R2 (set pki ca CA certificate 'MIIDnTCCAo.....='). Save it. The Private Key CA is the most important element of the PKI (set pki ca CA private key 'MIIEvwIBAD.....='). It must not be shared with anyone (including R2)

Second step. Generate an encryption key pair and X.509 certificate for each IPsec peer

Certificates must be generated on the CA, in our case on R1.

Use Operational Mode commands, not Configuration Mode. Do not forget to copy the lines with the keys and commands to set them (after the output lines "Configure mode commands to install")

```
vyos@R1:~$ generate pki certificate sign CA install R1
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)
Enter state: (Default: Some-State)
Enter locality: (Default: Some-City)
Enter organization name: (Default: VyOS)
Enter common name: (Default: vyos.io) R1
Do you want to configure Subject Alternative Names? [y/N] N
Enter how many days certificate will be valid: (Default: 365)
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
Configure mode commands to install:
set pki certificate R1 certificate 'MIIDrDCCA ..............='
set pki certificate R1 private key 'MIIEvgIBA..............O'
```

```
vyos@R1:~$ generate pki certificate sign CA install R2
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)
```

(continues on next page)

(continued from previous page)

```
Enter state: (Default: Some-State)
Enter locality: (Default: Some-City)
Enter organization name: (Default: VyOS)
Enter common name: (Default: vyos.io) R2
Do you want to configure Subject Alternative Names? [y/N] N
Enter how many days certificate will be valid: (Default: 365)
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
Configure mode commands to install:
set pki certificate R2 certificate 'MIIDrDCCAp...........='
set pki certificate R2 private key 'MIIEvgIBAD...........L'
```

Third step. Install keys and certificate in VyOS routers

On Router R1 (Root CA certificate is already there):

```
vyos@R1:~$ configure
vyos@R1# set pki certificate R1 certificate 'MIIDrDCCA ..............='
vyos@R1# set pki certificate R1 private key 'MIIEvgIBA..............O'
```

On the R2 router (Root CA needs to be added):

```
vyos@R2:~$ configure
vyos@R2# set pki ca CA certificate 'MIIDnTCCAo........='
vyos@R2# set pki certificate R2 certificate 'MIIDrDCCAp...........='
vyos@R2# set pki certificate R2 private key 'MIIEvgIBAD...........L'
```

Fourth step. IPsec configuration

Everything is ready to configure IPsec.

IPsec settings on R1:

```
set interfaces ethernet eth0 address '192.0.2.11/24'
set system host R1
set interfaces vti vti10 address 10.10.10.1/30
set vpn ipsec esp-group ESP_DEFAULT compression 'disable'
set vpn ipsec esp-group ESP_DEFAULT lifetime '3600'
set vpn ipsec esp-group ESP_DEFAULT mode 'tunnel'
set vpn ipsec esp-group ESP_DEFAULT pfs 'dh-group19'
set vpn ipsec esp-group ESP_DEFAULT proposal 10 encryption 'aes256gcm128'
set vpn ipsec esp-group ESP_DEFAULT proposal 10 hash 'sha256'
set vpn ipsec ike-group IKEv2_DEFAULT dead-peer-detection action 'hold'
set vpn ipsec ike-group IKEv2_DEFAULT dead-peer-detection interval '30'
set vpn ipsec ike-group IKEv2_DEFAULT dead-peer-detection timeout '120'
set vpn ipsec ike-group IKEv2_DEFAULT ikev2-reauth 'no'
set vpn ipsec ike-group IKEv2_DEFAULT key-exchange 'ikev2'
set vpn ipsec ike-group IKEv2_DEFAULT lifetime '10800'
set vpn ipsec ike-group IKEv2_DEFAULT mobike 'disable'
```

(continues on next page)

(continued from previous page)

```
set vpn ipsec ike-group IKEv2_DEFAULT proposal 10 dh-group '19'
set vpn ipsec ike-group IKEv2_DEFAULT proposal 10 encryption 'aes256gcm128'
set vpn ipsec ike-group IKEv2_DEFAULT proposal 10 hash 'sha256'
set vpn ipsec interface eth0
set vpn ipsec site-to-site peer 192.0.2.22 authentication id 'C=GB, ST=Some-State,␣
↪L=Some-City, O=VyOS, CN=R1'
set vpn ipsec site-to-site peer 192.0.2.22 authentication mode 'x509'
set vpn ipsec site-to-site peer 192.0.2.22 authentication remote-id 'C=GB, ST=Some-State,
↪ L=Some-City, O=VyOS, CN=R2'
set vpn ipsec site-to-site peer 192.0.2.22 authentication x509 ca-certificate CA
set vpn ipsec site-to-site peer 192.0.2.22 authentication x509 certificate R1
set vpn ipsec site-to-site peer 192.0.2.22 connection-type 'initiate'
set vpn ipsec site-to-site peer 192.0.2.22 ike-group 'IKEv2_DEFAULT'
set vpn ipsec site-to-site peer 192.0.2.22 ikev2-reauth 'inherit'
set vpn ipsec site-to-site peer 192.0.2.22 local-address 192.0.2.11
set vpn ipsec site-to-site peer 192.0.2.22 vti bind 'vti10'
set vpn ipsec site-to-site peer 192.0.2.22 vti esp-group 'ESP_DEFAULT'
set vpn ipsec options disable-route-autoinstall
```

IPsec settings on R2:

```
set interfaces ethernet eth0 address '192.0.2.22/24'
set system host R2
set interfaces vti vti10 address 10.10.10.2/30
set vpn ipsec esp-group ESP_DEFAULT compression 'disable'
set vpn ipsec esp-group ESP_DEFAULT lifetime '3600'
set vpn ipsec esp-group ESP_DEFAULT mode 'tunnel'
set vpn ipsec esp-group ESP_DEFAULT pfs 'dh-group19'
set vpn ipsec esp-group ESP_DEFAULT proposal 10 encryption 'aes256gcm128'
set vpn ipsec esp-group ESP_DEFAULT proposal 10 hash 'sha256'
set vpn ipsec ike-group IKEv2_DEFAULT dead-peer-detection action 'hold'
set vpn ipsec ike-group IKEv2_DEFAULT dead-peer-detection interval '30'
set vpn ipsec ike-group IKEv2_DEFAULT dead-peer-detection timeout '120'
set vpn ipsec ike-group IKEv2_DEFAULT ikev2-reauth 'no'
set vpn ipsec ike-group IKEv2_DEFAULT key-exchange 'ikev2'
set vpn ipsec ike-group IKEv2_DEFAULT lifetime '10800'
set vpn ipsec ike-group IKEv2_DEFAULT mobike 'disable'
set vpn ipsec ike-group IKEv2_DEFAULT proposal 10 dh-group '19'
set vpn ipsec ike-group IKEv2_DEFAULT proposal 10 encryption 'aes256gcm128'
set vpn ipsec ike-group IKEv2_DEFAULT proposal 10 hash 'sha256'
set vpn ipsec interface eth0
set vpn ipsec site-to-site peer 192.0.2.11 authentication id 'C=GB, ST=Some-State,␣
↪L=Some-City, O=VyOS, CN=R2'
set vpn ipsec site-to-site peer 192.0.2.11 authentication mode 'x509'
set vpn ipsec site-to-site peer 192.0.2.11 authentication remote-id 'C=GB, ST=Some-State,
↪ L=Some-City, O=VyOS, CN=R1'
set vpn ipsec site-to-site peer 192.0.2.11 authentication x509 ca-certificate CA
set vpn ipsec site-to-site peer 192.0.2.11 authentication x509 certificate R2
set vpn ipsec site-to-site peer 192.0.2.11 connection-type 'initiate'
set vpn ipsec site-to-site peer 192.0.2.11 ike-group 'IKEv2_DEFAULT'
set vpn ipsec site-to-site peer 192.0.2.11 ikev2-reauth 'inherit'
set vpn ipsec site-to-site peer 192.0.2.11 local-address 192.0.2.22
```

(continues on next page)

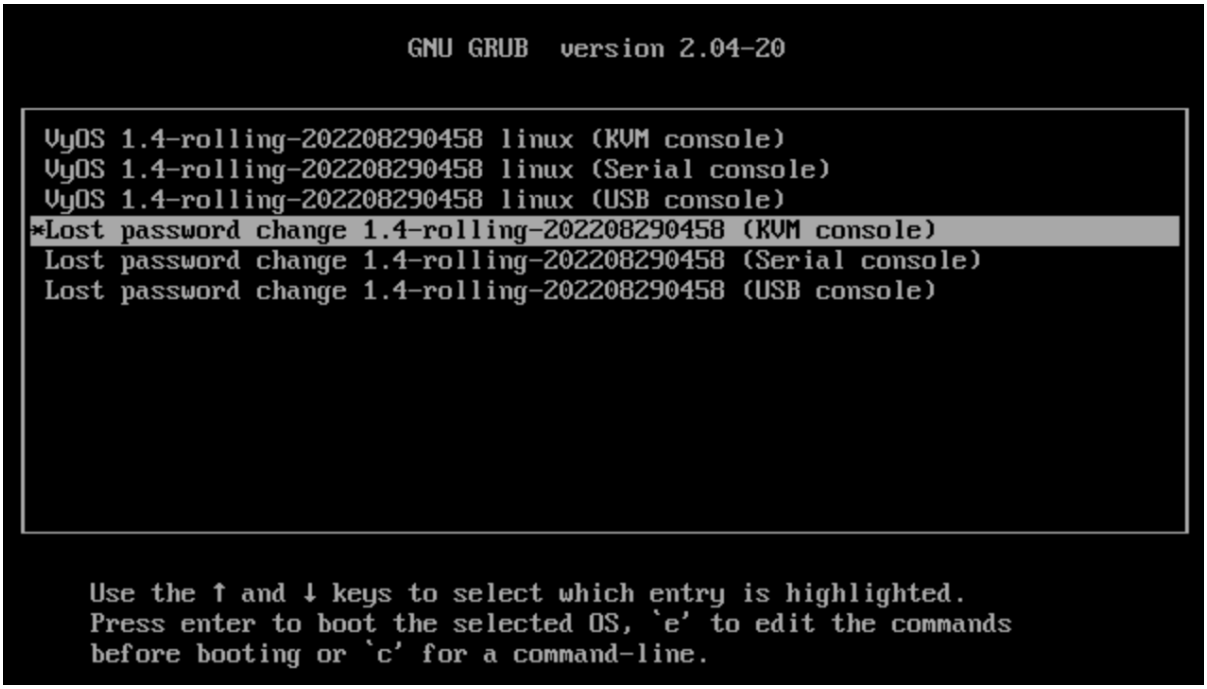
(continued from previous page)

```
set vpn ipsec site-to-site peer 192.0.2.11 vti bind 'vti10'
set vpn ipsec site-to-site peer 192.0.2.11 vti esp-group 'ESP_DEFAULT'
set vpn ipsec options disable-route-autoinstall
```

Note: Note the “authentication id” and “authentication remote-id”

1.2 Resetting the password

Using the console, restart the VyOS router. The GRUB menu appears. Select the relevant option from the GRUB menu and press Enter. The option must start with “Lost password change.”



The stand-alone user-password recovery tool starts running and prompts you to reset the local system user password.

```
Do you wish to reset the admin password? (y or n)
y
Which admin account do you want to reset?[vyos]
my_username
Enter my_username password:
Retype my_username password:
System will reboot in 10 seconds...
```