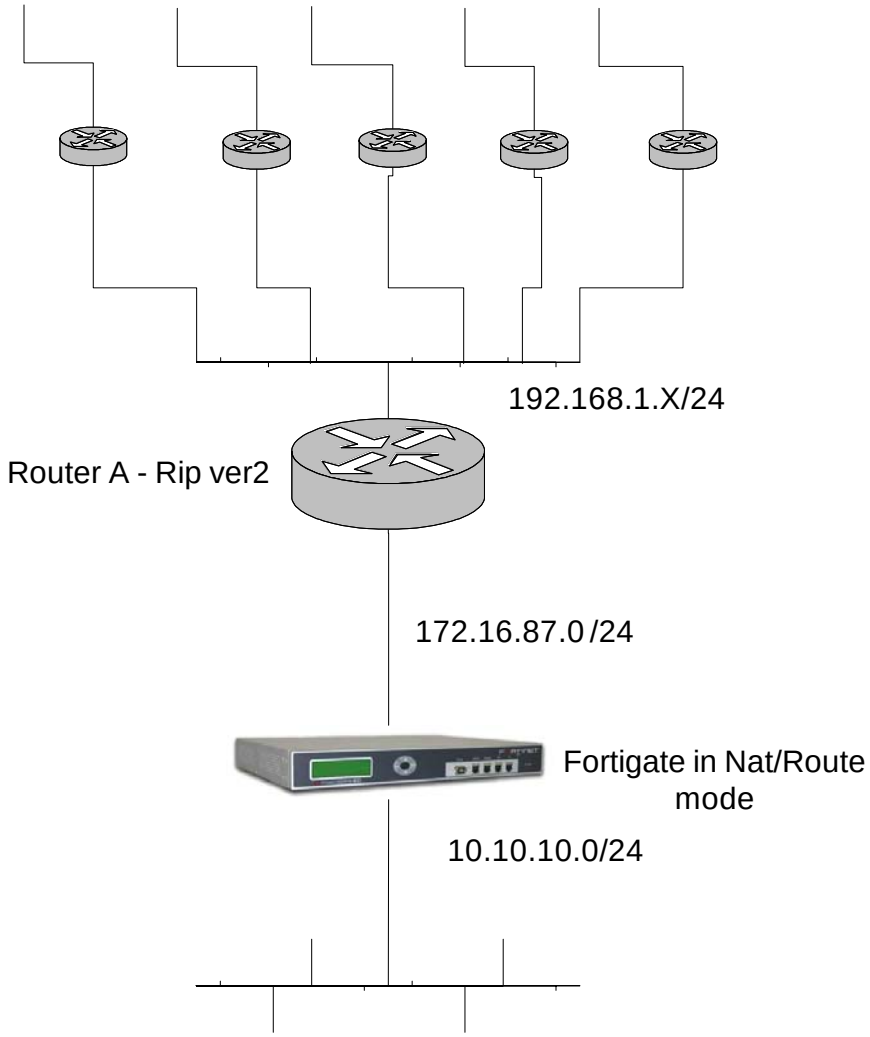
RIP Authentication - Cisco to Fortigate
FortiOS 2.80

Fig 1.1 - Sample network:



Network topology.

Figure 1.1 shows the sample network that is being described in this setup. The network can be any network that may be using RIP ver.2 to update routing information.

Router A shares Rip updates on the 192.168.1.0/24 network with the Fortigate. Fortigate requires Router A authenticate when sending Rip v.2 updates.

1. Configure Cisco Router A for Rip version 2.

```
>  config t
#  interface FastEthernet 0/0
#  ip address 192.168.1.2 255.255.255.0
#  router rip
#  network 192.168.0.0
#  network 172.16.87.0
#  version 2
```

2. Create keychains in Router A.

```
>  config t
# key chain rtrA
#  key 1
#  key-string 123
#  exit
#  key 2
#  key-string abc
```

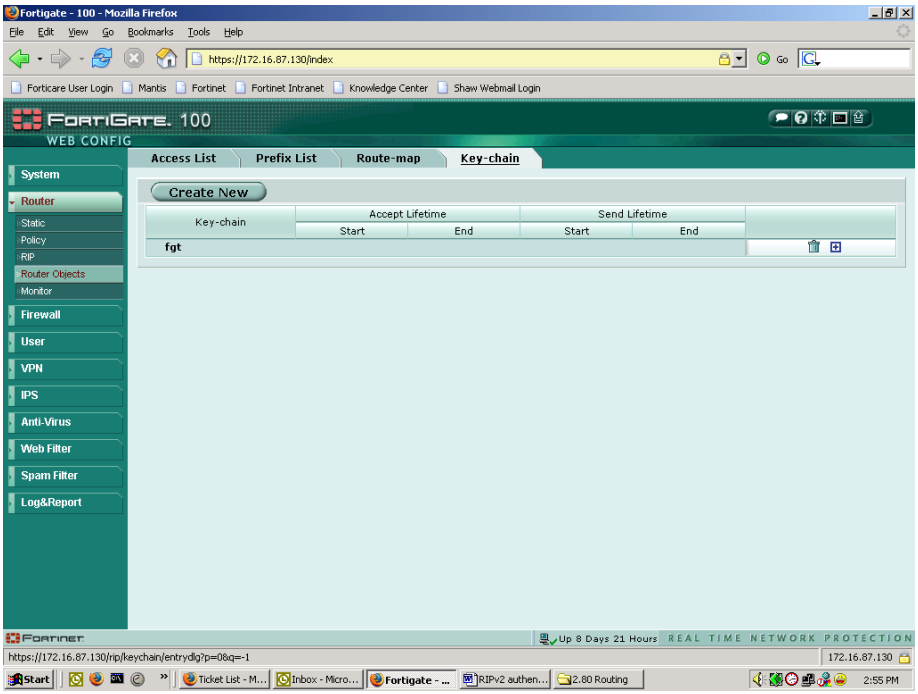
a. Configure authentication.

```
> config t
#  interface Fast Ethernet 0/0
#  ip rip authentication mode md5
#  ip rip authentication key-chain rtrA
```

3. Configure Fortigate for Rip version 2 using authentication.

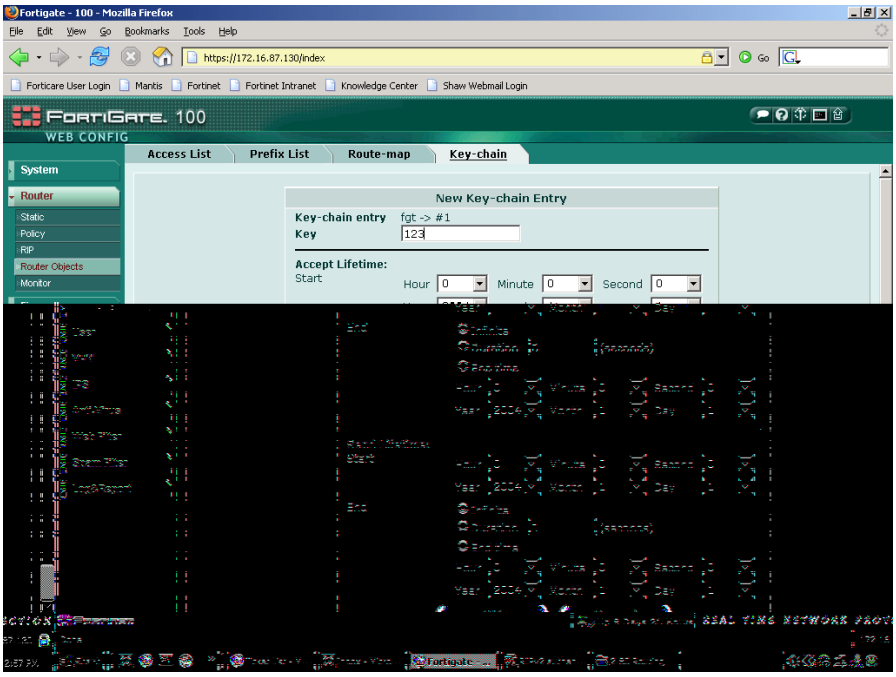
1. In Fortigate GUI, Router, Router Objects, KeyChain menu, add a new key chain.
2. Once this new chain is added, add the contents of the chain by selecting the plus sign button by the new key chain name.

Figure 3.1 Add keychain



3. Add the key contents and determine how long it will remain active. Example Figure 3.2

Figure 3.2 Keychain content and expiration

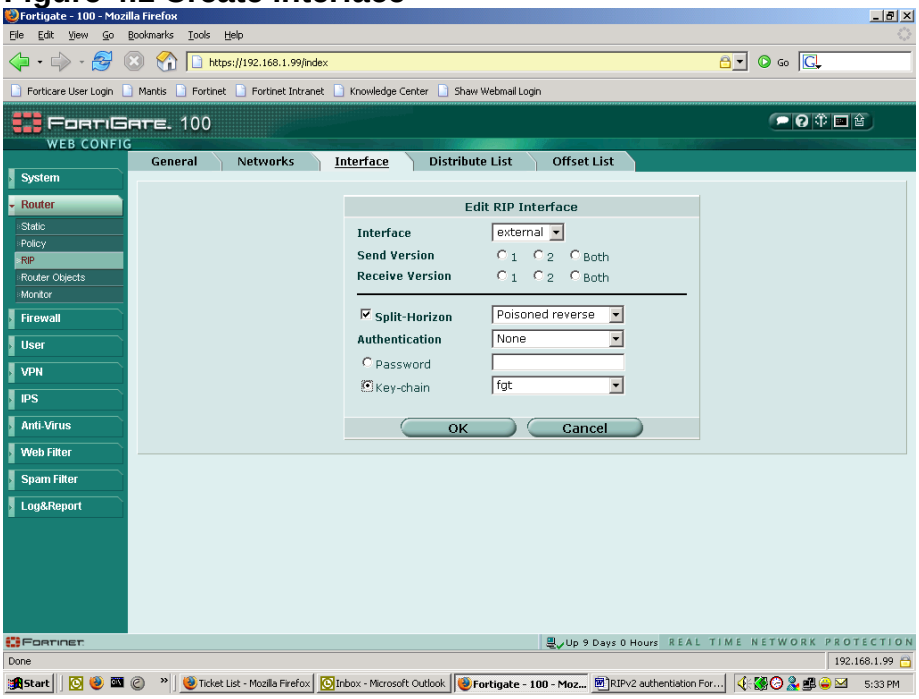


4. Router, RIP menus general tab. Enable RIP and designate a network for distribution.
   a. Enable RIP version 2 and designate a network.

4. Create Interface to be used when sending/receiving updates.

1. Create the Interface, figure 4.1, as the last step, which will specify on which Interface RIP information will be sent.
2. Router, RIP, general and Networks menu.
   a. Networks are 192.168.1.0/24 and 10.10.10.0/24
3. Choose the send and receiver versions and keychains and authentication to be used. Figure 4.1

Figure 4.1 Create interface



Diagnosing RIP configuration:

On the Fortigate, to get a simple output of what information is being shared and on what interface, use the get router RIP command.

get router rip:

```
get router rip info routing_table

Fortigate # get router info routing_table
Codes: K - kernel, C - connected, S - static, R - RIP, B - BGP
       O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2
       i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS
inter area
       * - candidate default

S*      0.0.0.0/0 [10/0] via 172.16.87.1, external
C       10.10.10.0/24 is directly connected, internal
C       172.16.87.0/24 is directly connected, external
```

Also:

```
Fortigate # get router info rip database

Codes: R - RIP, K - Kernel, C - Connected, S - Static, O - OSPF, I -
IS-IS,
       B - BGP

   Network            Next Hop         Metric From            If
Time
R  10.10.10.0/24                           1                internal
R  172.16.87.0/24                          1                external
```

For more in depth analysis of RIP events, use the “diag net router rip” set of commands

diag net router rip:

```
Fortigate-60 # diag net router rip
 all               Enable all debugging
 events            RIP events
 packet-receive    RIP receive events
 packet-send       RIP send events
```