Operating the Katzenpost mixnet

Table of Contents

Intro to do.

Management interface

Katzenpost provides a management interface that is accessed through a unix domain socket. The interface supports run-time changes to nodes without requiring a restart. By default, the management interface is disabled. To enable it,

For information about about configuring mixnet components, see....

The `socat` commandline utility can be use to connect to the management socket and issue commands. Connect with a commandline like so:

- `socat unix:/<path-to-data-dir>/management_sock STDOUT`

  The following commands are possible:

  - QUIT - Exit this management socket session.
  - SHUTDOWN - Cause the server to gracefully shutdown.
  - ADD_USER - Add a user and associate it with the given link key in either hex or base64. The syntax of the command is as follows:

    ```
    ADD_USER alice X25519_public_key_in_hex_or_base64
    ```

  - UPDATE_USER - Update the link key of a given user. The syntax of the command is as follows:

    ```
    UPDATE_USER alice X25519_public_key_in_hex_or_base64
    ```

  - REMOVE_USER - Remove a given user. The syntax of the command is as follows:

    ```
    REMOVE_USER alice
    ```

  - SET_USER_IDENTITY - Set a given user's identity key. The syntax of the command is as follows:

    ```
    SET_USER_IDENTITY alice X25519_public_key_in_hex_or_base64
    ```

  - REMOVE_USER_IDENTITY - Remove a given user's identity key. MUST be called before removing the user with the `REMOVE_USER` command. The synx of this command is as follows:

```
REMOVE_USER_IDENTITY alice
```

- USER_IDENTITY - Retrieve the identity key of the given user. The syntax of the command is as follows:

  ```
  USER_IDENTITY alice
  ```

- SEND_RATE - Sets the rate limiter to the given packets per minute rate.

  ```
  SEND_RATE 30
  ```

- SEND_BURST - Sets the rate limiter burst to the given maximum.

  ```
  SEND_BURST 4
  ```

Parameters (all) in server/config.

Go autogeneted docs: go to godocs.org and search for katezenpost/katzenpost. -- Baseic dev docs

Prometheus logging and graphing is to be recommended (has its own documents)

CLI usage for mix server components

Mix server components (mix nodes, gateway nodes, service nodes) may be controlled individually from the command line.

The mix server binary **pq-katzenpost-mixserver** has the following command-line usage:

```
$ pq-katzenpost-mixserver -h
Usage of ./pq-katzenpost-mixserver:
  -f string
        Path to the server config file. (default "katzenpost.toml")
  -g    Generate the keys and exit immediately.
```

The command output when generating keys looks like this:

```
./server -f my_katzenpost_mix_server.toml -g
22:51:55.377 NOTI server: Katzenpost is still pre-alpha.  DO NOT DEPEND ON IT F
22:51:55.377 NOTI server: AEZv5 implementation is hardware accelerated.
22:51:55.377 NOTI server: Server identifier is: 'example.com'
22:51:55.379 NOTI server: Server identity public key is: 2628F87F2806048C95F060
22:51:55.379 NOTI server: Server link public key is: CCDC5C105E649D543DF1CF397A
```

Note that if you choose to configure logging to a file one disk, you can implement log rotation by moving the log file and then sending the `HUP` to the authority server process. This will cause the daemon to rewrite the log file in the location specified by the config file.

Monitoring

`journalctl -u pq-katzenpost-mixserver -f -n 2000`

`iftop -t -s 18000 > log.txt &`

`bmon -p ens3`

Log the system stats and active process every 5 seconds

dwrob@hoh:~$ top -i -b -d 5 > top-watchdog.txt

Keep an eye on the active updating of that file

dwrob@hoh:~$ watch -d ls -l

Every 2.0s: ls -al top-watchdog.txt hoh: Sun Dec 4 11:06:17 2022

-rw-r--r-- 1 dwrob dwrob 16016638 Dec 4 11:06 top-watchdog.txt

Watch the actual updates

dwrob@hoh:~$ tail -f top-watchdog.txt

Capture net/disk/sys stats in CSV

dwrob@hoh:~$ dstat -tndcgy -N enp40s0 --output dstat.csv

And in general

```
dwrob@hoh:~$ bpytop
```

Service management

```
systemctl start pq-katzenpost-mixserver

systemctl stop pq-katzenpost-mixserver

systemctl restart pq-katzenpost-mixserver

systemctl enable pq-katzenpost-mixserver
```

Where are the files?

Docker test mixnet

As provided, the `docker` directory consists of a Makefile and and instructions for using it. Software prerequisites (other than Docker) are downloaded during installation, along with the Katzenpost source code, which is built and launched inside of a Docker container. For more information, see

Table 1.

Directory	File	Comment
`../katzenpost/docker`		
	`Makefile`	Makefile to build the test mixnet
	`README.rst`	Installation instructions
`../katzenpost/docker/voting_mixnet`		Only present after installation
`../katzenpost/docker/voting_mixnet/auth1`		
	authority.toml	
	identity.private.pem	
	identity.public.pem	

Single Katzenpost node in a production network

The example shows the components and configuration of a mix node. Other node types (gateway, service, and directory authority) have a corresponding binary executable, a TOML configuration file, a local private/public key pair, and public keys for each peer in the mixnet.

Table 2.

Directory	File	Comment
`/etc/pq-katzenpost-mixserver`		
	`katzenpost.toml`	Main configuration.
`/var/lib/pq-katzenpost-mixserver/`		
	`identity.private.pem`	Local node private identity key
	`identity.public.pem`	Local node public identity key
	`link.private.pem`	Local private key for encrypting Sphinx packages
	`link.public.pem`	Local public key for encrypting Sphinx packages
	`mixkey-145374.db`	Peer public identity key
	`mixkey-145375.db`	Peer public identity key (etc.)
`/usr/local/bin`		
	`pq-katzenpost-authority`	Directory authority executable
	`pq-katzenpost-mixserver`	Server executable (includes mix, gateway, and service nodes)

Using *gensphinx*

We need the required Go version...seems to be 1.23.

```
./gensphinx -h
Usage of ./gensphinx:
  -L int
        Number of mix layers. (default 3)
  -UserForwardPayloadLength int
        UserForwardPayloadLength (default 2000)
  -kem string
        Name of the KEM Scheme to be used with Sphinx
  -nike string
        Name of the NIKE Scheme to be used with Sphinx (default "x25519")
```

it might not be totally clear from the above usage that: -nike "" must be set if you want to use a KEM because you have to override the NIKE default value

not counting Gateway hop and service node hop, if "Number of mix layers" is set to 3 then that'd match what we normally deploy

but the super paranoid will want to increase that number

whereas in your description of gensphinx you didn't mention mix hop count

Tuning the Katzenpost mixnet

[introductory something]

This topic assumes that you have cloned the Katzenpost repository locally. The Python tuning script is located at the following location:

```
../katzenpost/tools/mixnet-params.py
```

Assuming uniform computational resources across all mix nodes in the network, the script compares a given Sphinx packets-per-second measurement with a set of tuning parameters, and assesses whether your Sphinx processing rate is fast enough.

Supplying the --help option displays a list of available configuration options.

```
$ python3 mixnet-params.py --help
Usage: mixnet-params.py [OPTIONS]

Options:
  --benchmark INTEGER
  --average-delay FLOAT      per second
  --gateways INTEGER
  --nodes-per-layer INTEGER
  --services INTEGER
  --users INTEGER
  --user-loops FLOAT         rate of decoy loops per second sent by users
  --user-traffic INTEGER     rate of real messages per second sent by user
  --node-loops FLOAT         rate of decoy loops per second sent by nodes
  --hops INTEGER
  -P, --LambdaP FLOAT        LambdaP (overrides --user-traffic)
  -L, --LambdaL FLOAT        LambdaL (overrides --user-loops)
  -M, --LambdaM FLOAT        LambdaP (overrides --node-loops)
  --help                     Show this message and exit.
```

```
git clone https://github.com/katzenpost/katzenpost.git;
cd katzenpost/core/sphinx
go test -bench=.

goos: linux
goarch: amd64
pkg: github.com/katzenpost/katzenpost/core/sphinx
cpu: 11th Gen Intel(R) Core(TM) i7-1165G7 @ 2.80GHz
BenchmarkSphinxCreatePackets/X25519_NIKE-8              792   1485541 ns/op
BenchmarkSphinxCreatePackets/X448_NIKE-8                469   2555925 ns/op
BenchmarkSphinxCreatePackets/CTIDH512_PQ_NIKE-8           1 3026375627 ns/op
BenchmarkSphinxCreatePackets/CTIDH512-X448_PQ_Hybrid_NIKE-8                1 30
BenchmarkSphinxCreatePackets/CTIDH1024_PQ_NIKE-8                           1 12
BenchmarkSphinxCreatePackets/CTIDH1024-X448_PQ_Hybrid_NIKE-8               1 12
BenchmarkSphinxCreatePackets/X25519_KEM-8                                1664
BenchmarkSphinxCreatePackets/X448_KEM-8                                  1090
BenchmarkSphinxCreatePackets/CTIDH512_PQ_KEM-8                              1 15
BenchmarkSphinxCreatePackets/CTIDH1024_PQ_KEM-8                             1 61
BenchmarkSphinxCreatePackets/MLKEM768_KEM-8                              2221
BenchmarkSphinxCreatePackets/sntrup4591761_KEM-8                           90  1
BenchmarkSphinxCreatePackets/FrodoKEM-640-SHAKE_KEM-8                      37  3
BenchmarkSphinxCreatePackets/Xwing_KEM-8                                 1203
BenchmarkSphinxCreatePackets/MLKEM768-X25519_KEM-8                       1016
BenchmarkSphinxCreatePackets/MLKEM768-X448_KEM-8                          793
```

```
BenchmarkSphinxCreatePackets/CTIDH512-X25519_PQ_Hybrid_KEM-8              1 140
BenchmarkSphinxCreatePackets/CTIDH1024-X448_PQ_Hybrid_KEM-8               1 569
BenchmarkSphinxUnwrap/X25519_NIKE-8                                     6342
BenchmarkSphinxUnwrap/X448_NIKE-8                                       4447
BenchmarkSphinxUnwrap/CTIDH512_PQ_NIKE-8                                   4 284
BenchmarkSphinxUnwrap/CTIDH512-X448_PQ_Hybrid_NIKE-8                       4 285
BenchmarkSphinxUnwrap/CTIDH1024_PQ_NIKE-8                                  1 118
BenchmarkSphinxUnwrap/CTIDH1024-X448_PQ_Hybrid_NIKE-8                      1 119
BenchmarkSphinxUnwrap/X25519_KEM-8                                     10000
BenchmarkSphinxUnwrap/X448_KEM-8                                        5158
BenchmarkSphinxUnwrap/CTIDH512_PQ_KEM-8                                    4 298
BenchmarkSphinxUnwrap/CTIDH1024_PQ_KEM-8                                   1 117
BenchmarkSphinxUnwrap/MLKEM768_KEM-8                                    8732
BenchmarkSphinxUnwrap/sntrup4591761_KEM-8                                165
BenchmarkSphinxUnwrap/FrodoKEM-640-SHAKE_KEM-8                           184
BenchmarkSphinxUnwrap/Xwing_KEM-8                                       6500
BenchmarkSphinxUnwrap/MLKEM768-X25519_KEM-8                             5428
BenchmarkSphinxUnwrap/MLKEM768-X448_KEM-8                               3285
BenchmarkSphinxUnwrap/CTIDH512-X25519_PQ_Hybrid_KEM-8                      4 288
BenchmarkSphinxUnwrap/CTIDH1024-X448_PQ_Hybrid_KEM-8                       1 121
PASS
ok   github.com/katzenpost/katzenpost/core/sphinx 177.826s
```

CLI usage for directory authorities

Directory authorities (dirauths) may be controlled individually from the command line.

The the dirauth binary **pq-katzenpost-authority** has the following command-pqline usage:

```
$ pq-katzenpost-authority -h
Usage of pq-katzenpost-authority:
  -f string
     Path to the authority config file. (default "katzenpost-authority.toml")
  -g Generate the keys and exit immediately.
  -v Get version info.
```

The `-f` parameter can be used to specify the full path and filename of the server configuration file, typically `/etc/pq-katzenpost-authority/katzenpost-authority.toml`.

The `-g` option is used to generate the public and private signing and link keys. By default, these must be manually copied to the directory defined by `DataDir` in /etc/pq-katzenpost-mixserver/