https://faelix.link/uknof40 — 2Mb

HOW WE FOUND A FIREWALL VENDOR BUG

# USING TELEPORT AS A BASTION JUMP HOST

# " THE INTERNET ISN'T WORKING! "

Calls to Exa Networks' support team

# THE TASK AT HAND

- Isn't affecting all customers
  - Initial suspicion of leased-line backhaul congestion...
  - ...but we found some DSL customers with problems too
- Intermittent, but not quite a heisenbug
- Manifested as timeout loading web pages
- All affected customers use Exa's new filtering service

# AIM TO TEST FROM CUSTOMERS' NETWORKS

- Put some probe devices in some customer networks
  - ...to be able to "ssh" into them, run measurements.
- Don't want customers to have to open ports on routers.
  - Some sort of NAT-piercing required.
- Security is vital:
  - Don't want probe to be an attack vector into customer.
- Team of staff need access.

SHOUT OUT #1

# IOT SECURITY

# (NETMCR #11)

@kooky_uk Tim Bray

SHOUT OUT #2

# SSH CERTIFICATES (NETMCR #13)

@TimJDFletcher Tim Fletcher

SHOUT OUT #3

# IOT SECURITY WITH PI.PE

# (NETMCR #17)

@steely_glint Tim Panton

SHOUT OUT #4

# RIPE ATLAS PROBE SECURITY (AQL IOT ROUNDTABLE)

@kistel Robert Kisteleki

# RIPE ATLAS

- Plug it in, gets address/DNS by DHCP
- Connects to RIPE bastion hosts using ssh (with provisioning)
- Creates tunnels to itself for telemetry, read all about it:
  - https://www.uknof.org.uk/uknof18/Kisteleki-Atlas.pdf
- Security rep is pretty good, e.g.
  - https://www.mdsec.co.uk/2015/09/an-introduction-to-hardware-hacking-the-ripe-atlas-probe/

# SSH BASTION HOSTS, WITH SSH CA

- The big players are doing it:
  - https://code.facebook.com/posts/365787980419535/scalable-and-secure-access-with-ssh/
  - https://github.com/Netflix/bless
- How to apply this pattern to our "IoT" probe project?

# WHY BOTHER USING TELEPORT?

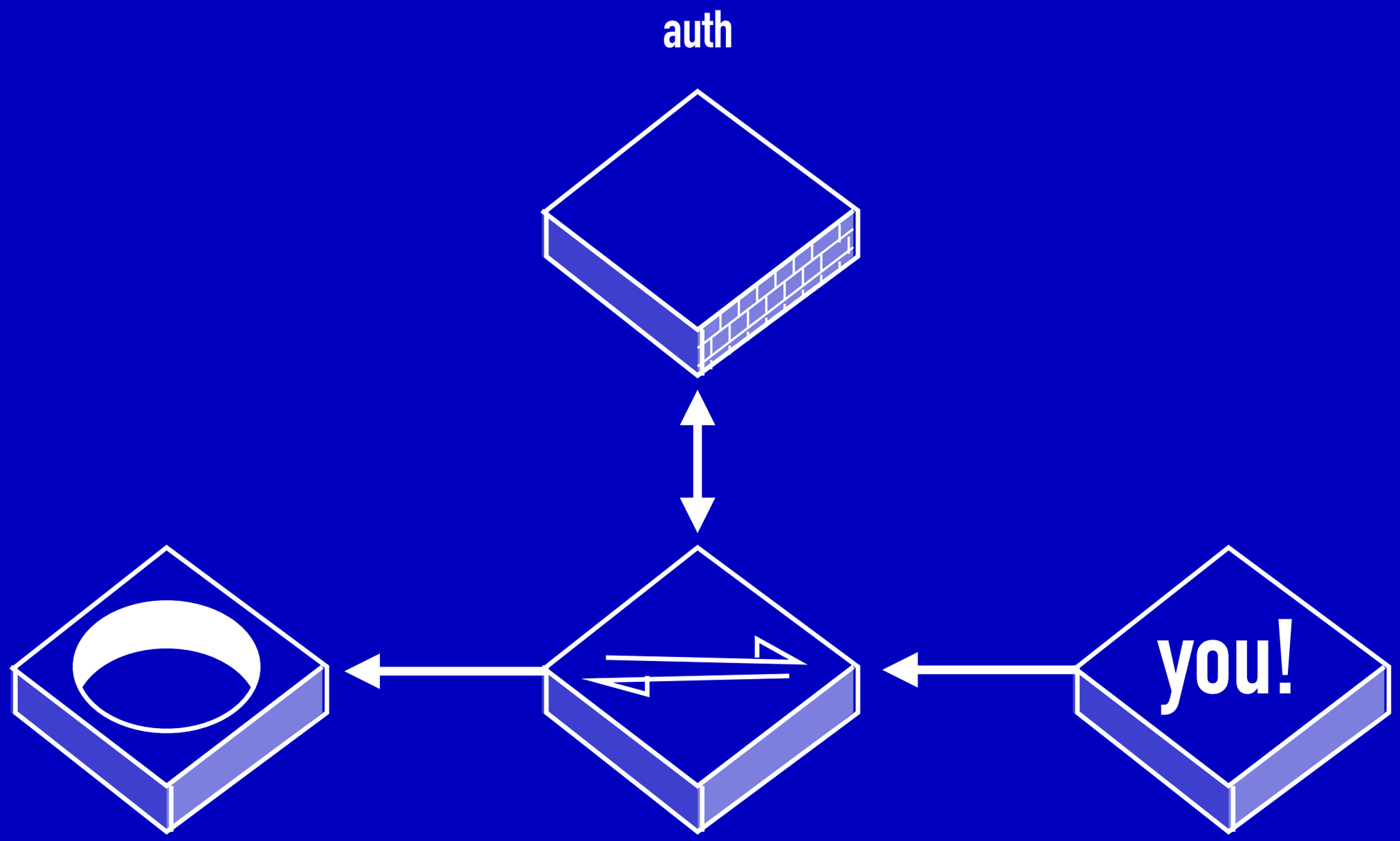
- **ssh CA** out of the box, compatible with OpenSSHd
- **2FA** out of the box (TOTP or U2F), no google_authenticator.pam
- ssh **through-the-web** out of the box
- Compliance Officer's dream: **session recording** jumphost.
  - ...and with "session_recording: proxy" it can do this for legacy sshd implementations too! [caveat: Security Officer]
- **Free OSS** < $aa$_startup_pricing_model < enterpri$$$e
  - $paid_editions feature include **RBAC**, LDAP/SASL integration

# THE SOLUTION

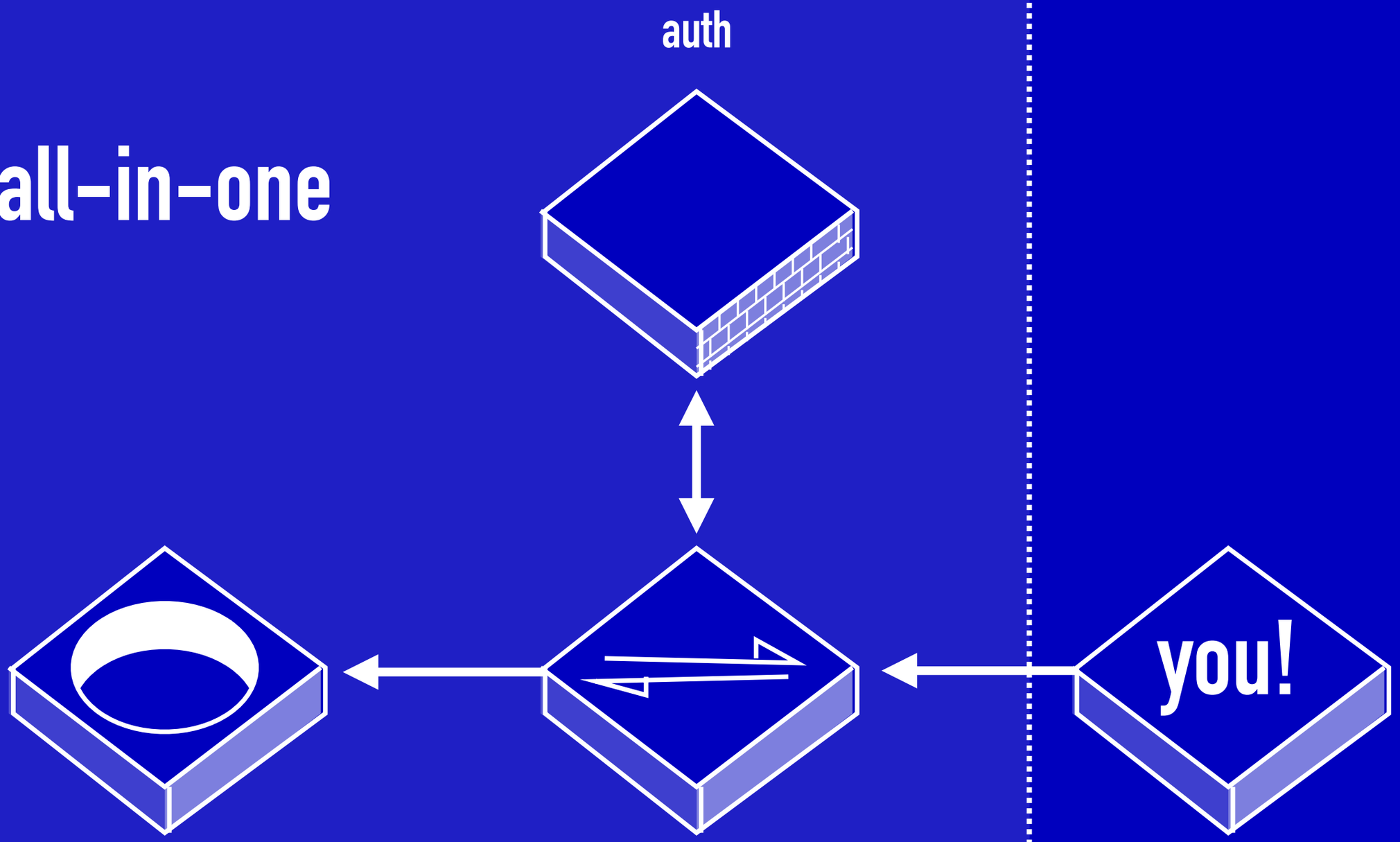
- Ansible script #1:
  - Deploys Teleport on a VM for bastion host
- Ansible script #2:
  - Installs Teleport on a Raspberry Pi
  - Preconfigures Teleport (as trusting cluster of bastion host)
- Bunch of Raspberry Pi / case / SD card combos
- Ship to customers with instructions about placement
  - Exa's software team can now run diagnostics

TELEPORT

# DEPLOYMENT


auth
you!
node
proxy
client
(tsh or https)

# all-in-one

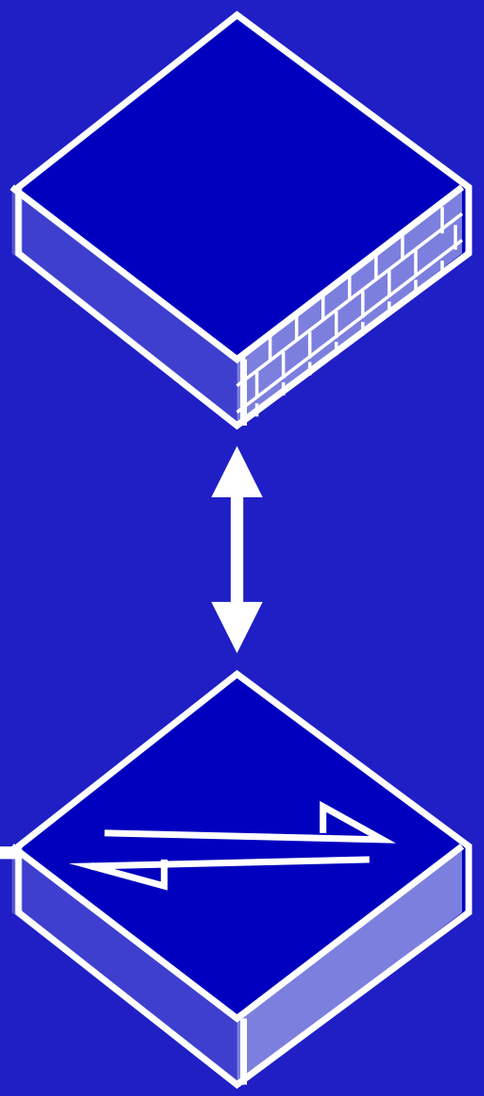


bastion

auth

node(s)

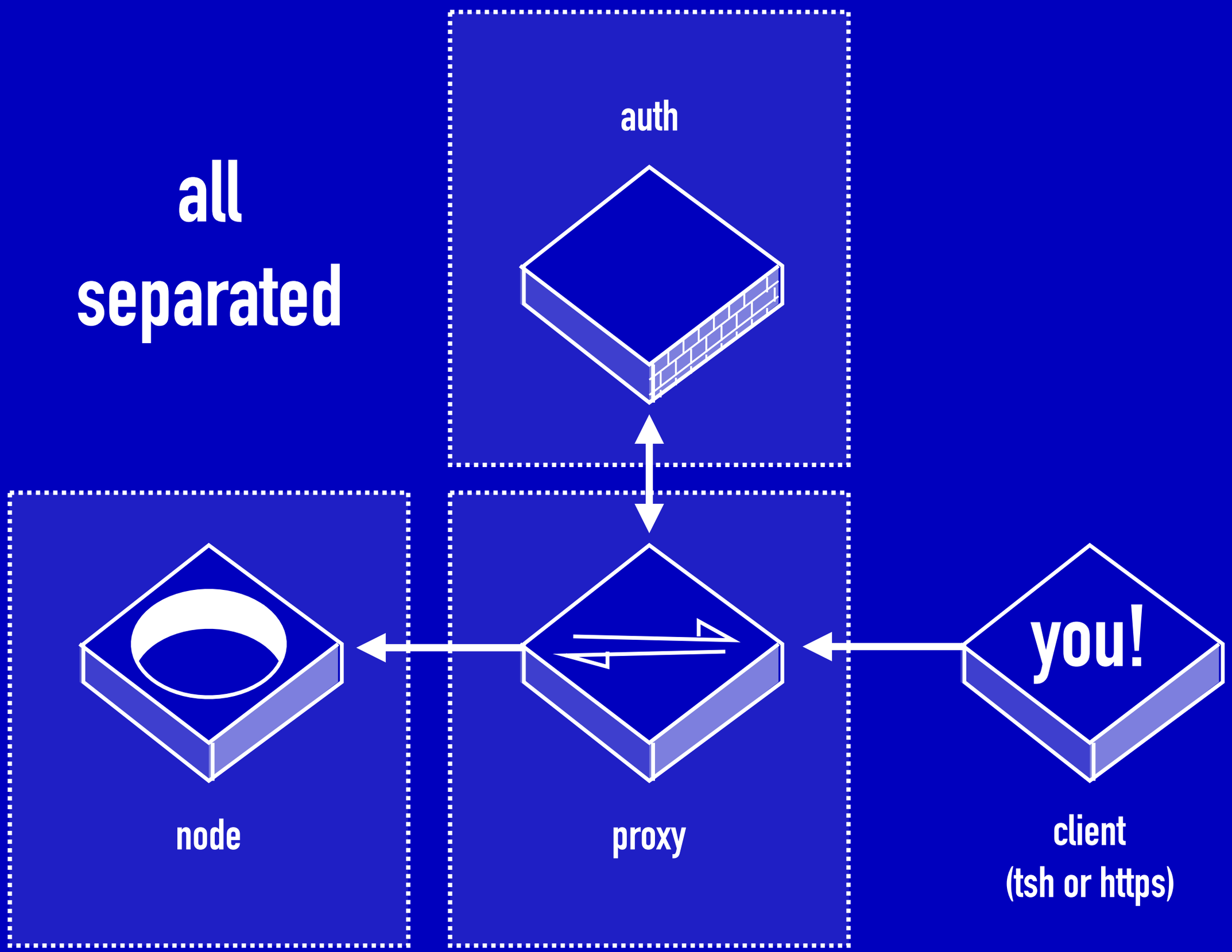
node



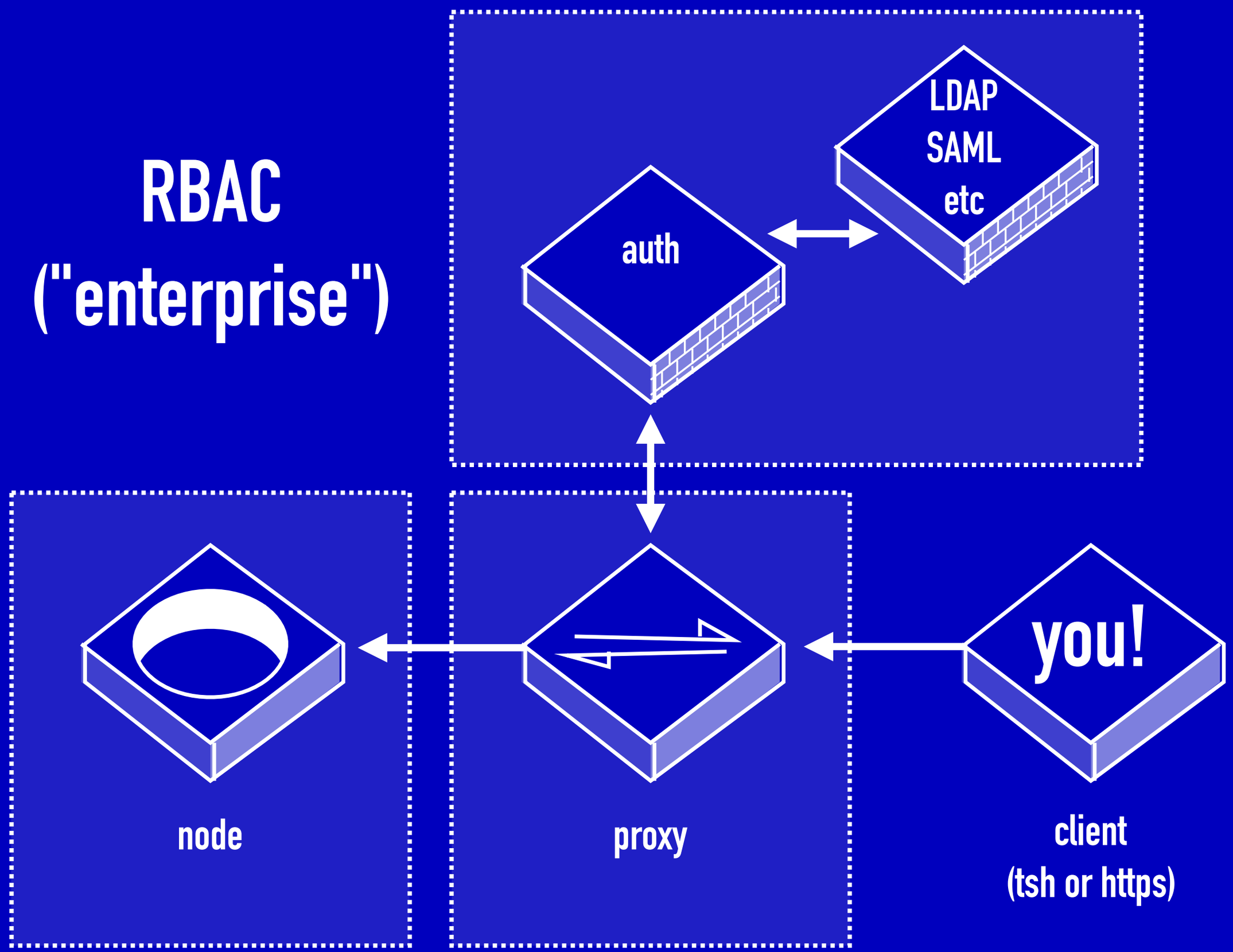
proxy


client
(tsh or https)

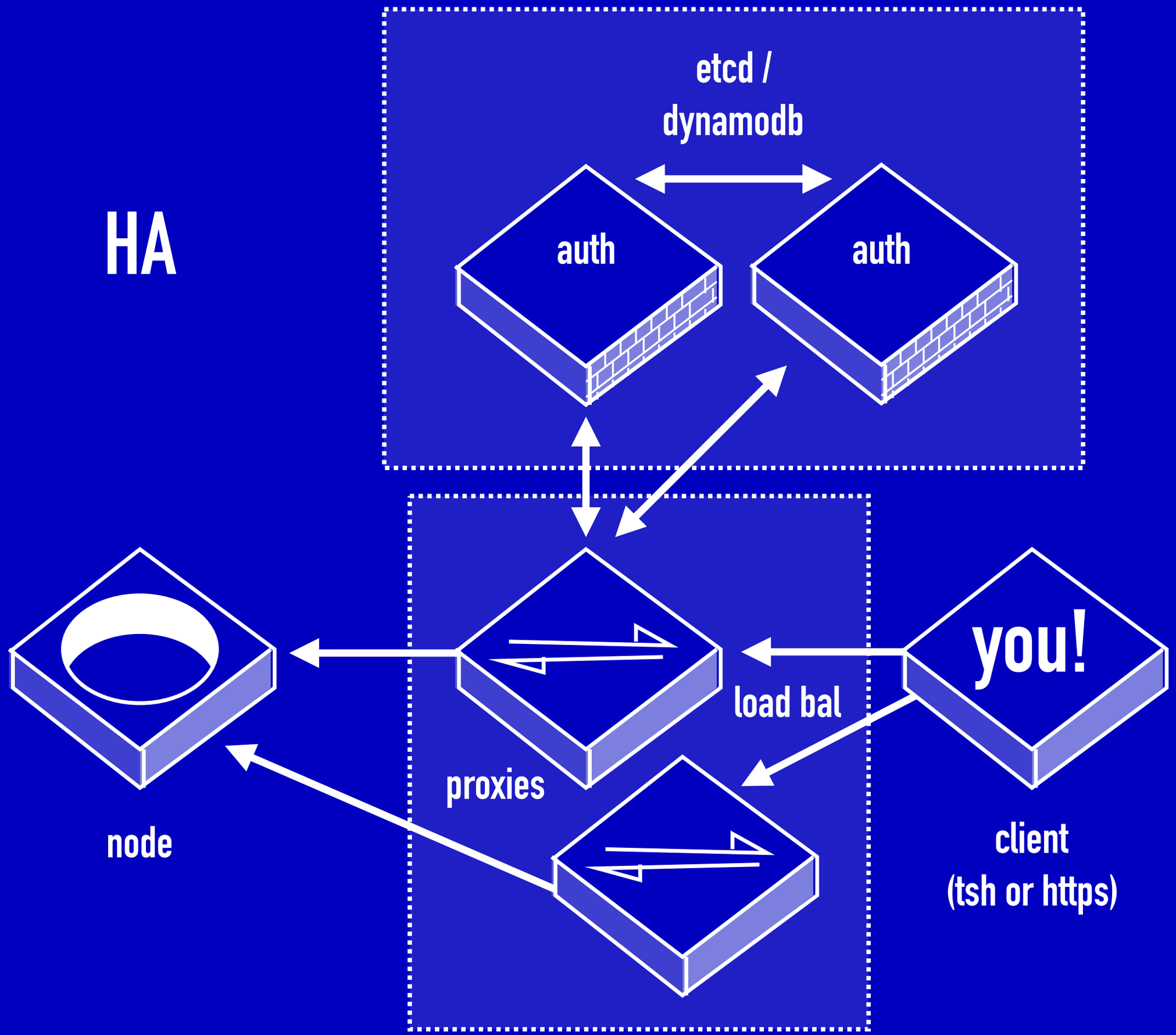
# all separated



# RBAC ("enterprise")



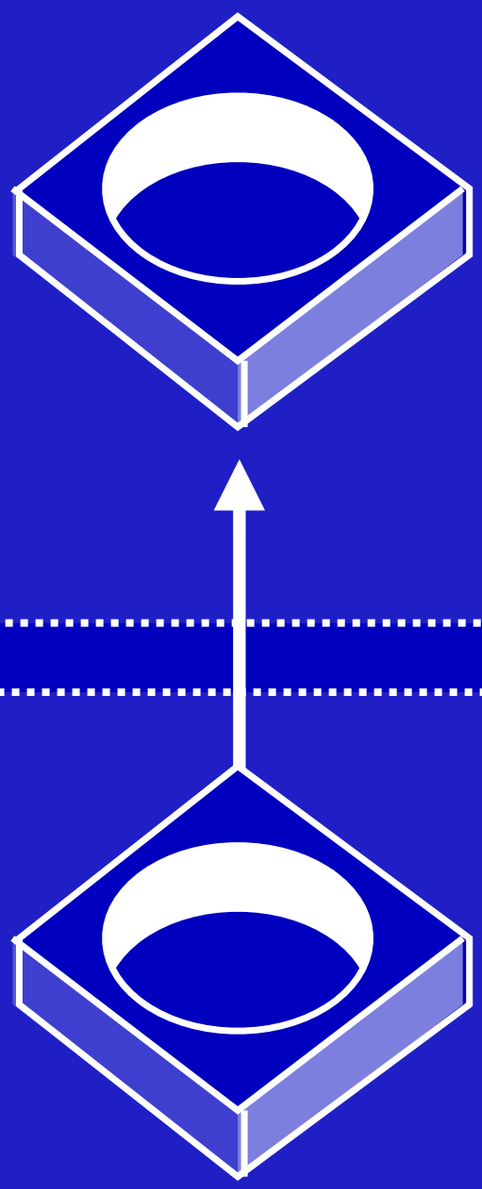
# HA

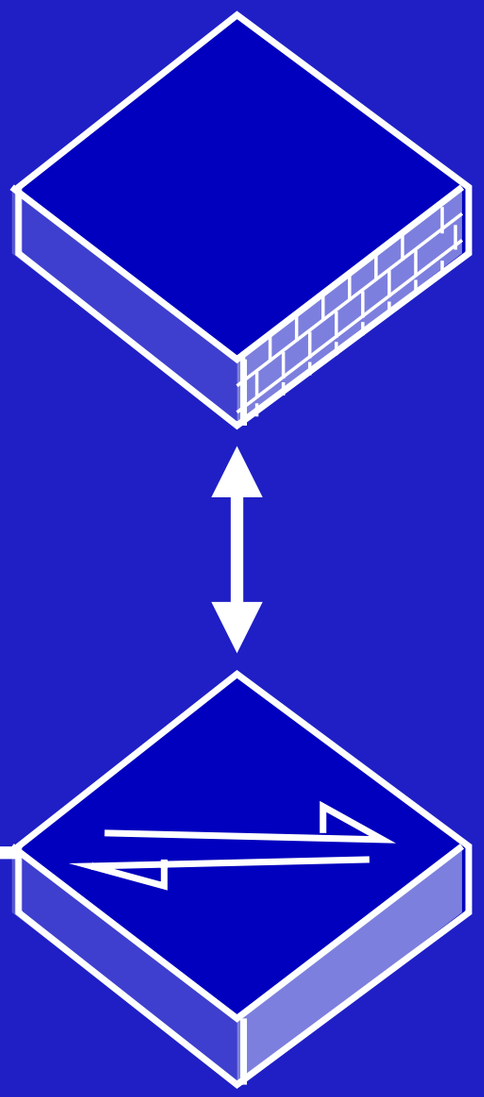

etcd /
dynamodb
auth
auth
load bal
proxies
you!
node
client
(tsh or https)

# bastion

another node

auth

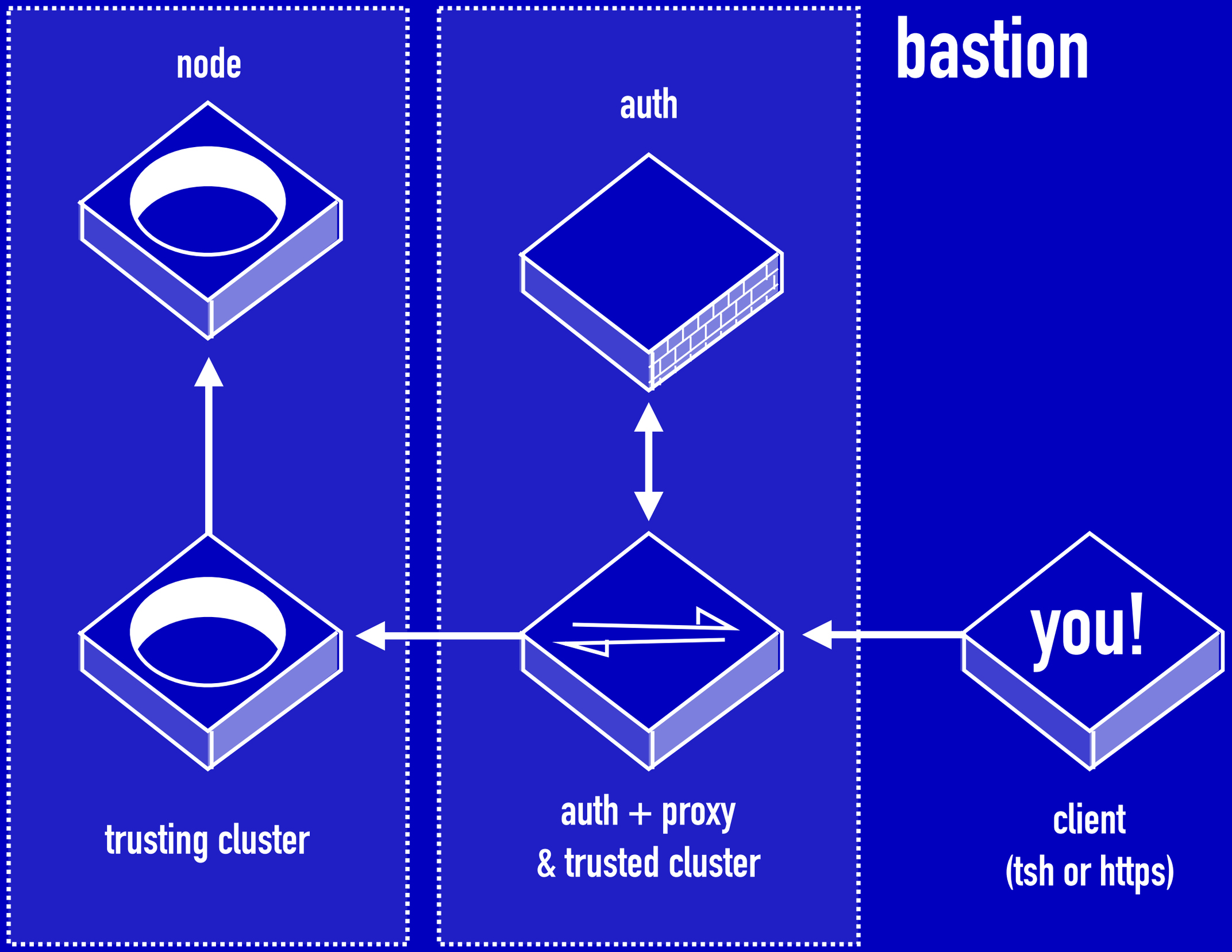




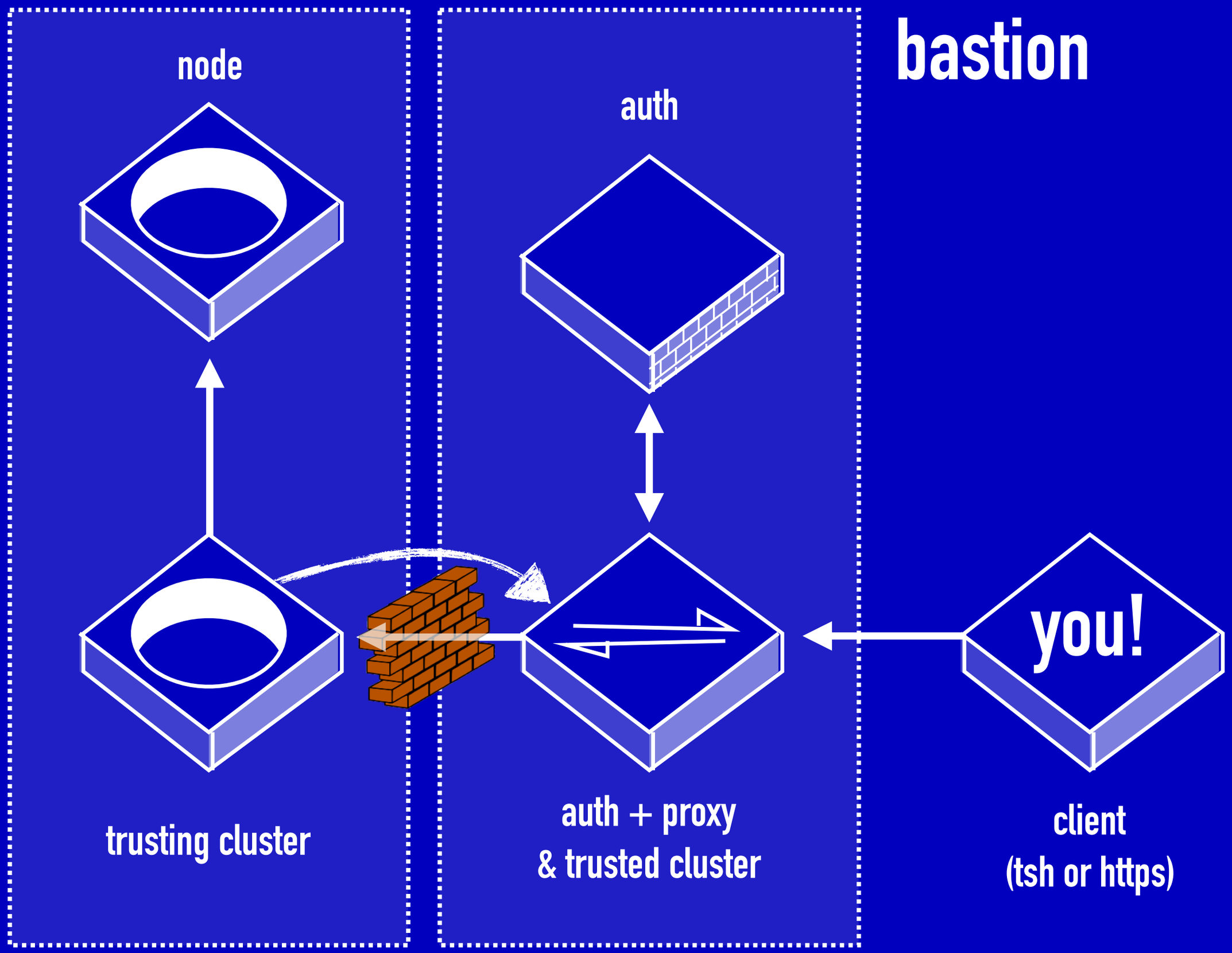

node
trusting cluster

auth + proxy
& trusted cluster

client
(tsh or https)


node
auth
bastion
you!
trusting cluster
auth + proxy
& trusted cluster
client
(tsh or https)

# bastion


node
auth
you!
trusting cluster
auth + proxy
& trusted cluster
client
(tsh or https)

```
tsh login
    --proxy teleport.example.com
    --user networkmoose
```

ssh-key -A

Teleport
BY GRAVITATIONAL

## Welcome to Teleport

marek.isalski

Password

123456

Login

**Google Authenticator**
Download Google Authenticator on your phone to access your two factor token

**New Account or forgot password?**
Ask for assistance from your Company administrator

M

## Nodes

| Hostname | Address |
|---|---|
| fulcrm197036 | 169.254.197.36:3022 |
| fulcrm197037 | 169.254.197.37:3022 |
| fulcrm197038 | 169.254.197.38:3022 |
| fulcrm200036 | 169.254.200.36:3022 |
| fulcrm200037 | 169.254.200.37:3022 |
| fulcrm200038 | 169.254.200.38:3022 |
| fulcrm200039 | 169.254.200.39:3022 |
| fulcrm201037 | 169.254.201.37:3022 |
| fulcrm201038 | 169.254.201.38:3022 |

```
root@fulcrm197036:~#
```

M

Cluster: fulcrm | Search... | login@hos

| Labels | Login as |
|---|---|
| role → base site → g | root |
| role → base site → g | root |
| role → base site → g | root |
| role → guts site → m | root |
| role → guts site → m | root |
| role → guts site → m | root |
| role → guts site → m | root |
| role → base site → m | root |
| role → base site → m | root |
| role → guts site → m | root |
| role → base site → m | root |
| role → base site → m | root |
| role → guts site → m | root |
| role → base site → w | root |
| role → base site → w | root |
| role → base site → w | root |
| role → shell | root |

"TWITCH FOR TERMINALS"

## Sessions

| Session ID | User |
|---|---|
| join 4a016316 ··· | marek [188.29.164.215] |
| play 63851632 ··· | marek [31.51.23.128] |
| play e5cd6928 ··· | marek [31.51.23.128] |
| play df7a5e6e ··· | marek [31.51.23.128] |
| play f8dc1d18 ··· | marek [90.155.74.40] |
| play 8e87e9a6 ··· | marek [90.155.74.40] |
| play 48df3876 ··· | marek [90.155.74.40] |
| play 21b48229 ··· | marek [127.0.0.1] |

```
[18995409.807928] [  630]     0   630    45747     1571       26
[18995409.807939] [26346]   107 26346     6858      107       16
[18995409.807949] [ 1788]     0  1788     3166       39       12
[18995409.807961] [ 6313]     0  6313    29041     3915       57
[18995409.807972] [ 6331]     0  6331   138127    12717      131
[18995409.807982] [ 6337]     0  6337    58951     4774       79
[18995409.807992] [ 6572]     0  6572   187483     1645       52
[18995409.808020] [11002]   107 11002  1407462   458715     1389
[18995409.808032] [11251]   107 11251     3387       35       13
[18995409.808043] [ 9994]   107  9994     3387       35       13
[18995409.808059] [ 9951]     0  9951     5082      144       15
[18995409.808069] Out of memory: Kill process 11002 (beam.smp) score
[18995409.808082] Killed process 11002 (beam.smp) total-vm:5629848kB
root@fulcrm201038:~# /et^C
root@fulcrm201038:~# ps ax | grep beam
10101 pts/0    S+     0:00 grep beam
root@fulcrm201038:~# /etc/init.d/rabbitmq-server restart
[ ok ] Restarting rabbitmq-server (via systemctl): rabbitmq-server.s
root@fulcrm201038:~#
```

▶ 03:36

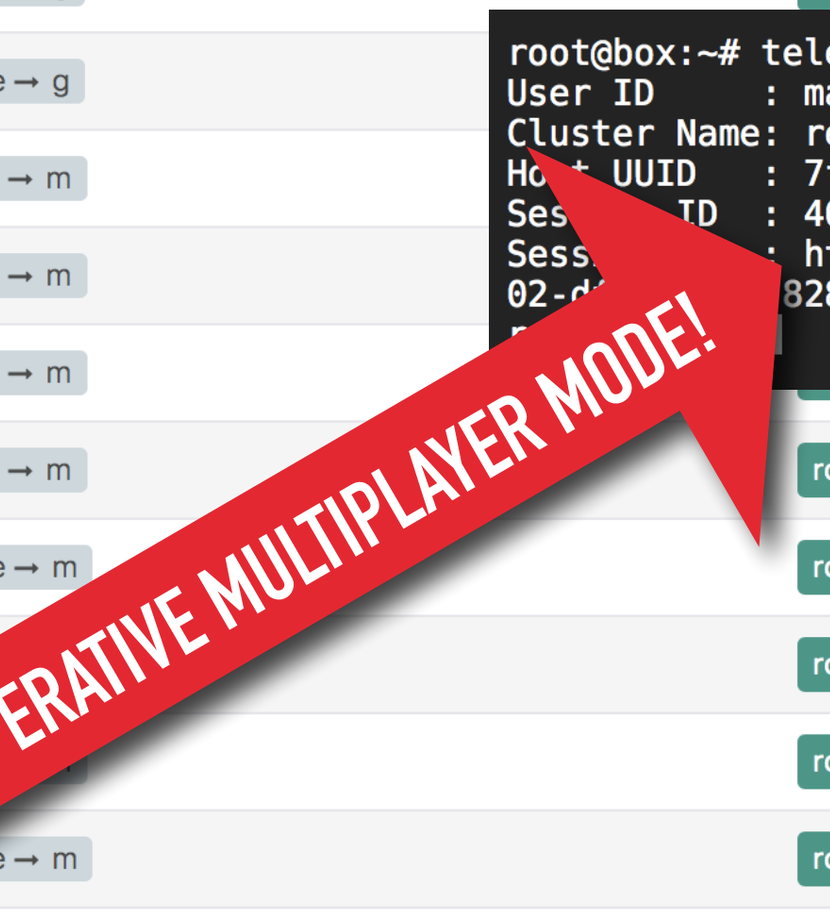
Cluster: fulcrm

Search...

login@hos

| Labels | Login as |
|---|---|
| role → base site → g | root |
| role → base site → g | root |
| role → base site → g | |
| role → guts site → m | |
| role → guts site → m | |
| role → guts site → m | |
| role → guts site → m | root |
| role → base site → m | root |
| | root |
| site → m | root |
| role → base site → m | root |
| role → guts site → m | root |
| role → base site → w | root |
| role → base site → w | root |
| role → base site → w | root |
| role → shell | root |

```
root@box:~# teleport status
User ID      : maz, logged in as root from 127.0.0.1 60986 3022
Cluster Name: rey.man.uk.teleport.faelix.net
Ho   UUID    : 7f3147bc-c31e-413e-8ebd-c1073fbd12fc
Ses      ID  : 46912402-df45-11e7-8286-aa0000ec2463
Sess         : https://teleport.faelix.net:3080/web/cluster/rey.man.uk
02-d    8286-aa0000ec2463
```




## Sessions

| Session ID | User |
|---|---|
| join 4a016316 ··· | marek [188.29.164.215] |
| play 63851632 ··· | marek [31.51.23.128] |
| play 48df3876 ··· | marek [90.155.74.40] |
| play 21b48229 ··· | marek [127.0.0.1] |

```
[18995409.807928] [  630]     0   630    45747     1571       26
[18995409.807939] [26346]   107 26346     6858      107       16
[18995409.807949] [ 1788]     0  1788     3166       39       12
[18995409.807961] [ 6313]     0  6313    29041     3915       57
[18995409.807972] [ 6331]     0  6331   138127    12717      131
[18995409.807982] [ 6337]     0  6337    58951     4774       79
[18995409.807992] [ 6572]     0  6572   187483     1645       52
[18995409.808020] [11002]   107 11002  1407462   458715     1389
[18995409.808032] [11251]   107 11251     3387       35       13
[18995409.808043] [ 9994]   107  9994     3387       35       13
[18995409.808059] [ 9951]     0  9951     5082      144       15
[18995409.808069] Out of memory: Kill process 11002 (beam.smp) score
[18995409.808082] Killed process 11002 (beam.smp) total-vm:5629848kB
root@fulcrm201038:~# /et^C
root@fulcrm201038:~# ps ax | grep beam
10101 pts/0    S+     0:00 grep beam
root@fulcrm201038:~# /etc/init.d/rabbitmq-server restart
[ ok ] Restarting rabbitmq-server (via systemctl): rabbitmq-server.s
root@fulcrm201038:~#
```

▶ 03:36


https://faelix.link/uknof40

# "...AND YOU WON'T BELIEVE WHAT HAPPENED NEXT..."

e: marek@faelix.net
t: @maznu