

VLAN Implementation Example

[*.Fluidity: Bring your telecoms infrastructure to the future*]

The VMware Lab

By **Charalampos Kapolonaris (Technical Lead)**
& Vasilios Koutlas (Software Tester)

.Fluidity VLAN Implementation Example

The Addressing Scheme

| .FLUIDITY VLAN EXAMPLE SYNOPSIS | | | |
|---------------------------------|--|---------------------------|--|
| .Fluidity Devices | External IP Address/External Interface | .Fluidity Device Password | List of Internal Interfaces on each .Fluidity Device |
| .Fluidity Server | 192.168.52.135/eth0 | _Fluidity-Server-2020 | Network 1: eth1 |
| .Fluidity Client 1 | 192.168.52.136/eth0 | _Fluidity_Client_1 | Network 2: eth1 |
| .Fluidity Client 2 | 192.168.52.137/eth0 | _Fluidity_Client_2 | Network 3: eth1 |

| VPN TUNNELING ADDRESSING SCHEME | | | | | |
|-----------------------------------|----------------|----------------|-----------------|-----------------|-------------------|
| Tunnel Connections | Server Address | Client Address | Subnet Mask | Network Address | Broadcast Address |
| Server - Client 1 (VPN NETWORK 1) | 192.168.54.1 | 192.168.54.2 | 255.255.255.252 | 192.168.54.0 | 192.168.54.3 |
| Server - Client 2 (VPN NETWORK 2) | 192.168.54.5 | 192.168.54.6 | 255.255.255.252 | 192.168.54.4 | 192.168.54.7 |

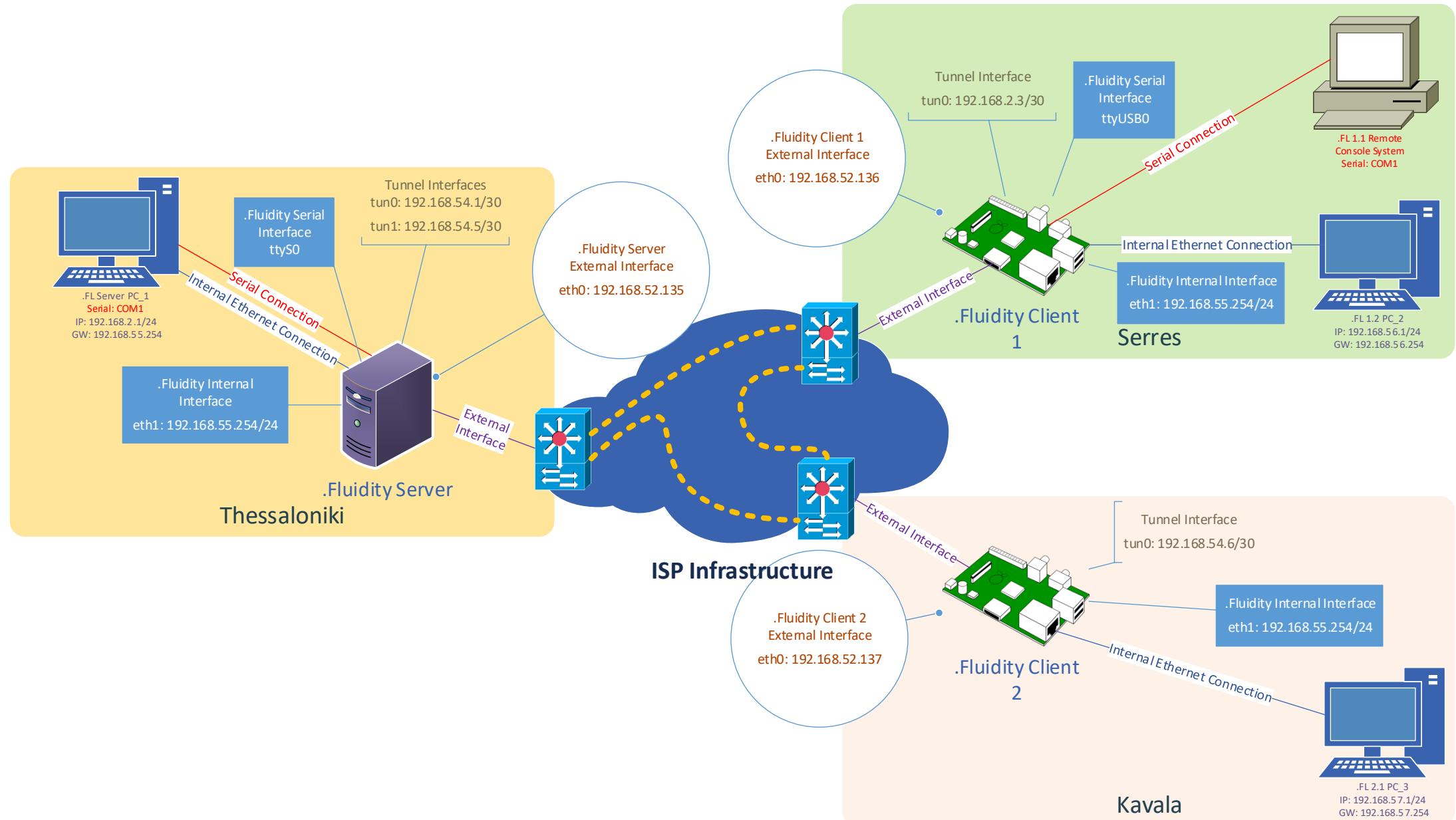
| SERIAL TUNNELING SCHEME | |
|-------------------------------------|--|
| Serial Tunnel to .FL Server | Serial Tunnel from .FL Client 1 |
| .FL Server PC_1 -> .Fluidity Server | .Fluidity Client 1 -> Remote Console System (FL 1.1) |

.Fluidity VLAN Implementation Example

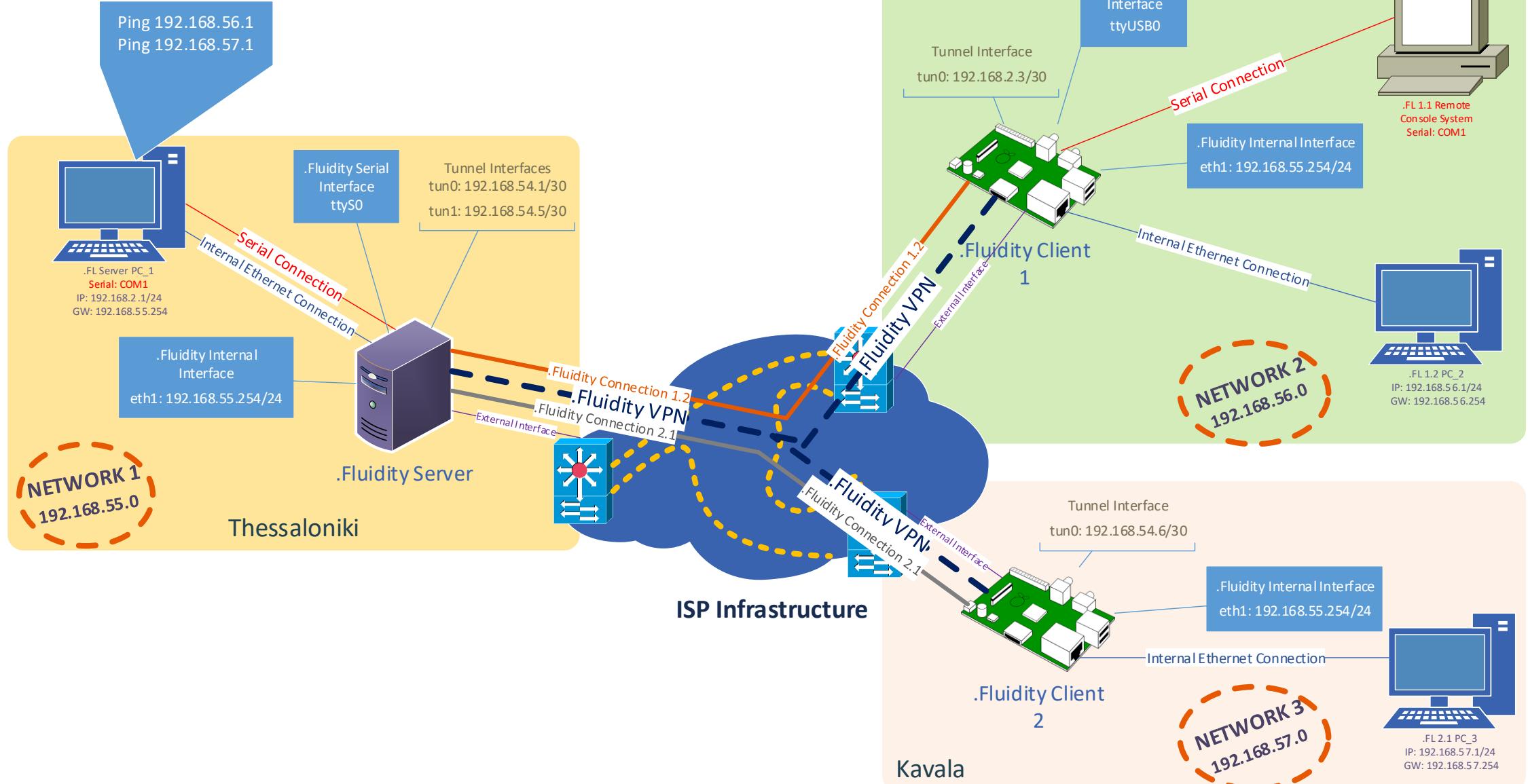
The Networking Scheme in Detail

| Devices Attached and the Networking Addressing Scheme in Detail | |
|---|-------------------|
| Network 1 | |
| CIDR Network Address | 192.168.55.0/24 |
| PC_1: | 192.168.55.1/24 |
| .Fluidity Server: | 192.168.55.254/24 |
| Broadcast Address | 192.168.55.255 |
| Network 2 | |
| CIDR Network Address | 192.168.56.0/24 |
| PC_2: | 192.168.56.1/24 |
| .Fluidity Client 1: | 192.168.56.254/24 |
| Broadcast Address | 192.168.56.255 |
| Network 3 | |
| CIDR Network Address | 192.168.57.0/24 |
| PC_3: | 192.168.57.1/24 |
| .Fluidity Client 3: | 192.168.57.254/24 |
| Broadcast Address | 192.168.57.255 |

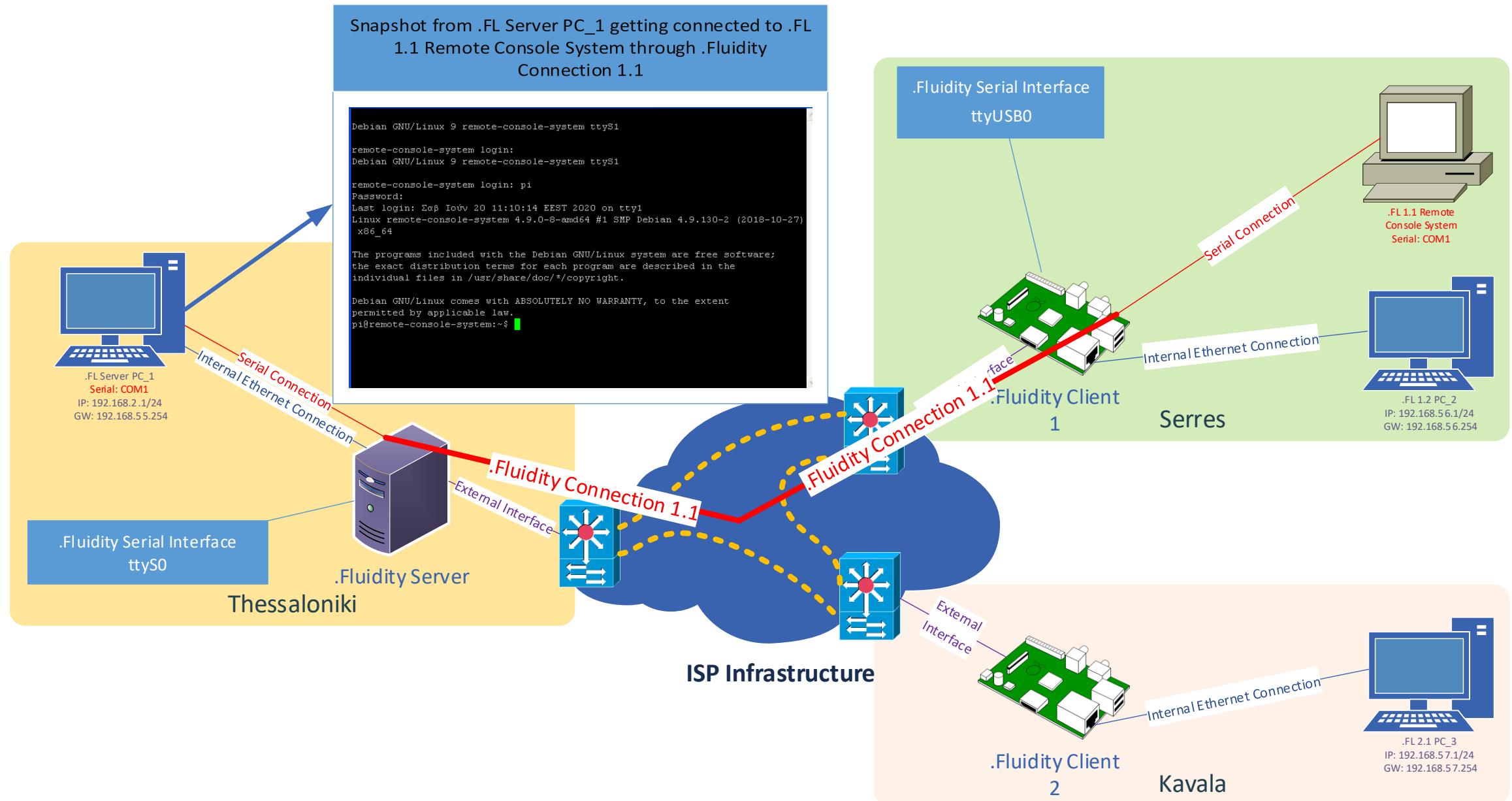
.Fluidity VLAN Example Visual Overview



.Fluidity VLAN Example VPN Networking Visual Overview



.Fluidity VLAN Example Serial Connectivity Visual Overview



.Fluidity VLAN Implementation Example

Step by step .Fluidity installation and configuration...

| Actions Performed | BASH Commands |
|---|--------------------|
| Load .Fluidity's Command Line Interface (CLI) | source Fluidity.sh |

| Actions Performed | .Fluidity Commands |
|--|---|
| Install the .Fluidity Server to device | installFluidity |
| Add the .Fluidity clients | |
| Add Client 1 | addFluidityClient 1 192.168.52.135 192.168.52.136 _Fluidity_Client_1 pi |
| Add Client 2 | addFluidityClient 2 192.168.52.135 192.168.52.137 _Fluidity_Client_2 pi |
| Attach networks to .Fluidity VPN network | |
| Attach network 1 to Server which is on eth1 | setInternalInterface eth1 |
| Attach network 2 to Client 1 which is on eth1 | Execute locally on Client 1: setInternalInterface eth1 |
| Attach network 3 to Client 2 which is on eth1 | Execute locally on Client 2: setInternalInterface eth1 |
| Add .Fluidity client connections | |
| Add a connection to Client 1 | addFluidityConnection 1 1 |
| Add a second connection to Client 1 | addFluidityConnection 1 2 |
| Add a connection to Client 2 | addFluidityConnection 2 1 |
| Do routing from .FL Server (Network 1) | |
| to Network 2 | addServerRoute ip route add 192.168.56.0/24 via 192.168.54.1 |
| to Network 3 | addServerRoute ip route add 192.168.57.0/24 via 192.168.54.5 |
| Do routing from .Fluidity Client 1 (Network 2) | |
| to Network 1 | addClientRoute 1 2 ip route add 192.168.55.0/24 via 192.168.54.2 |
| to Network 3 | addClientRoute 1 2 ip route add 192.168.57.0/24 via 192.168.54.2 |
| Do routing from .Fluidity Client 2 (Network 3) | |
| to Network 1 | addClientRoute 2 1 ip route add 192.168.55.0/24 via 192.168.54.6 |
| to Network 2 | addClientRoute 2 1 ip route add 192.168.56.0/24 via 192.168.54.6 |

.Fluidity VLAN Implementation Example

Lighting the Spark...

| List of VPN Connections | | | | | |
|---|-----------------|---|----------------------------|----------------------------|----------------------------|
| .Fluidity Client 1 Connection Parameters | | | | | |
| Connection Number | Connection Type | Server Listening Port | Server Tunnel Interface IP | Client Tunnel Interface IP | Tunnel Network Subnet Mask |
| 2 | Tunnel | 1441 | 192.168.54.1 | 192.168.54.2 | 30 |
| Initiate .Fluidity VPN connection to Client 1 | | <code>runFluidity -t 1 2 1441 192.168.54.1 192.168.54.2 30</code> | | | |
| Stop .Fluidity VPN connection to Client 1 | | <code>stopFluidity 1 2</code> | | | |
| .Fluidity Client 2 Connection Parameters | | | | | |
| Connection Number | Connection Type | Server Listening Port | Server Tunnel Interface IP | Client Tunnel Interface IP | Tunnel Network Subnet Mask |
| 1 | Tunnel | 1442 | 192.168.54.5 | 192.168.54.6 | 30 |
| Initiate .Fluidity VPN connection to Client 2 | | <code>runFluidity -t 2 1 1442 192.168.54.5 192.168.54.6 30</code> | | | |
| Stop .Fluidity VPN connection to Client 1 | | <code>stopFluidity 2 1</code> | | | |

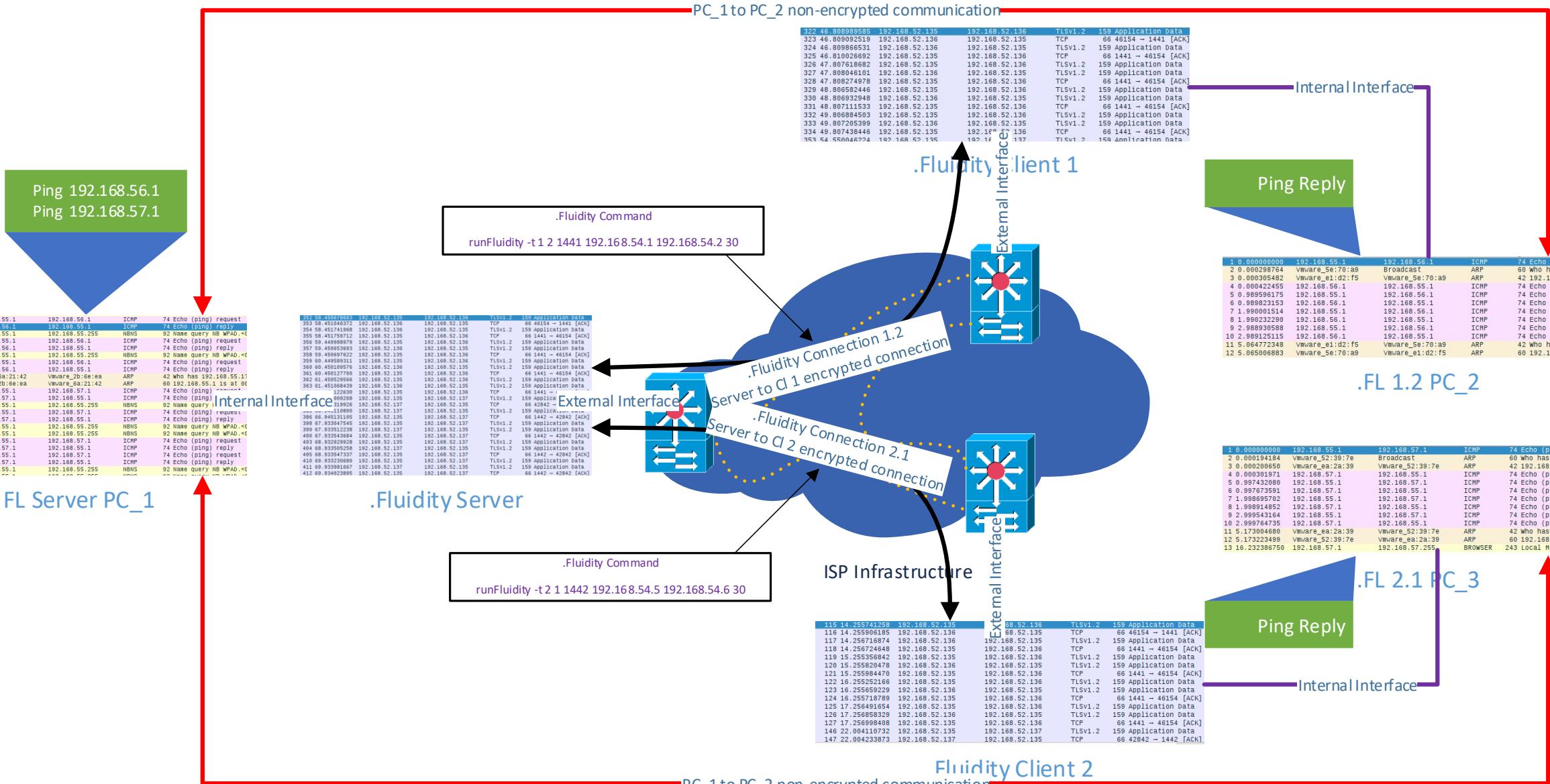
| List of Serial Connections | | | | | |
|--|-----------------|---|-------------------------|-------------------------|--------------|
| .Fluidity Client 1 Connection Parameters | | | | | |
| Connection Number | Connection Type | Server Listening Port | Server Serial Interface | Client Serial Interface | Serial Speed |
| 1 | Serial | 1440 | ttyS1 | ttyS1 | 115200 |
| Initiate .Fluidity serial connection to Client 1 | | <code>runFluidity -s 1 1 1440 ttyS1 ttyS1 115200</code> | | | |
| Stop .Fluidity serial connection to Client 1 | | <code>stopFluidity 1 1</code> | | | |

.Fluidity VLAN Implementation Example

[.Fluidity: Bring your telecoms infrastructure to the future]



The .Fluidity Network through Wireshark



.Fluidity VLAN Implementation Example

Step by step .Fluidity removal...

| Actions Performed | .Fluidity Commands |
|--|---|
| Remove routes from .FL Server (Network 1) | |
| to Network 2 | removeServerRoute ip route add 192.168.56.0/24 via 192.168.54.1 |
| to Network 3 | removeServerRoute ip route add 192.168.57.0/24 via 192.168.54.5 |
| Remove routes from .Fluidity Client 1 (Network 2) | |
| to Network 1 | removeClientRoute 1 2 ip route add 192.168.55.0/24 via 192.168.54.2 |
| to Network 3 | removeClientRoute 1 2 ip route add 192.168.57.0/24 via 192.168.54.2 |
| Remove routes from .Fluidity Client 2 (Network 3) | |
| to Network 1 | removeClientRoute 2 1 ip route add 192.168.55.0/24 via 192.168.54.6 |
| to Network 2 | removeClientRoute 2 1 ip route add 192.168.56.0/24 via 192.168.54.6 |
| Remove .Fluidity client connections | |
| Remove the #1 Connection from Client 1 | removeFluidityConnection 1 1 |
| Remove the #2 Connection from Client 1 | removeFluidityConnection 1 2 |
| Remove the #1 Connection from Client 2 | removeFluidityConnection 2 1 |
| Remove the .Fluidity clients | |
| Remove Client 1 | removeFluidityClient 1 |
| Remove Client 2 | removeFluidityClient 2 |
| Detach the networks from the .Fluidity VPN network | |
| Detach network 1 from Server which is on eth1 | removeInternalInterface eth1 |
| Detach network 2 from Client 1 which is on eth1 | Execute locally on Client 1: removeInternalInterface eth1 |
| Detach network 3 from Client 2 which is on eth1 | Execute locally on Client 2: removeInternalInterface eth1 |
| Remove the .Fluidity server | |
| ecryptFs unmount the .Fluidity Server folder | BASH: sudo umount Fluidity_Server |
| Remove the .Fluidity Server folder | BASH: rm -r Fluidity_Server |

.Fluidity VLAN Implementation Example – Visual Guided Tour

Step-by-step installation & configuration

```
pi@fluidity-server: ~
File Edit Tabs Help
pi@fluidity-server:~ $ source Fluidity.sh
pi@fluidity-server:~ $
```

1. source Fluidity.sh

Import .Fluidity's command set

```
pi@fluidity-server: ~
File Edit Tabs Help
pi@fluidity-server:~ $ installFluidity
```

2. installFluidity

Begin the installation process

```
Welcome to Fluidity first time setup utility.
Shall we proceed with the installation?
Type [yes]: Install Fluidity
Type [no]: Cancel and exit back to terminal
yes
```

2.1 installFluidity

Proceed? Yes or No?

```
pi@fluidity-server:~/Fluidity_Server
File Edit Tabs Help
Filename Encryption Key (FNEK) Signature [6329bc7f084af053]:
Attempting to mount with the following options:
ecryptfs_unlink_sigs
ecryptfs_fnek_sig=6329bc7f084af053
ecryptfs_key_bytes=32
ecryptfs_cipher=aes
ecryptfs_sig=6329bc7f084af053
WARNING: Based on the contents of [/root/.ecryptfs/sig-cache.txt],
it looks like you have never mounted with this key
before. This could mean that you have typed your
passphrase wrong.

Would you like to proceed with the mount (yes/no) : yes
Would you like to append sig [6329bc7f084af053] to
[/root/.ecryptfs/sig-cache.txt]
in order to avoid this warning in the future (yes/no) : yes
Successfully appended new sig to user sig cache file
Mounted eCryptfs

.ssh folder already exists
pi@fluidity-server:~/Fluidity_Server $
```

2.2 installFluidity

Finalizing the installation process

```
pi@fluidity-server:~/Fluidity_Server
File Edit Tabs Help
pi@fluidity-server:~/Fluidity_Server $ ifconfig
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500
inet 192.168.52.135 netmask 255.255.255.0 broadcast 192.168.52.255
inet6 fe80::96bc:ccfe%eth0 brd fe80::ff:fecc:96bc linklayer
ether 00:0c:29:71:2a:59 txqueuelen 1000 (Ethernet)
RX packets 390 bytes 47642 (46.5 KiB)
RX errors 0 dropped 0 overruns 0 frame 0
TX packets 330 bytes 45168 (44.1 KiB)
TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

eth1: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500
inet 192.168.55.254 netmask 255.255.255.0 broadcast 192.168.55.255
inet6 fe80::4678:e519:15f7:68ce brd fe80::ff:fe51:9678 linklayer
ether 00:0c:29:71:2a:63 txqueuelen 1000 (Ethernet)
RX packets 0 bytes 0 (0.0 B)
RX errors 0 dropped 0 overruns 0 frame 0
TX packets 24 bytes 3150 (3.0 KiB)
TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0
```

3. ifconfig

Observe the IP addresses on the externally connected eth0 interface and internally connected eth1 interface

```
pi@fluidity-server:~/Fluidity_Server
File Edit Tabs Help
pi@fluidity-server:~/Fluidity_Server $ addFluidityClient 1 192.168.52.135 192.168.52.136
_Fluidity_Client_1 pi
```

4. addFluidityClient 1

Add .Fluidity client 1 by using the IP addresses of the local (server) and remote (client) eth0 external designated interfaces

Next Slide

.Fluidity VLAN Implementation Example – Visual Guided Tour

Step-by-step configuration

Previous Slide

```
pi@fluidity-server:~/Fluidity_Server
Skipping adding existing rule
Skipping adding existing rule (v6)
Rule added
Status: active

To          Action    From
--          -----    ---
22/tcp      ALLOW     Anywhere
61263/tcp   ALLOW     192.168.52.135 # HFBCvIa7h 192.168.52.136
136         ALLOW     Anywhere (v6)

iptables: Bad rule (does a matching rule exist in that chain?).

Rule deleted
Rule deleted (v6)
iptables: Bad rule (does a matching rule exist in that chain?).

Seek And Encrypt token filename is: VFJK4FZYKJ
Seal 1 password is: CECbcQLrMemh2SZbar9Q==
Seal 2 password is: EPVpbp8VHqoW4CE7tq14EGA==
FlDaemon_SeekAndEncrypt.sh          100% 4569    7.2MB/s 00:00
FlDaemon_SeekAndEncrypt.service     100% 198     748.3KB/s 00:00
pi@fluidity-server:~/Fluidity_Server $
```

4.1 addFluidityClient 1

Finalizing client 1 installation

```
pi@fluidity-server:~/Fluidity_Server
Skipping adding existing rule
Skipping adding existing rule (v6)
Rule added
Status: active

To          Action    From
--          -----    ---
22/tcp      ALLOW     Anywhere
50923/tcp   ALLOW     192.168.52.135 # HFBCvIa7h 192.168.52.137
137         ALLOW     Anywhere (v6)

iptables: Bad rule (does a matching rule exist in that chain?).

Rule deleted
Rule deleted (v6)
iptables: Bad rule (does a matching rule exist in that chain?).

Seek And Encrypt token filename is: E4AWFEaL0Y
Seal 1 password is: e17ehnmJBINRRebVKLuRQ==
Seal 2 password is: 0b+NVngt681fG6i8DR44Rh==

FlDaemon_SeekAndEncrypt.sh          100% 4571    7.0MB/s 00:00
FlDaemon_SeekAndEncrypt.service     100% 198     697.3KB/s 00:00
pi@fluidity-server:~/Fluidity_Server $
```

5.1 addFluidityClient 2

Finalizing client 2 installation

```
pi@fluidity-server:~/Fluidity_Server
setInternalInterface eth1
Rule added
Rule added (v6)
Rule added
Rule added (v6)
pi@fluidity-server:~/Fluidity_Server $ sudo ufw status
Status: active

To          Action    From
--          -----    ---
Anywhere on eth1        ALLOW     Anywhere
Anywhere (v6) on eth1   ALLOW     Anywhere (v6)
Anywhere             ALLOW OUT   Anywhere on eth1
Anywhere (v6)          ALLOW OUT  Anywhere (v6) on eth1
pi@fluidity-server:~/Fluidity_Server $
```

6. setInternalInterface eth1

Server Side: Designate interface eth1 as an internal interface that traffic can go through it freely. Observe the orange frames indicating the change on firewall rules.

```
pi@fluidity-server:~/Fluidity_Server
pi@fluidity-server:~/Fluidity_Server $ addFluidityClient 2 192.168.52.135 192.168.52.137
_Fluidity_Client_2 pi
```

5. addFluidityClient 2

Add .Fluidity client 2 by using the IP addresses of the local (server) and remote (client) eth0 external designated interfaces

Next Slide

.Fluidity VLAN Implementation Example – Visual Guided Tour

Step-by-step configuration

Previous Slide

```
pi@fluidity-server: ~/Fluidity_Server
File Edit Tabs Help
pi@fluidity-server:~/Fluidity_Server $ addFluidityConnection 1 1
```

7. addFluidityConnection 1 1
Add connection 1 to client 1

```
pi@fluidity-server: ~/Fluidity_Server
File Edit Tabs Help
in order to avoid this warning in the future (yes/no) : yes
Successfully appended new sig to user sig cache file
Mounted eCryptfs
rm: cannot remove '/home/pi/Fluidity_Client/connection.1.1/tokenSlot/*': No such file or
directory
VFK3AFZYKJ
100% 65 164.1KB/s 00:00
.....
spawn openssl req -new -key servercon.1.1.key -x509 -days 3653 -subj /C=GR/ST=Serres/L=Se
rres/O=OTE Group/OU=Infrastructure Team/CN=192.168.52.135 -out servercon.1.1.crt
Enter pass phrase for servercon.1.1.key:
.....
spawn openssl req -new -key clientcon.1.1.key -x509 -days 3653 -subj /C=GR/ST=Serres/L=Se
rres/O=OTE Group/OU=Infrastructure Team/CN=192.168.52.136 -out clientcon.1.1.crt
Enter pass phrase for clientcon.1.1.key:
clientcon.1.1.crt
clientcon.1.1.pem
servercon.1.1.crt
100% 1391 2.4MB/s 00:00
100% 3265 5.7MB/s 00:00
100% 1391 3.0MB/s 00:00
pi@fluidity-server:~/Fluidity_Server $
```

7.1 addFluidityConnection 1 1
Finalizing connection 1 1 installation

```
pi@fluidity-server: ~/Fluidity_Server
File Edit Tabs Help
pi@fluidity-server:~/Fluidity_Server $ addFluidityConnection 1 2
```

8. addFluidityConnection 1 2
Add connection 2 to client 1

```
pi@fluidity-server: ~/Fluidity_Server
File Edit Tabs Help
Mounted eCryptfs
[1]- Done ssh $40$3 'bash -s' < ~/Fluidity_Server/client.$SSH_ID/conn
ection.$1/genSCRIPT_BlockProcess.$1.sh
rm: cannot remove '/home/pi/Fluidity_Client/connection.1.2/tokenSlot/*': No such file or
directory
VFK3AFZYKJ
25MHHqM+DyVNzNTr
PkrOHNHULMIIsaQX
B6YPlfa/4BtNWUy
100% 65 162.4KB/s 00:00
.....
spawn openssl req -new -key servercon.1.2.key -x509 -days 3653 -subj /C=GR/ST=Serres/L=Se
rres/O=OTE Group/OU=Infrastructure Team/CN=192.168.52.135 -out servercon.1.2.crt
Enter pass phrase for servercon.1.2.key:
.....
spawn openssl req -new -key clientcon.1.2.key -x509 -days 3653 -subj /C=GR/ST=Serres/L=Se
rres/O=OTE Group/OU=Infrastructure Team/CN=192.168.52.136 -out clientcon.1.2.crt
Enter pass phrase for clientcon.1.2.key:
clientcon.1.2.crt
clientcon.1.2.pem
servercon.1.2.crt
100% 1391 2.0MB/s 00:00
100% 3265 5.7MB/s 00:00
100% 1391 3.0MB/s 00:00
pi@fluidity-server:~/Fluidity_Server $
```

8.1 addFluidityConnection 1 2
Finalizing connection 1 2 installation

```
pi@fluidity-server: ~/Fluidity_Server
File Edit Tabs Help
pi@fluidity-server:~/Fluidity_Server $ addFluidityConnection 2 1
```

9. addFluidityConnection 2 1
Add connection 1 to client 2

```
pi@fluidity-server: ~/Fluidity_Server
File Edit Tabs Help
Mounted eCryptfs
rm: cannot remove '/home/pi/Fluidity_Client/connection.2.1/tokenSlot/*': No such file or
directory
E4AWEFaL0Y
De2R+5VpnR8pmy8N
RQg3F7A70z6uht
x7R8EG8t//oqbG
100% 65 161.5KB/s 00:00
.....
spawn openssl req -new -key servercon.2.1.key -x509 -days 3653 -subj /C=GR/ST=Serres/L=Se
rres/O=OTE Group/OU=Infrastructure Team/CN=192.168.52.135 -out servercon.2.1.crt
Enter pass phrase for servercon.2.1.key:
.....
spawn openssl req -new -key clientcon.2.1.key -x509 -days 3653 -subj /C=GR/ST=Serres/L=Se
rres/O=OTE Group/OU=Infrastructure Team/CN=192.168.52.137 -out clientcon.2.1.crt
Enter pass phrase for clientcon.2.1.key:
clientcon.2.1.crt
clientcon.2.1.pem
servercon.2.1.crt
100% 1391 2.3MB/s 00:00
100% 3265 4.9MB/s 00:00
100% 1391 3.1MB/s 00:00
pi@fluidity-server:~/Fluidity_Server $
```

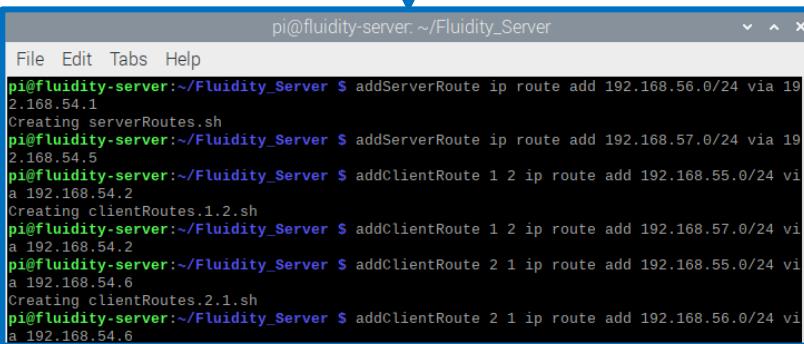
9.1 addFluidityConnection 2 1
Finalizing connection 2 1 installation

Next Slide

.Fluidity VLAN Implementation Example – Visual Guided Tour

Step-by-step configuration

Previous Slide



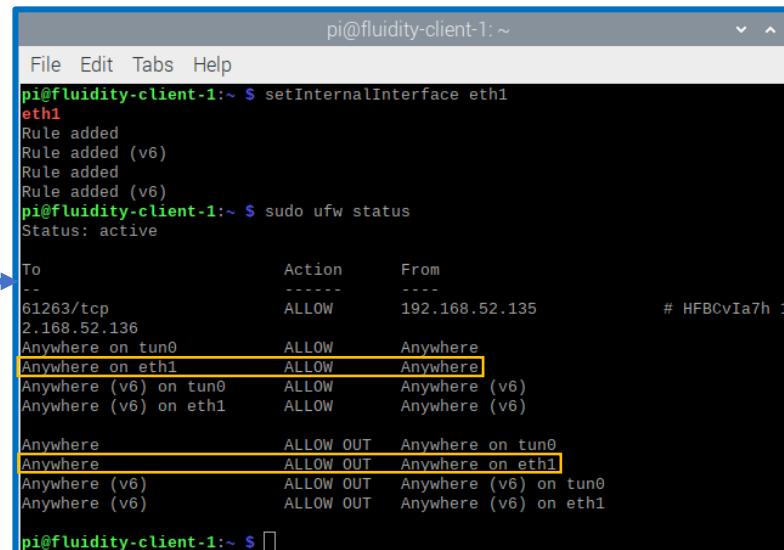
```
pi@fluidity-server:~/Fluidity_Server
File Edit Tabs Help
pi@fluidity-server:~/Fluidity_Server $ addServerRoute ip route add 192.168.56.0/24 via 192.168.54.1
Creating serverRoutes.sh
pi@fluidity-server:~/Fluidity_Server $ addServerRoute ip route add 192.168.57.0/24 via 192.168.54.5
Creating clientRoutes.1.2.sh
pi@fluidity-server:~/Fluidity_Server $ addClientRoute 1 2 ip route add 192.168.55.0/24 via 192.168.54.2
Creating clientRoutes.2.1.sh
pi@fluidity-server:~/Fluidity_Server $ addClientRoute 1 2 ip route add 192.168.57.0/24 via 192.168.54.2
pi@fluidity-server:~/Fluidity_Server $ addClientRoute 2 1 ip route add 192.168.55.0/24 via 192.168.54.6
Creating clientRoutes.2.1.sh
pi@fluidity-server:~/Fluidity_Server $ addClientRoute 2 1 ip route add 192.168.56.0/24 via 192.168.54.6
```

10. addServerRoute

- Instruct the server's OS to reach network 192.168.56.0/24 via the IP address 192.168.54.1
- Instruct the server's OS to reach network 192.168.57.0/24 via the IP address 192.168.54.5

10. addClientRoute

- Instruct client 1 connection 2 to reach network 192.168.55.0/24 via the IP address 192.168.54.2
- Instruct client 1 connection 2 to reach network 192.168.57.0/24 via the IP address 192.168.54.2
- Instruct client 2 connection 1 to reach network 192.168.55.0/24 via the IP address 192.168.54.6
- Instruct client 2 connection 1 to reach network 192.168.56.0/24 via the IP address 192.168.54.6



```
pi@fluidity-client-1:~ $ setInternalInterface eth1
eth1
Rule added
Rule added (v6)
Rule added
Rule added (v6)
pi@fluidity-client-1:~ $ sudo ufw status
Status: active

To                         Action      From
--                         --          --
61263/tcp                  ALLOW       192.168.52.135   # HFBCvIa7h 19
2.168.52.136
Anywhere on tun0             ALLOW      Anywhere
Anywhere on eth1             ALLOW      Anywhere
Anywhere (v6) on tun0        ALLOW      Anywhere (v6)
Anywhere (v6) on eth1        ALLOW      Anywhere (v6)

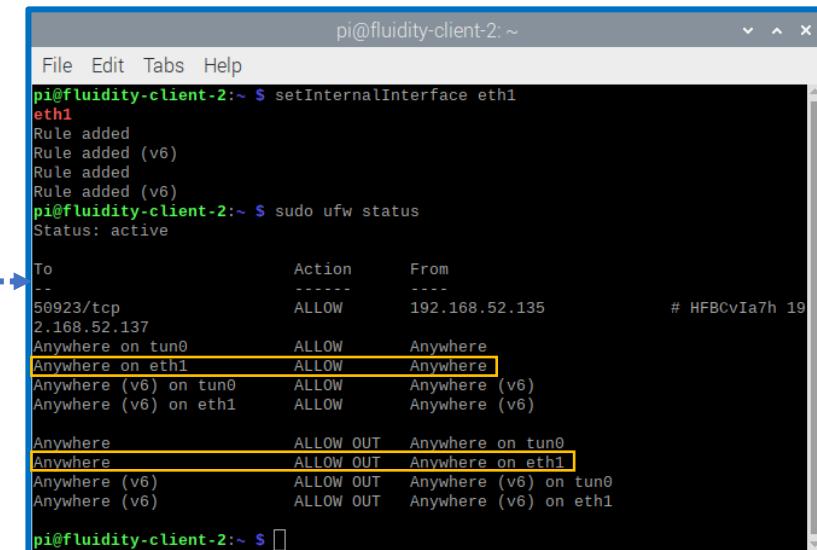
Anywhere                      ALLOW OUT   Anywhere on tun0
Anywhere                      ALLOW OUT   Anywhere on eth1
Anywhere (v6)                  ALLOW OUT   Anywhere (v6) on tun0
Anywhere (v6)                  ALLOW OUT   Anywhere (v6) on eth1

pi@fluidity-client-1:~ $
```

10. setInternalInterface eth0

Client 1 Side

- Designate interface eth0 as an internal interface that traffic can go through it freely.
- Observe the orange frames indicating the change on firewall rules.



```
pi@fluidity-client-2:~ $ setInternalInterface eth1
eth1
Rule added
Rule added (v6)
Rule added
Rule added (v6)
pi@fluidity-client-2:~ $ sudo ufw status
Status: active

To                         Action      From
--                         --          --
50923/tcp                  ALLOW       192.168.52.135   # HFBCvIa7h 19
2.168.52.137
Anywhere on tun0             ALLOW      Anywhere
Anywhere on eth1             ALLOW      Anywhere
Anywhere (v6) on tun0        ALLOW      Anywhere (v6)
Anywhere (v6) on eth1        ALLOW      Anywhere (v6)

Anywhere                      ALLOW OUT   Anywhere on tun0
Anywhere                      ALLOW OUT   Anywhere on eth1
Anywhere (v6)                  ALLOW OUT   Anywhere (v6) on tun0
Anywhere (v6)                  ALLOW OUT   Anywhere (v6) on eth1

pi@fluidity-client-2:~ $
```

11. setInternalInterface eth0

Client 2 Side

- Designate interface eth0 as an internal interface that traffic can go through it freely.
- Observe the orange frames indicating the change on firewall rules.



Next Slide

.Fluidity VLAN Implementation Example – Visual Guided Tour

.Fluidity execution

Previous Slide

pi@fluidity-server: ~/Fluidity_Server

File Edit Tabs Help

pi@fluidity-server:~/Fluidity_Server \$ runFluidity -s 1 1 1440 ttyS1 ttyS1 115200

12. runFluidity –s

Execute .Fluidity and link serial devices through an ethernet tunnel. This is .Fluidity for client 1 and connection 1, through port 1440, for local serial device at ttyUSB0, client serial device at ttyUSB0 for speed 9600.

pi@fluidity-server: ~/Fluidity_Server

File Edit Tabs Help

```
ls: cannot access '/home/pi/Fluidity_Client/connection.1.1/tokenSlot/resetSSL.txt': No such file or directory
servercon.1.1.pem MD5 is: bd367ce9a88d01ff1d28133a4154458e
servercon.1.1.crt MD5 is: bd367ce9a88d01ff1d28133a4154458e
clientcon.1.1.pem MD5 is: 9e82eee3f3ef428b0e9b12ac3d6242cf
clientcon.1.1.crt MD5 is: 9e82eee3f3ef428b0e9b12ac3d6242cf
doAClientServerMD5EquivalencyCheck PASSED
servercon.1.1.pem SHA256 is: a3fe671d18d66dc06f9c9fa7f46841b8
servercon.1.1.crt SHA256 is: a3fe671d18d66dc06f9c9fa7f46841b8
clientcon.1.1.pem SHA256 is: bb3f90252fa5f658f6a65f9934140506
clientcon.1.1.crt SHA256 is: bb3f90252fa5f658f6a65f9934140506
doAClientServerSHA256EquivalencyCheck PASSED
spawn socat openssl:192.168.52.135:1440,verify=1,cert=clientcon.1.1.pem,cafile=servercon.1.1.crt, /dev/ttyS1,b115200,echo=0,raw
Enter PEM pass phrase:tcp 0 0 192.168.52.135:1440 192.168.52.136:58340 ESTABLISHED 4659/socat
1440 ALLOW IN Anywhere
1440 (v6) ALLOW IN Anywhere (v6)

[3] Done reportWhenLinkIsEstablished $1 $3
[4] Done openTheTunnelInterfaces $1 $2 $3 $4 $9
[5]- Done deleteTokenFromClient $1 $3 $5 $6
[6]+ Done reportWhenFirewallRulesAreAdded $1 $3
pi@fluidity-server:~/Fluidity_Server $
```

12.1 runFluidity –s

.Fluidity reports that both MD5 and SHA256 SSL certificate hashes match, that for port 1440 a TCP link is established and that a firewall rule was added allowing traffic through port 1440.

pi@fluidity-server: ~/Fluidity_Server

File Edit Tabs Help

pi@fluidity-server:~/Fluidity_Server \$ runFluidity -t 1 2 1441 192.168.54.1 192.168.54.2 30

13. runFluidity –t

Execute .Fluidity and establish a tunnel link. The tunnel will consist of IP addresses 192.168.54.1 and 192.168.54.2 on server and client, respectively, to securely connect the networks attached on each .Fluidity device.

pi@fluidity-server: ~/Fluidity_Server

File Edit Tabs Help

```
servercon.1.2.pem MD5 is: d94192e22c2d70305675075d1de47eb
servercon.1.2.crt MD5 is: d94192e22c2d70305675075d1de47eb
clientcon.1.2.pem MD5 is: 24174a9cf4c022c7ff7af4bed74c5940
clientcon.1.2.crt MD5 is: 24174a9cf4c022c7ff7af4bed74c5940
doAClientServerMD5EquivalencyCheck PASSED
servercon.1.2.pem SHA256 is: 32906a30e0f95f02b033d1a6e19d83d5
servercon.1.2.crt SHA256 is: 32906a30e0f95f02b033d1a6e19d83d5
clientcon.1.2.pem SHA256 is: e5014222541d05e322adfa35de781a00
clientcon.1.2.crt SHA256 is: e5014222541d05e322adfa35de781a00
doAClientServerSHA256EquivalencyCheck PASSED
spawn sudo socat openssl:192.168.52.135:1441,verify=1,cert=clientcon.1.2.pem,cafile=servercon.1.2.crt, TUN:192.168.54.2/30,up
Enter PEM pass phrase:ready to execute
Error: Nexthop has invalid gateway.
tcp 0 0 192.168.52.135:1441 192.168.52.136:33340 ESTABLISHED -
```

1441 ALLOW IN Anywhere
1441 (v6) ALLOW IN Anywhere (v6)

```
[5] Done reportWhenLinkIsEstablished $1 $3
[6] Done openTheTunnelInterfaces $1 $2 $3 $4 $9
[7]- Done deleteTokenFromClient $1 $3 $5 $6
[8]+ Done reportWhenFirewallRulesAreAdded $1 $3
pi@fluidity-server:~/Fluidity_Server $
```

13.1 runFluidity –t

.Fluidity reports that both MD5 and SHA256 SSL certificate hashes match, that for port 1441 a TCP link is established and that a firewall rule was added allowing traffic through port 1441.

Next Slide

.Fluidity VLAN Implementation Example – Visual

Guided Tour

.Fluidity execution and a closer look to the SOCAT generated tunnels.

Previous Slide

```
pi@fluidity-server:~/Fluidity_Server
File Edit Tabs Help
pi@fluidity-server:~/Fluidity_Server $ runFluidity -t 2 1 1442 192.168.54.5 192.168.54.6 30
```

14. runFluidity -t

Execute .Fluidity and establish a tunnel link. The tunnel will consist of IP addresses 192.168.54.5 and 192.168.54.6 on server and client, respectively, to securely connect the networks attached on each .Fluidity device.

```
pi@fluidity-server:~/Fluidity_Server
File Edit Tabs Help
servercon.2.1.pem MD5 is: a2ccc367a4b5c5904ff28cf59544b713
servercon.2.1.crt MD5 is: a2ccc367a4b5c5904ff28cf59544b713
clientcon.2.1.pem MD5 is: b001bd728d789932421854da5eb5d591
clientcon.2.1.crt MD5 is: b001bd728d789932421854da5eb5d591
doClientServerMD5EquivalencyCheck PASSED
servercon.2.1.pem SHA256 is: c46122a83c16a69a331464156213a45a
servercon.2.1.crt SHA256 is: c46122a83c16a69a331464156213a45a
clientcon.2.1.pem SHA256 is: 7437eb4d95e78430bc737a913c870533
clientcon.2.1.crt SHA256 is: 7437eb4d95e78430bc737a913c870533
doClientServerSHA256EquivalencyCheck PASSED
spawn sudo socat openssl:192.168.52.135:1442,verify=1,cert=clientcon.2.1.pem,cafile=servercon.2.1.crt, TUN:192.168.54.6/30,up
Enter PEM pass phrase:RTNETLINK answers: File exists
tcp      0      0 192.168.52.135:1442  192.168.52.137:51974  ESTABLISHED -
ready to execute
1442          ALLOW IN    Anywhere
1442 (v6)      ALLOW IN    Anywhere (v6)
[7] Done          reportWhenLinkIsEstablished $1 $3
[8] Done          openTheTunnelInterfaces $1 $2 $3 $4 $9
[9]- Done         deleteTokenFromClient $1 $3 $5 $6
[10]+ Done        reportWhenFirewallRulesAreAdded $1 $3
pi@fluidity-server:~/Fluidity_Server $
```

14.1 runFluidity -t

.Fluidity reports that both MD5 and SHA256 SSL certificate hashes match, that for port 1442 a TCP link is established and that a firewall rule was added allowing traffic through port 1442.

```
tun0: flags=4305<UP,POINTOPOINT,RUNNING,NOARP,MULTICAST> mtu 1500
inet 192.168.54.1 netmask 255.255.255.252 destination 192.168.54.1
inet6 fe80::19c9:b1ae:a9c3:cc7b prefixlen 64 scopeid 0x20<link>
unspec 00-00-00-00-00-00-00-00-00-00-00-00-00-00-00 txqueuelen 500 (UNSPEC)
RX packets 68 bytes 3264 (3.1 KiB)
RX errors 0 dropped 0 overruns 0 frame 0
TX packets 67 bytes 3216 (3.1 KiB)
TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

tun1: flags=4305<UP,POINTOPOINT,RUNNING,NOARP,MULTICAST> mtu 1500
inet 192.168.54.5 netmask 255.255.255.252 destination 192.168.54.5
inet6 fe80::d0f4:3834:e840:a80b prefixlen 64 scopeid 0x20<link>
unspec 00-00-00-00-00-00-00-00-00-00-00-00-00-00 txqueuelen 500 (UNSPEC)
RX packets 68 bytes 3264 (3.1 KiB)
RX errors 0 dropped 0 overruns 0 frame 0
TX packets 68 bytes 3264 (3.1 KiB)
TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0
```

15.1 SERVER SIDE: ifconfig

Once the link is up, tun0 and tun1 interfaces are created. Observe tun0 and tun1 IP addresses and network masks for the demonstrated ifconfig output.

```
tun0: flags=4305<UP,POINTOPOINT,RUNNING,NOARP,MULTICAST> mtu 1500
inet 192.168.54.2 netmask 255.255.255.252 destination 192.168.54.2
inet6 fe80::d8a6:b249:91c3:d8bb prefixlen 64 scopeid 0x20<link>
unspec 00-00-00-00-00-00-00-00-00-00-00-00-00-00 txqueuelen 500
```

15.2 CLIENT SIDE: ifconfig

For client 1, observe the tun0 IP address and network mask for the demonstrated ifconfig output.

```
tun0: flags=4305<UP,POINTOPOINT,RUNNING,NOARP,MULTICAST> mtu 1500
inet 192.168.54.6 netmask 255.255.255.252 destination 192.168.54.6
inet6 fe80::299f:800c:48aa:759d prefixlen 64 scopeid 0x20<link>
unspec 00-00-00-00-00-00-00-00-00-00-00-00-00-00 txqueuelen 500
```

15.3 CLIENT SIDE: ifconfig

For client 2, observe the tun0 IP address and network mask for the demonstrated ifconfig output.

Next Slide

.Fluidity VLAN Implementation Example – Visual Guided Tour

A closer look to active link firewall statuses and .Fluidity's reporting commands.

Previous Slide

```
pi@fluidity-server: ~/Fluidity_Server
File Edit Tabs Help
To Action From
-- ---- -
Anywhere on eth1 ALLOW Anywhere
1440 ALLOW Anywhere
1441 ALLOW Anywhere
Anywhere on tun0 ALLOW Anywhere
1442 ALLOW Anywhere
Anywhere on tun1 ALLOW Anywhere

Anywhere (v6) on eth1 ALLOW Anywhere (v6)
1440 (v6) ALLOW Anywhere (v6)
1441 (v6) ALLOW Anywhere (v6)
Anywhere (v6) on tun0 ALLOW Anywhere (v6)
1442 (v6) ALLOW Anywhere (v6)
Anywhere (v6) on tun1 ALLOW Anywhere (v6)

Anywhere ALLOW OUT Anywhere on eth1
Anywhere ALLOW OUT Anywhere on tun0
Anywhere ALLOW OUT Anywhere on tun1
Anywhere (v6) ALLOW OUT Anywhere (v6) on eth1
Anywhere (v6) ALLOW OUT Anywhere (v6) on tun0
Anywhere (v6) ALLOW OUT Anywhere (v6) on tun1
```

16. SERVER SIDE: ufw status

Observe the rules created allowing traffic for ports 1440, 1441 and 1442 for the active .Fluidity connections [1.1], [1.2], [2.1].

```
pi@fluidity-server:~/Fluidity_Server $ showLinkStatus 1 1
Fluidity Connection ID: 1.1
Fluidity Flavour: Serial Link
Serial Link Speed: 115200
Server Listening Port: 1440
Server Serial Interface: ttys1
Server IP Address: 192.168.52.135
Client Serial Interface: ttys1
Client IP Address: 192.168.52.136
Client Username: pi
Netstat Reports: ESTABLISHED
Fluidity Connection Status: ACTIVE
```

17.1 showLinkStatus 1 1
showLinkStatus enables us to see the current .Fluidity link status.

```
pi@fluidity-server:~/Fluidity_Server $ showLinkStatus 1 2
Fluidity Connection ID: 1.2
Fluidity Flavour: Tunnel Link
Server Listening Port: 1441
Server IP Address: 192.168.52.135
Server Tunnel IP Address: 192.168.54.1
Client IP Address: 192.168.52.136
Client Tunnel IP Address: 192.168.54.2
Network Subnet Mask: 30
Client Username: pi
Netstat Reports: ESTABLISHED
Fluidity Connection Status: ACTIVE
```

17.2 showLinkStatus 1 2
showLinkStatus enables us to see the current .Fluidity link status.

```
pi@fluidity-server:~/Fluidity_Server $ showLinkStatus 2 1
Fluidity Connection ID: 2.1
Fluidity Flavour: Tunnel Link
Server Listening Port: 1442
Server IP Address: 192.168.52.135
Server Tunnel IP Address: 192.168.54.5
Client IP Address: 192.168.52.137
Client Tunnel IP Address: 192.168.54.6
Network Subnet Mask: 30
Client Username: pi
Netstat Reports: ESTABLISHED
Fluidity Connection Status: ACTIVE
```

17.3 showLinkStatus 2 1
showLinkStatus enables us to see the current .Fluidity link status.

Enjoy your .Fluidity!

