SYNACKTIV

Ica2Tcp

A SOCKS proxy for Citrix

Hugo Clout - SSTIC 2022

2022/06/01

https://github.com/synacktiv/ica2tcp

Who are we ?

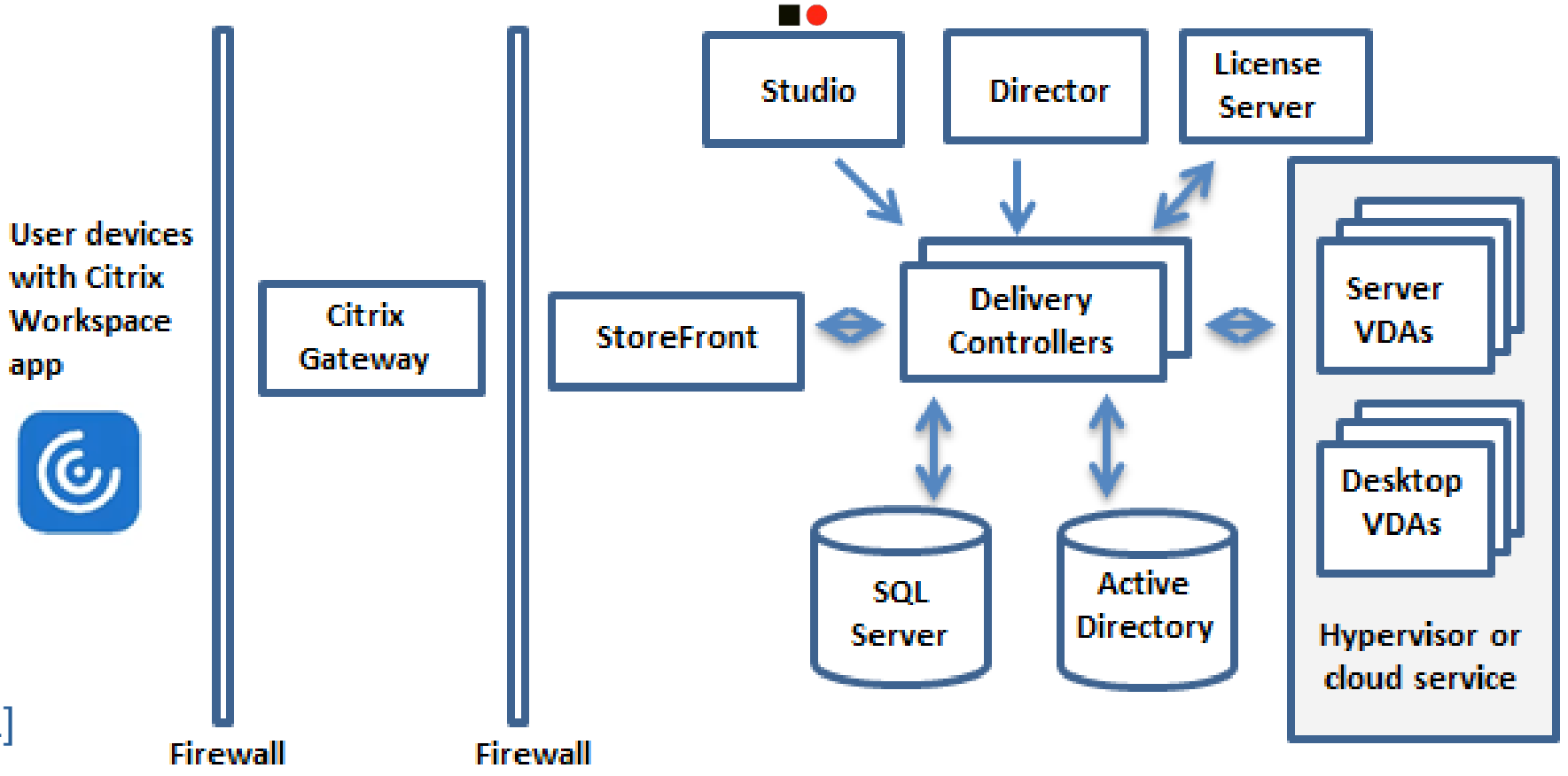
- **Hugo Clout**
  - Pentester for a year
- **Synacktiv**
  - Offensive security
  - 100 ninjas: pentest, reverse engineering, development, DFIR
  - We are hiring!
- **Thanks Mouad Abouhali (m00dy)**

Agenda

- **The needs**
  - Definitions
  - Context and use cases
- **The tool**
  - ICA and Virtual Channels
  - How it works
- **Usage and demonstration**
- **Detection and prevention**

Ica2Tcp - Definitions

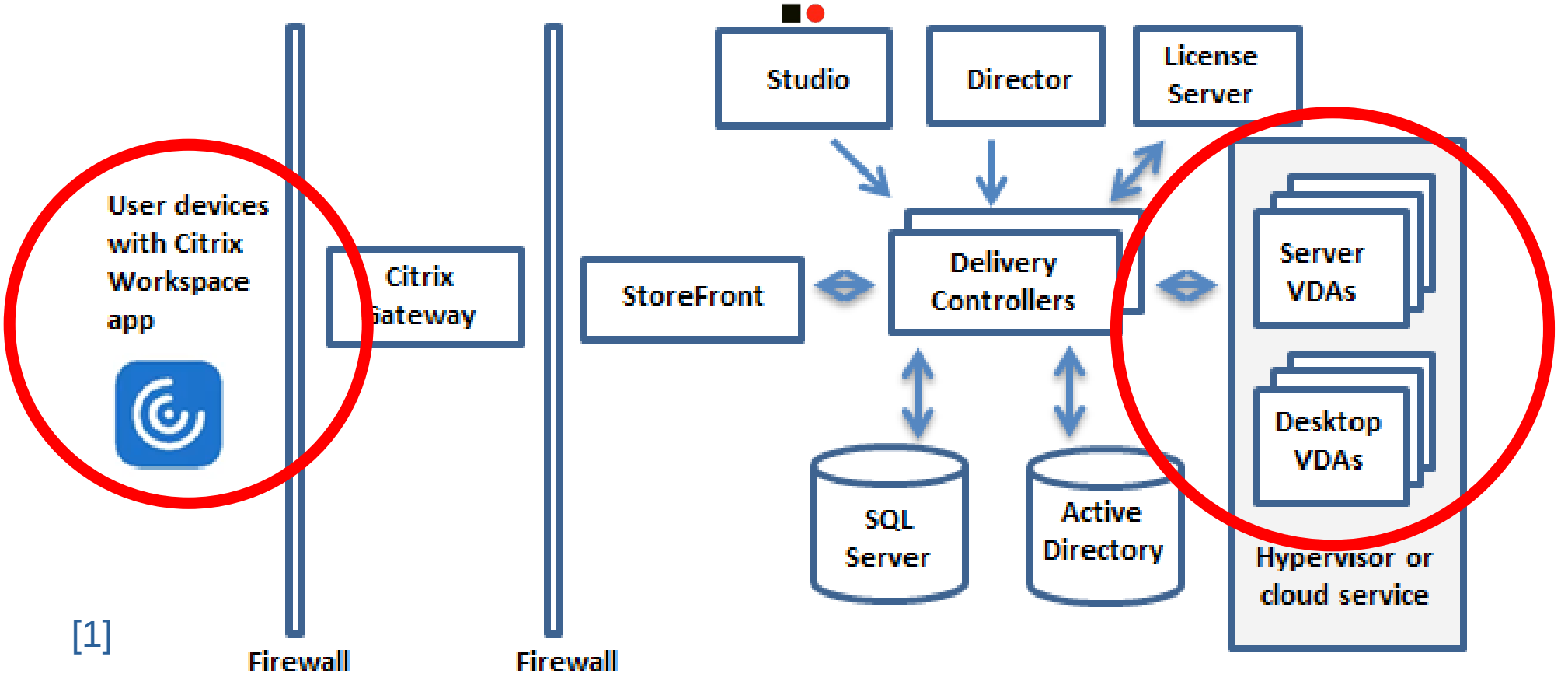
Citrix – Main elements



[1]

Ica2Tcp - Definitions

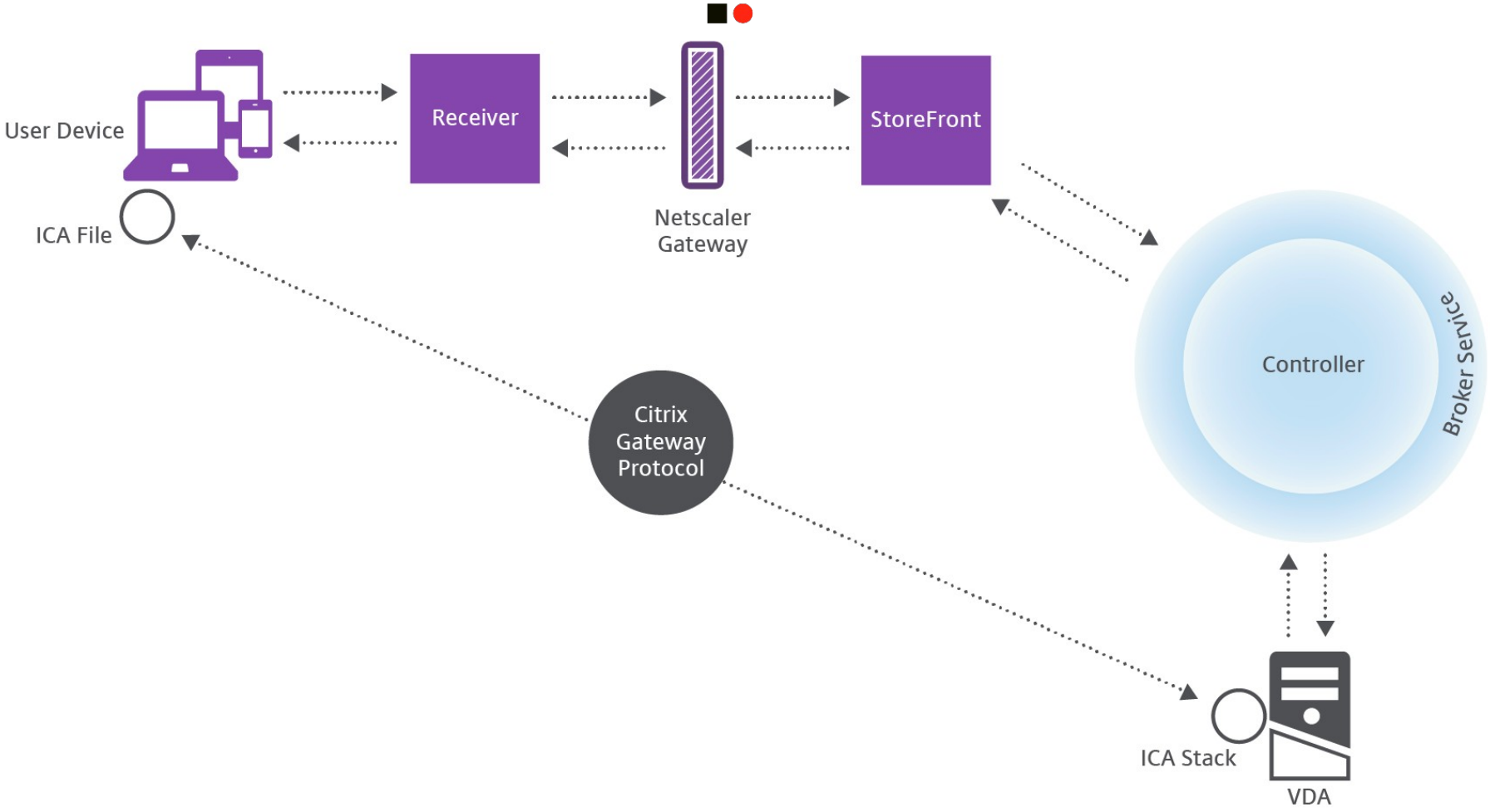
Citrix – Main elements



[1]

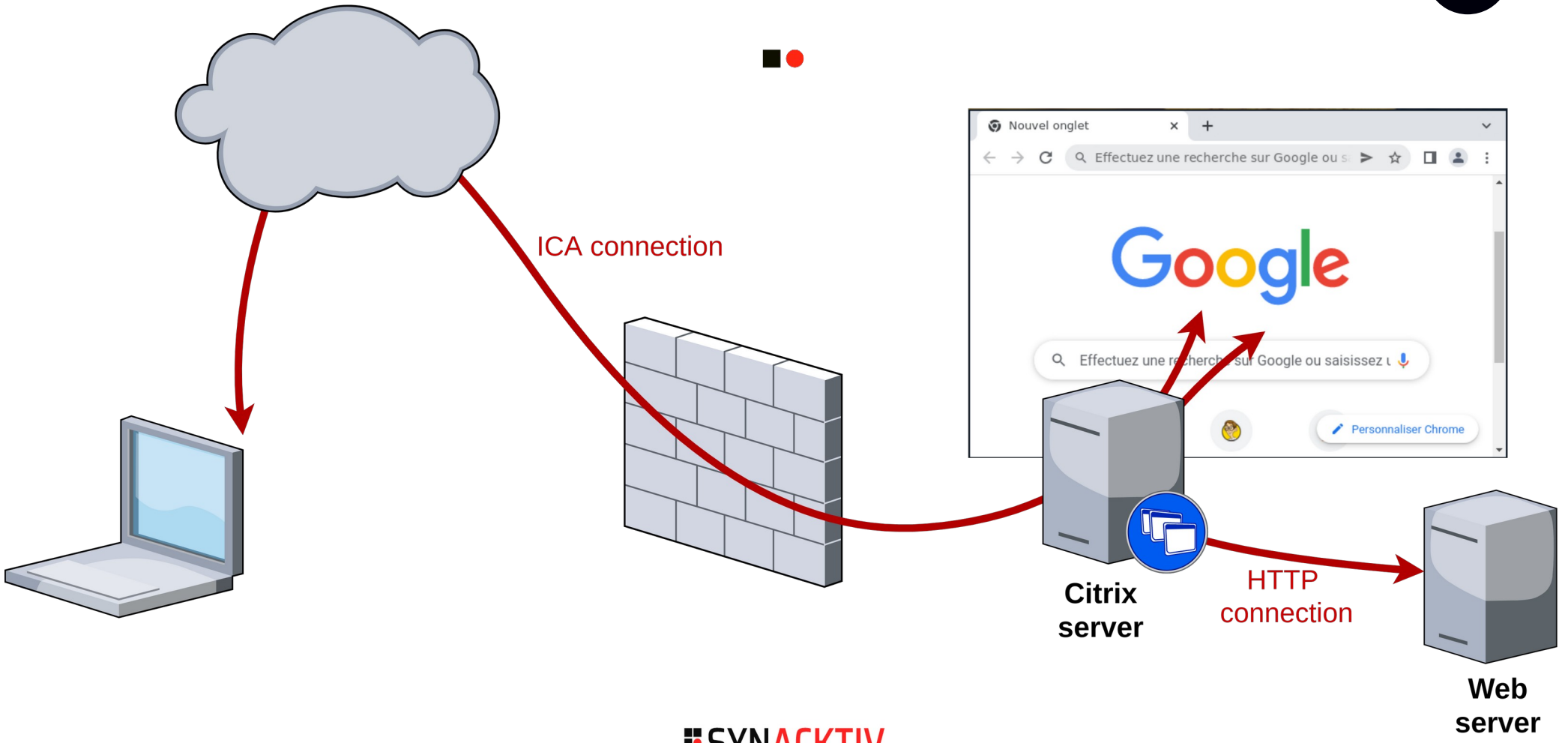
Ica2Tcp - Definitions

Citrix – Connection establishment

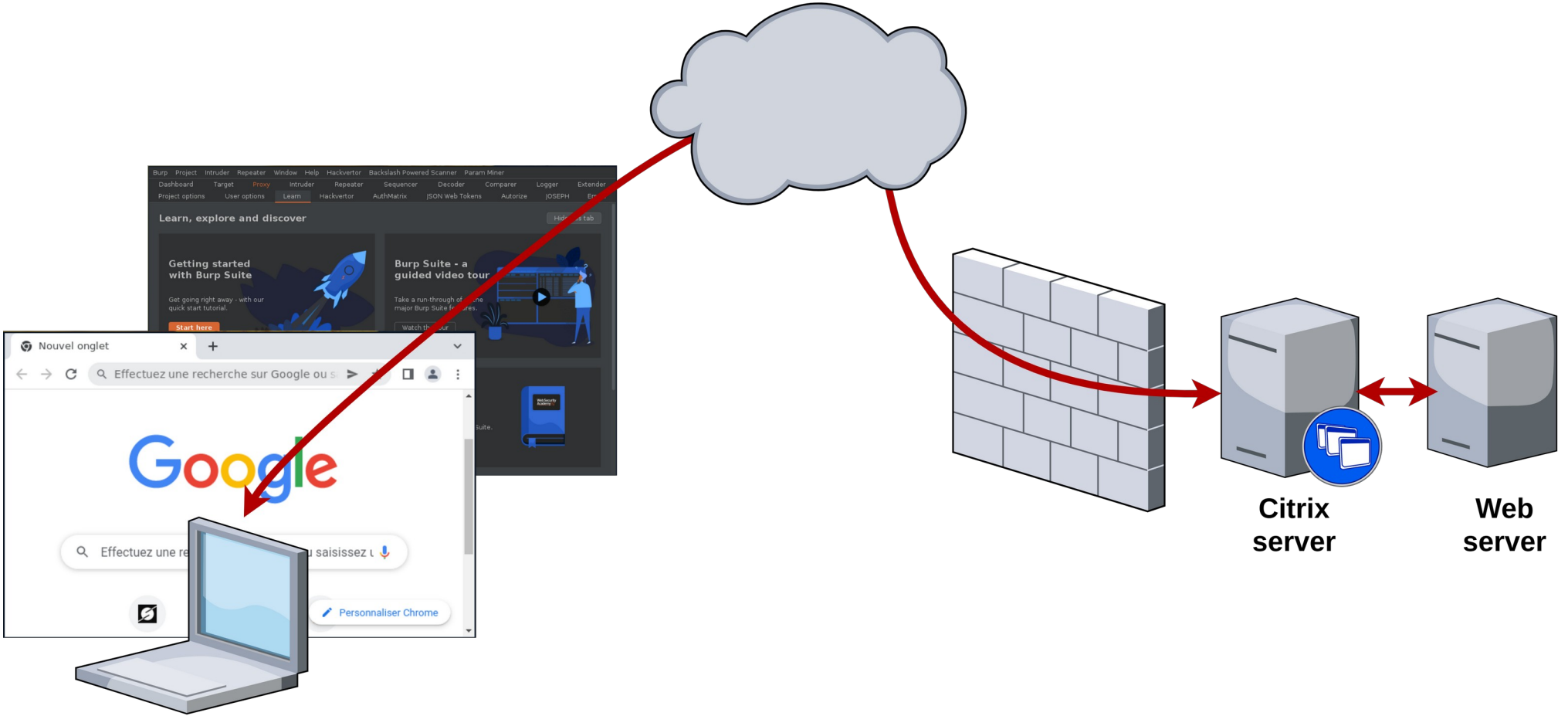


[2]

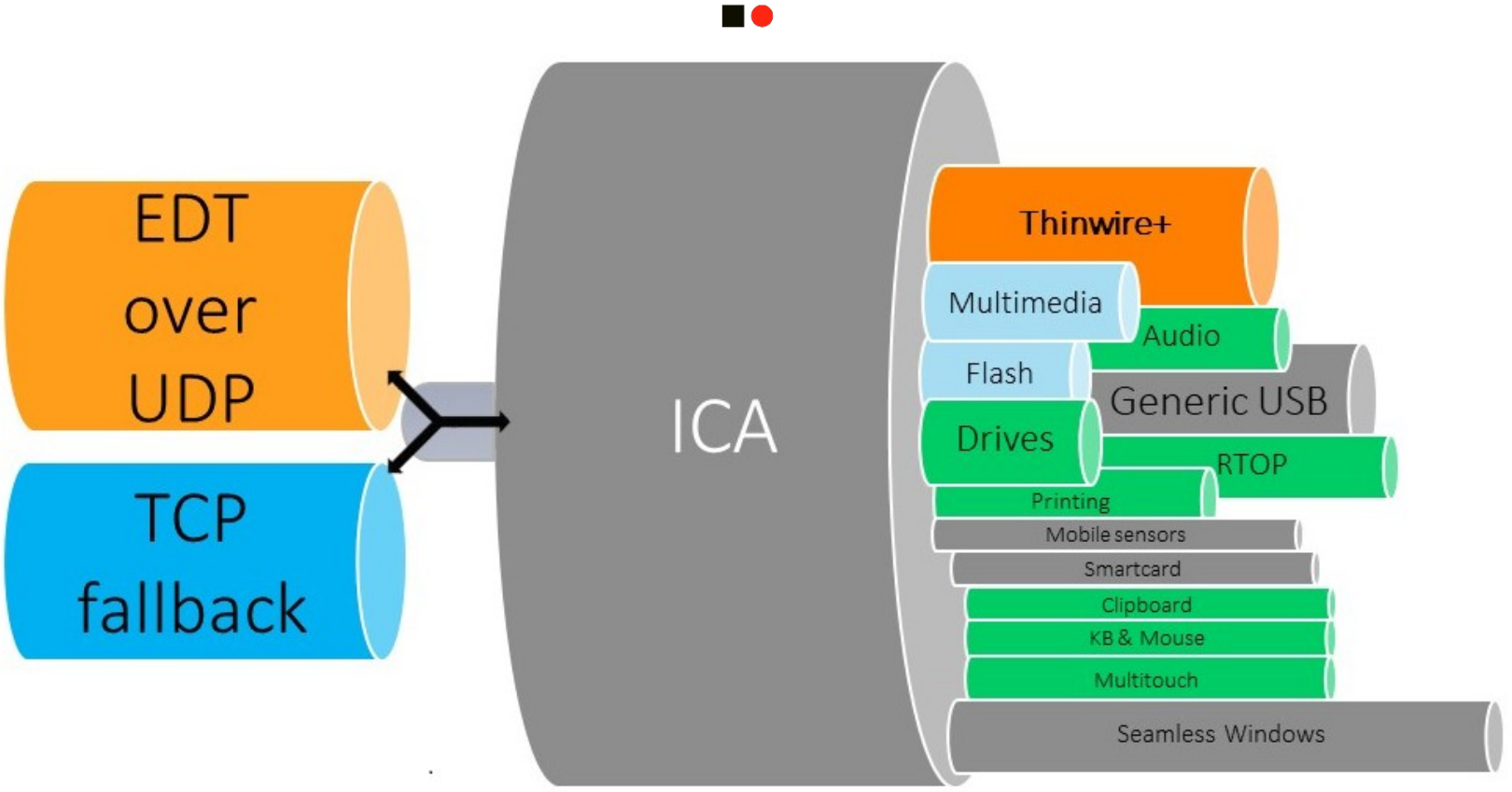
Ica2Tcp – Context and use cases



Ica2Tcp – Context and use cases



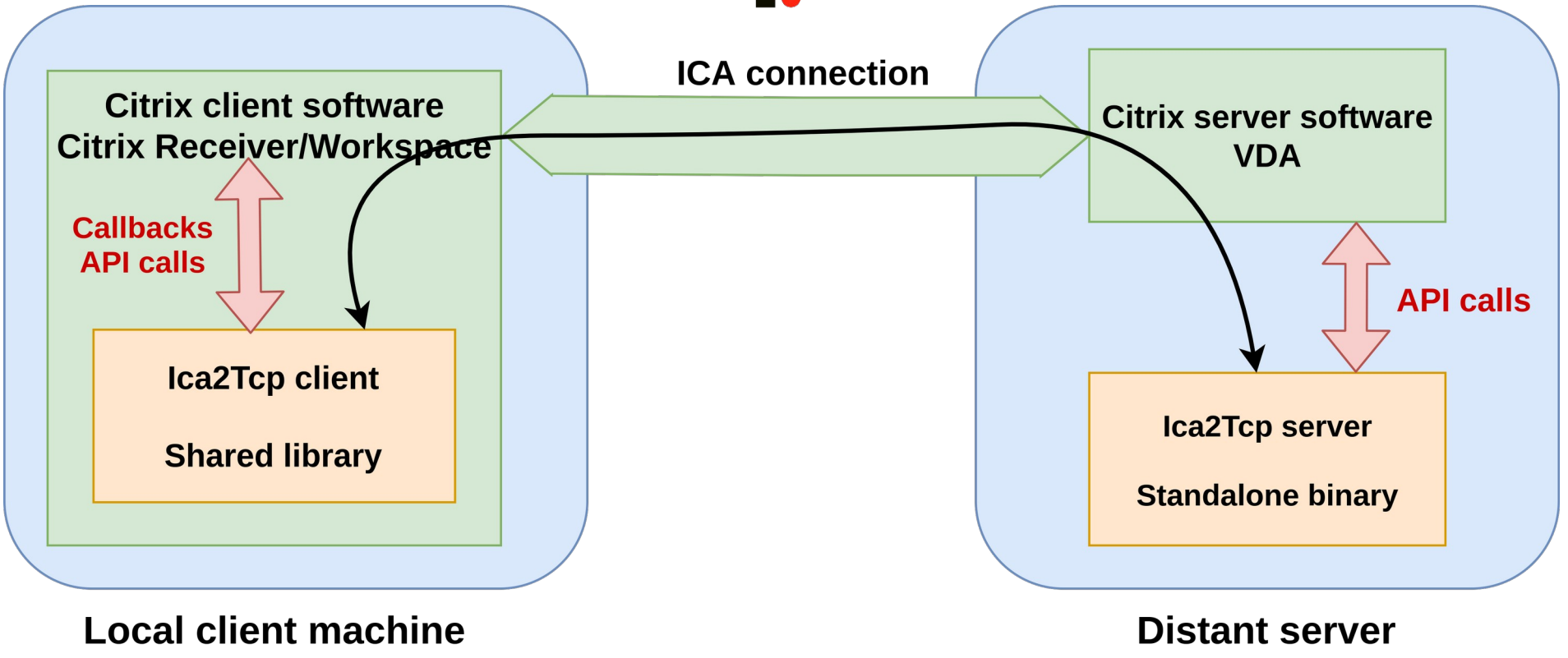
Ica2Tcp – ICA and Virtual Channels



[3]

Ica2Tcp – ICA and Virtual Channels

Developing custom Virtual Channels using the SDK



Ica2Tcp – How it works

The ICA packets arrive:

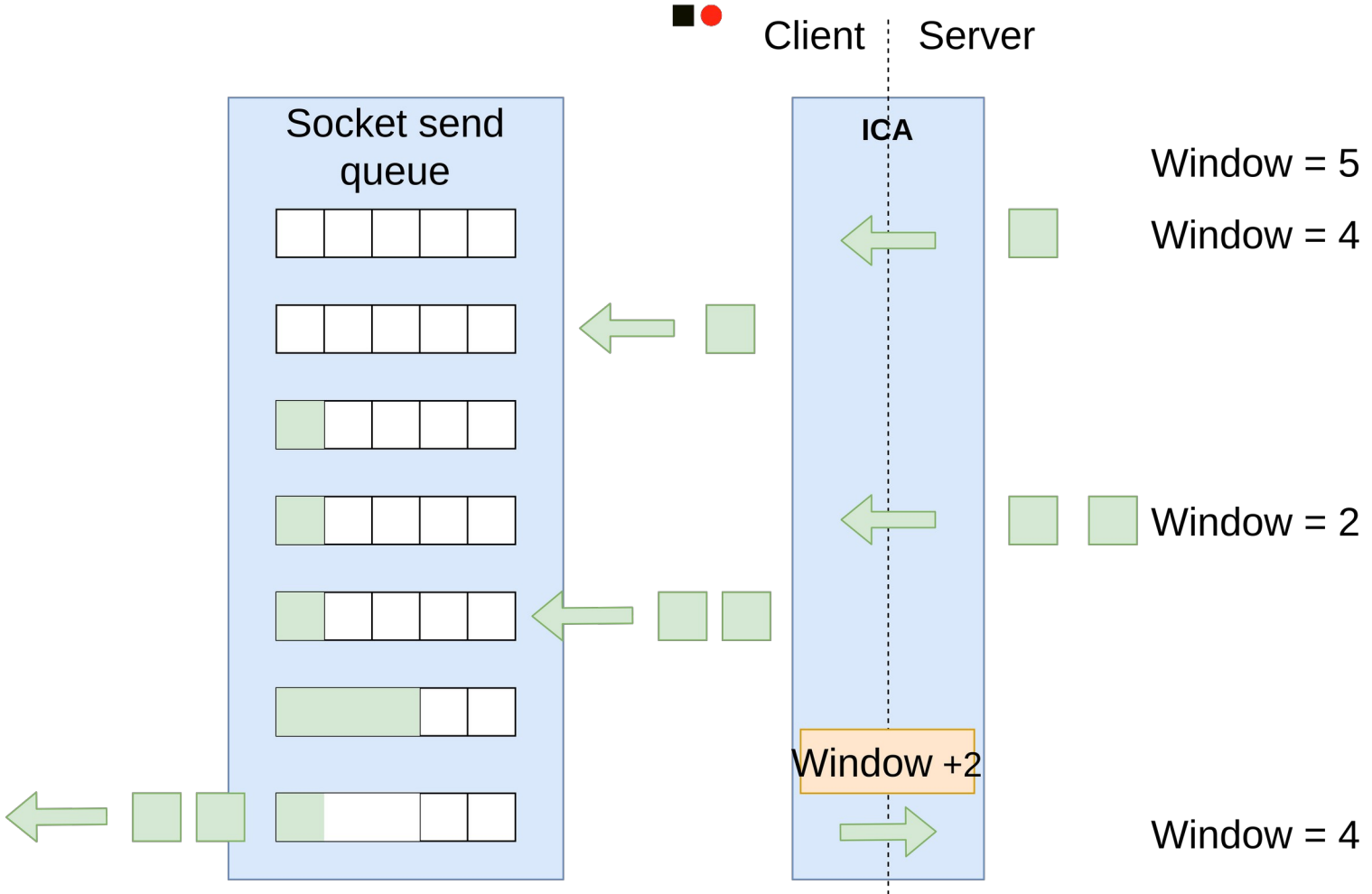
- Complete
- In the right order

To be implemented:

- Flow control
- Socket multiplexing
- Exposure of a SOCKS interface

Ica2Tcp – How it works

Sliding window



Ica2Tcp – How it works

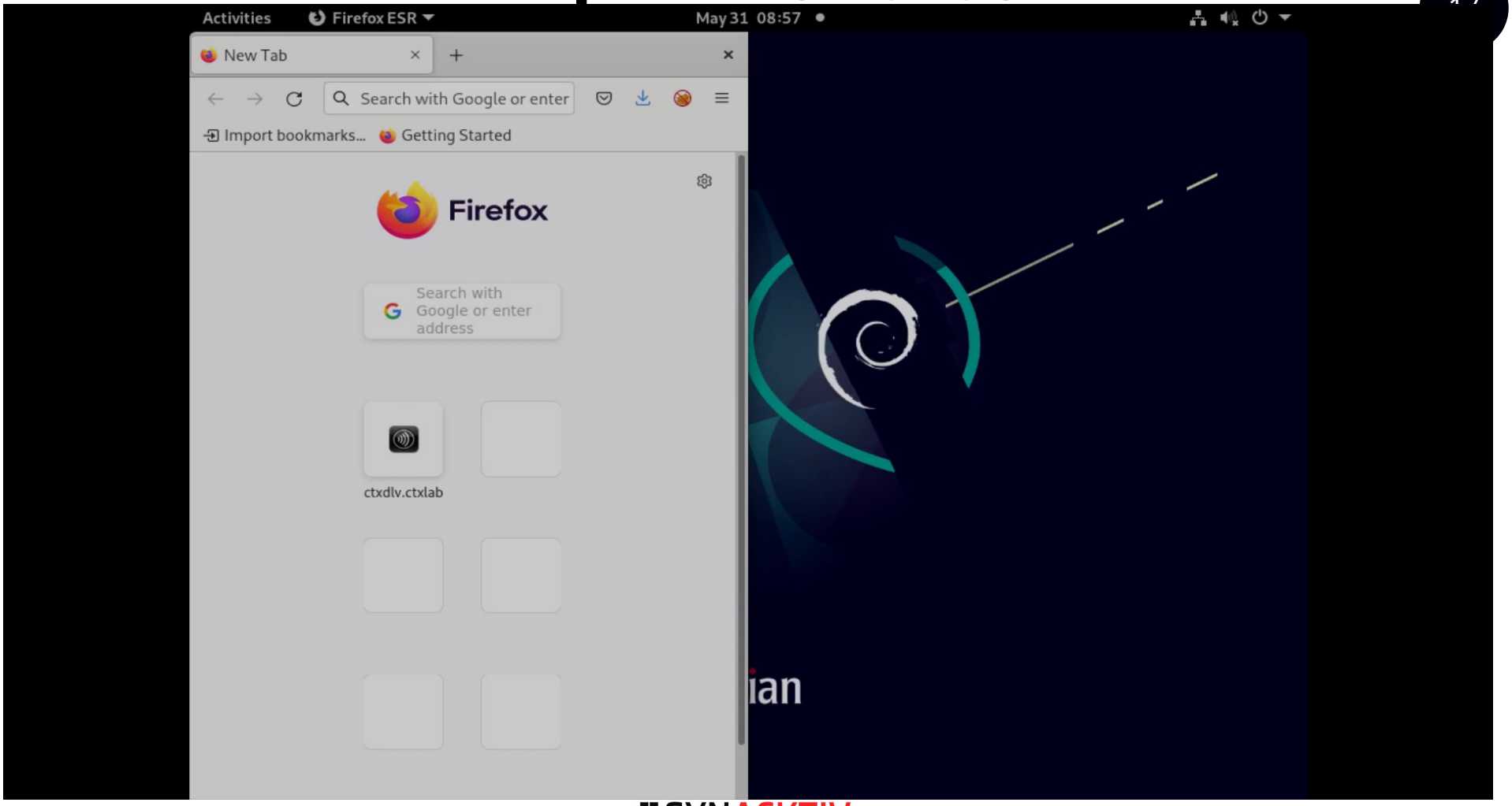
Partial implementation of RFC1928

- Protocol version: 0x05-Version 5
- Method selection: 0x00-No authentication required
- Commands: 0x01-CONNECT
- Address Type: 0x01-IPv4, 0x03-Domain Name, 0x04-IPv6

Ica2Tcp – Prerequisites and usage

- Server: Windows only
- Client: Linux for now
- Compiled on Linux: GCC and MinGW

Ica2Tcp – Demonstration



Ica2Tcp – Detection and prevention

- ***Virtual Channel Allow Lists***
  - Available since CVAD 2006 (June 2020)
  - Enabled by default since CVAD 2109 (October 2021)
- **Using Windows GPO mechanism or Citrix Studio**
  - `CTXCVC1,C:\Program Files\Application\run.exe`
  - `CTXCVC1,C:\Program Files\Application\run.exe,C:\Program Files\Application\run2.exe`

Ica2Tcp – Detection and prevention

- **Logging in the VDA Windows event log**
  - *<username> tried to open custom virtual channel <vcName>*
  - *<username> opened custom virtual channel <vcName>*
  - *Custom virtual channel <vcName> cannot be opened by process <processName>*
  - *Custom virtual channel <vcName> has been opened by process <processName>*

Bibliography

- [1] https://docs.citrix.com/en-us/citrix-virtual-apps-desktops/media/components-new-op.png
- [2] https://docs.citrix.com/en-us/xenapp-and-xendesktop/7-15-ltsr/media/user-connections.png
- [3] https://docs.citrix.com/en-us/citrix-virtual-apps-desktops/media/hdx-1.png

https://www.linkedin.com/company/synacktiv
https://twitter.com/synacktiv
Our publications : https://synacktiv.com