P2P advanced troubleshooting guide

for ISP and wide network operators

Introduction

What is this guide?
This is troubleshooting guide to P2P easy connection Dahua protocol.

To whom this guide is written?
This guide is for operators, network experts and engineer who need to troubleshoot Dahua P2P NAT traveral protocol issues on their WAN or on their managed equipements.

To whom this guide is NOT for?
This guide is NOT people who would like to connect a simple installation to P2P.

I am not an network export and I want to make P2P working
Troubleshooting P2P is quite complex, we recommand to use **Port address translation** as alternative.

Summary

1. Firewall and managed network
Cybersecurity configuration

2. NAT Topologies
Reminder on existing architectures

3. Topologies detection & routing algorithm
Network topology detection and STUN/TURN

4. Known issues
Most found problems

5. Troubleshooting steps
Advanced troubleshooting

6. P2P alternatives
Professional solution and work-arrounds

1. Firewall and managed network

Firewall and managed network

Firewall configuration and managed routers

Due to the nature of firewall protected network, **P2P is not compliant with a firewall protected network**.

Once the NAT is established, the traffic is re-routed on-the-fly with a changing port-remote_address couple which will be detected by the firewall and blocked.

As the UDP ports are dynamics and remote IP also, it is not enough to open all UDP ports, you have to configure the firewall to give to any IP that are potentially a STUN or TURN server or a remote client.

All remote cloud services IP might be used, for Europe for example you would have to allow all IP addresses from Amazon Cloud Services and all IP addresses from any European ISP (assuming your customer will only connect from Europe).

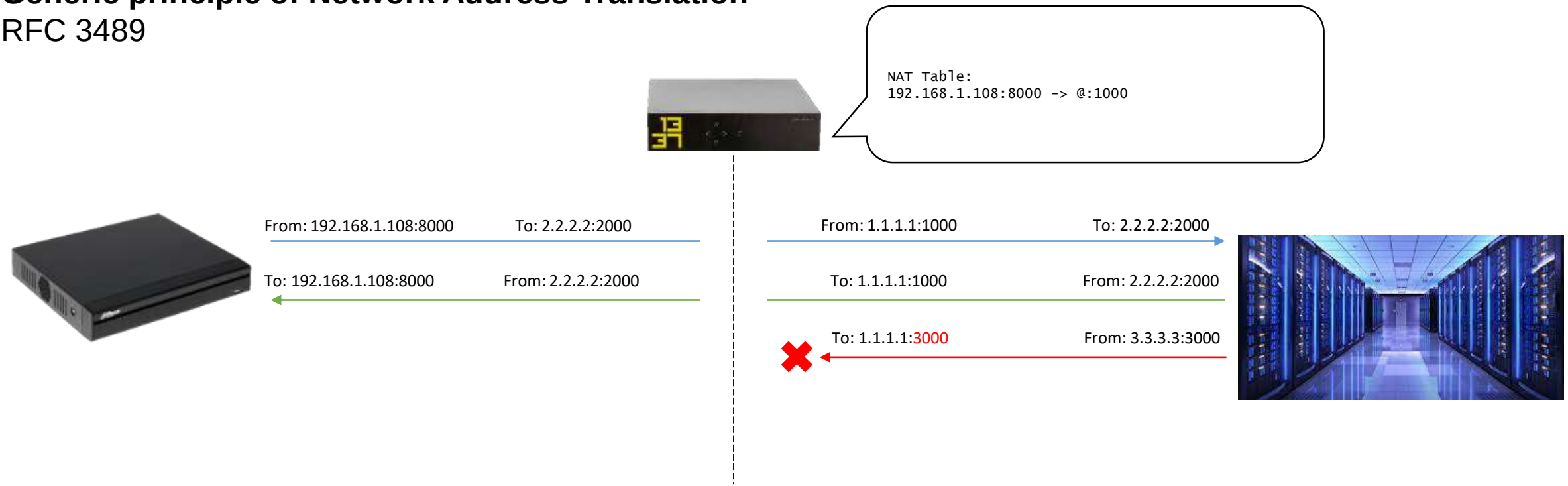
If firewall is really needed, check the information documentation: https://support.dahuafrance.fr/cyber/

2. NAT Topologies

Types of NAT

Generic principle of Network Address Translation

RFC 3489



Local IP remplaced by External (public) IP
An external random* port is opened

*except for symetric NAT

Types of NAT

Full cone NAT

NAT Table:
192.168.1.108:8000 -> @:1000

From: 192.168.1.108:8000 To: 2.2.2.2:2000

To: 192.168.1.108:8000 From: 2.2.2.2:2000

To: 192.168.1.108:8000 From: 2.2.2.2:**3000**

To: 192.168.1.108:8000 From: **3.3.3.3:3000**

From: 1.1.1.1:1000 To: 2.2.2.2:2000

To: 1.1.1.1:1000 From: 2.2.2.2:2000

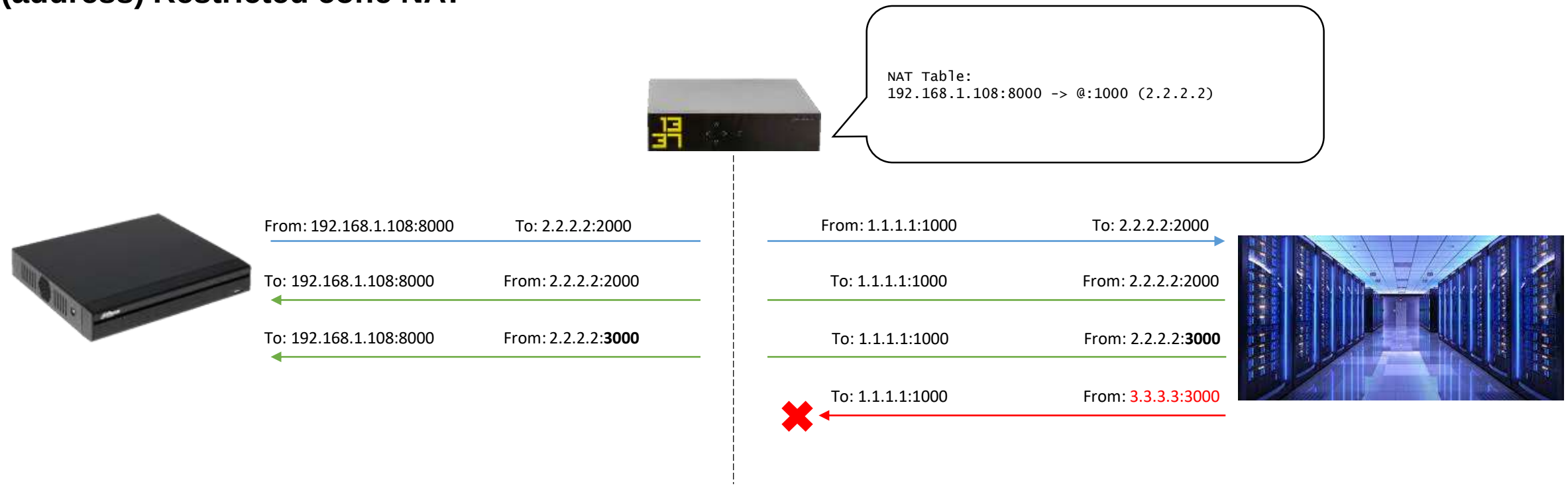
To: 1.1.1.1:1000 From: 2.2.2.2:**3000**

To: 1.1.1.1:1000 From: **3.3.3.3:3000**

Any host can contact the external port

Types of NAT

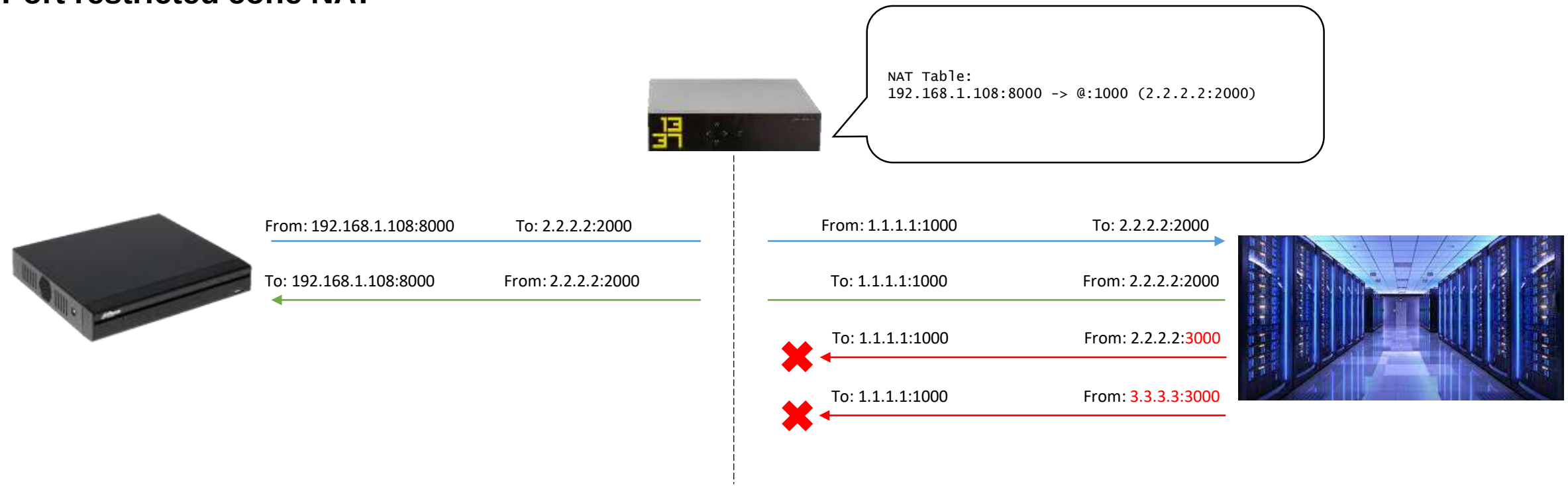
(address) Restricted cone NAT



Only the remote host can contact contact back from any of its port

Types of NAT

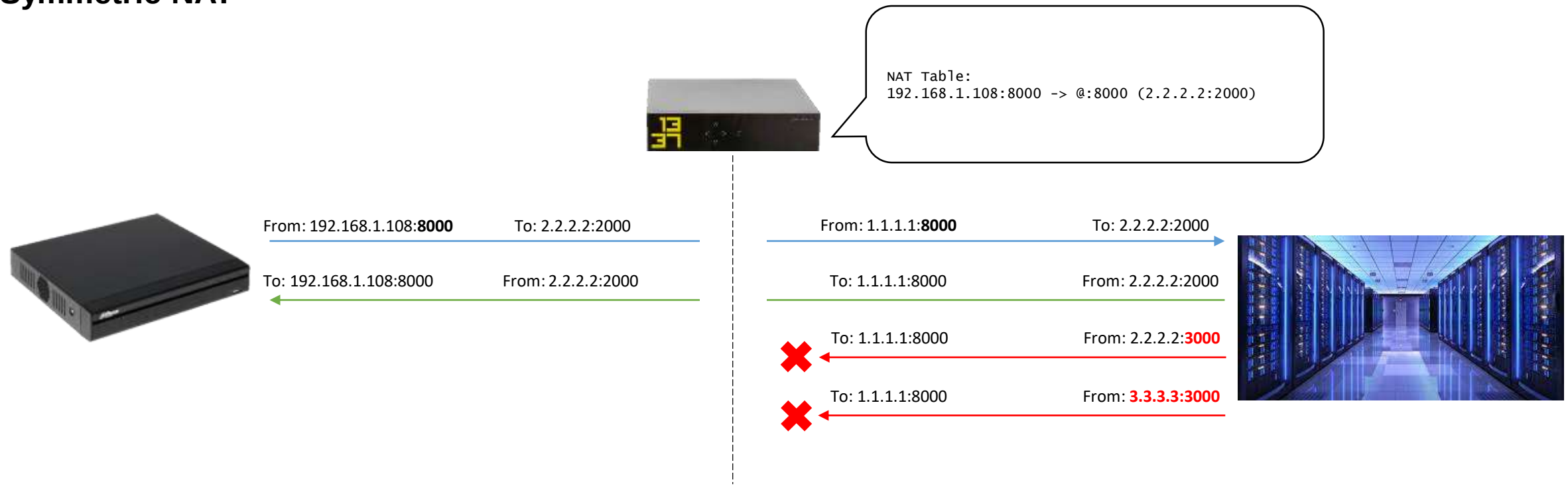
Port restricted cone NAT



Only the remote host can contact contact back and from the same port we sent packet

Types of NAT

Symmetric NAT

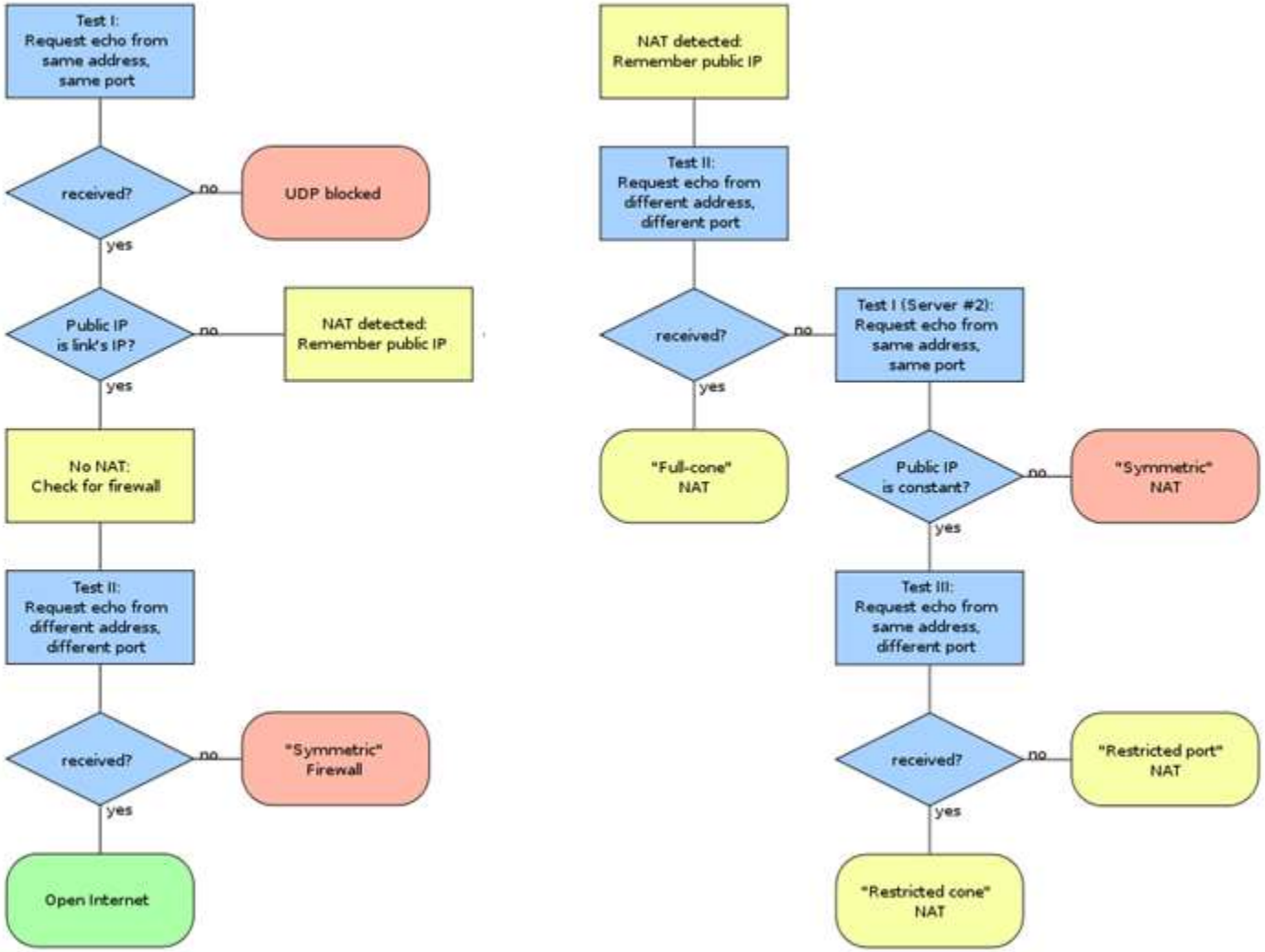


Routeur tries, if possible, to use same source port to expose on internet
Only the remote host can contact contact back and from the same port we sent packet

3. Topologies detection & routing algorithm

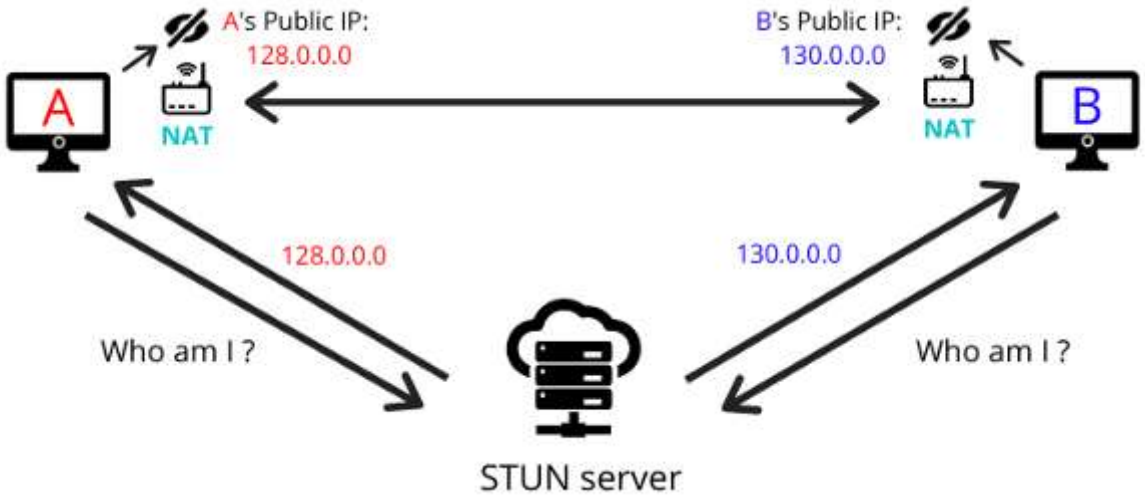
Network topology detection

Network type detection



Network topology detection

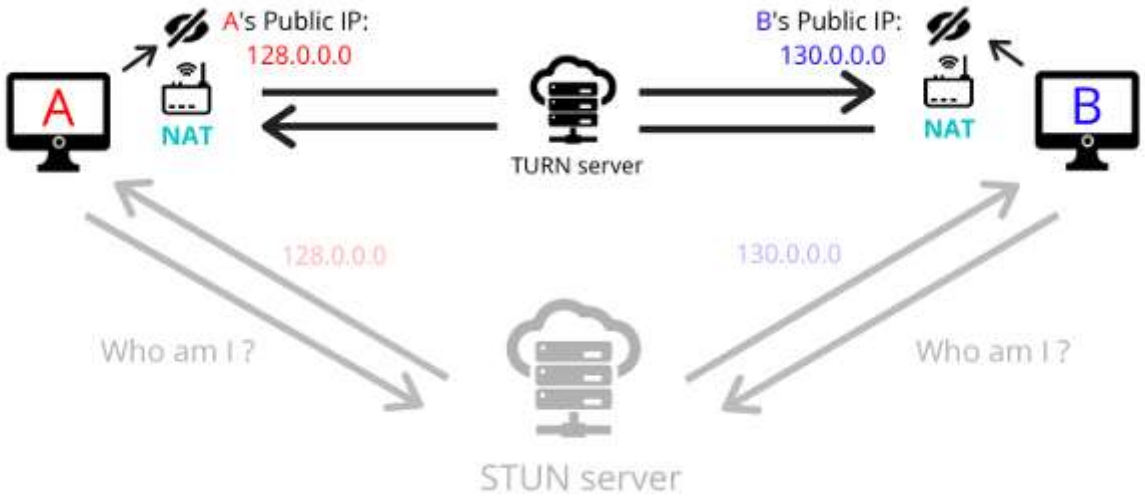
STUN



STUN server provides information from outside (IP address, contacted port, etc.).
STUN server is used to detect local network topology.

Network topology detection

TURN



TURN server is the ultimate choice (failback mode) when not option exists to connect two peers together directly.

5. Knwon issues

There is many known issues that should be checked at first hand:

1. Check if customer is using a firewall or a secured routeur
2. Check is the operator is not performing a NAT also (e.g Bouygues Telecom)
3. Check if the IPv4 is really unique for each operator client and has not port sharing (e.g. Free Telecom)
4. Check if there is not a symetric NAT performed on the router (e.g. Orange Telecom)
5. Check if there is no restricition on the NAT by the operator (e.g. Orange Telecom)

5. Troubleshooting steps

First checks

1. Check the known issues
2. Check if the device is declared online
3. Test the device on another operator network
4. Test another device on the same network
5. Test same remote device from another operator network
6. Test from another remote device

5. Troubleshooting steps

Qualitative analysis

7. Identify the topology on both sides of the network and check if compliant
8. When possible check routeur NAT table to identify which port and which is not
9. Perform network catpure, either:

- using a port mirroring on a switch
- or using USB stick on the Dahua NVR and going into Maintain / Network / Test and start capture clicking on Sniffer Packet Backup on related LAN.
- stop and start the P2P while performing capture.
- send the file contact to Dahua with network capture and SN: julien.blitte@dahuatech.com

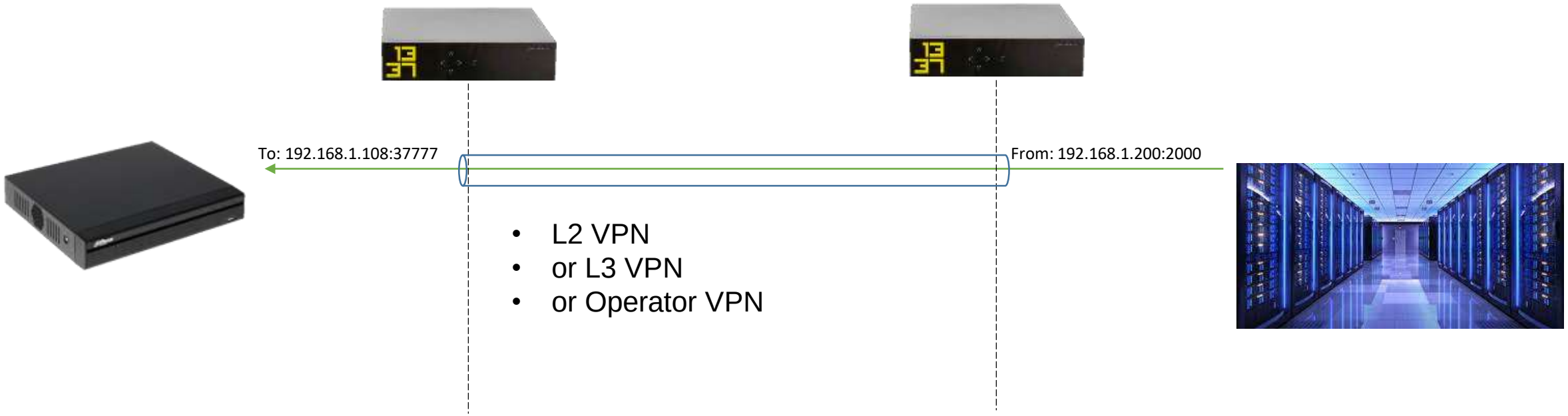
Alternatives

10. Use altenatives as describe after

6. P2P alternatives

P2P Alternatives

VPN

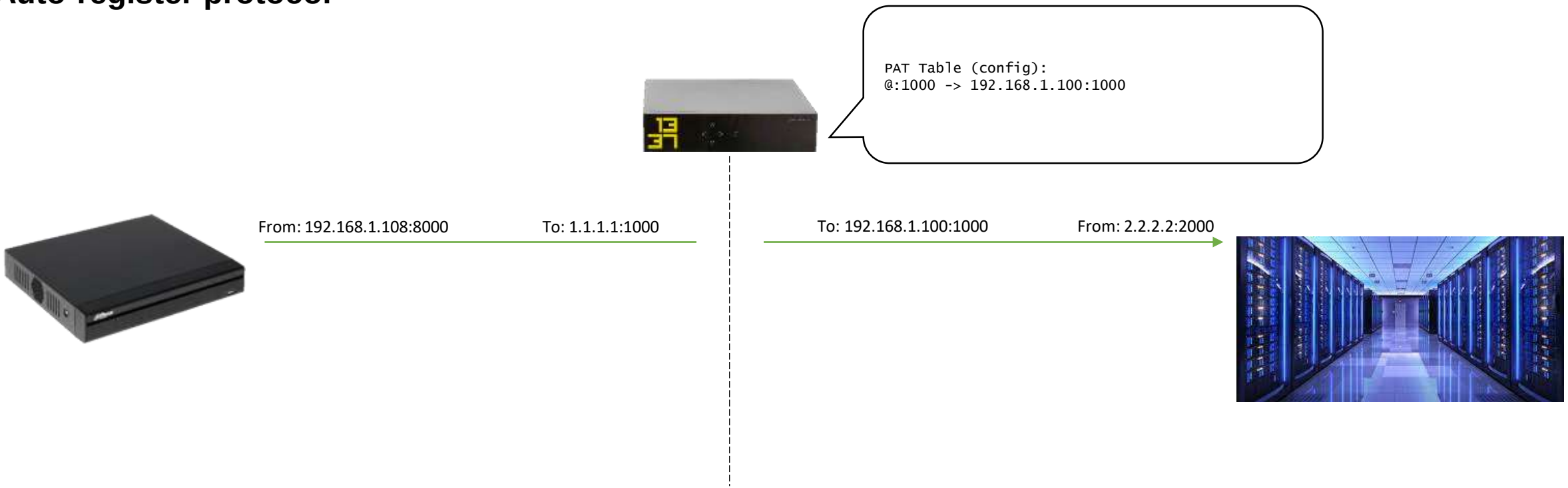


This is safe and reliable solution but involves some fees (advanced routers with VPN or operator VPN)

This is recommanded solution for secured sites.

P2P Alternatives

Auto-register protocol



The exposed port is on remote service provider so security can be contrôlled.
The connection is reversed (Dahua equipment connects itself to remote station).

This is recommanded solution for Remote Alarm Monitoring Center and video service provider.

P2P Alternatives

Fixed IPv6 protocol

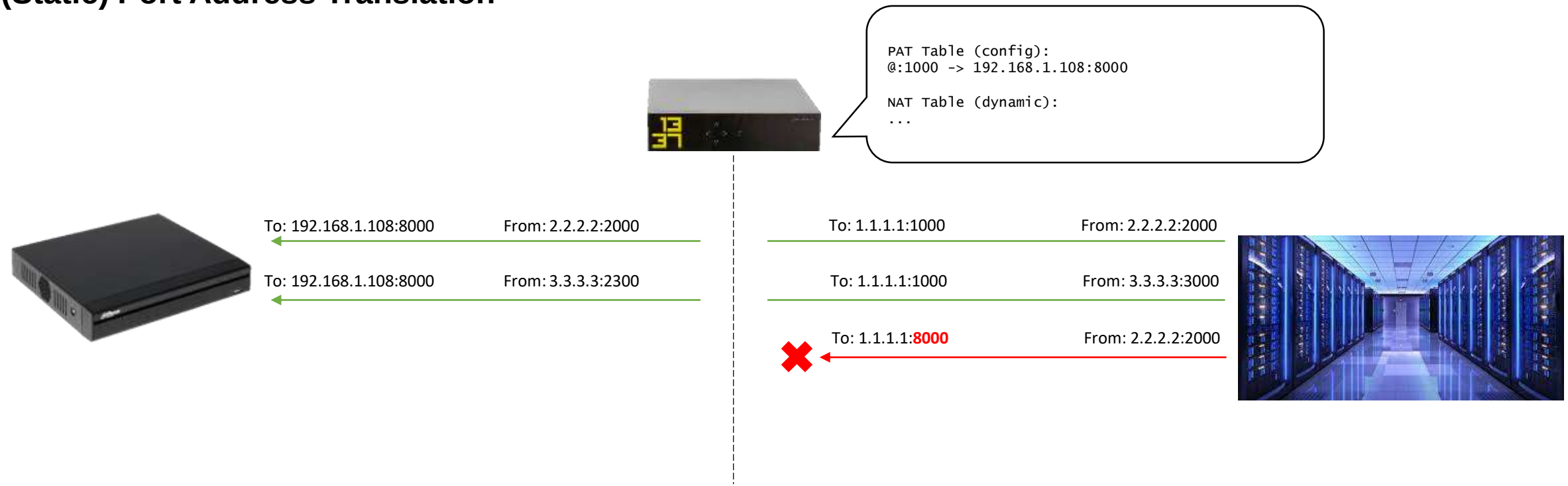
To: [2001:1000::1]:1000

From: [2001:2000::1]:2000

The port is exposed on a IPv6 public address.
Any remote hosts that knows the IPv6 and port can access the device. Public IPv6 must be fixed.
This is recommanded solution for IPv6 both sides native networks.
For security reason, external port should always be different than default device port

P2P Alternatives

(Static) Port Address Translation



Routeur always exposes a defined port and redirect it to same device and port
Any remote hosts that knows the port can access the device. Public IP must be fixed.
This is recommanded solution for small businesses and personnal homes.
For security reason, external port should always be different than default device port

P2P Alternatives

Additionnal router

Add an external and dedicated ASDL or fibre connecion with no connection to existing network.

This is recommanded solution for complex and network managed sites where no previous solution are available.

P2P Alternatives

DMZ

```
Configuration:
DMZ = 192.168.1.108

NAT Table (dynamic):
...
```

To: 192.168.1.108:**1000** From: 2.2.2.2:2000

To: 192.168.1.108:**8000** From: 2.2.2.2:2000

To: 192.168.1.108:**4000** From: 2.2.2.2:3000

To: 192.168.1.108:**5000** From: 3.3.3.3:3000

To: 1.1.1.1:**1000** From: 2.2.2.2:2000

To: 1.1.1.1:**8000** From: 2.2.2.2:2000

To: 1.1.1.1:**4000** From: 2.2.2.2:2000

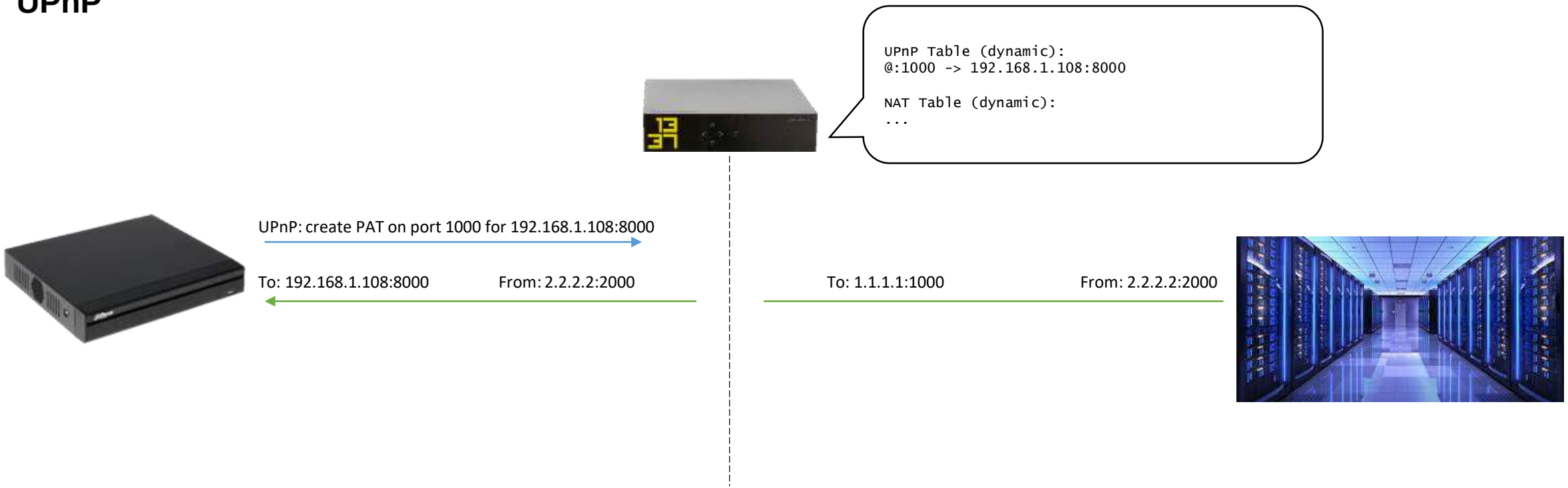
To: 1.1.1.1:**5000** From: 3.3.3.3:3000

Routeur forwards all incoming requests to the same device on the network with same destination port

This configuration is a security suicide. All the ports are exposed.

P2P Alternatives

UPnP



Device detects router and provide dynamically port to forward. Public IP must be fixed.

This might be at risk (default port exposed, customer unaware)