RIPE NCC
RIPE NETWORK COORDINATION CENTER

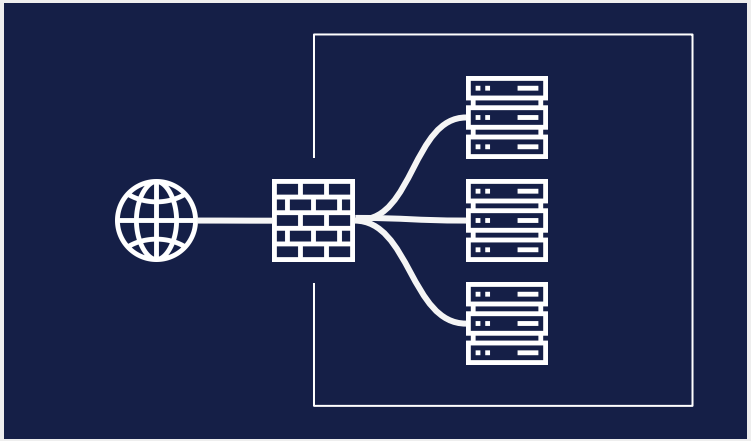
# IP-based access controls

## Why they might not be a good idea

**Ondřej Caletka | RIPE NCC |** 12 September 2024

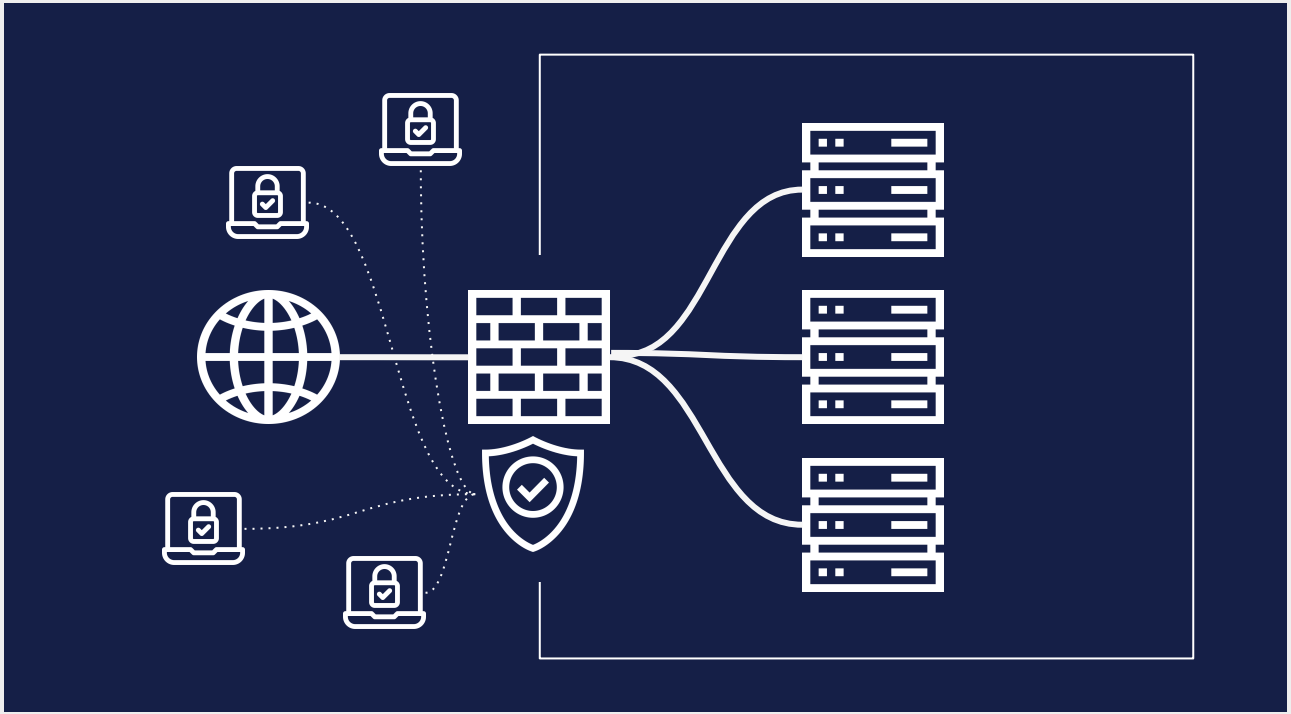
# What is an IP-based restriction

- Restricting access to resources **based on client's IP address**
- **That's what firewalls do!**
- Works well within private networks
- But everything is **in the cloud** nowadays!



# Getting people into the IP-restricted space

## Use VPN!



# Public cloud enters the scene

## We still need to know which users are ours!

# Example 1: CDN

- An on-prem WWW server **gets a CDN** deployed in front of it
- Users are connecting to **one of the edge servers** all around the world
- The content gets eventually **pulled from the on-prem origin server**
- **Some privileged actions** are allowed only from the **on-prem IP addresses**
- **But the users are connecting to the CDN edge!**
    - Should we **tunnel traffic** to the CDN edge via our VPN?



# Cloud is dynamic

- DNS is a **load-balancing/failover mechanism** for many cloud applications
- DNS response is **generated in real-time** after receiving the query
- IP addresses can change **not only in time** but also based on **who is asking**
- Trying to **chase which IP addresses** the service uses is a **cat-and-mouse game**



# Cloud is public

- There is **public Internet** in front of the Cloud
- **Anything can happen** there
- IP addresses are **neither encrypted nor authenticated**



# Possible solution: full-tunnel VPN

## Also known as a big trombone

**People from distant countries** will definitely enjoy the **increased latency on everything**

# Proper solution: cryptographic authentication of users

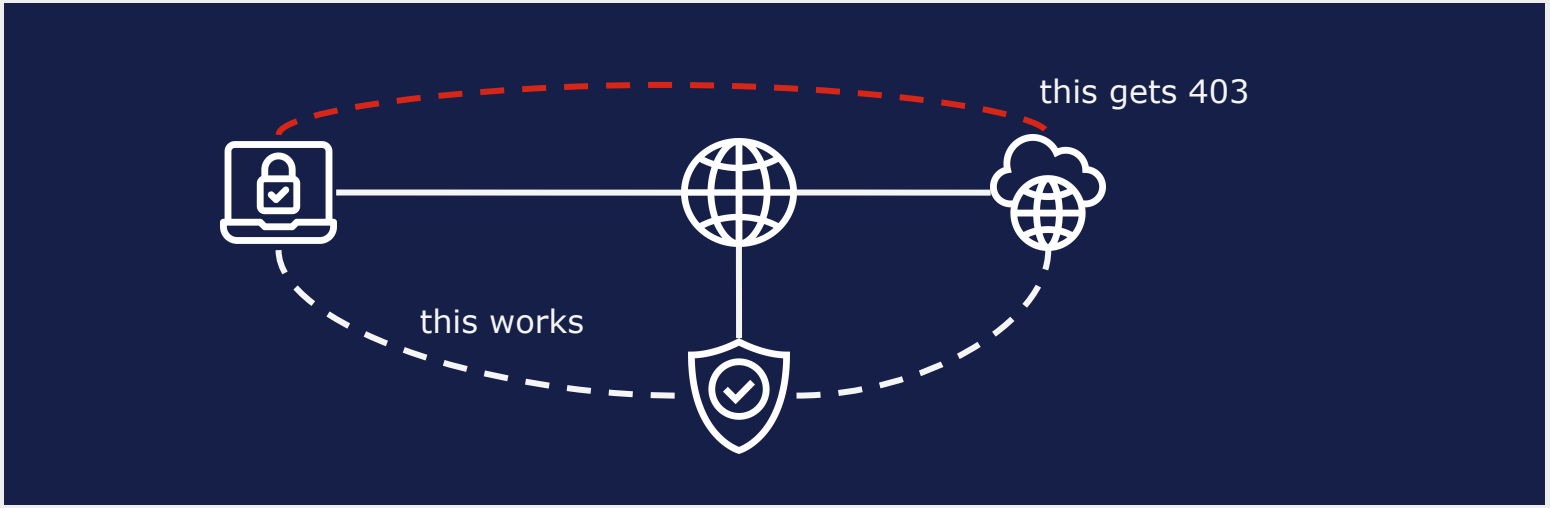
- Let the users **log in**, preferably using a **Single Sign-On**
- Get an **cryptographic assertion** that the **user is authenticated**
- Use this **instead of client's IP address**
  - It is much more **stronger and reliable**
  - With cryptographic assertion, you **shouldn't care** about the IP address the client is using



# It can get even worse...

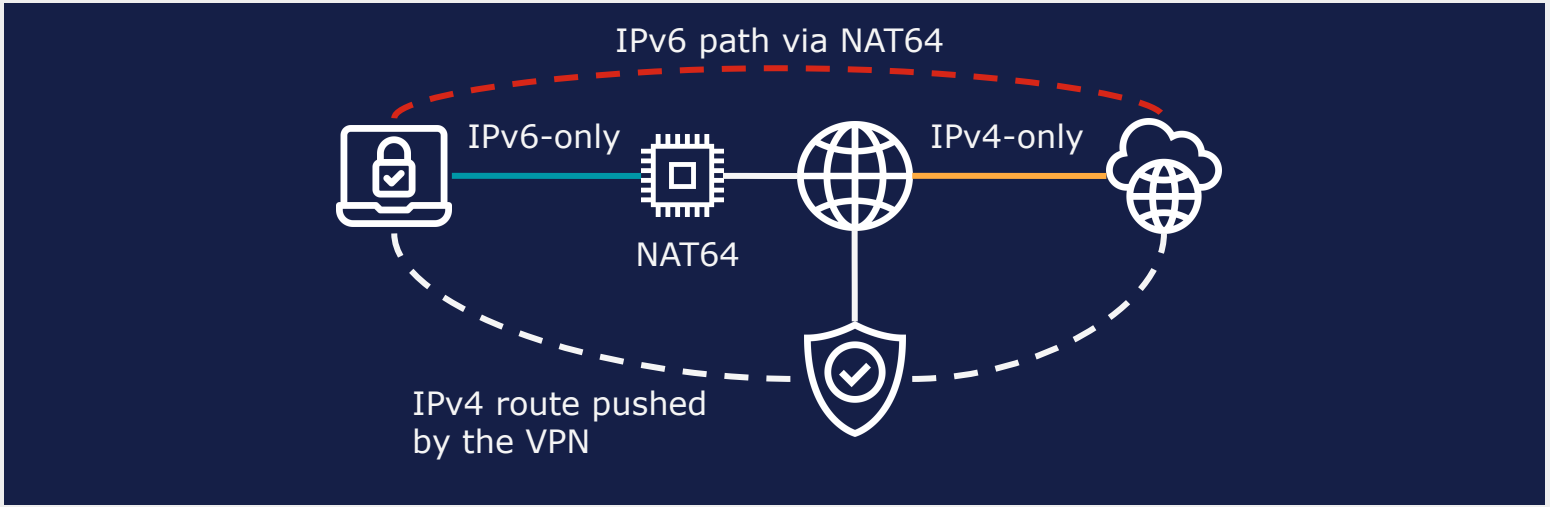
# Example 2: IP-restricted IPv4-only SaaS in the public cloud

- An application in the public cloud **authenticated using SSO**
- Yet still set up to only allow access from a **specific on-prem IP address**
- Access from other addresses is **blocked on the Application layer** (403 Forbidden)



# Clients connects to a network with NAT64/DNS64

- DNS64 creates **a synthetic IPv6 address** for the IPv4-only resource
- Client will **prefer IPv6 over IPv4**
- IPv6 connection via NAT64 gateway **bypasses the VPN**
- Happy eyeballs will not help since it is **not a transport layer problem**



RIPE NCC
RIPE NETWORK COORDINATION CENTER

# Please don’t use broken IP-based restrictions

# Questions, feedback & dialogue