



NIC Cloud
Connect

Oslo Spektrum
November 7 - 9

Sami Laiho

Zero Trust MicroSegmentation for FREE!



Create a strong password

Create a strong password with a mix of letters,
numbers and symbols

Password

ChuckNorris

Confirm

ChuckNorris

 Password is too strong



Show password

Next



Sami Laiho

Chief Research Officer

/ MVP

- IT Admin since 1996 / MCT since 2001
- MVP in Windows OS since 2011
- "100 Most Influential people in IT in Finland" – TiVi'2019→
- Specializes in and trains:
 - Troubleshooting
 - Windows Internals
 - Security, Social Engineering, Auditing
- Trophies:
 - Best Session at Advanced Threat Summit 2020
 - Best Speaker at NIC, Oslo 2016, 2017, 2019, 2020 and 2022
 - Ignite 2018 – Session #1 and #2 (out of 1708) !
 - TechEd Europe and North America 2014 - Best session, Best speaker
 - TechEd Australia 2013 - Best session, Best speaker





X (ex-Twitter) @samilaiho

Bluesky: @samilaiho.com

LinkedIn

Microsegmentation

ZScaler

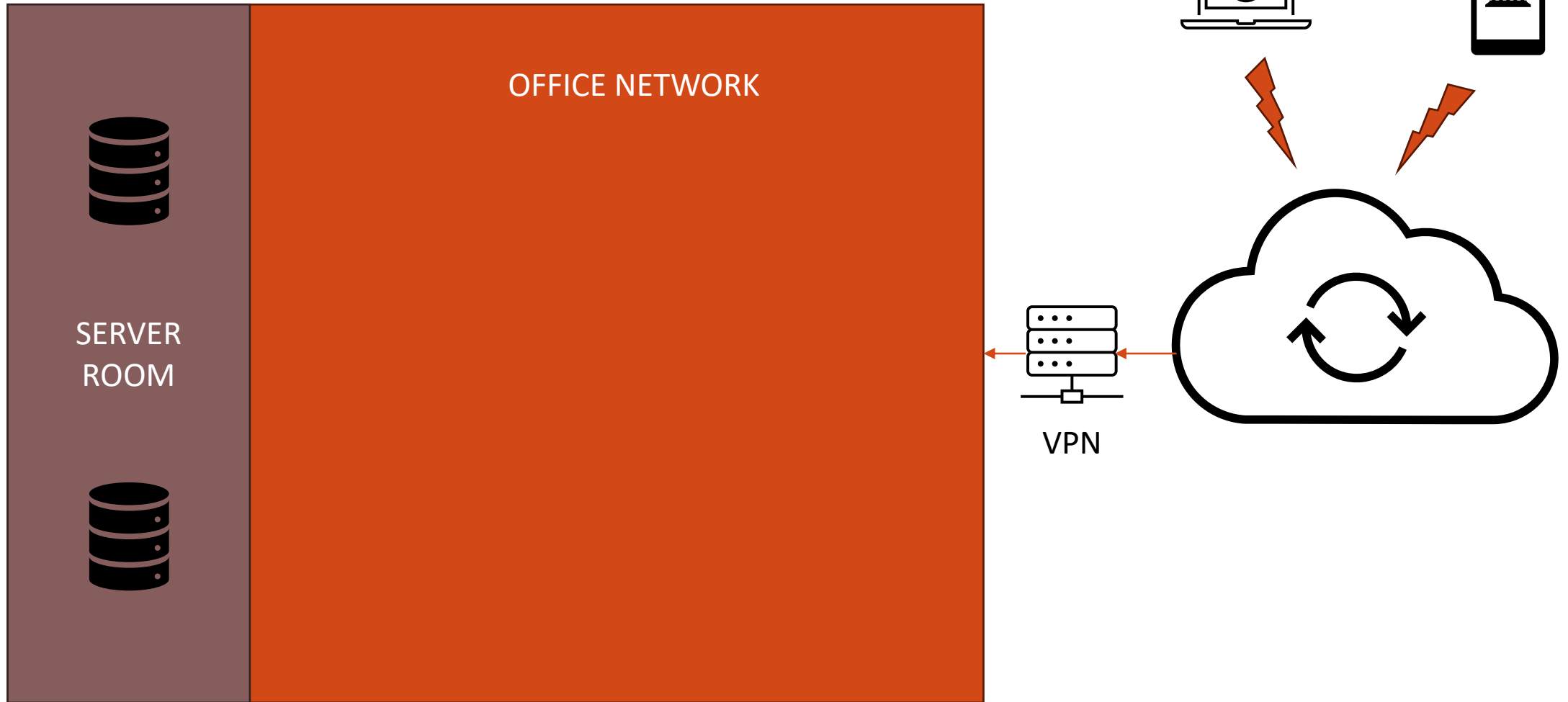
- Network segmentation is best used for north-south traffic (i.e., the traffic that moves into and out of the network). With network segmentation, an entity, such as a user, is trusted once inside a designated zone of the network.
- Microsegmentation, on the other hand, is best used for east-west traffic, or traffic that moves across the data center or cloud network—server-to-server, application-to-server, and so on. Simply put, network segmentation is like a castle's outer walls and moat, whereas microsegmentation is like the guards standing at each of the castle's interior doors.

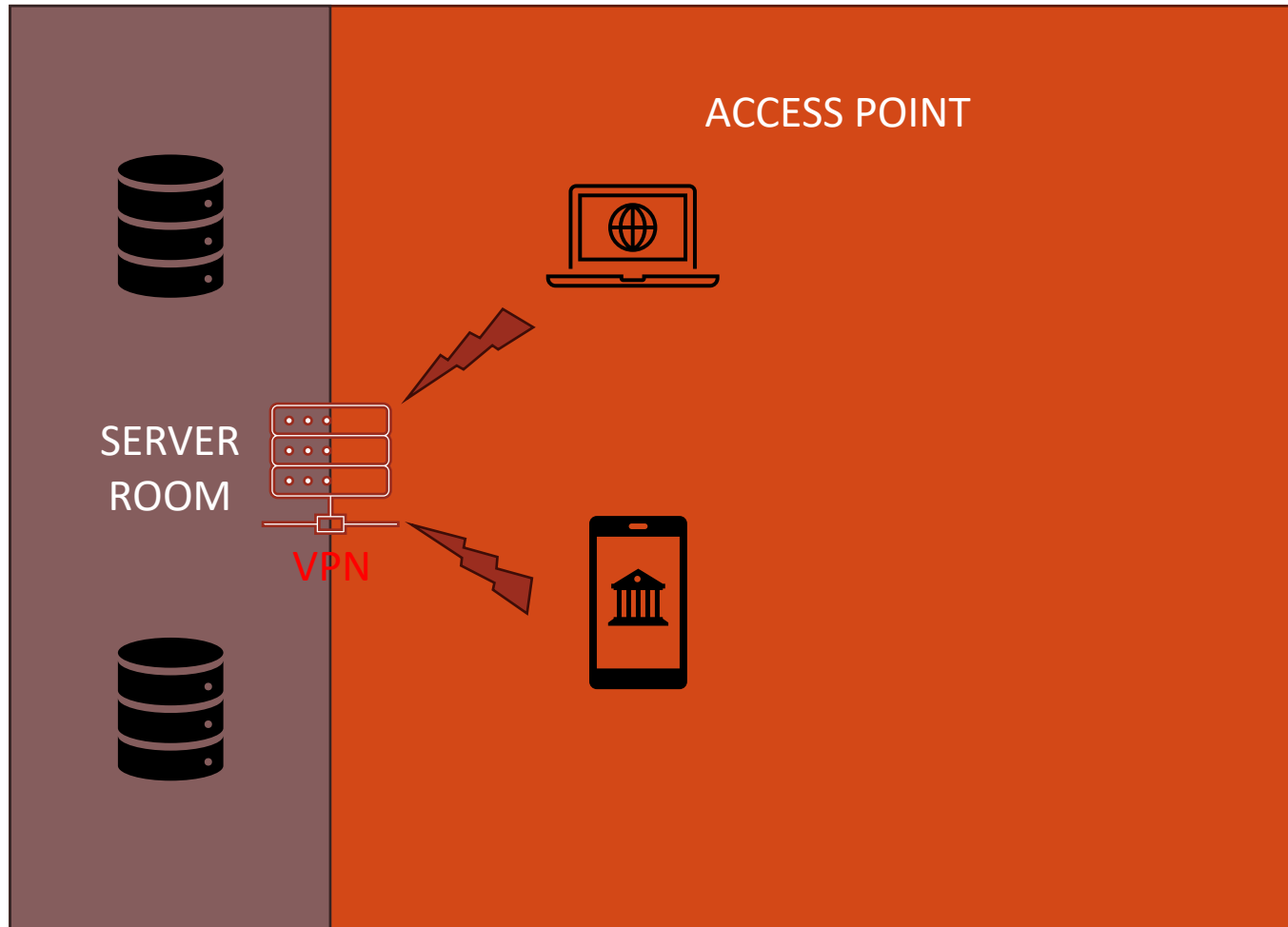
Micro-Segmentation

- Controlling flow between every node or every app
- Controlling “East-West”, instead of “North-South”

What are we Being Offered?

Move the VPN-border





WireGuard or IPsec

IPsec

IPsec – Why?

- Protecting a computer against attacks and malicious code
- Protecting your network
- Creating network segments without LAN/VLAN
- Verifying the integrity of the traffic
- Verifying the identity of the endpoints
- Encrypting traffic
- “Which port to which port” → “From who to which port”
- More allowed traffic if the source is identified, and not as much with ports or IPs

IPsec – What?

- IPsec is a protocol suite
 - AH (*Authenticating Headers*)
 - ESP (*Encapsulating Security Payload*)
 - IKE(v2) (Internet Key Exchange)
 - AuthIP
- Added after IPv4
- Requirement for IPv6 enabled device to support
- Protects communications
 - Identity, Integrity and Encryption – separately
 - Between two nodes, two networks or on top of a VPN
- Works on the Network layer of the OSI model
 - Not just for TCP but also UDP, ICMP, GRE, OSPF etc.

Speaking IPsec

- Both endpoints need to be configured to speak IPsec
 - Connection Security Rule needs to be configured
 - For example:
 - Server Requires IPsec
 - Client is OK to speak IPsec
- Most common problem is that the client won't speak IPsec!

Active devices

- Enterprise-level printers can have a certificate for IPsec
- If you don't require IPsec for outbound connections, you can still print
 - You might not get a "Printing Done" notification from the printer though

IPsec with non-Microsoft OS's

- Linux can speak IPsec – at least with certificates
- IPsec is well supported since Linux Kernel version 2.6
 - *FreeS/WAN*, Openswan- and Strongswan-solutions available if nothing else
- Mac OS X usually requires 3rd party solutions
 - IPSecuritas etc.
- iOS
 - Can have a cert and speak IPsec
- Android
 - Can have a cert and speak IPsec
- Remember that you don't have to have IPsec on every node!

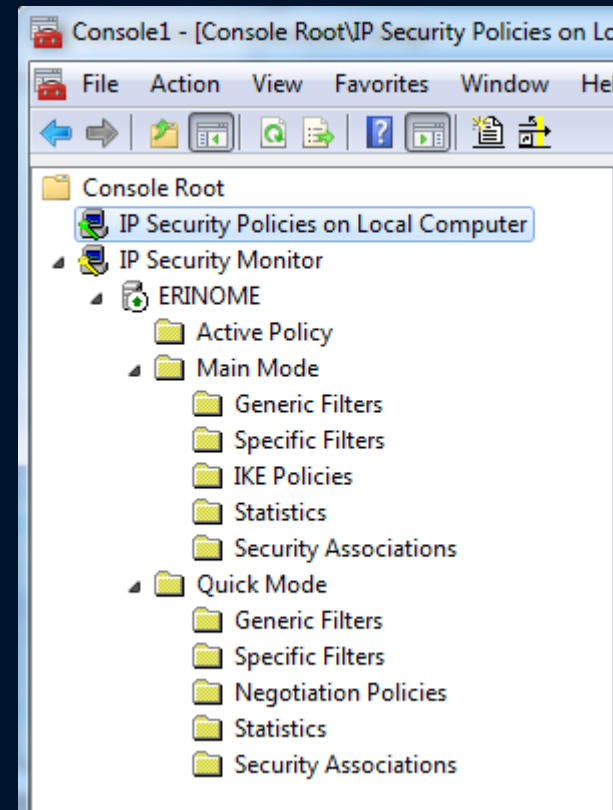
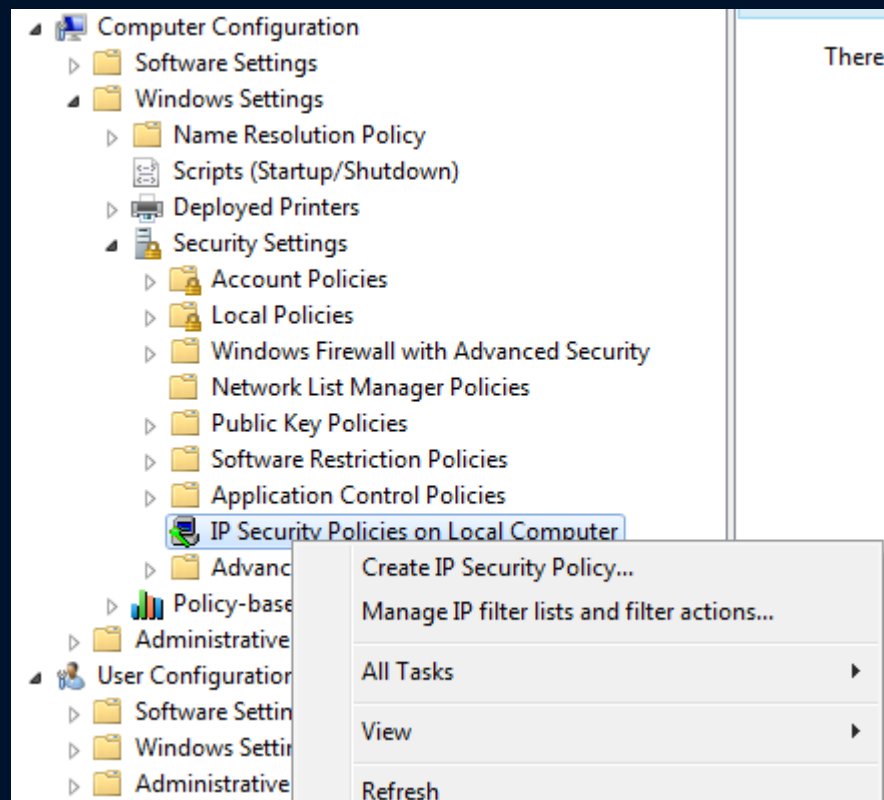
Authentication

- Computers
 - Kerberos
 - Certificate
 - Shared Secret
- Users
 - Kerberos
 - NTLMv2
 - User Certificate
- Health Certificate
 - NAP is deprecated
- Multiple allowed – Kerberos for domain computers, Certs for workgroup

RAW facts

- Easy only since Windows 7
- Requirement for outbound connections requires a proxy to access Google
- Encrypt only if needed (Windows 10/11 does it by default)
- Remember to educate support personel

Older versions



Firewall and IPsec together

The image displays three overlapping screenshots of the Windows Firewall 'New Inbound Rule Wizard' dialog boxes, illustrating the configuration steps for a rule that integrates with IPsec.

Leftmost Screenshot (Action Step):

- Title:** New Inbound Rule Wizard
- Section:** Action
- Instruction:** Specify the action to be taken when a connection matches the conditions specified in the rule.
- Steps:** Rule Type, Program, Protocol and Ports, Scope, Action, Users, Computers, Profile, Name.
- Options:**
 - ☐ Allow the connection. This includes connections that are protected with IPsec.
 - ☒ Allow the connection if it is secure. This includes only connections that have been authenticated and will be secured using the settings in IPsec properties and the Rule node. (Customize... button)
 - ☐ Block the connection.

Middle Screenshot (Users Step):

- Title:** New Inbound Rule Wizard
- Section:** Users
- Instruction:** Specify the users that are allowed to make the connection specified by this rule.
- Steps:** Rule Type, Program, Protocol and Ports, Scope, Action, Users, Computers, Profile, Name.
- Authorized users:**
 - ☐ Only allow connections from these users.
 - (Empty list box)
- Exceptions:**
 - ☐ Skip this rule for connections from these users.
 - (Empty list box)
- Note:** user identities can only be verified if an authentication method that carries user identity is used.

Rightmost Screenshot (Computers Step):

- Title:** New Inbound Rule Wizard
- Section:** Computers
- Instruction:** Specify the computers that are allowed to make the connection specified by this rule.
- Steps:** Rule Type, Program, Protocol and Ports, Scope, Action, Users, Computers, Profile, Name.
- Authorized computers:**
 - ☐ Only allow connections from these computers:
 - (Empty list box) [Add... Remove]
- Exceptions:**
 - ☐ Skip this rule for connections from these computers:
 - (Empty list box) [Add... Remove]
- Note:** computer identities can only be verified if an authentication method that carries computer identity is used.
- Buttons:** < Back, Next >, Cancel.

Good run-through for PAWs

- <https://improsec.com/tech-blog/setup-rdp-dc-jumphost-paw-ipsec>

How I use IPsec

- Require Inbound, Request Outbound
- Kerberos for users and computers
- Exclude hard cases – You don't need to get to 100%!
- Buy printers (etc) that can have a certificate if you need to – YOU RARELY DO!

POC

- You can use “Shared Secrets” for Proof of Concept (or home use and such)

DEMO - IPsec

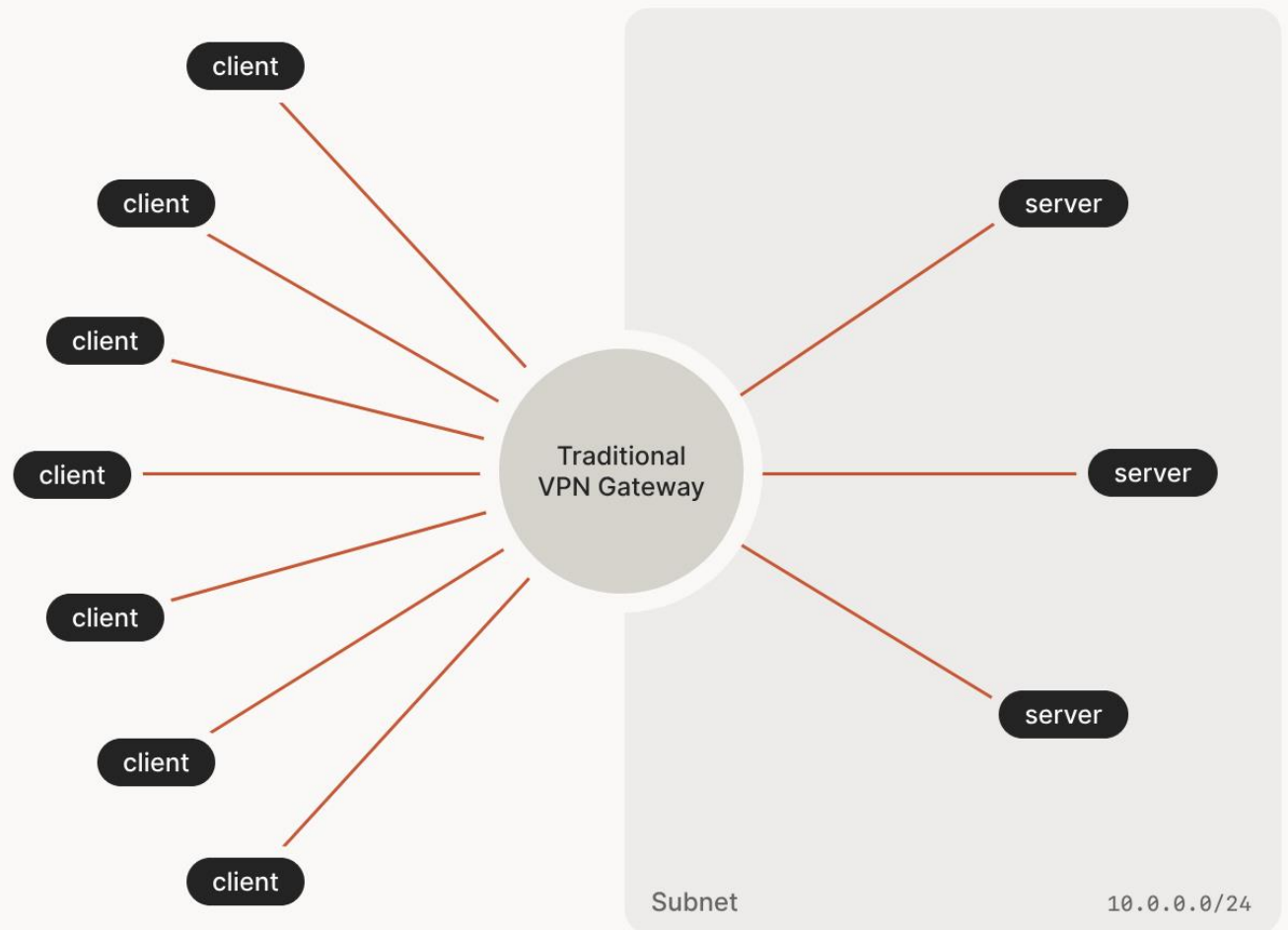
Domain Isolation – Frankfurt DC

STUDENT-computers into IPsec and PING CSV1

RDP-protection

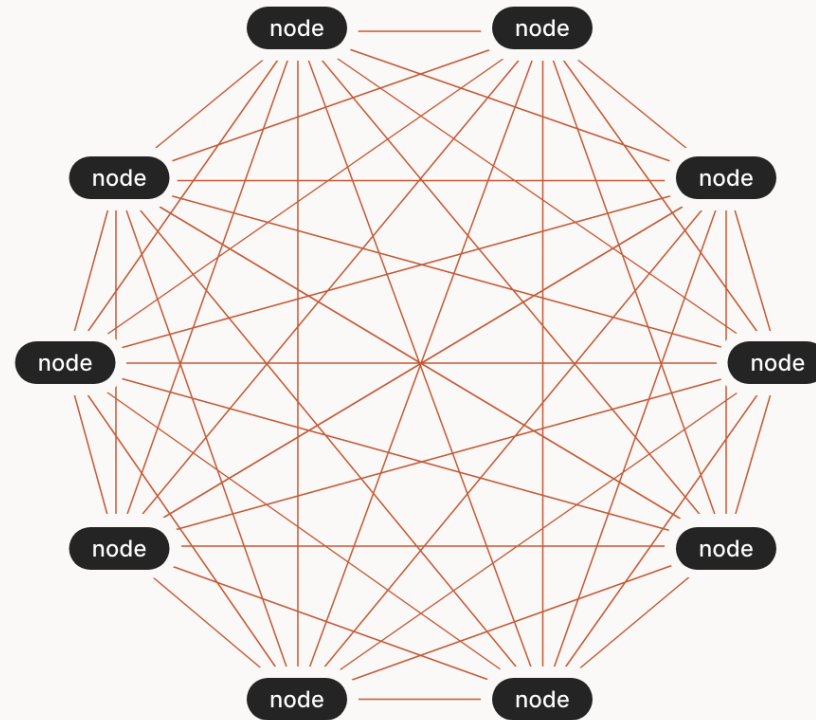
WireGuard

Traditional VPN



WireGuard

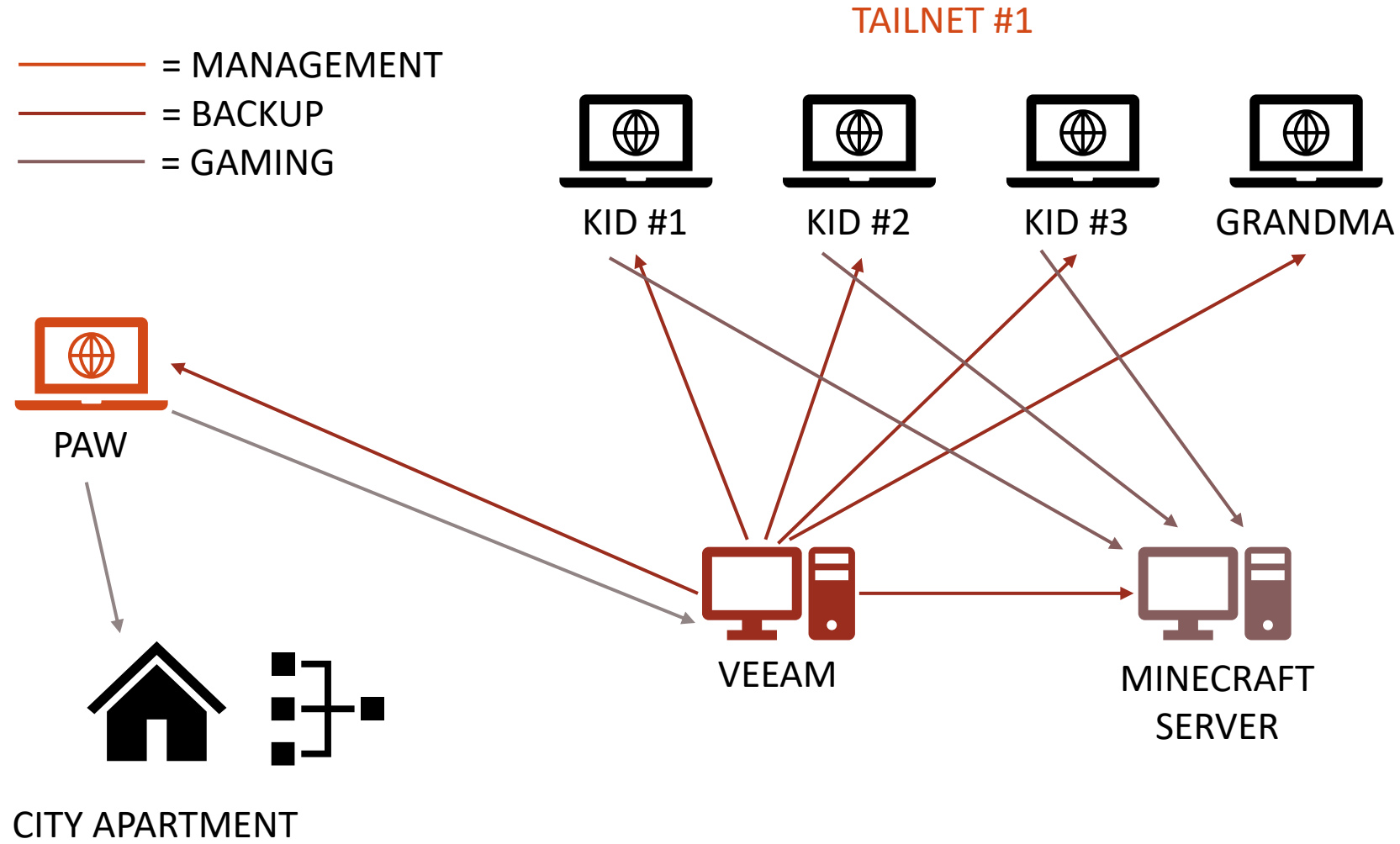
MESH



$n(n-1) = 90$ WireGuard endpoints (for 45 connections)

Zero Trust with my Children







Access Controls

Define a policy for which devices and users are allowed to connect in your network. [Learn more](#) →

 Edit file

 Preview changes

 Preview rules

```
30     "dst": ["autogroup:self:*"],
31   },
32   // Servers can access devices tagged tag:SIENITIE on limited ports
33   {
34     "action": "accept",
35     "src": ["tag:SERVER"],
36     "dst": ["tag:SIENITIE:*"],
37   },
38   {
39     "action": "accept",
40     "src": ["tag:SERVER"],
41     "dst": ["tag:SIENITIE:49152-65535"],
42   },
43   // SIENITIE can access devices tagged tag:SERVER on limited ports
44   {
45     "action": "accept",
46     "src": ["tag:SIENITIE"],
47     "dst": ["tag:SERVER:10005"],
48   },
```

TAILNET #2

—— = TRUE ZERO TRUST



WIFE

DEMO - WireGuard

TAIL1 GPUUpdate

TAIL2 to Domain

Changing TAGS

Latency

“In Security, don’t
let perfect be the
enemy of good”

Contact

- sami@adminize.com
- Twitter: @samilaiho
- Free newsletter: <http://eepurl.com/F-Goj>
- My trainings:
 - <https://corellia.fi/sami-laiho-courses/>
 - <https://win-fu.com/dojo/>
 - Free for one month!!
 - Promo Code: TRIAL2023

