Connecting Remotely Like a Pro

CONTACT@ADAMFURMANEK.PL

HTTP://BLOG.ADAMFURMANEK.PL

FURMANEKADAM

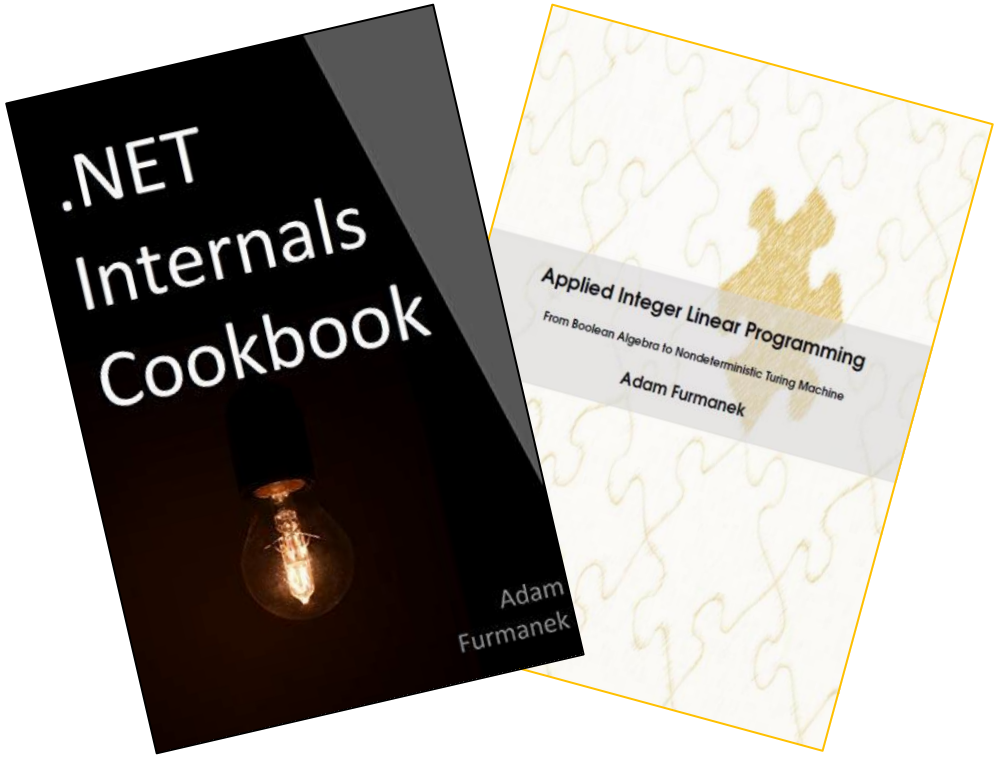
About me

Software Engineer, Blogger, Book Writer, Public Speaker.
Author of ***Applied Integer Linear Programming*** and ***.NET Internals Cookbook***.

http://blog.adamfurmanek.pl

contact@adamfurmanek.pl

furmanekadam



Random IT Utensils

IT, operating systems, maths, and more.

Agenda

Split Tunnel, VPN, VNC, RDP, OpenSSH.

Link Aggregation with Multicast.

TCP over ICMP, TCP over DNS.

Intel AMT.

Full Tunnel, Jump Host, Disk2vhd, TCP over File System, TCP over Pipe, SSLH.

Video conferences and container separation.

Supercharging your workstation.

Summary.

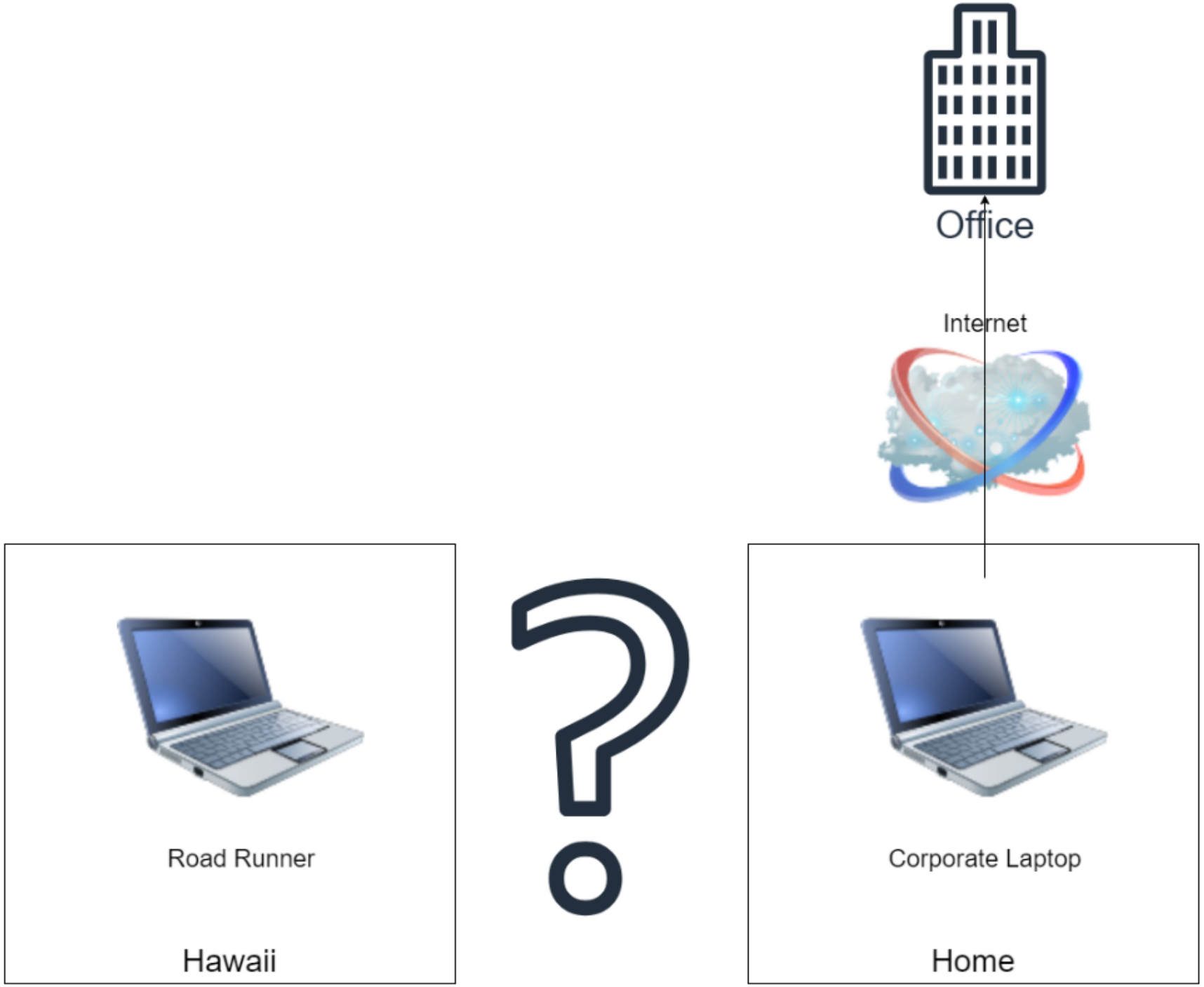
Problem statement

Problem statement

I want to fly to Hawaii, but I don’t want to take the **corporate laptop** with me.

I want to take another laptop that I call **road runner** which is my personal device. I’m going to use it to work remotely.

How to do it?


Office
Internet
Road Runner
Hawaii
Corporate Laptop
Home

Legal considerations

You may not be allowed to work remotely at all.

You may not be allowed to work from another country.

You may not be allowed to use non-corporate machine.

You may not be allowed to take the machine to another country.

You may not be allowed to work from public places.

CONSULT YOUR LEGAL AND SECURITY DEPARTMENTS.

Privacy Screen

MUST HAVE when you work from public places (restaurants, airports, trains).

Around 20 USD.

Remember that it doesn’t give full confidentiality.

Always wear your headphones.

Always watch for cameras and CCTV.

Avoid typing confidential information as much as possible.

Practical considerations

Companies are legally allowed to monitor your activity and how you use the machine.

There are multiple solutions to monitor clicks, keyboard, network activity, running applications, filesystem, USB drives, elevation and much more.

Do not use your corporate machine for private purposes.

Consult company policies for password management, allowed applications, administrator/root permissions, and other.

Better safe than sorry.

The best way to work remotely?

Just ask your IT department if they have the infrastructure to connect to the intranet from outside of the VPN.

Protocols

Visual connection

REMOTE DESKTOP PROTOCOL - RDP

Supports display reconfiguration.

Supports logging into an existing session, or creating new session. Supports concurrent sessions.

Can forward KVM, speakers, microphone, graphics card, USB devices, shortcuts, hotkeys, clipboard.

Can work with 0.5 Mbps connection.

Microsoft supports basically all client platforms.

VIRTUAL NETWORK COMPUTING - VNC

Doesn’t support display reconfiguration.

Supports logging into an existing session only.

Can forward KVM only (there are extensions, though).

Requires fast connection. Use Hextile algorithm if possible.

Visual connection

X11 FORWARDING

Supports display reconfiguration.

Supports creating new session only. Supports concurrent sessions.

Can forward KVM, shortcuts, hotkeys, clipboard. There are extensions.

Requires fast connection.

XPRA

Supports display reconfiguration.

Supports logging into an existing session. Supports concurrent sessions.

Can forward KVM, shortcuts, hotkeys, clipboard. There are extensions.

Requires fast connection.

Command line connection

SECURE SHELL (SSH)

Supports creating new session only. Supports concurrent sessions.

Can forward keyboard, and ports.

Must have for everyone!

POWERSHELL REMOTING - PSREMOTING

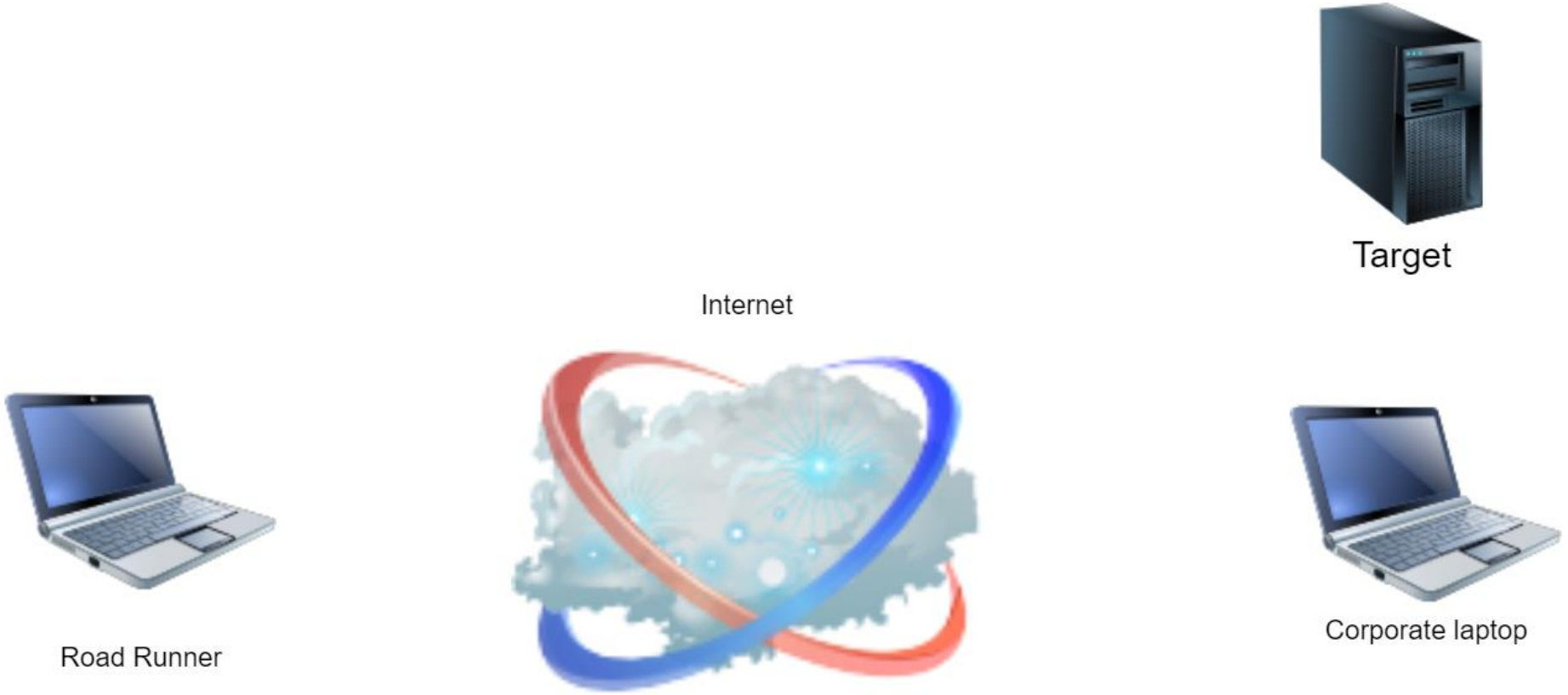
Supports creating new session only. Supports concurrent sessions.

Can forward keyboard.

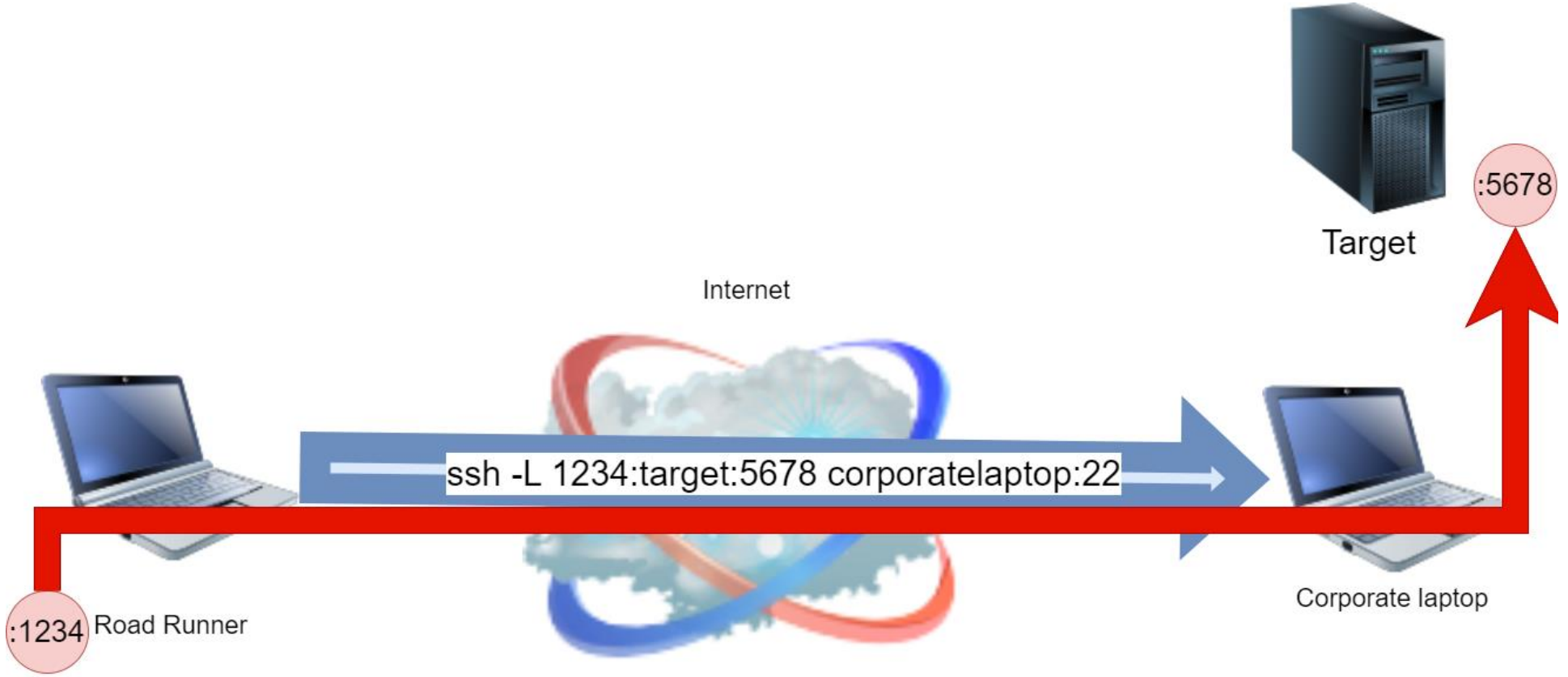
Uses HTTP behind the scenes.

Very nasty configuration.

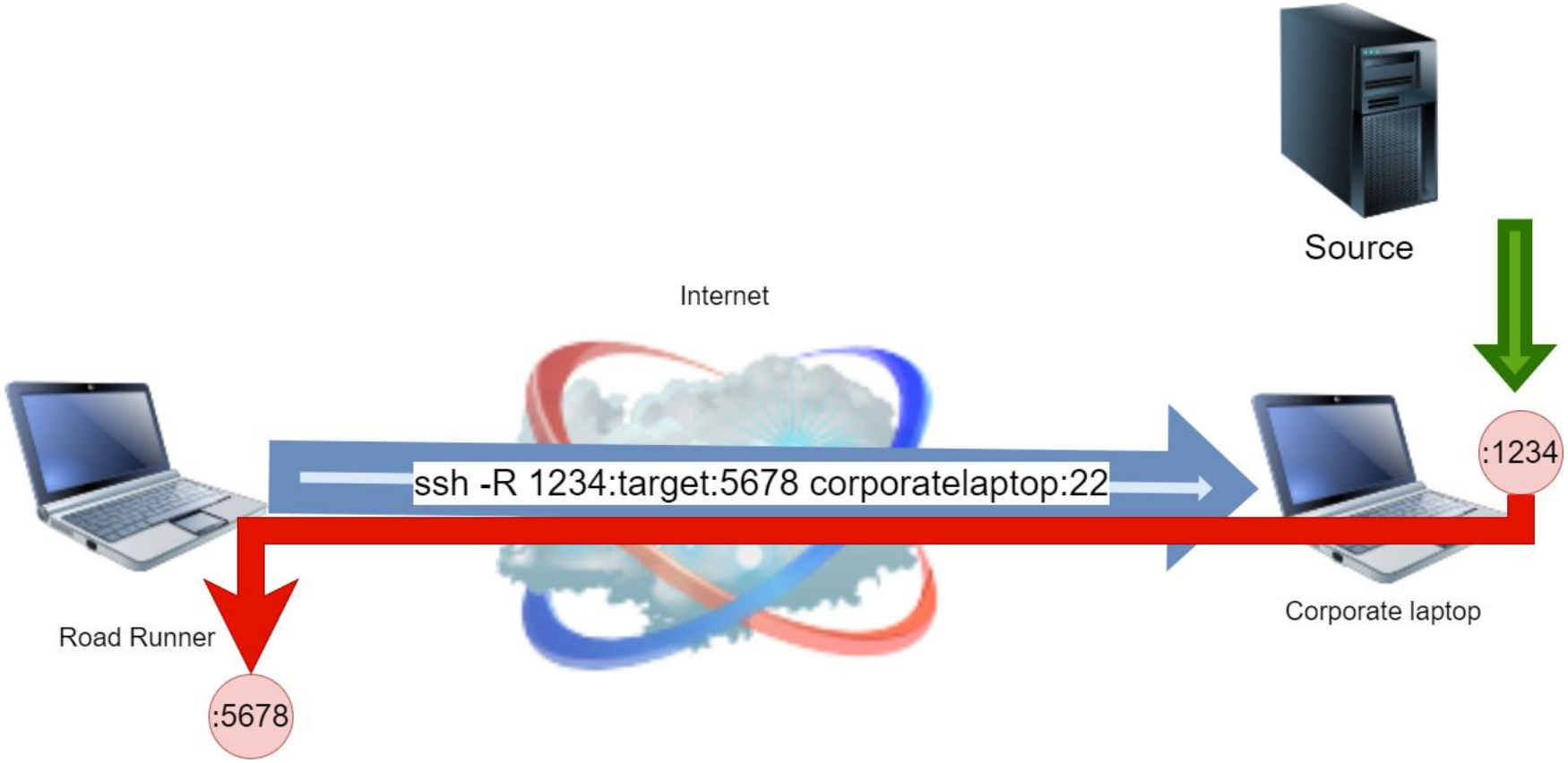
SSH Tunneling



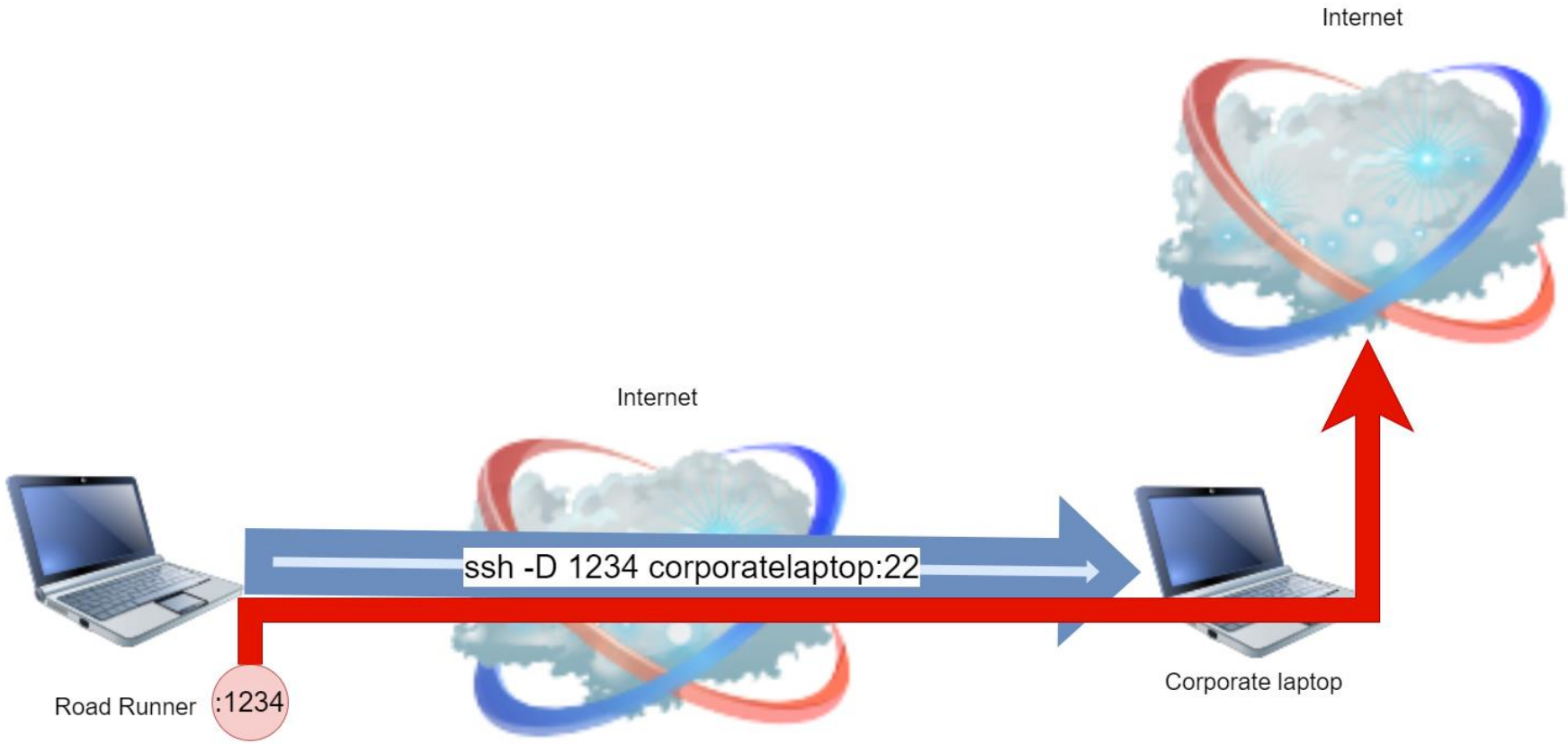
SSH Tunneling – Local Forwarding



SSH Tunneling – Remote Forwarding



SSH Tunneling – Dynamic Forwarding (SOCKS)



Dynamic Forwarding Demo

FOXYPROXY

SSH Forwarding

This is the killer feature! We can multiplex connections.

Once we have **one connection** to the target, we can do anything.

If you ever need to route multiple connections in hard network conditions, then route OpenSSH and use forwarding.

I want to connect to my machine

SCENARIO

VPN

Virtual Private Network.

Routes and encrypts traffic, DNS.

Can use proprietary protocols, well-known non-HTTP protocols (L2TP, PPP), HTTP-based protocols (SSTP), or even HTTPS proxy.

Typically works in one of two modes:

- Split tunnel – routes only corporate traffic, everything else stays the same
- Full tunnel – routes WHOLE traffic, typically modifies *route table* to disallow any changes

Cisco AnyConnect, Windows built-in implementation, Zscaler, Microsoft Intune, OpenConnect, OpenVPN.

Split tunnel

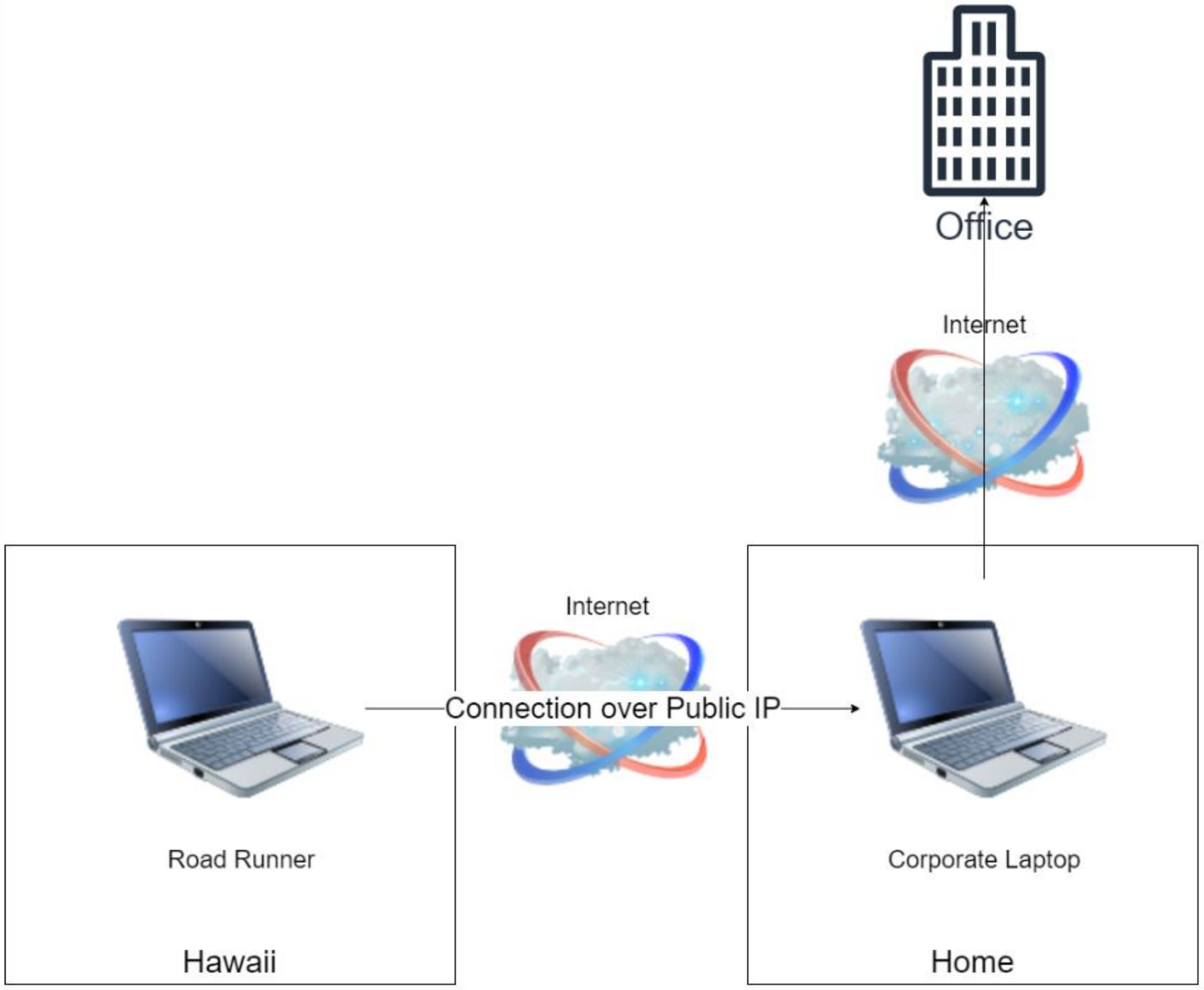
Very rare setup. Consider yourself lucky ;)

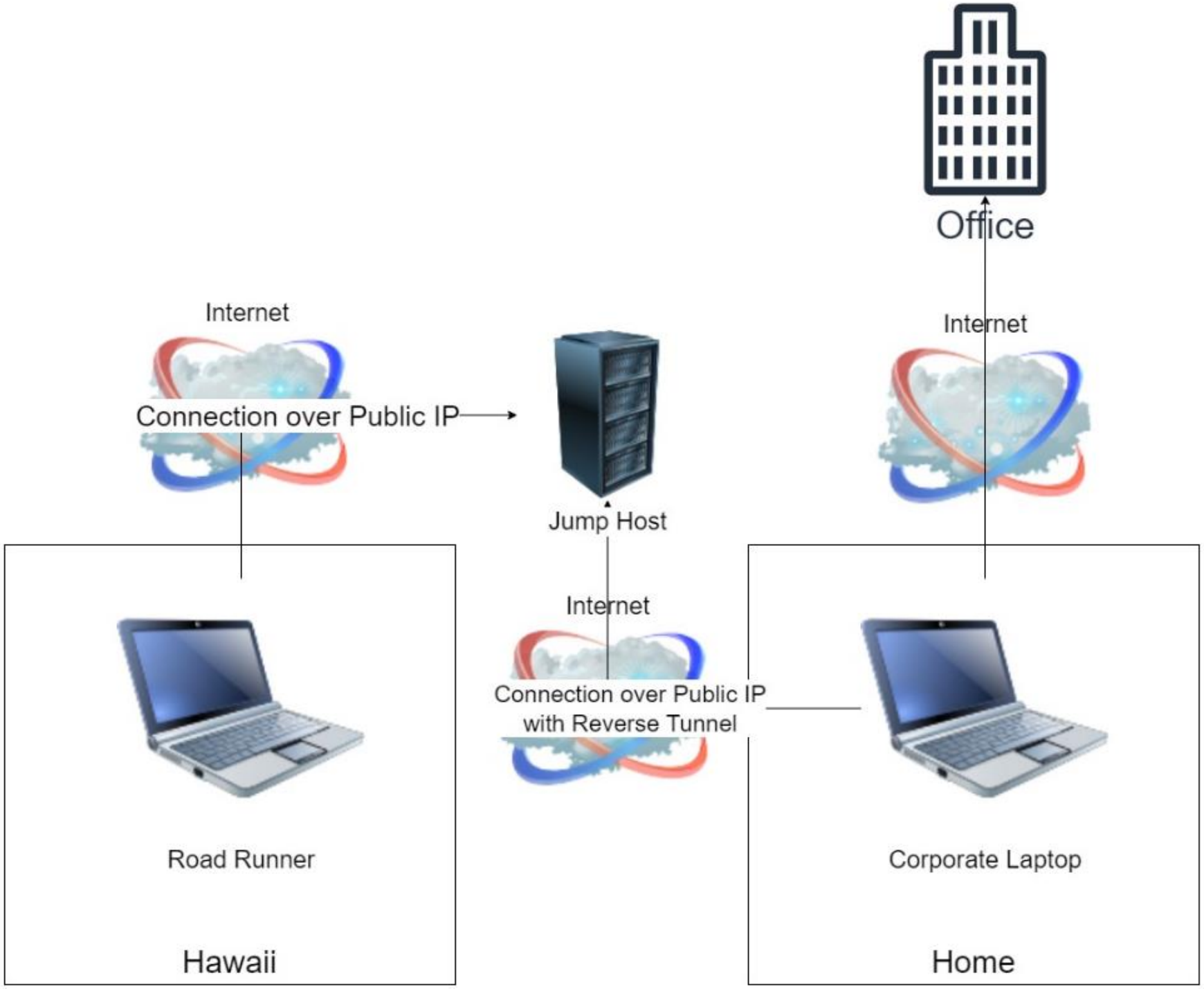
The machine has regular connectivity to the Internet, so we can use Internet-wide solutions.

Company may still track the network traffic or running applications.

If we have IPv4 or IPv6 that is achievable from the wide Internet, then we can use anything.

Otherwise, we need to configure VPN or Reverse Tunnel.


Office
Internet
Internet
Connection over Public IP
Road Runner
Hawaii
Corporate Laptop
Home


Office
Internet
Internet
Connection over Public IP
Jump Host
Internet
Connection over Public IP
with Reverse Tunnel
Road Runner
Corporate Laptop
Hawaii
Home

Some practical considerations

Don’t expose services on default ports.

Use strong passwords and public keys.

Check logs for attacks.

Configure your firewall properly.

Have your own domain and use A records. Much easier to migrate servers.

Keep an eye on reflect attacks.

I am on a train and my connection is laggy

SCENARIO

What goes wrong on a train?

Tunnels, bridges, mountains, railways far away from city centers.

No service.

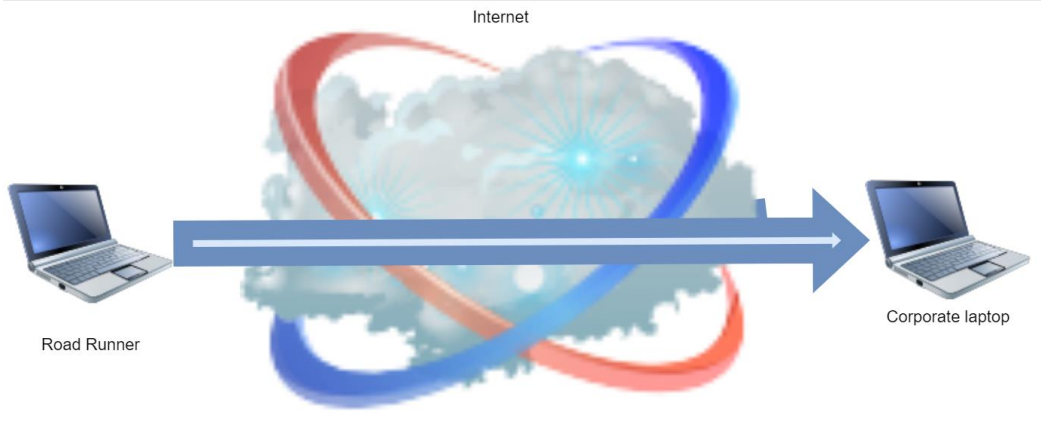
Slow handover between access points.

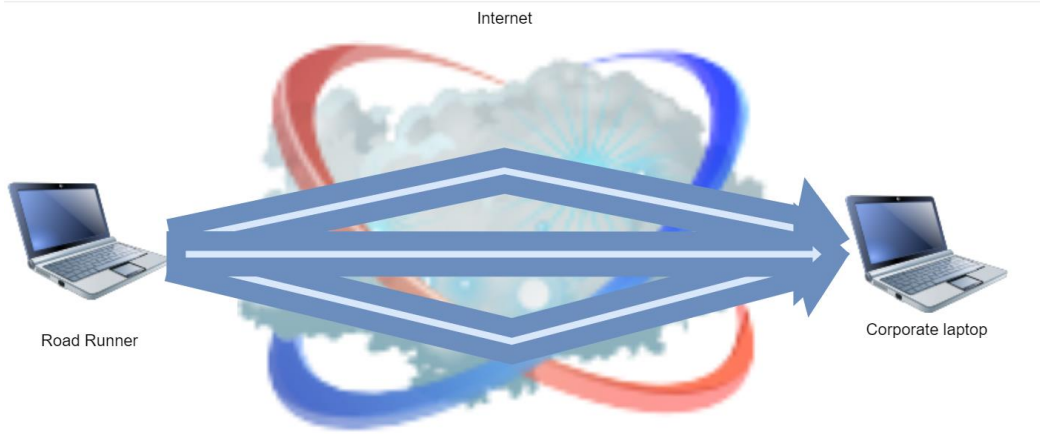
Handover between technologies.

Mobile network forcing us to us slower technologies.

Roaming.

What if


Internet
Road Runner
Corporate laptop


Internet
Road Runner
Corporate laptop

Link aggregation

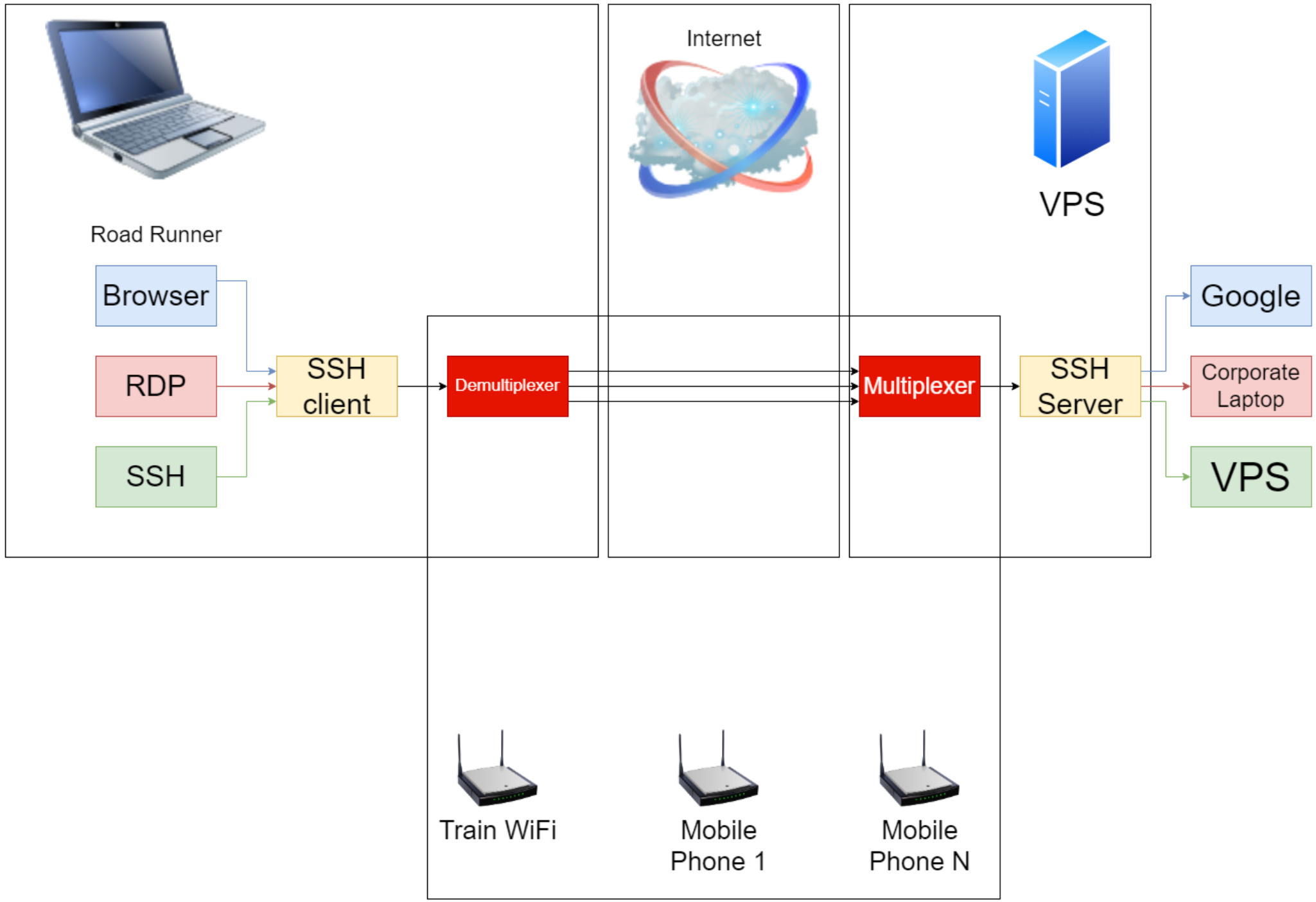
In computer networking, link aggregation is the **combining of multiple network connections** in parallel by any of several methods.

Also known as trunking, bundling, bonding, channeling, teaming.

Standards like 802.3ad, 802.1AX, Link Aggregation Control Protocol (LACP).

Various policies:

- Round-robin – we send packets in sequential order using all Network Interfaces (NICs)
- Active-backup – only one NIC is active, and we switch to another one if the primary fails
- **Broadcast – we send each packet using every NIC**
- Adaptive load balancing – we measure links and choose the fastest one as we go


Internet
VPS
Road Runner
Browser
RDP
SSH
SSH client
Demultiplexer
Multiplexer
SSH Server
Google
Corporate Laptop
VPS
Train WiFi
Mobile Phone 1
Mobile Phone N

Link aggregation with broadcast demo

Practical considerations

SIM cards may be dirt cheap, so we can buy many of them (think about major mobile providers in your country).

If you need multiple connections to the same domain, but you need different credentials, then put aliases in /etc/hosts.

Phone may downgrade network quality. Use ***#4636#*** or ***ForceLTE*** application (Android).

This is better for phone calls than regular GSM.

Some stats: train route from Kraków to Gdańsk (around 600 km):

Network	Sent	Received
Pendolino WiFi	15.6 MB	354 MB
Play	15.1 MB	339 MB
T-Mobile	14.4 MB	213 MB

I am on a plane and my connection is weird

SCENARIO

What wrong with plane (airport, hotel, city hotspot…)?

Weird ***portals*** for getting connection.

Time-limited connections.

Price.

Blocked ports (that’s why we have SSTP).

Chat-only connections.

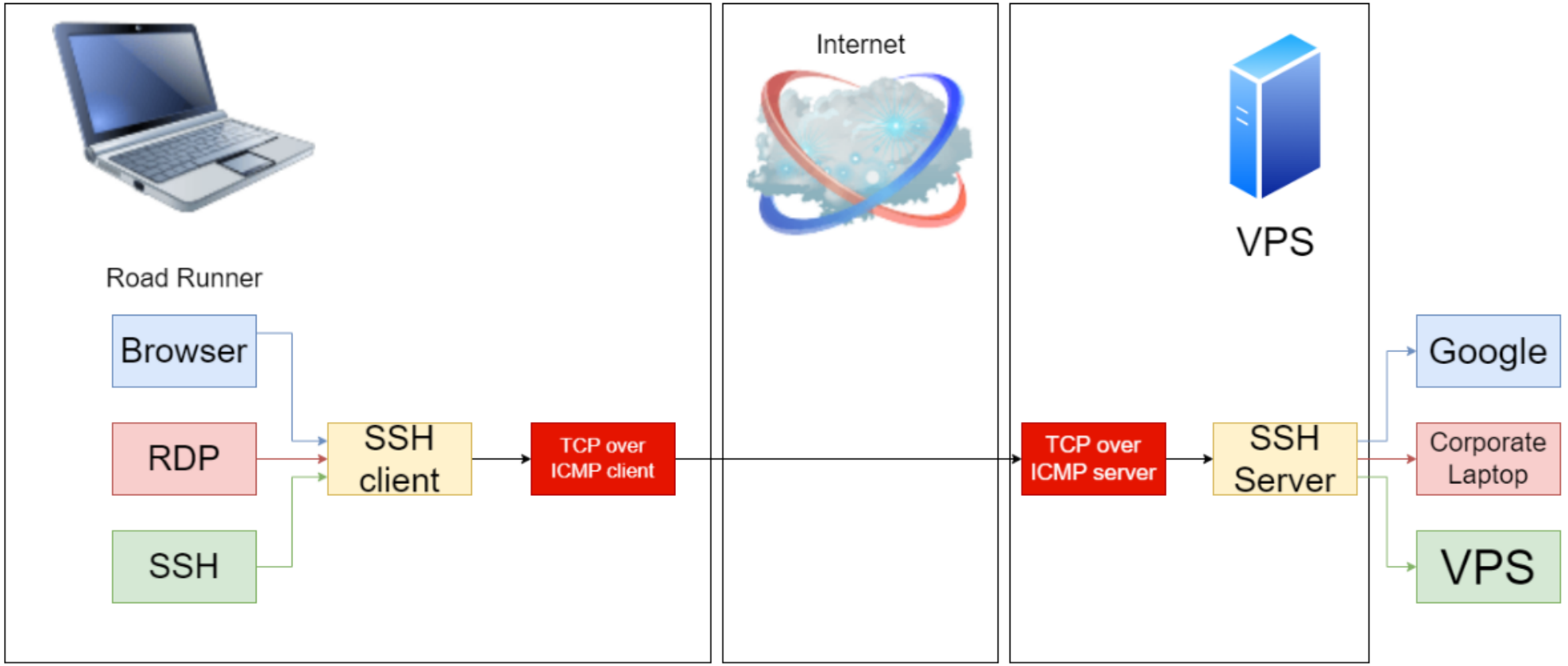
TCP over ICMP

Internet Control Message Protocol (ICMP, also known as ping).

It is sometimes allowed to pass through despite other ports being blocked.

ICMP can achieve “near-native” speed.

TCP over ICMP



TCP over ICMP demo

TCP over DNS

Domain Name Server (DNS) supports multiple record types: A, CNAME, TXT.

It’s hierarchical. When one server cannot answer the query, the server asks another server for help.

Idea:

- Let’s configure domain a.com
- Let’s encode packet using Base16. We get something like ***abc123456***
- We then ask the server about domain ***abc123456.a.com***

This is slow. Very, very slow. SSH will barely work. Not production ready.

TCP over DNS demo

My corporate laptop died

SCENARIO

Intel Management Engine with Intel Active Management Technology

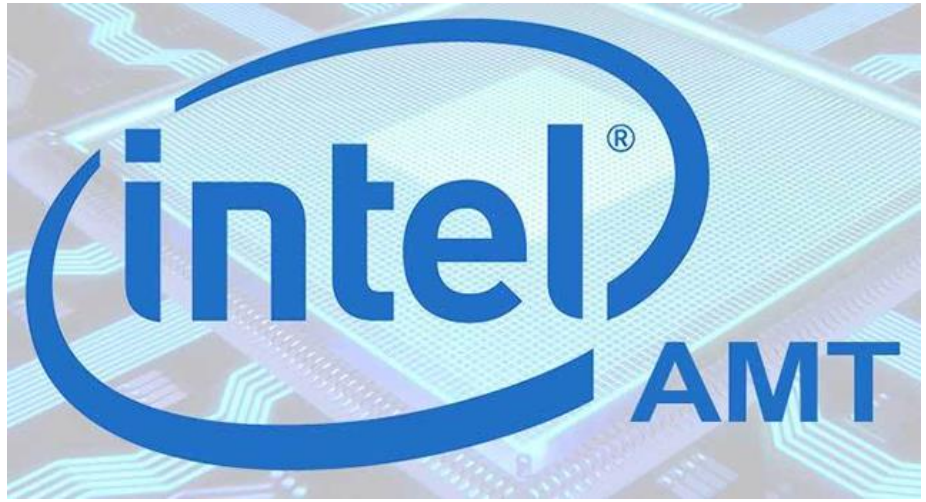
Modern Intel CPUs have built-in operating system (based on Minix).

Once enabled, the system is active **all the time**. Even if the machine is turned off.

AMT uses built-in Ethernet card or WiFi connection.

AMT exposes remote console with web server, VNC connection, and others.

We can query the machine, restart it, or connect remotely.



Intel Management Engine with Intel Active Management Technology

Part of Intel vPro (one of many components).

This requires motherboard support (most of the times). The addon is called Management Engine BIOS extension (MEBx).

We can configure AMT without the extension (in theory).

Multiple configuration modes: Host-Based Configuration (HCU), Remote Configuration Service (RCS).

CPU cannot trust anyone. The user is an attacker!

AMD has equivalent technology called DASH.

Enterprise-ready systems use AMT under the hood: CIRA, Beyond Trust (previously Bomgar).

Some attacks used AMT – Ring -3 rootkit.

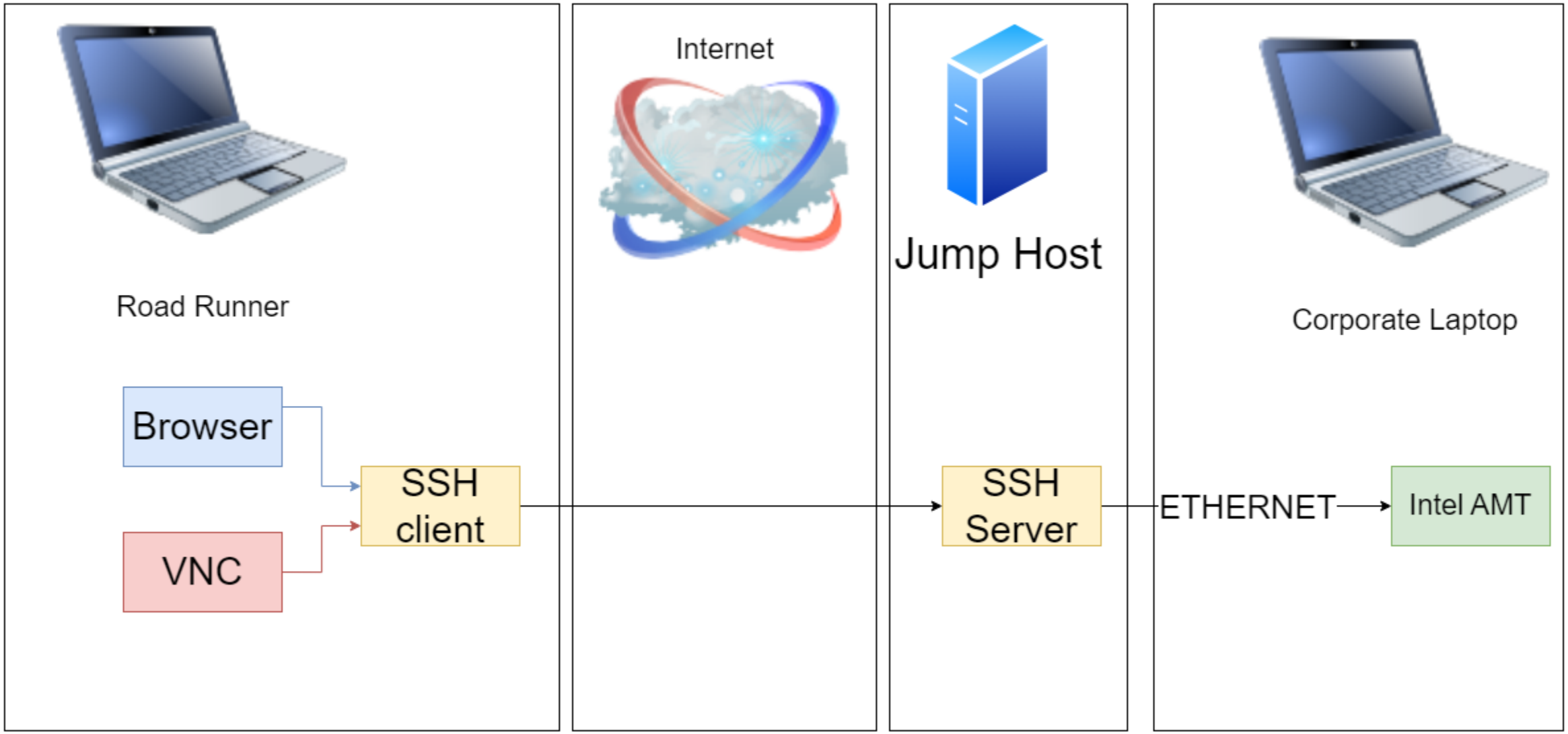
AMT can be blocked on the firewall/router.

AMT cannot use Ethernet card plugged in via USB.

Intel® Flex Memory Access	Yes
Intel® Identity Protection Technology ‡	Yes
Intel® Smart Response Technology	Yes
Intel® My WiFi Technology	Yes

Security & Reliability

Intel vPro® Eligibility ‡	Intel vPro® Platform
Intel® AES New Instructions	Yes
Secure Key	Yes
Intel® Software Guard Extensions (Intel® SGX)	Yes with Intel® ME
Intel® Memory Protection Extensions (Intel® MPX)	Yes
Intel® Trusted Execution Technology ‡	Yes
Execute Disable Bit ‡	Yes
Intel® OS Guard	Yes
Intel® Boot Guard	Yes
Intel® Stable IT Platform Program (SIPP)	Yes
Intel® Virtualization Technology (VT-x) ‡	Yes
Intel® Virtualization Technology for Directed I/O (VT-d) ‡	Yes
Intel® VT-x with Extended Page Tables (EPT) ‡	Yes


Internet
Jump Host
Road Runner
Corporate Laptop
Browser
VNC
SSH client
SSH Server
ETHERNET
Intel AMT

Intel AMT demo

Practical considerations

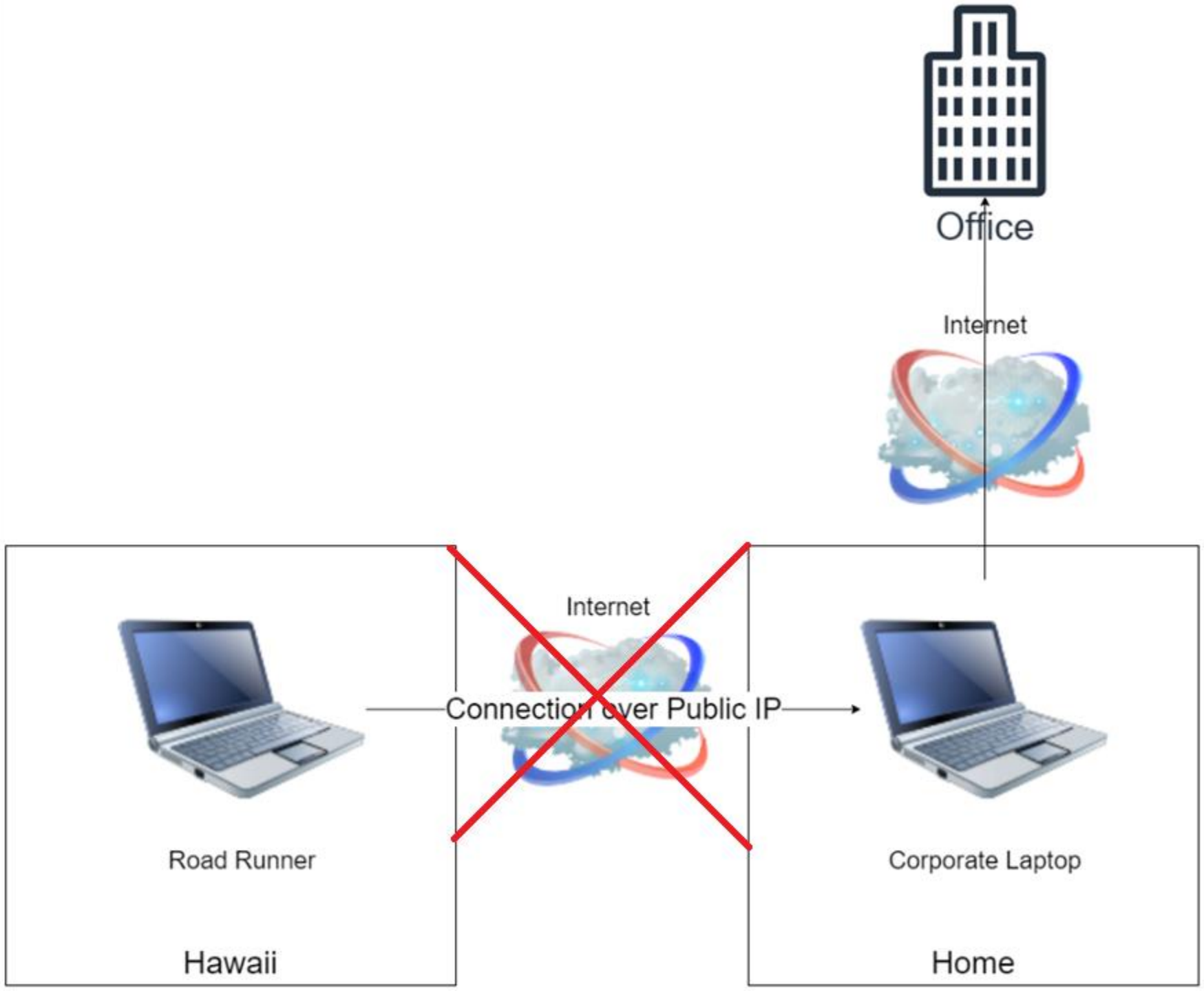
You can use any cheap Windows-based tablet as a jump host (they cost 30 USD).

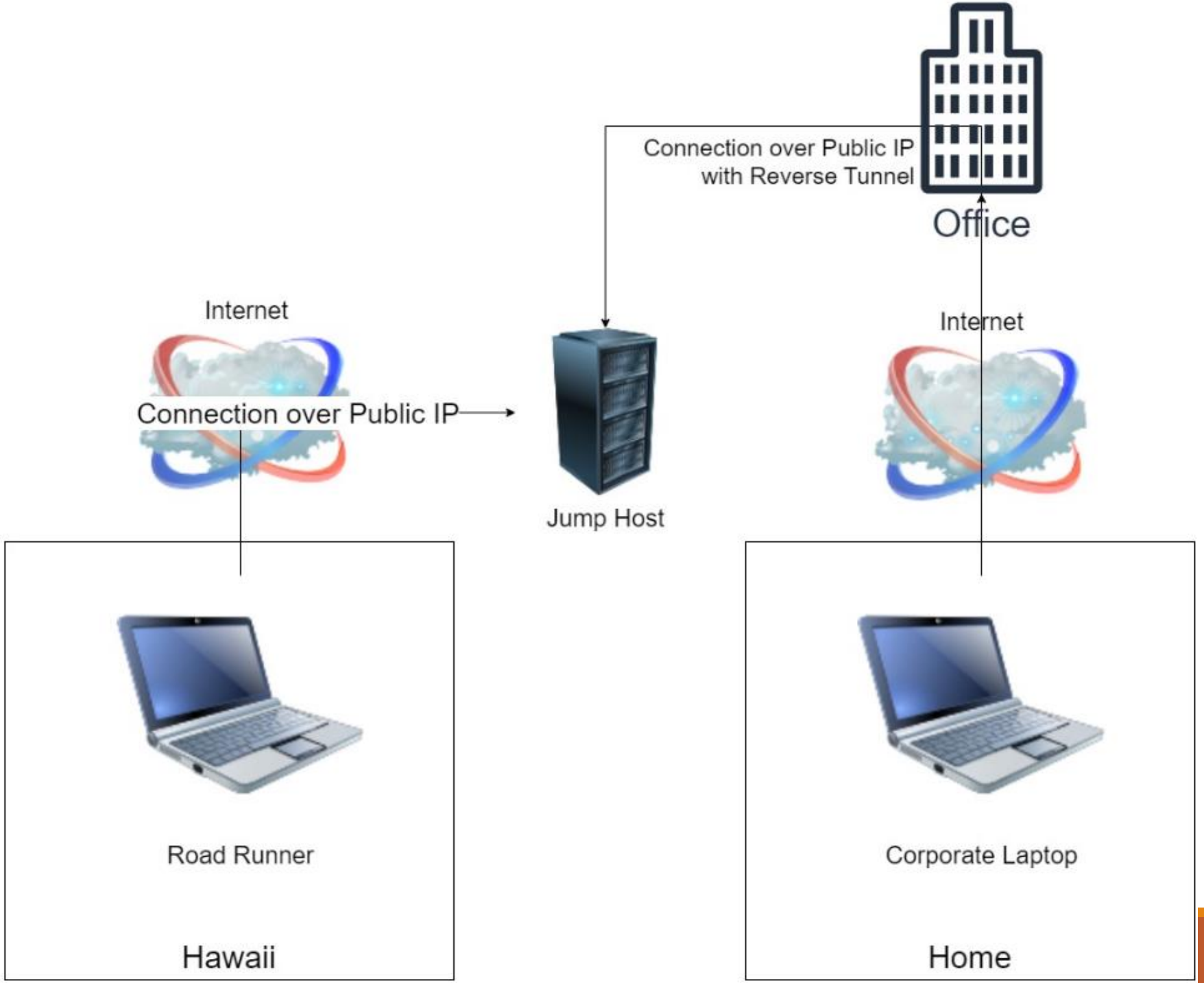
Make sure you have redundant network connectivity.

Don’t expose AMT over the Internet!

I have a full tunnel and I want to connect to my machine

SCENARIO


Office
Internet
Internet
Connection over Public IP
Road Runner
Hawaii
Corporate Laptop
Home


Office
Connection over Public IP
with Reverse Tunnel
Internet
Connection over Public IP
Jump Host
Internet
Road Runner
Hawaii
Corporate Laptop
Home

Full tunnel

Typical setup.

Machine has no regular connectivity to the Internet, so we cannot connect to it from the wide Internet.

Whole network traffic goes through the VPN provider. Traffic within LAN is typically blocked.

Typically implemented with route tables and network driver.

We can configure the reverse tunnel, but the company will see the connection.

Direction connection won’t work.

Connection via jump host will work, but it will go through the company network.

Intel AMT connection will still work, but AMT is not RDP.

How to escape the tunnel?

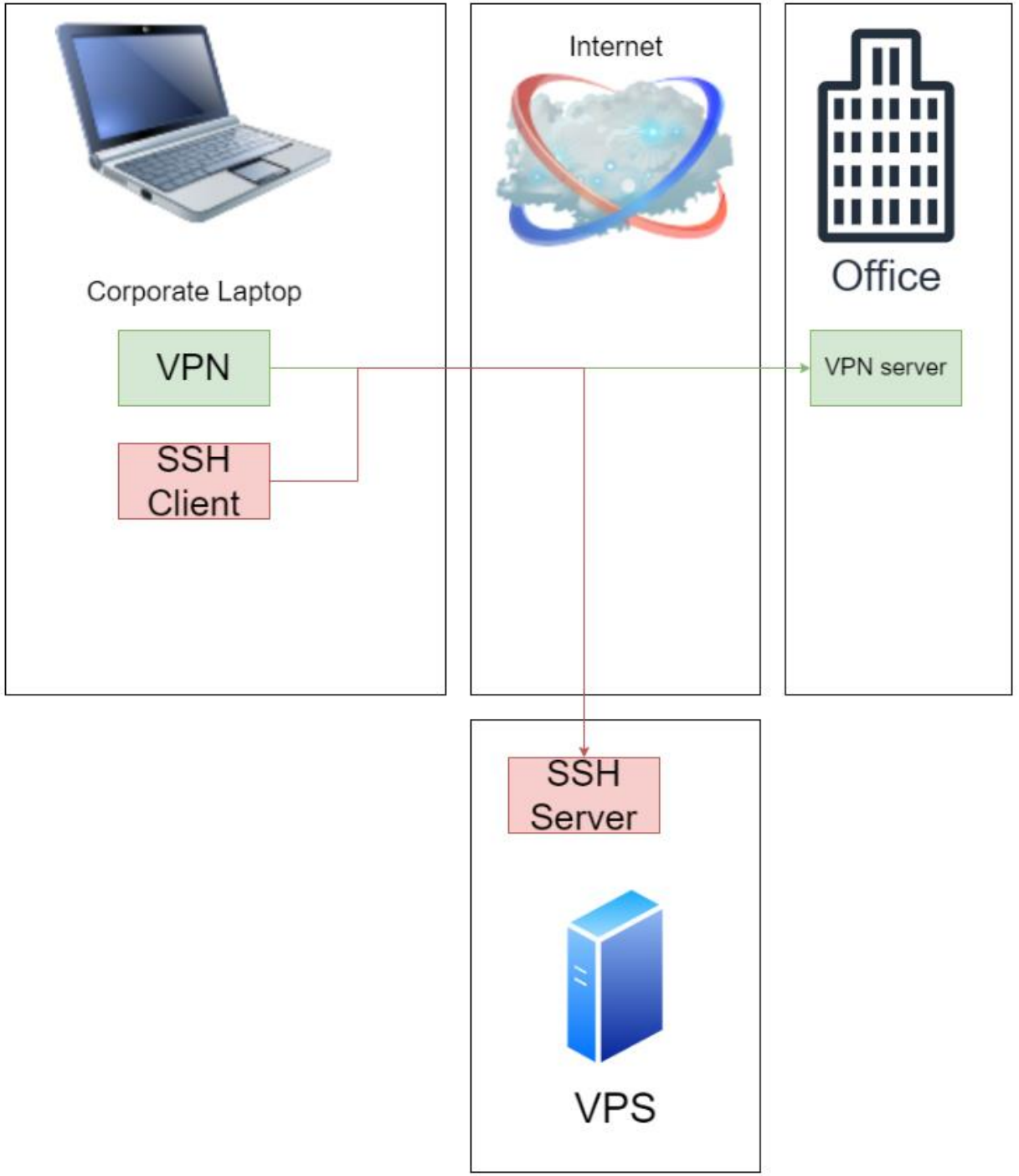
SSLH

A SSL/SSH multiplexer based on regular expressions.

We can tell TLS connection from SSH by examining first packet:

- If it’s binary, then we’re opening a connection for TLS negotiation
- If it’s textual, then we’re opening an OpenSSH connection

We can configure connection that will be allowed by the firewall and route table, but hijack it to create a reverse tunnel.


Internet
Corporate Laptop
VPN
SSH Client
Office
VPN server
SSH Server
VPS

SSLH demo

Can I abandon the corporate laptop?

SCENARIO

Disk2vhd

What's the easiest way to control the environment in which the machine is running? Virtualize everything.

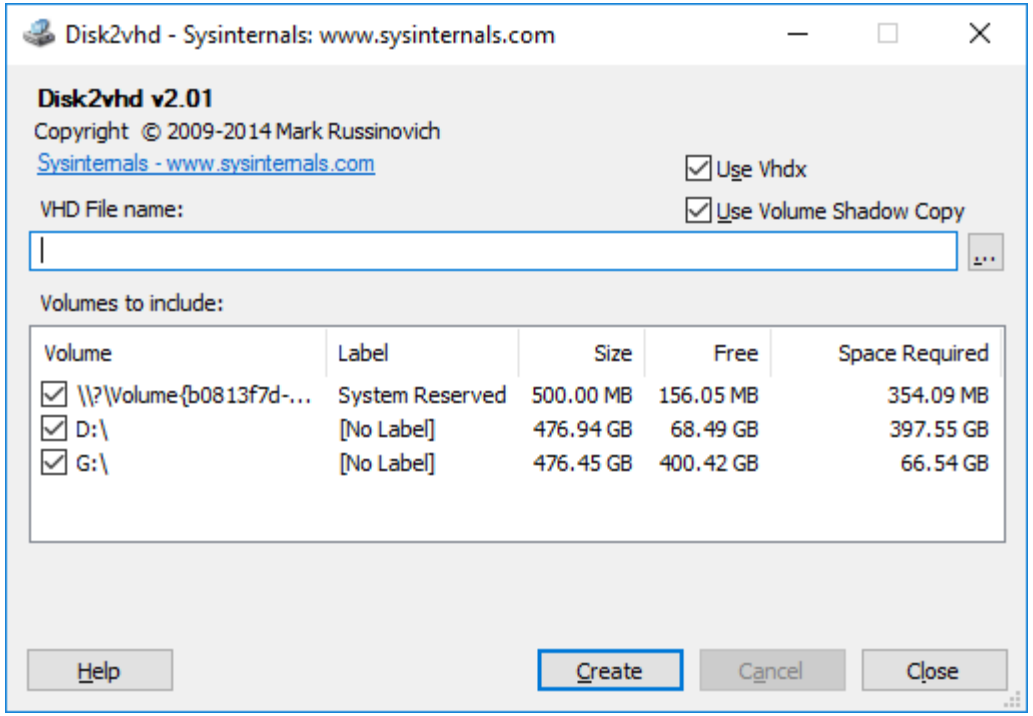
But how do I virtualize the corporate machine?

Disk2vhd can transform live physical machine into a virtual hard drive.

We can then boot it up with Hyper-V, Native Boot, or whatever else.

https://learn.microsoft.com/en-us/sysinternals/downloads/disk2vhd

Be careful with Active Directory and hostnames.



How to run the created machine

NATIVE BOOT

Available from Windows 7. Can boot the operating system from a VHD file directly.

Near native performance.

Bitlocker is not supported.

Works flawlessly with portable SSD drive. The bootloader can be installed on the drive entirely.

VHD can be booted with multiple laptops.

Docker and Hyper-V will work.

FULL VIRTUALIZATION

Can be fast enough if we have nested virtualization

Docker and Hyper-V may not work.

We need some hypervisor as the host (Hyper-V, VMware, VirtualBox).

We can use Windows To Go as a hosting platform for the hypervisor:

- We install Windows on a portable drive
- **Bitlocker is supported**
- Machine can be booted with multiple laptops
- Similar approach works for Linux
- Docker and Hyper-V will work.

We can use cloud as a hosting platform!

Connecting to a virtual machine

Hypervisor gives some way of connecting KVM to the machine.

Hyper-V supports *enhanced session* that uses RDP protocol. This connection bypasses network stack and works with full-tunnel.

What if we need an SSH tunnel to the virtual machine with a full-tunnel VPN?

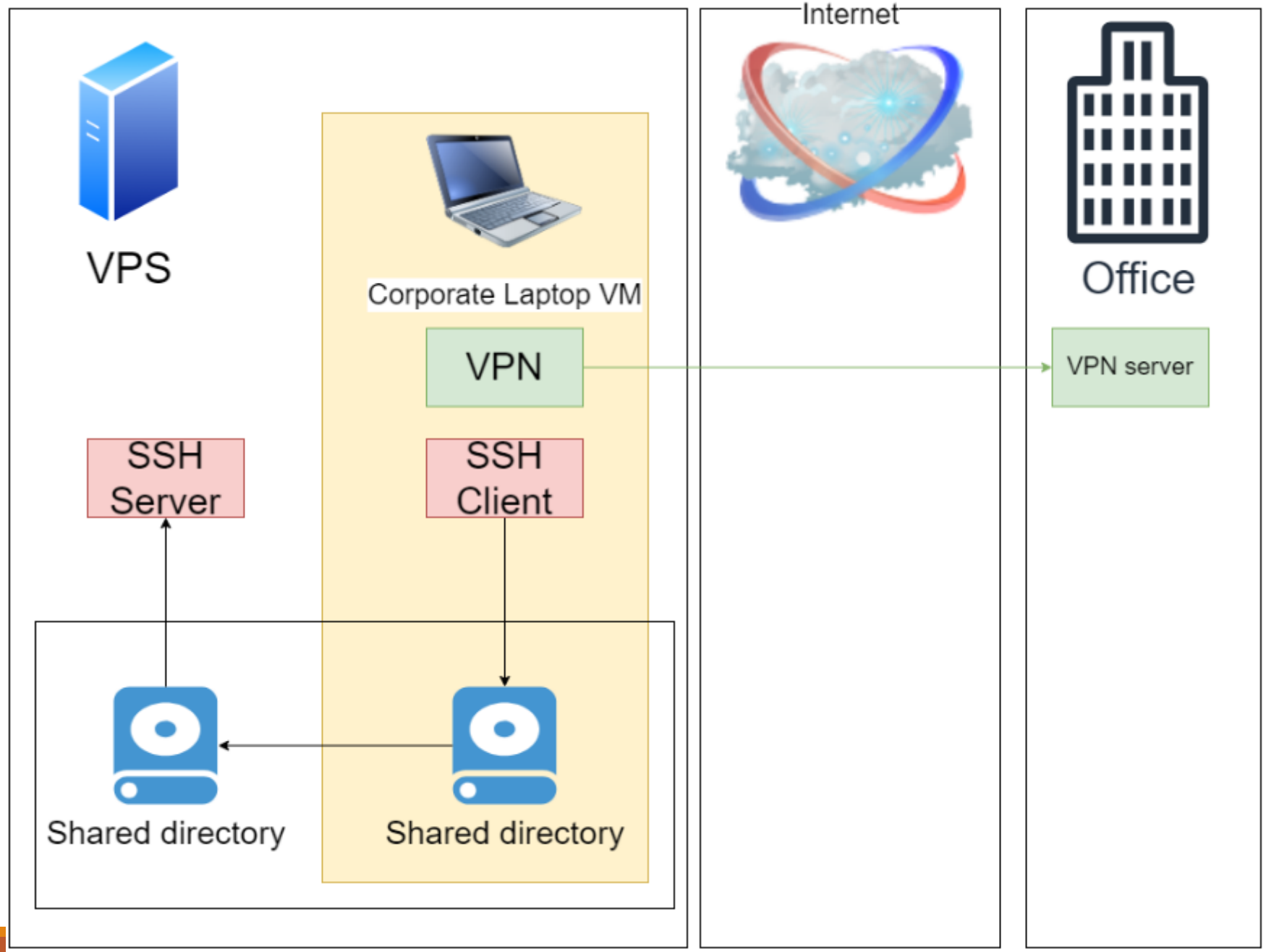
TCP over Filesystem

Full tunnel applications control the network stack.

We need to route the traffic outside of the networking.

In computer science, everything is a queue. Let’s use a fancy implementation with a filesystem.

Once we have a virtual machine, everything becomes trivial.


Internet
VPS
Corporate Laptop VM
Office
VPN
VPN server
SSH Server
SSH Client
Shared directory
Shared directory

TCP over Filesystem demo

TCP over IPC

We can do the same with IPC instead.

Serial Ports are implemented as Named Pipes by most of the hypervisors.

We are limited by the number of bauds. That’s pretty slow.

Summary

SPLIT TUNNEL

Intel AMT for KVM.

Direction connection or *jump host* or *SSLH* for full experience.

Use *jump host* and *AMT* as backup.

FULL TUNNEL

Intel AMT for KVM.

SSLH or *jump host* for full experience.

Use *SSLH* and *AMT* as backup.

VIRTUALIZED MACHINE

Hypervisor session for KVM.

SSLH or *TCP over Filesystem* or *TCP over IPC* or *jump host* for full experience.

Use *SSLH* and *Hypervisor session* as backup.

Comparison

Solution	Works with split tunnel	Works with full tunnel	Works with physical laptop	Interrupted by admin in split tunnel	Interrupted by admin in full tunnel	Requires root	Performance	Supports things beyond KVM
Direct connection	Yes	No	Yes	Unlikely	Unlikely	Maybe	Great	Yes
Jump Host	Yes	Yes	Yes	Unlikely	Likely	Maybe	Great	Yes
Intel AMT	Yes	Yes	Yes	Unlikely	Unlikely	Yes	Medium	No
SSLH	Yes	Yes	Yes	Unlikely	Unlikely	Maybe	Great	Yes
Hypervisor session	Yes	Yes	No	Unlikely	Unlikely	Yes	Great	No
TCP over Filesystem	Yes	Yes	No	Unlikely	Unlikely	Yes	Great	Yes
TCP over IPC	Yes	Yes	No	Unlikely	Unlikely	Yes	Medium	Yes

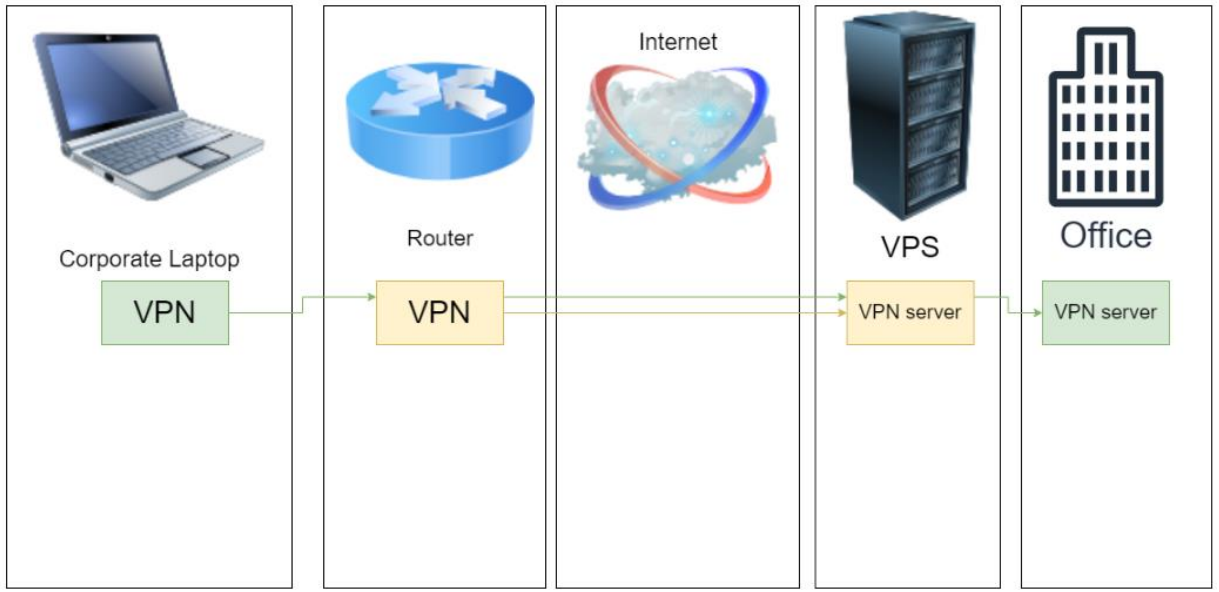
I need a VPN over VPN

SCENARIO

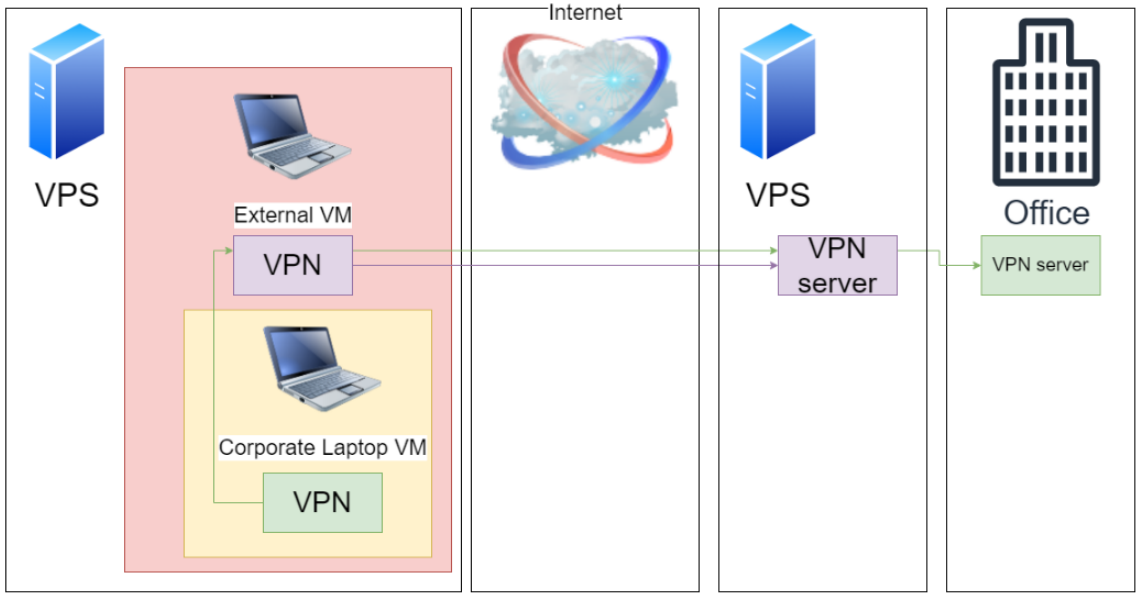
VPN inside another VPN

We can configure router along the way with a separate VPN.

May not work if we need a specific VPN type.



We can use VM inside a VM.



We can nest more VPNs if needed.

I have a video call and I need to share my screen

SCENARIO

RDP, speakers, microphone, screen

You can forward speakers and microphone over RDP.

RDP reencodes audio by default. This introduces significant delay (measured in seconds). This can be changed on the client or in Group Policy.

Microphone has lower quality, especially with nested RDP.

If possible, connect from the road runner machine (should work for Google Meets, MS Teams, Slack, Zoom).

You can use proxy over SSH. This may be hard for native applications.

You can use full-tunnel VPN to the corporate laptop. Mind the **DNS leak** vulnerability when you configure your tunnel. Mind the geolocation API.

Solution: **Use browser.**

Browsers

FIREFOX

Two fantastic extensions: **Multi-Account Containers** and **Tree Style Tab**.

Some video applications may not be supported by their owners (Facebook Messenger).

CHROME

There is no Multi-Account Containers. Use **CentBrowser** fork with Multilogin tabs + **FoxyProxy** extension.

Or use multiple profiles in Google Chrome/ Microsoft Edge.

Video applications generally work well.

Screen sharing

Do not share the screen from the road runner.

Connect to the same meeting twice: once from road runner, once from corporate laptop.

Others may notice you connect from two places, depending on the platform you use:

- Google Meets will show your account twice, but you can connect easily
- MS Teams will not show that you're connected from many places
- Zoom will show you twice

Some platforms do not let you join the meeting twice from the same account. You can always try joining without logging in (some meetings may not allow that).

You may be able to join from another place over GSM. You can use VoIP number to do that over the Internet.

GSM

GSM is not encrypted. **It may not be safe to use it**.

Regular call may be expensive. Check if your meetings platform supports local phone numbers.

GSM may have low audio quality.

Regular phone call may show your phone number.

Attendees may not recognize who is dialing in.

VPN and geolocation

Geolocation services may report your location incorrectly.

This may cause alerts that a new device is connecting from an insecure location.

No matter who is to blame for the invalid location, you want to avoid it. Verify your IP addresses with multiple services.

Well-known providers may have more issues.

Services may block you if you connect from a virtualized infrastructure. Google does that, IRC does that, e-mail servers do that.

Instead of installing VPN on the mobile device, you may want to configure the VPN on your router.

Connecting from mobile phone

The same rules apply to mobile devices.

Use JuiceSSH + Firefox + FoxyProxy to route traffic over SSH.

You may not be able to route native mobile applications over SSH proxy. Use full-tunnel VPN to your corporate laptop instead.

Or use Google Chrome browser - just select “Desktop mode” and meetings should work.

Notice, that you can share the screen the same way as before. Just RDP to your corporate laptop from the mobile device.

If you want to block incoming GSM calls while you’re in the video conference, use **call barring** or **call forwarding**.

Road runner and microphone over RDP

Scenario	Speaker	Microphone	Parallel meetings	Notes
Browser	No delay. Good audio quality.	No delay. Good audio quality.	Yes	Might be little clumsy with chat.
Native application	No delay. Good audio quality	No delay. Good audio quality.	Not on mobile	Might be hard to route over tunnel (especially on mobile).
Single-level RDP	Around 1 second delay. Good audio quality.	No delay. Moderate audio quality.	Yes	Acceptable if needed, but definitely not comfortable.
Single-level RDP with headphones.	Around 1 second delay. Good audio quality.	No delay. Moderate audio quality. Microphone from headphones may not be used on mobile device (phone may use built-in one).	Yes	Acceptable, but may be even less convenient.
Multi-level RDP	2+ seconds delay. Good audio quality.	No delay. Very low audio quality.	Yes	Probably won’t work.

I need 2FA

SCENARIO

2-Factor Authentication

SMS messages may not be delivered abroad. **Use virtual phone number.**

Some tokens may not work with mobile devices. Get your adapters.

Some tokens may not work over RDP, despite the USB redirection. Check that in advance.

Tokens have multiple working modes, they may hash the URL, they may generate One-Time Password (OTP), they may use clocks or just counters.

Some tokens support generating backup keys, or even generating a set of keys that don’t expire.

Always have a backup key.

I can't attend the call but I still want to see it

SCENARIO

Recording a meeting

Most platforms support recording a meeting out of the box.

The recording is then delivered via cloud.

Attendees will be notified that the meeting is being recorded.

If there is no built-in support for recording, then launch OBS on your corporate laptop.

I'm an architect and I need to use a whiteboard

SCENARIO

Whiteboard

Having a whiteboard is very useful for on-line meetings.

Laptops with touch screens are great.

Mobile devices with touch screens are also okay (although, a little small).

You can get an external monitor with touch capabilities. Just make it duplicate your primary screen, and then share Paint or any other drawing application.

I don't feel like sitting the whole day

SCENARIO

Good furniture

You may find it hard to believe, but the **color of your furniture may be important**!

I need more screens

SCENARIO

More screens

WINDOWS

Use **virtual desktops**: Task View or VirtuaWin.

Plug USB adapters to get more screens.

Use Indirect Display Driver + OBS to physically split one monitor into multiple smaller ones.

Remember to unfocus your RDP session with CTRL+ALT+HOME.

Use touchpad gestures to quickly move between desktops.

MAC

User **virtual desktops**.

Use screens that work with your Mac.

Use desktops, touchpad gestures.

Use BetterDisplay to physically split one monitor into multiple smaller ones.

I need to charge

SCENARIO

Charging

You can charge your laptop via USB-C most of the times.

You can use regular power adapter, docking station, or your monitor.

Your monitor can actually work as a docking station.

You can connect multiple monitors over one USB-C with Daisy Chaining.

Powerbank can charge your laptop. Just make sure you have enough USB-C ports to support all your peripherals.

Cookbook

SCENARIO

Cookbook

Get yourself a dedicated server located in a country of your choice. Make sure geolocation works. Configure full-tunnel VPN and OpenSSH server. Configure virtualization.

Turn your corporate laptop into a virtual machine and run it on your dedicated server.

Configure TCP over Filesystem or SSLH.

Configure your Road Runner to use VPN to your dedicated server and SSH tunnels. Use Road Runner to attend meetings.

Configure your mobile device to use full-tunnel VPN. Configure messaging apps.

Get a local phone number with lots of data. Bring all 2FA tokens, powerbanks, and adapters.

Take your privacy screen with you. Do not leak confidential information.

Fly to Hawaii.

Q&A

References

https://github.com/yrutschle/sslh - SSLH

https://www.cyberciti.biz/faq/remotely-access-intel-amt-kvm-linux-desktop/ - Intel AMT

http://blog.adamfurmanek.pl/2022/01/29/availability-anywhere-part-10/ - Link Aggregation with Broadcast (channel bonding)

https://getfoxyproxy.org/downloads/ - FoxyProxy

https://addons.mozilla.org/en-US/firefox/addon/multi-account-containers/ - Multi-Account Containers

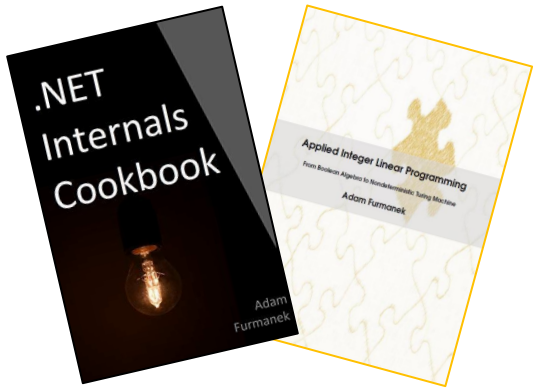
https://addons.mozilla.org/en-US/firefox/addon/tree-style-tab/ - Tree Style Tab

https://www.centbrowser.com/ - CentBrowser

https://blog.adamfurmanek.pl/2022/12/23/availability-anywhere-part-17/ - Splitting screen into multiple smaller ones

https://learn.microsoft.com/en-us/sysinternals/downloads/disk2vhd - Disk2vhd

https://blog.adamfurmanek.pl/2022/11/12/availability-anywhere-part-12/ - TCP over Filesystem



Random IT Utensils

IT, operating systems, maths, and more.

Thanks!

CONTACT@ADAMFURMANEK.PL

HTTP://BLOG.ADAMFURMANEK.PL

FURMANEKADAM