

# VIRTUAL PRIVATE NETWORKS

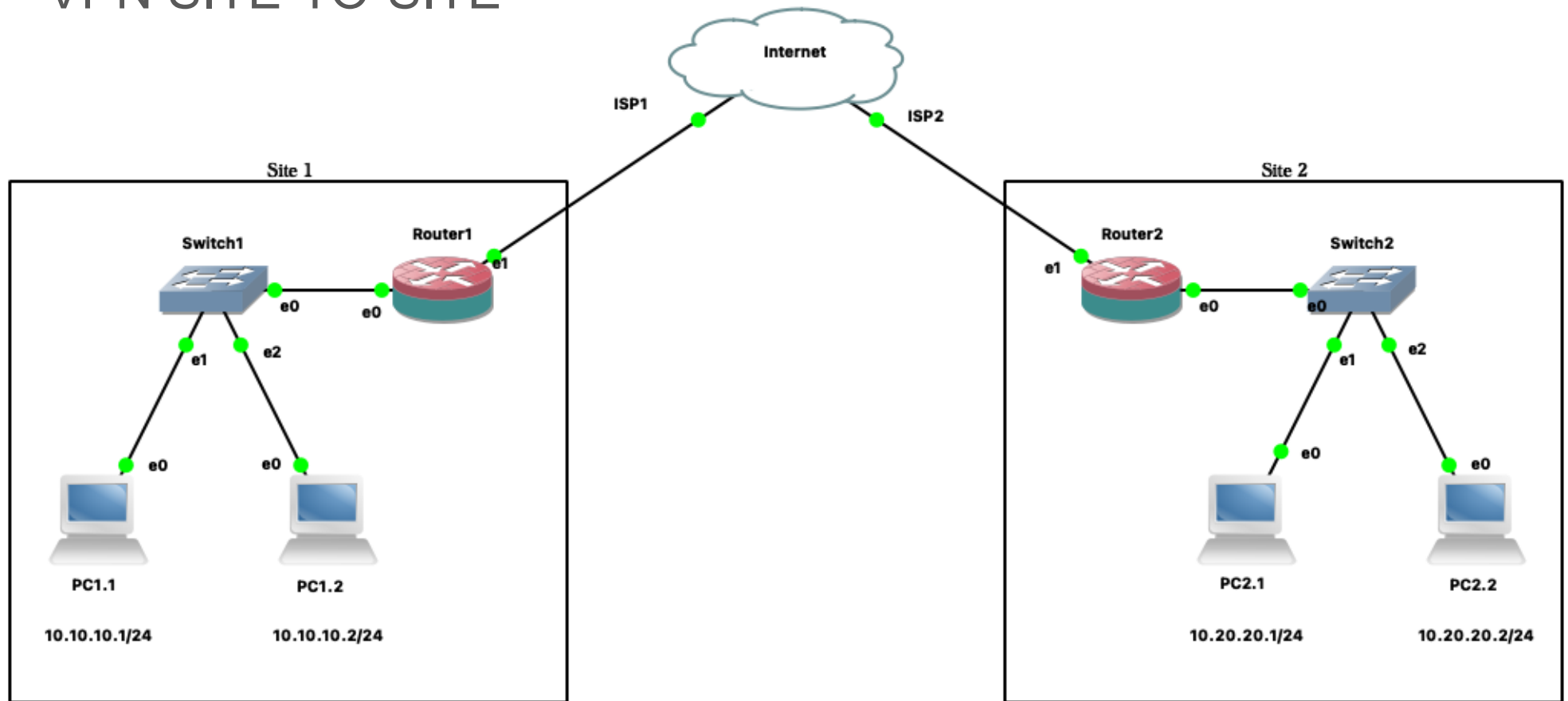
# VIRTUAL PRIVATE NETWORK (VPN)

- Isolate networks through **Authentication**
  - Certificates (Private Key, Public certificate)
  - Password
  - Source IP Restrictions
  - Password and Certificates
- “Route” Private IPs over the Internet
  - Need only one Public (routable) IP address
- End-to-end encryption
- Less legitimate (grey area) use cases:
  - “Hide” your IP
    - NordVPN
    - Tor Network
  - “Hide” geolocation
    - Netflix, Disney+

# VPN USE CASES

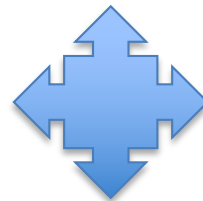
- Present certain parts of the network to authenticated parties
  - Isolate Datacentre
    - Giving privileged access to Systems administrators
    - Only exposing certain services/devices
  - Isolate Lab equipment from the rest of the network
    - A higher level of control than a VLAN
- Remote Login to corporate network
  - E.g.: Global Protect
- Share corporate networks between two or more organisations

# VPN SITE-TO-SITE



Depending on the configuration:

Site 1 can access Site 2  
Site 2 can access Site 1



Site 1 can access Site 2  
Site 2 can't access Site 1

Site 1 can access whole of Site 2  
Site 2 can access only parts of Site 1

# OpenVPN

- Open-Source VPN Server
- <https://www.openvpn.net>
- Community & Enterprise versions
- Encryption using OpenSSL 3+
  
- Client:
  - OpenVPN Connect
    - Windows (7, 8, 10, and 11)
    - Mac OS
    - Linux
      - Script for Debian/Ubuntu included, others from:
      - <https://openvpn.net/cloud-docs/owner/connectors/connector-user-guides/openvpn-3-client-for-linux.html>



# INSTALL OpenVPN CLIENT



- Download the client from the event page:
  - <https://events.ufs.ac.za/event/3500>
    - Software: openvpn-connect (1<sup>st</sup> = Windows, 2<sup>nd</sup> MAC)
- Download your OpenVPN profile:
  - <https://gw.examplesdomain.com:3443>
    - » Or
  - <https://events.ufs.ac.za/event/3500>
    - Software: certs.zip
- Install the profile and connect to the VPN

GNS<sub>3</sub>

# GNS<sub>3</sub>

- Graphical Network Simulator-3 (GNS<sub>3</sub>)
- Emulator to design and deploy network topologies/software solutions
- Used by industry professionals
- Runs on MS Windows, Mac OS, GNU Linux, Unix, FreeBSD
- Open Source
- Downloadable from:  
<https://gns3.com/>
- Appliances (\*.gns3a files) on the marketplace:  
<https://gns3.com/marketplace/>





# GNS<sub>3</sub> USAGE

- Test your networks before you build them to reduce the time needed to get a production network up and running
- Run the OS that emulates the actual behaviour of network hardware
- Test 20+ different network vendors in a risk-free virtual environment
- Customized topologies and labs within GNS<sub>3</sub> for network certification training
- Connect GNS<sub>3</sub> to the actual network
- Can load unlimited devices, only limitation is host's CPU & RAM
- Can be installed on a dedicated server or workstation

## GNS<sub>3</sub> TERMINOLOGY

**GNS3** → GUI (Graphical User Interface)

**Dynamips** → Emulator for hardware - IOS (Cisco OS)

**Dynagen** → Beginning Front End for Dynamips

**Pemu** → Cisco PIX Firewall Emulator Based on Qemu

**(Win)Pcap** → Packet Capture Library (Driver for Sniffer)

**Wireshark** → Network Monitoring / Listening to Network

**VPCS** → **Virtual PCs (Virtual Computer)** → Adding a virtual computer.

**VMware VMS** → VMware Virtual Machines → Including virtual machines in topology with VMware Workstation.

**VirtualBox VMS** → VirtualBox Virtual Machines → Including virtual machines in topology with VirtualBox.

**IOU Devices** → A real Layer2 and Layer3 Switch lets you use all the features of your network device by adding an IOS image.

# GNS<sub>3</sub> LAB PRACTICE

# GNS<sub>3</sub>

- Download from: <https://gns3.com/> or Events page
  - Linux: <https://docs.gns3.com/docs/getting-started/installation/linux/>
- Perform standard installation,
- **Don't install (We will only use the remote server)**
  - Local VM / Server
  - Dynamips
- Add/enable:
  - GNS WebClient
  - WinPCAP
  - Wireshark
  - VCPS
  - TightVNC Viewer
  - Solar-Putty
  - Virt-viewer



# SERVER INFORMATION:

- Connect to the VPN first
- Open GNS3
- Preferences >> Server
- Disable Local Server
- Add the following as server:
  - Host: 10.200.0.1XX
  - Port: 30XX
  - User: ern\_admin
  - Password: Leggings:Nutcase:Daybed:Cut3:Gradation
- Replace XX with your user id
  - E.g.
    - Host: 10.200.0.105
    - Port 3005



# ACCESS GNS<sub>3</sub> FROM VNC



- If you are unable to connect/install the VNC client.
- Connect to a VNC session:  
<https://gns3.examplesdomain.com/>
- User: usrXX
- Password: Your:Password:Provided:On:The:Events:Page
- Replace XX with your user id
  - E.g.
    - usr05