GDS

DRAFT

Sharing WAN circuits in shared buildings

1. Introduction

Each organisation has their own IT team and can deliver their own independent solutions to meet their users' needs. They generally have a contract with a single provider for a private national network. This works well but can be wasteful when sharing office buildings between multiple organisations. A tenfold increase in bandwidth is generally available for 2-3 times the cost so there is the potential of a 70-80% saving where 10 organisations with similar requirements can share their connectivity.

This blueprint aims to allow links to be shared across different organisations with:

- minimal change to network infrastructure
- full control of IP addressing and traffic routing
- clear demarcation of responsibilities

2. Executive summary

This document provides a set of patterns for shared external network connectivity in shared government offices. It provides:

- the ability to share two internet and two Public Service Network (PSN) links per building or building cluster leading to greater efficiency
- higher available bandwidth as peaks will be spread amongst a larger number of diverse users and a larger shared link can be purchased

- a pattern for allowing end user devices with ‘always on’ Virtual Private Networks (VPN) to connect to their home gateway
- a pattern to provide access to the enterprise network to devices not using a client VPN.
- methods for government organisation IT departments to maintain visibility and control

3. Technical solution

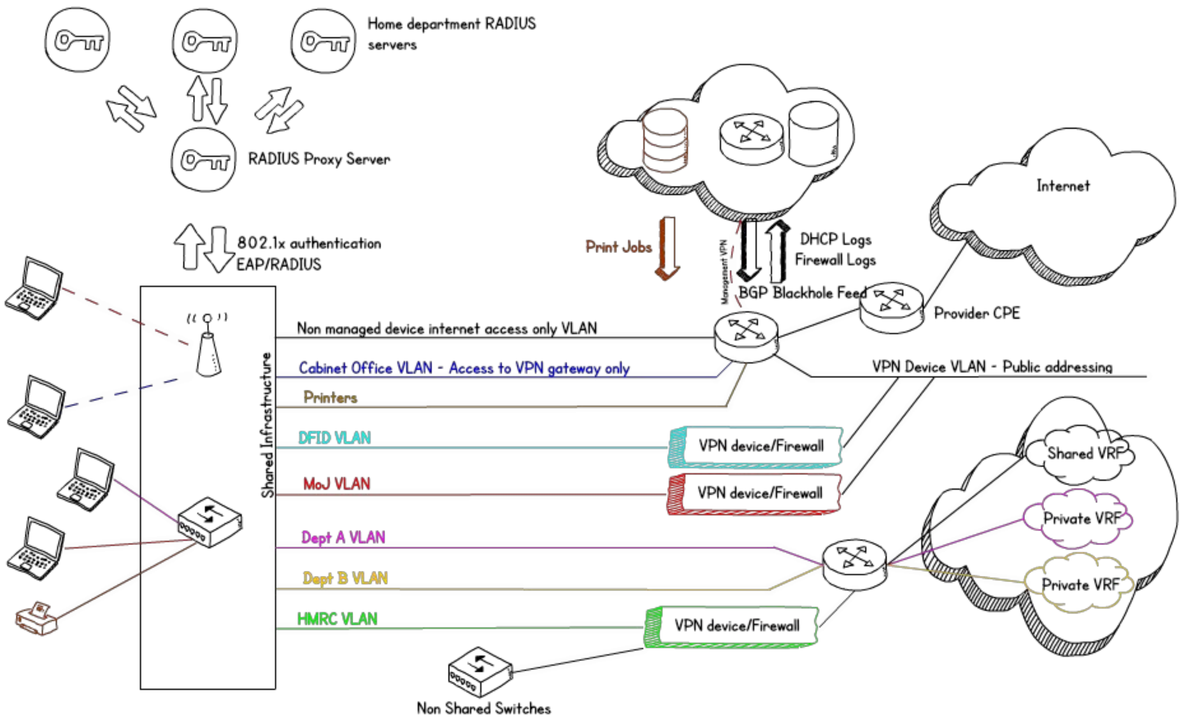
The shared workplace network uses certificates to grant end user devices network access. Each organisation’s user group is allocated their own Virtual LAN (VLAN) to which a pair of VPN devices managed by their home organisation IT are connected. This also means that each organisation controls their own IP address allocation to clients and IP routing.

Alternatively the organisation can opt to not install devices and implement ‘always on’ VPN clients on their end user devices.

The internet gateway provides direct internet access to ‘always on’ VPN users and visitors only, all managed devices will use their existing organisation’s internet gateway service. Content filtering will be on a best effort basis using a filtered DNS provider, however the gateway should enforce the use of this service by blocking any other (unfiltered) DNS servers.

The internet gateway also provides firewalled connectivity for the individual departments’ VPN routers.

A central print solution is accessed via a VPN terminated on the Internet gateway which is the subject of a shared printing blueprint.



Each organisation can decide which of the following three connectivity options is best suited to their requirements:

3.1 ‘Always on’ VPN

An organisation using an ‘always on’ VPN for their end user devices does not need to install any additional infrastructure. The building’s shared RADIUS server recognises the device certificate and connects the user to an ‘always on’ VPN VLAN which only allows VPN traffic.

3.2 A VPN router per organisation

The individual organisation’s VLAN is taken back to a shared cabinet in the main comms room for the building, where each organisation has their own managed VPN router/firewall.

The organisation can then decide to connect back via the internet or via the Public Services Network (PSN) depending on their requirements. Those organisations with their main applications in a public cloud will probably choose to use a VPN over the internet. Those with existing PSN connectivity to their datacentres will most likely prefer to use a VPN over the PSN as it delivers an assured path.

Local break out to a cloud based web filtering service or cloud applications can be used to avoid the added latency of internet traffic traversing the datacentre. Adoption of this depends on the organisation’s user and security requirements.

The connectivity from the end user’s device to their organisation’s VPN device is at layer 2 giving their IT team full control over the IP allocation and addressing.

The organisation should make a decision on how many users will be the threshold for installing the VPN endpoint, below which they use the remote access solution via the internet.

3.3 Private VRF over a PSN connection

An organisation can make arrangements with their WAN service provider to extend their network to any PSN network vendor connected to a site. The organisation should install a firewall or router to allocate IP addresses to their users and protect their WAN from threats.

We are working with PSN vendors to find ways to make this easier and create a standard process.

4. Technical requirements

4.1 Shared internet gateways

Solution providers need to install a single internet gateway service per building cluster to be used by everyone in those buildings. Although described as a single gateway it needs to include multiple devices to provide high availability.

The internet gateway must:

- support the bandwidth required for the site
- establish a Virtual Private Network (VPN) to a central point by acting as an Internet Key Exchange (IKEv2) client using next generation encryption
- export firewall and web request logs including the full address of unencrypted requests and the destination address of encrypted connections to a central service via the VPN

- export logs of IP addresses allocated to clients via the VPN
- continue to function if any single component fails
- provide accurate timestamps using Network Time Protocol (NTP)

4.2 Shared WAN connectivity

Solution providers must provide resilient connectivity to both the internet and to the PSN so that government organisations can connect to their resources in the most appropriate way.

The WAN connectivity must deliver:

- a resilient pair of internet connections
- a resilient pair of PSN connections - supporting private VRFs where available
- public IP address range for the internet VPN endpoint DMZ
- PSN IP address range for the PSN VPN endpoint DMZ

The resilient connections can be split across two buildings located together, where appropriates. This should provide extra diversity and easier load sharing between the two links as the users in each building can use their local link but fail over to the other building in case of failure. For a single building infrastructure, the two cabinets and link termination equipment should be as far apart as possible. Different comms rooms should be considered to avoid total sustained outage from a single fire or flooding event.

For a pair of connections to be considered resilient, as a minimum they must use different building entry points and be diversely routed never sharing the same duct. Consideration should be given to using two different network providers for these links where possible, taking care to ensure the providers are not using common underlying components.

Consideration should be given to an active-active approach, so in normal circumstances both links are around 50% average utilisation or less, this will give a better service by reducing contention during spikes at peak times while still allowing fail over.

4.3 VPN device colocation

Solution providers must assist government organisations with installing firewall(s) or other VPN termination equipment in shared cabinets located in suitably secured and controlled comms rooms.

Solution providers must deliver:

- two shared cabinets as far apart as possible, preferably in different buildings in each building cluster for installing a number of VPN routers (one pair per organisation)
- top of rack switch port giving a connection access to the internet, PSN or private VRF as requested by each organisation - ports can be preallocated to reduce management overhead
- a top of rack switch port giving access to each organisation’s internal VLAN on the shared infrastructure
- patching to the organisation’s switches if they have implemented their own

Organisations wishing to use buildings that follow this pattern must:

- comply with the requirements in the shared workplace network blueprint
- provide either a pair of VPN routers or enough client VPN capacity for the number of users at a given site
- inform the service provider of their chosen pattern of connectivity
- provide different physical interfaces on their VPN routers for their own LAN switches (if installed) and the shared infrastructure switches