# Virtual Desktop Connector

## PRODUCT FEATURES

- Entirely Linux-based
- Each instance can be allocated a unique ID
- Customisable
- IPv6 ready
- 2048-bit encryption
- Completely Portable

## PRODUCT BENEFITS

- Very easy to support - just works!
- When staff leave or the media is lost, just disable that key
- Can apply any desired skinning using standard web skills
- Customer is in control - generate and use as many copies as you want
- Allows local authority to meet the Coco standards

The Penguin Factory™

## Securing the Network Beachheads...

Remote Access. If it's Worth Doing it's Worth Doing Well.

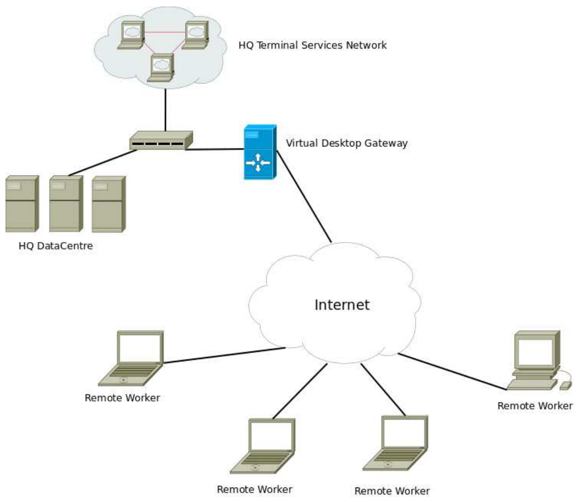
We are the first to say that not all staff need the same remote access. At the Penguin Factory we want to see you with the most secure, most appropriate access policies, so we start by asking "who needs to access what from where?" Once you have identified those who need remote access, particularly remote desktop access, then you need to decide how to deliver it.

Authentication is definitely part of the challenge. Security is actually decreased by too many confusing authentication methods as user invariably bypass them or write passwords on post-it notes. Blending the right mix of operability and protection is key.

Then there's the remote environment. We always assume remote access is happening from a hostile network, because very often it is. Home networks are very often compromised, WIFI hotspots present well-known dangers and at the bottom of the scale there are public access Internet terminals. You must treat all connections as completely untrusted until they have proved their credentials.

VPN's are popular but can be a major source of headaches as in effect they are expanding your border to include everything the remote user is also connected to. In effect you have just allowed access to your vital data to computer systems that are not subject to the standard IT Security and Operations policies. Whether the remote user intends it or not, this can be a back-door to viruses, hackers or data theft.

By deploying the Virtual Desktop Connection - a virtual "sandbox" if you like - you can ensure that the only devices that you allow through are a secure environment that only you are in control of. A secure environment that does not allow information to leak out through copy and paste buffers, that does not run risk of viruses or act as a network bridgehead for onward attacks on your data. Customisable to your needs and your specifications.



Remote Clients connecting to HQ resources securely