

# Client Connectivity

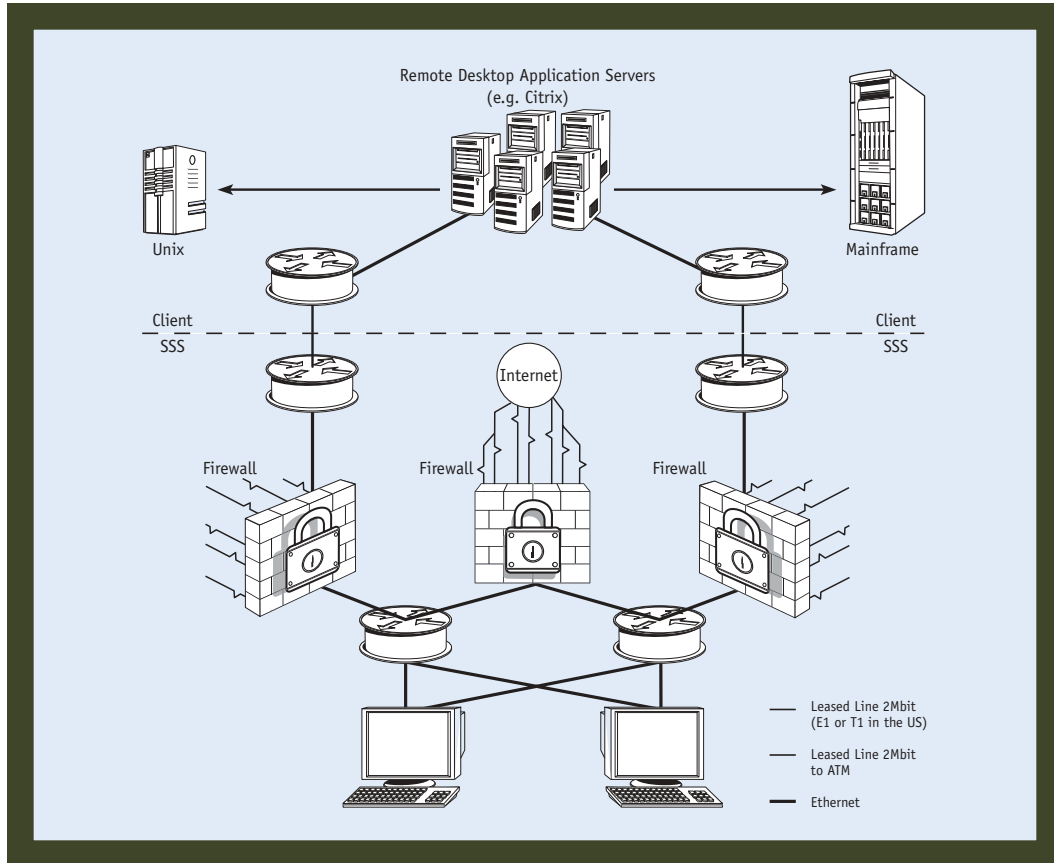
The majority of Strategic Systems Solutions engagements are carried out at one or more of our global offices, employing dedicated connectivity links to our clients' infrastructure. When a new client relationship is initiated, several members of the Technical Services Group (TSG) will meet with the appropriate members of the client's technical infrastructure group.

Key areas of discussion include:

- number of users
- security
- platforms
- technologies
- connectivity options
- support relationships and escalations

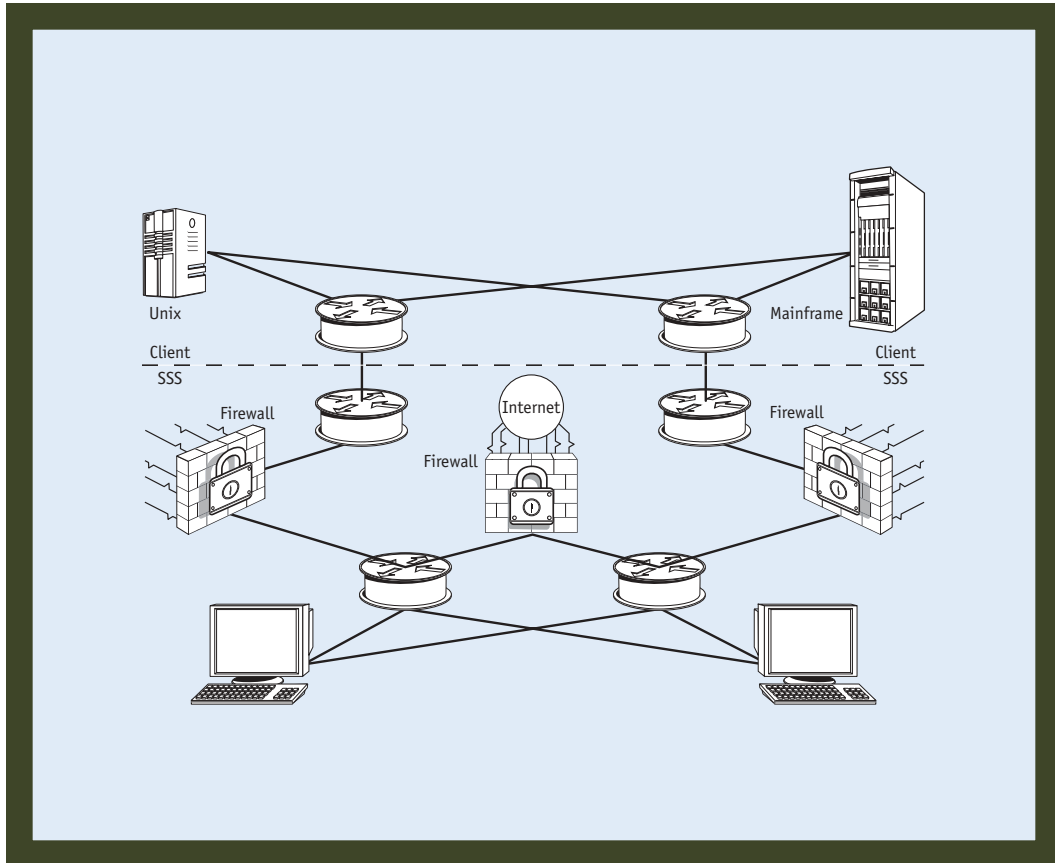
In this document, we have provided three connectivity diagrams which we consider to be the most flexible for our clients as well as SSS. Any of these options can have varying levels of resilience depending on the SLA associated with the work that is being done. There are many more ways of connecting (including client-managed VPN) but these are our preferred options.

## Firewalled Remote Desktop



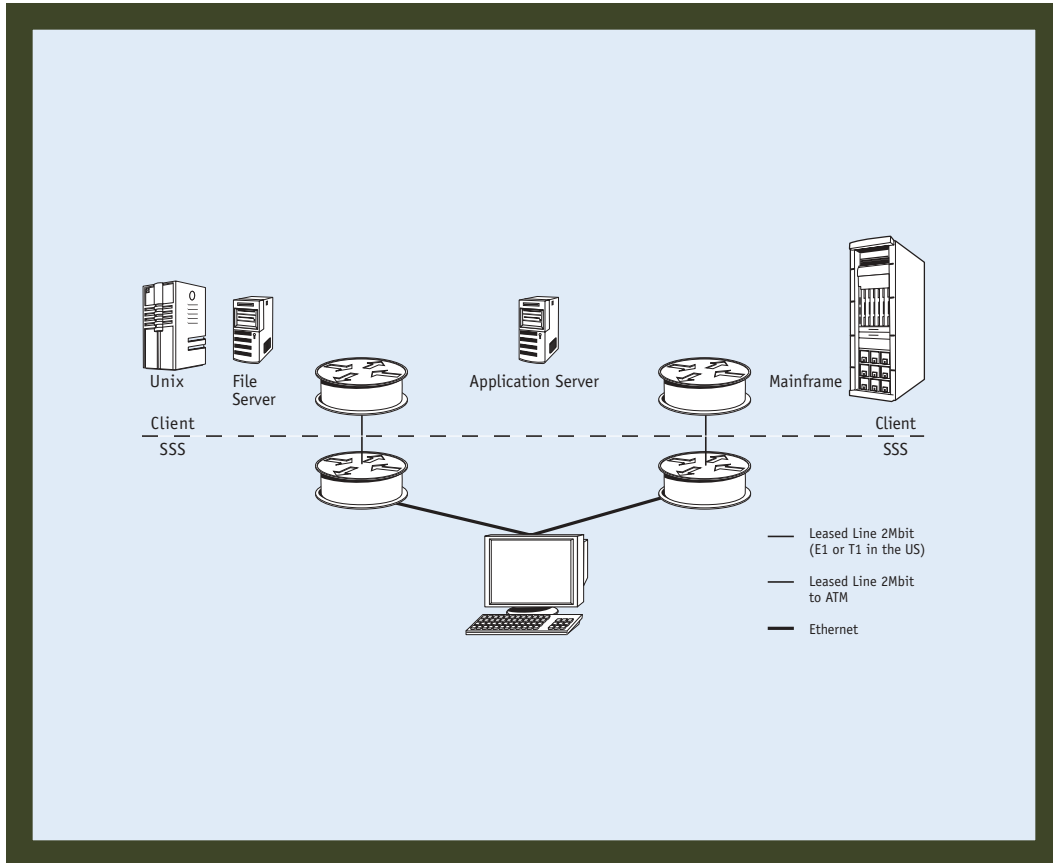
Depending on the location of the client destination systems, each continent may warrant its own remote desktop farm. Firewalls are placed on either side of the perimeter on all connections. Client-managed firewalls on the client side and SSS-managed firewalls on the SSS side of the links. Firewalls only allow access to the authentication services and remote desktop application servers.

## Firewalled Direct



The best option when there is a finite number of client resources that need to be worked on (e.g. mainframe or large UNIX environment). The only software required at SSS is a terminal emulator. This work can usually be supported by opening an IP address through the firewall with access to a TCP port (e.g. port 23 on the IP of the mainframe).

## Open Direct



Each SSS office in this setup would have carrier-independent leased line(s) connections from routers in our premises to routers in the client premises. There are no firewalls on the links, but the routers are used to occasionally block access depending on network security threats. SSS maintains the LAN hardware and software and the client maintains the WAN links.