

## Assumptions

Users will connect to a variety of networks in multiple locations with the purpose to perform work related tasks. The locations include "home office", other offices, at home and other locations while travelling. We also assume that security rules are hard implemented, i.e. the user should not be able to "turn off" security at will. We also assume that 80% of IT related information theft is "internal", i.e. the largest security threat are internal leaks rather than third party hackers.

Strategies for security	Quality of Service QoS (VoIP support)	End-to-end security in applications	Complexity of usage	Mobility	Local printers	"device dependence"	Support for all scenarios
WEP/WPA/802.1x	Yes	No	No alteration of user behaviour	Only local	Yes	No	No
IPSEC VPN	No	No	Users must learn to use new software	No/VERY weak NAT support in the standard	No	Yes – demands software client	No
SSL VPN	No	No	Users must learn to use new software	Full mobility	No	Yes – generally demands software client	No
Application based security	Yes	Yes	No alteration of user behaviour	Full mobility	Yes	No	Yes

\* **GREEN** = The solution full fills the strategies in a good way.