



Network VPN Standards

Introduction

Security periodically revises the level of encryption required for IPSEC as well as various parameters around these. Below is the current revision of levels required within TFL for IPSEC.

Standards

Component	Value
Data Integrity	SHA1
Data Encryption	AES-256
PFS (Phase 2)	None
IKE v1 mode	Main Mode (default)
Diffie Hellman (Phase 1)	Group 2 (1024 bits) (default)
SA Renegotiate Time	1440 min (IKE phase 1) 3600 sec (IPSEC phase 2)
TfL firewall IP	X.X.X.X
TfL Encryption Domain	Already configured on the TfL firewall, may require amendment
3rd Party firewall IP	To be supplied by 3 rd Party
3rd Party Encryption Domain	To be supplied by 3 rd Party
Shared Secret Key	To be agreed with 3 rd Party