



mashme

VPN FEATURES

L2TP+IPSec specs

Protocol	Port	Description
TCP	1701	L2TP
UDP	500	IKE manage encryption keys
UDP	4500	IPSEC NAT - Traversal mode
ESP(50)		IPSEC
AH(51)		ISEC

L2TP

Max MTU	1450
Max MRU	1450
Authentication	mschap2, mschap1, chap, pap



IKE2

Phase	Cipher role	Cipher
Phase1	Encryption	aes-128 cbc, aes-192 cbc, aes-256 cbc
	Integrity	sha1
	prf	sha1
	Diffie-Hellman (DH)	Group 2 (modp_1024), Group 14 (modp_2048)
	Phase 1 lifetime	36,000 seconds (10 hours)
Phase 2	Encryption	aes-cbc-128, aes-cbc-192, aes-cbc-256
	Integrity	sha1
	PFS Algorithm	Group 2 (modp_1024), Group 14 (modp_2048)
	Diffie-Hellman (DH)	Group 2 (modp_1024), Group 14 (modp_2048)
	Phase 2 lifetime	10,800 seconds (3 hours)