

Microsoft Windows IPsec Proposals when using L2TP/IPsec

Phase 1 Proposals												
	Windows XP Service Pack 1				Windows Vista Service Pack 1				Windows 7			
	“No encryption”	“Optional encryption”	“Required encryption”	“Maximum strength”	“No encryption”	“Optional encryption”	“Required encryption”	“Maximum strength”	“No encryption”	“Optional encryption”	“Required encryption”	“Maximum strength”
1	untested	untested	3des, sha1, group2		untested	untested	Aes-256, sha1, “unknown” group		untested	untested	Aes-256, sha1, “unknown” group	
2			3des, md5, group2				Aes-128, sha1, “unknown” group				Aes-128, sha1, “unknown” group	
3			des, sha1, group1				3des, sha1, “unknown” group				Aes-256, sha1, “unknown” group	
4			des, md5, group1				3des, sha1, group2				3des, sha1, “unknown” group	
5											3des, sha1, group2	

Phase 2 Proposals												
	Windows XP Service Pack 1				Windows Vista Service Pack 1				Windows 7			
	“No encryption”	“Optional encryption”	“Required encryption”	“Maximum strength”	“No encryption”	“Optional encryption”	“Required encryption”	“Maximum strength”	“No encryption”	“Optional encryption”	“Required encryption”	“Maximum strength”
1	untested	untested	3des, md5, mode transport		untested	untested	Aes-128, sha1, mode transport	Aes-256, sha1, mode transport	untested	untested	Aes-128, sha1, mode transport	Aes-256, sha1, mode transport
2				AH, sha1, mode transport			3des, sha1, mode transport				3des, sha1, mode transport	
3				3des, no hash, mode transport			AH, sha1, mode transport				des, sha1, mode transport	
4				AH, md5, mode transport				Aes-256, no hash, mode transport				
5				AH, sha1, mode transport								
6				3des, sha1, mode transport								