

Internet Key Exchange (IKEv2) Transform Types

RFC4306

	Type
RESERVED	0
Encryption Algorithm (ENCR)	1 (IKE and ESP)
Pseudo-random Function (PRF)	2 (IKE)
Integrity Algorithm (INTEG)	3 (IKE, AH, optional in ESP)
Diffie-Hellman Group (D-H)	4 (IKE, optional in AH & ESP)
Extended Sequence Numbers (ESN)	5 (AH and ESP)
Reserved IANA	6-240
Private Use	241-255

Transform Types 1-5

Transform Type 1 (Encryption Algorithm)

Name	Number	Defined In
RESERVED	0	
ENCR_DES_IV64	1	(RFC1827)
ENCR_DES	2	(RFC2405), [DES]
ENCR_3DES	3	(RFC2451)
ENCR_RC5	4	(RFC2451)
ENCR_IDEA	5	(RFC2451), [IDEA]
ENCR_CAST	6	(RFC2451)
ENCR_BLOWFISH	7	(RFC2451)
ENCR_3IDEA	8	(RFC2451)
ENCR_DES_IV32	9	
RESERVED	10	
ENCR_NULL	11	(RFC2410)
ENCR_AES_CBC	12	(RFC3602)
ENCR_AES_CTR	13	(RFC3664)
Reserved IANA	14-1023	
Private Use	1024-65535	

Transform Type 4 (Diffie-Hellman Group)

Name	Number
768-bit MODP	1
1024-bit MODP	2
more DH groups	

Transform Type 3 (Integrity Algorithm)

Name	Number
NONE	0
AUTH_HMAC_MD5_96	1
AUTH_HMAC_SHA1_96	2
AUTH_DES_MAC	
AUTH_KPDK_MD5	
AUTH_AES_XCBC_96	
Reserved IANA	
Private Use	

Transform Type 2 (Pseudo-random Function)

Name	Number
RESERVED	0
PRF_HMAC_MD5	1
PRF_HMAC_SHA1	
PRF_HMAC_TIGER	
PRF_AES128	
Reserved IANA	
Private Use	

Copyright © IT charts.com