IPSEC

packetlife.net

Protocols	Encryption Algorithms				
Internet Security Association and Key Management Protocol (ISAKMP) A framework for the negotiation and management of		Туре	Key Length (Bits)	Strength	
	DES	Symmetric	56	Weak	
security associations between peers (traverses UDP/500)	3DES	Symmetric	168	Medium	
Internet Key Exchange (IKE)	AES	Symmetric	128/192/256	Strong	
Responsible for key agreement using asymmetric cryptography	RSA	Asymmetric	1024+	Strong	
Encapsulating Security Payload (ESP) Provides data encryption, data integrity, and peer authentication: IP protocol 50		Hashing Algorithms			
		Length (Bits) Strength			
Authentication Header (AH)	M	D5 128	Mediur	n	
Provides data integrity and peer authentication, but not data encryption; IP protocol 51		IKE Phases			
IPsec Modes	Phase 1 A bidirectional ISAKMP SA is established between peers to provide a secure management channel (IKE in main or aggressive mode)				
Original L2 IP TCP/UDP					
Transport L2 IP ESP/AH TCP/UDP	Phase 1.5 (optional) Xauth can optionally be implemented to enforce user authentication				
Tunnel Mode L2 New IP ESP/AH IP TCP/UDP Transport Mode	Phase 2 Two unidirectional IPsec SAs are established for data transfer using separate keys (IKE quick				
The ESP or AH header is inserted behind the IP header; the IP header can be authenticated but not encrypted		mode)			
IP header can be authenticated but not encrypted		Те	rminology		
IP header can be authenticated but not encrypted Tunnel Mode A new IP header is created in place of the original; this allows for encryption of the entire original packet	Data I Secure has not	Te ntegrity hashing (HM, been altered	rminology AC) is used to ens in transit	sure data	
IP header can be authenticated but not encrypted Tunnel Mode A new IP header is created in place of the original; this allows for encryption of the entire original packet Configuration	Data I Secure has not	Te ntegrity hashing (HM been altered confidentialit	rminology AC) is used to ens in transit ty	sure data	
IP header can be authenticated but not encrypted Tunnel Mode A new IP header is created in place of the original; this allows for encryption of the entire original packet Configuration Crypto isakmp policy 10 encryption aes 256	Data In Secure has not Data C Encrypt interce	Te ntegrity hashing (HM, been altered confidentialit tion is used to pted by a thir	rminology AC) is used to ens i in transit ty o ensure data can d party	sure data not be	
IP header can be authenticated but not encrypted Tunnel Mode A new IP header is created in place of the original; this allows for encryption of the entire original packet Configuration ISAKMP Policy encryption aes 256 hash sha authentication pre-share	Data In Secure has not Data C Encrypt intercep Data O Authen	Te ntegrity hashing (HM, been altered tion is used to pted by a thir brigin Authe tication of the	rminology AC) is used to ensite in transit o ensure data can d party ntication e SA peer	sure data not be	
IP header can be authenticated but not encrypted Tunnel Mode A new IP header is created in place of the original; this allows for encryption of the entire original packet Configuration Crypto isakmp policy 10 encryption aes 256 hash sha authentication pre-share group 2 lifetime 3600 ISAKMP Pre-Shared Key	Data In Secure has not Data C Encrypt intercep Data O Authem Anti-re Sequen discard	Te ntegrity hashing (HM, been altered confidentialit tion is used to pted by a thir tication of the tication of the ceplay duplicate page	rminology AC) is used to ensite in transite o ensure data cand d party ntication e SA peer are used to detect ckets	sure data not be	
IP header can be authenticated but not encrypted Tunnel Mode A new IP header is created in place of the original; this allows for encryption of the entire original packet Configuration ISAKMP Policy encryption aes 256 hash sha authentication pre-share group 2 lifetime 3600 ISAKMP Pre-Shared Key crypto isakmp key 1	Data In Secure has not Data C Encrypt intercep Data O Authen Authen Sequen discard Hash N	Te ntegrity hashing (HM, been altered confidentialit tion is used to pted by a thir Drigin Auther tication of the eplay ace numbers a duplicate pace	rminology AC) is used to ensite in transite o ensure data cand d party htication e SA peer are used to detect ckets hentication Cod	sure data not be : and e (HMAC)	
IP header can be authenticated but not encrypted Tunnel Mode A new IP header is created in place of the original; this allows for encryption of the entire original packet Configuration Crypto isakmp policy 10 ISAKMP Policy encryption aes 256 hash sha authentication pre-share group 2 lifetime 3600 ISAKMP Pre-Shared Key crypto isakmp key 1 MySecretKey address 10.0.0.2 IPsec Transform Set crypto_ipsec_transform-set_MyTS_esp-aes_256_esp-sha-hmac	Data In Secure has not Data C Encrypt intercep Data O Authen Anti-re Sequen discard Hash M A hash provide	Te ntegrity hashing (HM, been altered confidentiality tion is used to pted by a thir Drigin Auther tication of the tication of the aduplicate pace Message Aut of the data a a message aut	rminology AC) is used to ensite in transite o ensure data cand d party htication e SA peer are used to detect ckets hentication Cod nd secret key use chenticity	sure data not be and e (HMAC) d to	
IP header can be authenticated but not encrypted Tunnel Mode A new IP header is created in place of the original; this allows for encryption of the entire original packet Configuration Crypto isakmp policy 10 ISAKMP Policy encryption aes 256 hash sha authentication pre-share group 2 lifetime 3600 ISAKMP Pre-Shared Key crypto isakmp key 1 MySecretKey address 10.0.0.2 IPsec Transform Set crypto ipsec transform-set MyTS esp-aes 256 esp-sha-hmac mode tunnel IPsec Profile	Data In Secure has not Data C Encrypt interce Data O Authen Authen Sequen discard Hash M A hash provide Diffie- A share insecur	Te ntegrity hashing (HM, been altered confidentialit conf	rminology AC) is used to ensi- l in transit b ensure data can d party ntication e SA peer are used to detect ckets hentication Cod nd secret key use chenticity :hange is established ove public and private	sure data not be and e (HMAC) d to er an e keys	
IP header can be authenticated but not encrypted Tunnel Mode A new IP header is created in place of the original; this allows for encryption of the entire original packet Configuration Crypto isakmp policy 10 ISAKMP Policy encryption aes 256 hash sha authentication pre-share group 2 lifetime 3600 ISAKMP Pre-Shared Key crypto isakmp key 1 MySecretKey address 10.0.0.2 IPsec Transform Set crypto ipsec transform-set MyTS esp-aes 256 esp-sha-hmac mode tunnel IPsec Profile crypto ipsec profile MyProfile	Data In Secure has not Data C Encrypt interce Data O Authem Anti-re Sequen discard Hash N A hash provide Diffie- A share insecur	Te ntegrity hashing (HM, been altered confidentiality tion is used to pted by a thir Drigin Auther tication of the tication of the ticate numbers a duplicate pac Message Aut of the data a message aut Hellman Exc ed secret key e path using	rminology AC) is used to ensite in transite ty o ensure data cand d party htication e SA peer are used to detect ckets hentication Cod nd secret key use thenticity change is established over public and private	sure data not be and e (HMAC) ed to er an e keys	
IP header can be authenticated but not encrypted Tunnel Mode A new IP header is created in place of the original; this allows for encryption of the entire original packet Configuration Crypto isakmp policy 10 ISAKMP Policy encryption aes 256 hash sha authentication pre-share group 2 lifetime 3600 ISAKMP Pre-Shared Key crypto isakmp key 1 MySecretKey address 10.0.0.2 IPsec Transform Set crypto ipsec transform-set MyTS esp-aes 256 esp-sha-hmac mode tunnel IPsec Profile set transform-set MyTS	Data In Secure has not Data C Encrypt intercep Data O Authem Anti-re Sequen discard Hash N A hash provide Diffie- A share insecur	Te ntegrity hashing (HM, been altered confidentiality tion is used to pted by a thir origin Auther tication of the ce numbers a duplicate pace Message Aut of the data a e message aut Hellman Exc ed secret key e path using Trou	rminology AC) is used to ensi- in transit be ensure data can d party ntication are used to detect ckets hentication Cod nd secret key use chenticity hange is established ove public and private	sure data not be and e (HMAC) ed to er an e keys	
IP header can be authenticated but not encrypted Tunnel Mode A new IP header is created in place of the original; this allows for encryption of the entire original packet Configuration Crypto isakmp policy 10 ISAKMP Policy encryption aes 256 hash sha authentication pre-share group 2 lifetime 3600 ISAKMP Pre-Shared Key crypto isakmp key 1 MySecretKey address 10.0.0.2 IPsec Transform Set crypto ipsec transform-set MyTS esp-aes 256 esp-sha-hmac mode tunnel IPsec Profile set transform-set MyTS interface Tunnel0 Virtual Tunnel Interface in eddrese 172 16 0 1 255 255 255	Data In Secure has not Data C Encrypt interce Data O Authem Anti-re Sequen discard Hash M A hash provide Diffie-I A share insecur	Te ntegrity hashing (HM, been altered confidentialit tion is used to pted by a thir rigin Auther tication of the tication of the tication of the tication of the ticate pad duplicate pad duplicate pad the data a message auther Hellman Exc ed secret key e path using Trou rypto isakm	rminology AC) is used to ensi- in transit by o ensure data can d party ntication e SA peer are used to detect ckets hentication Cod nd secret key use thenticity hange is established over public and private bleshooting p sa	sure data not be and e (HMAC) ef to er an e keys	
IP header can be authenticated but not encrypted Tunnel Mode A new IP header is created in place of the original; this allows for encryption of the entire original packet Configuration Crypto isakmp policy 10 encryption aes 256 hash sha authentication pre-share group 2 lifetime 3600 ISAKMP Pre-Shared Key crypto isakmp key 1 MySecretKey address 10.0.0.2 IPsec Transform Set crypto ipsec transform-set MyTS esp-aes 256 esp-sha-hmac mode tunnel IPsec Profile set transform-set MyTS interface Tunnel0 ip address 172.16.0.1 255.255.255.252 tunnel source 10.0.0.1	Data In Secure has not Data C Encrypt interce Data O Authen Authen Authen discard Hash M A hash provide Diffie- A share insecur Show c	Te ntegrity hashing (HM, been altered confidentiality tion is used to pted by a thir origin Auther tication of the ce numbers a duplicate pac Message Aut of the data a e message aut Hellman Exc ed secret key e path using Trou rypto isakm rypto isakm	rminology AC) is used to ensi- in transit be ensure data can d party htication e SA peer are used to detect ckets hentication Cod nd secret key use chenticity hange is established over public and private bleshooting p sa p policy	sure data not be and e (HMAC) d to er an e keys	
IP header can be authenticated but not encrypted Tunnel Mode A new IP header is created in place of the original; this allows for encryption of the entire original packet Configuration Crypto isakmp policy 10 ISAKMP Policy encryption aes 256 hash sha authentication pre-share group 2 lifetime 3600 ISAKMP Pre-Shared Key crypto isakmp key 1 MySecretKey address 10.0.0.2 IPsec Transform Set crypto ipsec transform-set MyTS esp-aes 256 esp-sha-hmac mode tunnel IPsec Profile set transform-set MyTS interface Tunnel0 Virtual Tunnel Interface ip address 172.16.0.1 255.255.255.252 tunnel source 10.0.0.1 tunnel destination 10.0.0.2 tunnel mode ipsec ipv4	Data In Secure has not Data C Encrypt intercep Data O Authen Authen Anti-re Sequen discard Hash N A hash provide Diffie-I A share insecur show c show c	Te ntegrity hashing (HM, been altered confidentiality tion is used to pted by a thir rigin Auther tication of the confidentiality tication of the tication of the confidentiality tication of the co	rminology AC) is used to ensite in transite ty o ensure data can d party htication e SA peer are used to detect ckets hentication Cod nd secret key use thenticity change is established over public and private bleshooting p sa p policy sa	sure data not be and e (HMAC) ed to er an e keys	
IP header can be authenticated but not encrypted Tunnel Mode A new IP header is created in place of the original; this allows for encryption of the entire original packet Configuration Crypto isakmp policy 10 ISAKMP Policy encryption aes 256 hash sha authentication pre-share group 2 lifetime 3600 ISAKMP Pre-Shared Key crypto isakmp key 1 MySecretKey address 10.0.0.2 IPsec Transform Set crypto ipsec transform-set MyTS esp-aes 256 esp-sha-hmac mode tunnel IPsec Profile set transform-set MyTS interface Tunnel0 Virtual Tunnel Interface ip address 172.16.0.1 255.255.255.252 tunnel source 10.0.0.1 tunnel destination 10.0.0.2 tunnel mode ipsec ipv4 tunnel protection ipsec profile MyProfile	Data In Secure has not Data C Encrypt interce Data O Authem Anti-re Sequen discard Hash N A hash provide Diffie-I A share insecur Show C show C show C	Te ntegrity hashing (HM, been altered confidentiality tion is used to pted by a thir origin Auther tication of the confidentiality tication of the tication of the confidentiality tication of the c	rminology AC) is used to ensi- in transit be ensure data can d party htication e SA peer are used to detect ckets hentication Cod nd secret key use thenticity hange is established over public and private bleshooting p sa p policy sa transform-set	sure data not be and e (HMAC) ed to er an e keys	