Silver Peak Security Algorithms

Silver Peak Systems, Inc.
1.877.210.7325 (toll-free in USA)
+1.408.935.1850
www.silver-peak.com

Data Path

The table below describes the IKE/IPsec algorithms supported in underlay tunnels between Silver Peak devices and IPsec tunnels to third party devices or cloud services.

VXOA Release	Key Management		IPsec	
8.2.0+	**Authentication**	**Key Exchange**	**Encryption**	**Message digest/hash/HMAC**
IPsec UDP mode (default for Silver Peak underlay tunnels)	Through Secure Zero Touch Provisioning	Proprietary, through Orchestrator	AES-128-CBC, AES-256-CBC (default)	SHA2 (SHA256, SHA384, SHA512), SHA1 (default)
3rd party IPsec tunels (passthrough tunnels)	IKEv2 (recommended), IKEv1 Custom/auto-generated Pre-Shared Keys, no cetificates	DH Group 14 (2048bit) - (recommended) 1, 2, 5, 15, 16, 17, 18	NULL, AES-128-CBC, AES-256-CBC (recommended)	SHA2 (SHA256, SHA384, SHA512), SHA1 (recommended)
Regular IPsec mode with IKE (for Silver Peak underlay tunels)	IKEv2 (default), IKEv1 Custom/auto-generated Pre-Shared Keys, no certificates	DH Group 14 (2048bit) - (default) 15, 16, 17, 18	AES-128-CBC, AES-256-CBC (default)	SHA2 (SHA256, SHA384, SHA512), SHA1 (default)
8.1.9.0+	**Authentication**	**Key Exchange**	**Encryption**	**Message digest/hash/HMAC**
IPsec UDP mode (default for Silver Peak underlay tunnels)	Through Secure Zero Touch Provisioning	Proprietary, through Orchestrator	AES-128-CBC, AES-256-CBC (default)	SHA2 (SHA256, SHA384, SHA512), SHA1 (default)
3rd party IPsec tunels (passthrough tunnels)	IKEv1 (custom/auto-generated pre-shared keys, no certificates)	DH Group 14 (2048bit) - (recommended) 1, 2, 5, 15, 16, 17, 18	NULL, AES-128-CBC, AES-256-CBC (recommended)	SHA2 (SHA256, SHA384, SHA512), SHA1 (recommended)
Regular IPsec mode with IKE (for Silver Peak underlay tunels)	IKEv1 (custom/auto-generated pre-shared keys, no certificates)	DH Group 14 (2048bit) - (default) 15, 16, 17, 18	AES-128-CBC, AES-256-CBC (default)	SHA2 (SHA256, SHA384, SHA512), SHA1 (default)
8.1.6.0+	**Authentication**	**Key Exchange**	**Encryption**	**Message digest/hash/HMAC**
IPsec UDP mode (default for Silver Peak underlay tunnels)	Through Secure Zero Touch Provisioning	Proprietary, through Orchestrator	AES-128-CBC, AES-256-CBC (default)	SHA2 (SHA256, SHA384, SHA512), SHA1 (default)
Regular IPsec mode with IKE (for Silver Peak underlay tunels)	IKEv1 (custom/auto-generated pre-shared keys, no certificates)	DH Group 14 (2048bit) - (default) 15, 16, 17, 18	AES-128-CBC, AES-256-CBC (default)	SHA2 (SHA256, SHA384, SHA512), SHA1 (default)
	Authentication	**Key Exchange**	**Encryption**	**Message digest/hash/HMAC**
8.1.0-8.1.5.x Regular IPsec mode with IKE, (default for Silver Peak underlay tunnels)	IKEv1 (custom/auto-generated pre-shared keys, no certificates)	DH Group 14 (2048bit) - (default), DH Group 1, 2, 5 (deprecated)	AES-128-CBC, AES-256-CBC (default)	SHA2 (SHA256, SHA384, SHA512), SHA1 (default)
8.0 Regular IPsec mode with IKE, (default for Silver Peak underlay tunnels)			AES-128-CBC, AES-256-CBC (default)	SHA1
7.3 Regular IPsec mode with IKE, (default for Silver Peak underlay tunnels)			AES-128-CBC	SHA1

Additional Parameters	
8.2.1+	
Dead Peer Detection	On, every 5 minutes
8.1.6+	
IPsec UDP key rotation	Default: every day, can be configured per hour, at the minimum
NAT traversal	On, keepalive is eight seconds
Perfect Forward Secrecy (PFS) for IPsec UDP mode	Proprietary algorithm
PFS for IPsec mode and third-party tunnels	The same DH groups under “Key Exchange” are also supported for PFS. Additionally, a PFS “disable” option is possible.

Silver Peak Systems, Inc.
1.877.210.7325 (toll-free in USA)
+1.408.935.1850
www.silver-peak.com

Appliance WebUI

The table below describes the ciphers used by the VXOA software for WebUI on Silver Peak EdgeConnect, VX/NX devices.

Release		TLS Certificate			Appliance as TLS server: TLS between web browser and appliance				
8.0.x and later	Works with	Signature Hash	Public Key	Certificate Format	Server Key exchange	Server Authentication	Encryption	Protocol	Message Authentication
TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384	TLS1.2	SHA256	RSA , 2048bits plus	PEM	ECDHE_RSA	RSA	AES128-CBC	TLS 1.2	SHA1
TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256	TLS1.2			Self-signed and CA-signed			AES256-CBC		SHA256
TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA	TLS1.2						AES128-GCM		SHA384
TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384	TLS1.2						AES256-GCM		
TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256	TLS1.2	Disabled: Null, DES, RC4, MD5, PSK, IDEA, Export							
TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA	TLS1.2								

Orchestrator

The table below describes the ciphers used by the Silver Peak Orchestrator/GMS devices.

Orchestrator (GMS) Release		TLS Certificate			Orchestrator as TLS server: TLS session to appliance, cloud portal, client web browser				
8.0.x and later	Works with	Signature Hash	Public Key	Certificate Format	Server Key Exchange	Server Authentication	Encryption	HMAC	Protocol
TLS_DHE_RSA_WITH_AES_256_CBC_SHA256	TLS1.2	SHA256	RSA, 2048bits	PEM	DHE_RSA	RSA	AES128-CBC	SHA1	TLS 1.2
TLS_DHE_RSA_WITH_AES_256_CBC_SHA	TLS1.2			Self-signed and CA-signed	ECDHE_RSA		AES256-CBC	SHA256	
TLS_DHE_RSA_WITH_AES_128_CBC_SHA	TLS1.2						AES128-GCM	SHA384	
TLS_DHE_RSA_WITH_AES_128_GCM_SHA256	TLS1.2						AES256-GCM		
TLS_DHE_RSA_WITH_AES_128_CBC_SHA256	TLS1.2	Disabled: SSL, SSLv2, SSLv3, .*NULL.*, .*RC4.*, .*MD5.*, .*DES.*, .*DSS.*							
TLS_DHE_RSA_WITH_AES_256_GCM_SHA384	TLS1.2								
TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256	TLS1.2								
TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA	TLS1.2								
TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384	TLS1.2								
TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256	TLS1.2								
TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384	TLS1.2								
TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA	TLS1.2								

Silver Peak Systems, Inc.
1.877.210.7325 (toll-free in USA)
+1.408.935.1850
www.silver-peak.com

SSL Acceleration

The table below describes the ciphers used by the SSL proxy feature on the Silver Peak VXOA software running on EdgeConnect, NX/VX devices. New releases support all the ciphers of older releases.

VXOA Release	Key Exchange	Authentication	Ciphers	Message Authentication	Protocol	Cert Format	Supported extension	Curves Supported
8.1.9.1	RSA	RSA	AES128	MD5	ssl v3	PEM	All previous	All previous, plus x25519
	DHE_RSA	ECDSA	AES256	SHA1	TLS 1.0	PFX		
	ECDHE_RSA		AES128-GCM	SHA2 (SHA 384 supported)	TLS 1.1			
			AES256-GCM		TLS 1.2			
			RC4					
			3DES					
8.x	RSA	RSA	AES128	MD5	ssl v3	PEM	All previous, plus EXTENDED_MASTER_SECRET	sect163k1, sect163r1, sect163r2, sect193r1, sect193r2, sect233k1, sect233r1, sect239k1, sect283k1, sect283r1, sect409k1, sect409r1, sect571k1, sect571r1, secp160k1, secp160r1, secp160r2, secp192k1, prime192v1, secp224k1, secp224r1, secp256k1, prime256v1, secp384r1, secp521r1
	DHE_RSA		AES256	SHA1	TLS 1.0	PFX		
	ECDHE_RSA		AES128-GCM	SHA2 (SHA 384 supported)	TLS 1.1			
			AES256-GCM		TLS 1.2			
			RC4					
			3DES					
7.3.x	RSA	RSA	AES128	MD5	ssl v3	PEM	SSL_EXT_TRUSTED_CA_KEYS: SSL_EXT_SESSION_TICKET: SSL_EXT_HEARTBEAT: SSL_EXT_ALPN: SSL_EXT_STATUS_REQUEST: SSL_EXT_STATUS_REQUEST_V2: SSL_EXT_NEXT_PROTOCOL_NEGOTIATION: SSL_EXT_SERVER_NAME: SSL_EXT_MAX_FRAGMENT_LENGTH: SSL_EXT_RENEGOTIATION_INFO: SSL_EXT_ELLIPTIC_CURVES: SSL_EXT_EC_POINT_FORMATS: SSL_EXT_SIGNATURE_ALGORITHMS:	
	DHE_RSA		AES256	SHA1	TLS 1.0	PFX		
	ECDHE_RSA		AES128-GCM	SHA2 (SHA 384 supported)	TLS 1.1			
			AES256-GCM		TLS 1.2			
			RC4					
			3DES					
6.2.x	RSA	RSA	AES128	MD5	ssl v3	PEM		
			AES256	SHA1	TLS 1.0	PFX		
			RC4	SHA2 (SHA 256 supported)	TLS 1.1			
			3DES		TLS 1.2			

Silver Peak Security Algorithms

Silver Peak Systems, Inc.
1.877.210.7325 (toll-free in USA)
+1.408.935.1850
www.silver-peak.com

Network Memory

The table below describes the ciphers used by the VXOA software for Network Memory on-disk encryption on Silver Peak Edge Connect, VX/NX devices.

VXOA Release	Network Memory Ciphers
8.1.x	AES128

SNMPv3

The table below describes the ciphers used by the VXOA software SNMPv3 functionality on Silver Peak Edge Connect, VX/NX devices.

VXOA Release	SNMPv3 Ciphers
8.1.x	AES128 (encryption), SHA1 (hashing/integrity)

SSH

The table below describes the ciphers used by the VXOA software for SSH on Silver Peak Edge Connect, VX/NX devices.

VXOA Release	SSH Ciphers[1]
8.1.x	AES128 (encryption),SHA1 (hashing/integrity)

[1] SSHv2.0 only, Linux kernel based