The following refers to the IKE/IPsec datapath implementation of overlay tunnels between Silver Peak devices.

VXOA Release	Key Management		IPsec	
7.3 (Regular "IPsec" mode with IKE)	**Authentication**	**Key Exchange**	**Encryption**	**Message digest/hash/HMAC**
	IKE. Custom/auto-generated Pre-Shared Keys, no certificates	DH Group 14 (2048bit)	AES-128-CBC	SHA1
8.0 (Regular "IPsec" mode with IKE)	**Authentication**	**Key Exchange**	**Encryption**	**Message digest/hash/HMAC**
	IKE. Custom/auto-generated Pre-Shared Keys, no certificates	DH Group 14 (2048bit)	AES-128-CBC, AES-256-CBC	SHA1
8.1.0-8.1.5.x (Regular "IPsec" mode with IKE)	**Authentication**	**Key Exchange**	**Encryption**	**Message digest/hash/HMAC**
	IKE. Custom/auto-generated Pre-Shared Keys, no certificates	DH Group 14 (2048bit)	AES-128-CBC, AES-256-CBC	SHA2 (SHA256, SHA384, SHA512), SHA1(default)
8.1.6+ IPsec UDP mode without IKE is default. Regular "IPsec" mode is also supported.			**Encryption**	**Message digest/hash/HMAC**
	Through Secure Zero Touch Provisioning	Proprietary, through Orchestrator	AES-128-CBC, AES-256-CBC	SHA2 (SHA256, SHA384, SHA512), SHA1(default)

Other parameters (till 8.1.5.x)	
DPD	On, every 5 minutes
IKE Mode	IKEv1, Main
Nat traversal	On, keepalive 8secs
IKE Lifetime/Rekey	12hrs
IPsec Lifetime/Rekey	60mins
IKE pre-shared key rotation	Every week
Other parameters (8.1.6+)	
IPsec UDP Key Rotation	Default every day, can be configured per hour, at the minimum

Appliance WebUI

The following refers to the ciphers used by the VXOA software for WebUI on Silver Peak Edge Connect, VX/NX devices.

Release	
8.0.x and later	**Works with**
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_CBC_SHA	TLS1.2
TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384	TLS1.2
TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256	TLS1.2
TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA	TLS1.2

TLS Certificate			Appliance as TLS server: TLS between web browser and appliance				openssl keygen can
Signature Hash	**Public Key**	**Certificate Format**	**Key exchange**	**Encryption**	**Protocol**	**HMAC**	
SHA256	RSA , 2048bits	PEM	DHE_RSA	AES128-CBC	TLS 1.2	SHA1	secp256k1
		Self-signed and CA-signed		AES256-CBC		SHA256	secp384r1
				AES128-GCM		SHA384	secp521r1
				AES256-GCM			prime256v1

Disabled: Null, DES, RC4, MD5, PSK, IDEA, Export

NOTE: TLS protocol implemented within EdgeConnect and NX devices uses only algorithms specified above.

The following refers to the ciphers used by the Silver Peak Orchestrator/GMS devices.

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								
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								

Disabled: SSL, SSLv2, SSLv3, .*NULL.*, .*RC4.*, .*MD5.*, .*DES.*, .*DSS.*

NOTE: TLS protocol implemented within EdgeConnect and NX devices uses only algorithms specified above.

The following refers to the ciphers used by the SSL proxy feature on the Silver Peak VXOA software running on Edge Connect, NX/VX devices.

VXOA Release	Key Exchange	Ciphers	Digest	Protocol	Cert Format	Supported extension
6.2.x	RSA RSA	AES128 AES256 RC4 3DES	MD5 SHA1 SHA2 (SHA 256 supported)	ssl v3 TLS 1.0 TLS 1.1 TLS 1.2	PEM PFX	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:
7.3.x	RSA DHE ECDHE	AES128 AES256 AES128-GCM AES256-GCM RC4 3DES	MD5 SHA1 SHA2 (SHA 384 supported)	ssl v3 TLS 1.0 TLS 1.1 TLS 1.2	PEM PFX	**Support for all 6.2.x and following** 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:
8.x	RSA (confirm 2048bits) DHE (confirm 2048bits) ECDHE (confirm 224 bits)	AES128 AES256 AES128-GCM AES256-GCM RC4 3DES	MD5 SHA1 SHA2 (SHA 384 supported)	ssl v3 TLS 1.0 TLS 1.1 TLS 1.2	PEM PFX	**Same as 7.3** EXTENDED_MASTER_SECRET

NOTE: TLS protocol implemented within EdgeConnect and NX devices uses only algorithms specified above.

The following refers to 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

The following refers to 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)

The following refers to the ciphers used by the VXOA software for SSH on Silver Peak Edge Connect, VX/NX devices.

VXOA Release	SSH Ciphers	Notes
8.1.x	AES128 (encryption), SHA1 (hashing/integrity)	SSHv2.0 only, Linux kernel based