Cloud Software Group

NetScaler MPX

Hardware Models: 8900 FIPS, 9100 FIPS, 15000-50G FIPS series
Part numbers: 8905 FIPS, 8910 FIPS, 8920 FIPS, 9120 FIPS, 9130 FIPS, 9140 FIPS, 9160 FIPS, 9180 FIPS, 9195 FIPS, 15030-50G FIPS, 15040-50G FIPS, 15060-50G FIPS, 15080-50G FIPS, 15100-50G FIPS, 15120-50G FIPS
Firmware Version: 13.1.FIPS

FIPS 140-3 Non-Proprietary Security Policy

FIPS Security Level: 2
Document Version: 0.4

Prepared for:

Cloud Software Group

Cloud Software Group
851 Cypress Creek Road
Fort Lauderdale, FL 33309
United States of America

Phone: +1 954 267 3000
www.cloud.com

Prepared by:

Corsec

Corsec Security, Inc.
12600 Fair Lakes Circle, Suite 210
Fairfax, VA 22033
United States of America

Phone: +1 703 267 6050
www.corsec.com

Abstract

This is a non-proprietary Cryptographic Module Security Policy for the NetScaler MPX (version: 13.1.FIPS) from Cloud Software Group (Cloud). This Security Policy describes how the NetScaler MPX meets the security requirements of Federal Information Processing Standards (FIPS) Publication 140-3, which details the U.S. and Canadian government requirements for cryptographic modules. More information about the FIPS 140-3 standard and validation program is available on the National Institute of Standards and Technology (NIST) and the Canadian Centre for Cyber Security (CCCS) Cryptographic Module Validation Program (CMVP) website at http://csrc.nist.gov/groups/STM/cmvp.

This document also describes how to run the module in a secure Approved mode of operation. This policy was prepared as part of the Level 2 FIPS 140-3 validation of the module. The NetScaler MPX is referred to in this document as NetScaler MPX or the module.

References

This document deals only with operations and capabilities of the module in the technical terms of a FIPS 140-3 cryptographic module security policy. More information is available on the module from the following sources:

- The Cloud Software Group website (www.cloud.com) contains information on the full line of services and solutions from Cloud.
- The search page on the CMVP website (https://csrc.nist.gov/Projects/cryptographic-module-validation-program/Validated-Modules/Search) can be used to locate and obtain vendor contact information for technical or sales-related questions about the module.

Document Organization

ISO/IEC 19790 Annex B uses the same section naming convention as *ISO/IEC 19790* section 7 - Security requirements. For example, Annex B section B.2.1 is named “General” and B.2.2 is named “Cryptographic module specification,” which is the same as *ISO/IEC 19790* section 7.1 and section 7.2, respectively. Therefore, the format of this Security Policy is presented in the same order as indicated in Annex B, starting with “General” and ending with “Mitigation of other attacks.” If sections are not applicable, they have been marked as such in this document.

Table of Contents

List of Tables

List of Figures

1. General

The Netscaler product line optimizes delivery of applications over the Internet and private networks. It is an Application Delivery Controller (ADC) that performs application-specific traffic analysis to intelligently distribute, optimize, and secure L4-L7[1] network traffic for web-applications. All these capabilities are combined into a single, integrated appliance for increased productivity, with lower overall total cost of ownership.

These hardware-based appliances employ a multi-core processor design and are available in a wide range of appliance configurations, from sub gigabit throughput to 50 Gbps[2]. Each leverages a fully hardened and secure operating system.

These appliances are installed in the data center between the clients and the internal customer network. All client requests and server responses pass through it. The internal customer network hosts all load-balancing and authentication services, such as LDAP[3], Kerberos, and SAML[4]. The module's features are enabled, and the configured policies are then applied to incoming and outgoing traffic. Figure 1 is an illustration of a typical deployment.

[1] L4-L7 – Layer 4 – Layer 7
[2] Gbps – Gigabits per second
[3] LDAP – Lightweight Directory Access Protocol
[4] SAML – Security Assurance Markup Language

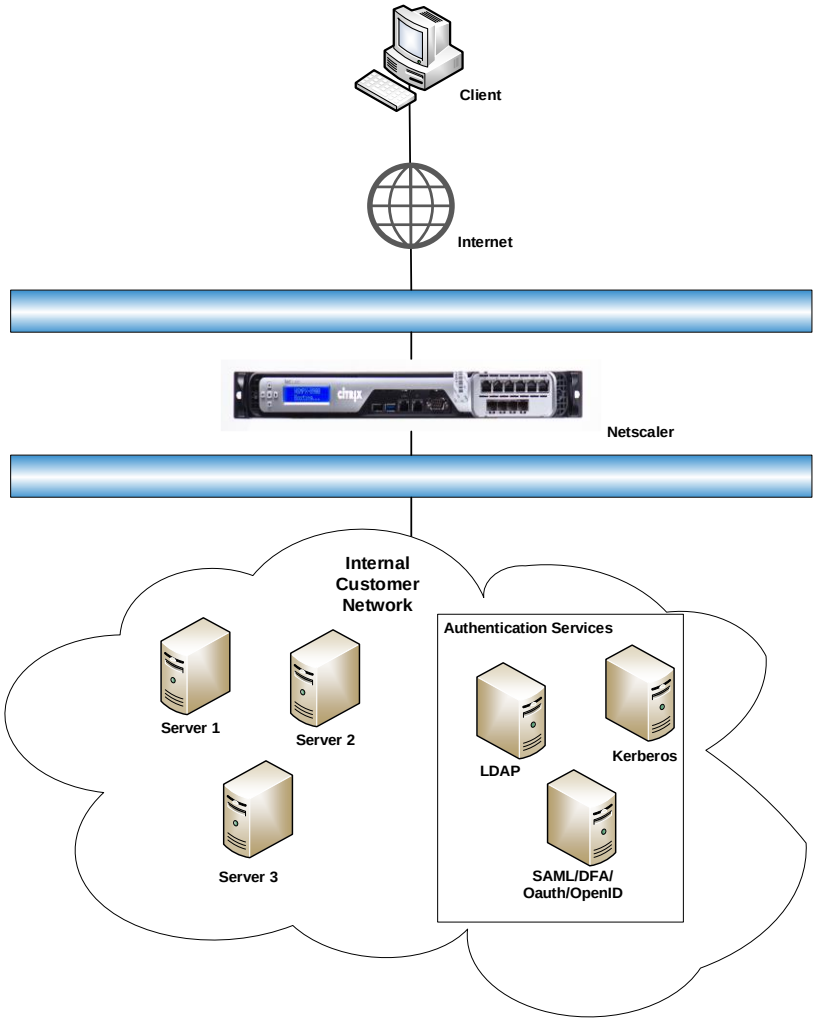

Figure 1 – Typical NetScaler MPX Deployment

The feature set can be broadly categorized as consisting of switching features, security and protection features, and server-farm optimization features:

- Switching features – When deployed in front of application servers, the NetScaler MPX ensures optimal distribution of traffic by the way in which it directs client requests. Administrators can segment application traffic according to information in the body of an HTTP[5] or TCP[6] request, and on the basis of L4–L7 header information such as URL[7], application data type, or cookie. Numerous load balancing algorithms and extensive server health checks improve application availability by ensuring that client requests are directed to the appropriate servers.

- Security and protection features – NetScaler MPX security and protection features protect web applications from Application Layer attacks. The MPX allows legitimate client requests and can block

[5] HTTP – Hypertext Transfer Protocol
[6] TCP – Transmission Control Protocol
[7] URL – Uniform Resource Locator

malicious requests. It provides built-in defenses against denial-of-service (DoS) attacks and supports features that protect against legitimate surges in application traffic that would otherwise overwhelm the servers. An available built-in firewall protects web applications from Application Layer attacks, including buffer overflow exploits, SQL[8] injection attempts, cross-site scripting attacks, and more. In addition, the firewall provides identity theft protection by securing confidential corporate information and sensitive customer data.

- Optimization features – Optimization features offload resource-intensive operations, such as SSL[9] processing, data compression, client keep-alive, TCP buffering, and the caching of static and dynamic content from servers. This improves the performance of the servers in the server farm and therefore speeds up applications. The MPX supports several transparent TCP optimizations, which mitigate problems caused by high latency and congested network links, accelerating the delivery of applications while requiring no configuration changes to clients or servers.

The NetScaler MPX hardware platform consists of a Control Plane processing function (providing all configuration and management processing functions) and one to seven Data Plane(s), which provide data packet processing functions. All configuration and management activities are performed at the workstation through the web-based GUI[10], REST[11]ful Nitro API[12], and CLI[13] interfaces. The GUI includes a configuration utility for configuring the appliance and a statistical utility called Dashboard.

NetScaler MPX is validated at the FIPS 140-3 section levels shown in Table 1.

Table 1 – Security Level per FIPS 140-3 Section

ISO/IEC 24759 Section 6. [Number Below]	FIPS 140-3 Section Title	Security Level
1	General	2
2	Cryptographic Module Specification	2
3	Cryptographic Module Interfaces	2
4	Roles, Services, and Authentication	3
5	Software/Firmware Security	2
6	Operational Environment	N/A
7	Physical Security	2
8	Non-Invasive Security	N/A[14]
9	Sensitive Security Parameter Management	2
10	Self-tests	2
11	Life-Cycle Assurance	2
12	Mitigation of Other Attacks	N/A

[8] SQL – Structured Query Language
[9] SSL – Secure Sockets Layer
[10] GUI – Graphical User Interface
[11] REST – Representational State Transfer
[12] API – Application Programming Interface
[13] CLI – Command Line Interface
[14] N/A – Not applicable

2. Cryptographic Module Specification

NetScaler MPX is a hardware module with a multiple-chip standalone embodiment.

2.1 Operational Environments

The module was tested and found to be compliant with FIPS 140-3 requirements using the hardware models listed in Table 2. Note that all models within a model family employ the same chassis, ports/interfaces, and memory/storage devices. All models across all families run the same operating system and application firmware.

Table 2 – Cryptographic Module Tested Configurations

Model	Hardware (Part Number and Version)	Firmware Version	Distinguishing Features
8900 FIPS series	8905 FIPS	13.1.FIPS	• Intel Xeon E5-2620 v4 (Broadwell) • 5Gbps L4/L7 throughput for SME[15]
	8910 FIPS	13.1.FIPS	• Intel Xeon E5-2620 v4 (Broadwell) • 10Gbps L4/L7 throughput for SME
	8920 FIPS	13.1.FIPS	• Intel Xeon E5-2620 v4 (Broadwell) • 20Gbps L4/L7 throughput for SME
9100 FIPS series	9110 FIPS	13.1.FIPS	• Intel Xeon Silver 4310T (Ice Lake) • 20Gbps L4/L7 throughput for SME
	9120 FIPS	13.1.FIPS	• Intel Xeon Silver 4310T (Ice Lake) • 20Gbps L4/L7 throughput for SME
	9130 FIPS	13.1.FIPS	• Intel Xeon Silver 4310T (Ice Lake) • 30Gbps L4/L7 throughput for SME
	9140 FIPS	13.1.FIPS	• Intel Xeon Silver 4310T (Ice Lake) • 40Gbps L4/L7 throughput for SME
	9160 FIPS	13.1.FIPS	• Intel Xeon Silver 4310T (Ice Lake) • 60Gbps L4/L7 throughput for SME
	9180 FIPS	13.1.FIPS	• Intel Xeon Silver 4310T (Ice Lake) • 80Gbps L4/L7 throughput for SME
	9195 FIPS	13.1.FIPS	• Intel Xeon Silver 4310T (Ice Lake) • 95Gbps L4/L7 throughput for SME
15000-50G FIPS series	15020-50G FIPS	13.1.FIPS	• Intel Xeon E5-2620 v4 (Broadwell) • 30Gbps L4/L7 throughput for MLE[16]
	15030-50G FIPS	13.1.FIPS	• Intel Xeon E5-2620 v4 (Broadwell) • 30Gbps L4/L7 throughput for MLE
	15040-50G FIPS	13.1.FIPS	• Intel Xeon E5-2620 v4 (Broadwell) • 40Gbps L4/L7 throughput for MLE

[15] SME – Small and Medium Enterprise
[16] MLE – Medium and Large Enterprise

Model	Hardware (Part Number and Version)	Firmware Version	Distinguishing Features
	15060-50G FIPS	13.1.FIPS	• Intel Xeon E5-2620 v4 (Broadwell) • 60Gbps L4/L7 throughput for MLE
	15080-50G FIPS	13.1.FIPS	• Intel Xeon E5-2620 v4 (Broadwell) • 80Gbps L4/L7 throughput for MLE
	15100-50G FIPS	13.1.FIPS	• Intel Xeon E5-2620 v4 (Broadwell) • 100Gbps L4/L7 throughput for MLE
	15120-50G FIPS	13.1.FIPS	• Intel Xeon E5-2620 v4 (Broadwell) • 120Gbps L4/L7 throughput for MLE

2.2 Algorithm Implementations

The module includes the following cryptographic libraries that provide basic cryptographic functionalities and support secure networking protocols:

- Netscaler Control Plane Cryptographic Library v1.0 (Cert. A3942)
- Netscaler Data Plane Cryptographic Library v1.0 (Cert. A3943)
- Intel hardware cryptographic accelerator v1.0 (Cert. A3944)
- NetScaler CPU Jitter Entropy Source v.3.4.0 (Cert. A3513)

2.2.1 Netscaler Control Plane Cryptographic Library

Table 3 lists the Approved algorithms implemented in the Netscaler Control Plane Cryptographic Library.

Table 3 – Approved Algorithms (Netscaler Control Plane Cryptographic Library)

CAVP Certificate[17]	Algorithm and Standard	Mode / Method	Description / Key Size(s) / Key Strengths	Use / Function
A3942	**AES** *FIPS PUB[18] 197*	CBC[19], CTR[20]	128, 192, 256	Encryption/decryption
		CFB128[21]	128	Encryption/decryption
A3942	**AES** *NIST SP 800-38D*	GCM[22]	128, 256	Encryption/decryption
Vendor Affirmed	**CKG**[23] *NIST SP 800-133rev2 Compliant to SP 800-133rev2 Section 4.*	-	-	Cryptographic key generation

[17] This table includes vendor-affirmed algorithms that are approved but CAVP testing is not yet available.
[18] PUB – Publication
[19] CBC – Cipher Block Chaining
[20] CTR – Counter
[21] CFB – Cipher FeedBack
[22] GCM – Galois Counter Mode
[23] CKG – Cryptographic Key Generation.

CAVP Certificate[17]	Algorithm and Standard	Mode / Method	Description / Key Size(s) / Key Strengths	Use / Function
A3942	**CVL**[24] *NIST SP 800-135rev1*	KDF (IKE[25] v1/v2, SSH[26], SNMP[27], TLS[28] v1.0/v1.1)	-	Key derivation *No parts of the IKE, SSH, SNMP and TLS protocols, other than the KDFs, have been tested by the CAVP and CMVP.*
A3942	**CVL** *RFC[29] 5246* *RFC 7627*	KDF (TLS v1.2)	-	Key derivation *No part of the TLS protocol, other than the KDF, has been tested by the CAVP and CMVP.*
A3942	**DRBG**[30] *NIST SP 800-90Arev1*	Counter-based w/ derivation function	AES-256	Deterministic random bit generation
A3942	**ECDSA**[31] *FIPS PUB 186-4*	Secret generation modes: Testing candidates, extra bits	P-224, P-256, P-384, P-521	Key pair generation
		-	P-224, P-256, P-384, P-521	Public key validation
		-	P-224, P-256, P-384, P-521 (SHA2-224, SHA2-256, SHA2-384, SHA2-512)	Digital signature generation
		-	P-224, P-256, P-384, P-521 (SHA-1, SHA2-224, SHA2-256, SHA2-384, SHA2-512)	Digital signature verification
A3942	**HMAC**[32] *FIPS PUB 198-1*	SHA-1, SHA2-256, SHA2-384, SHA2-512	112 (minimum)	Message authentication *The module supports the truncation of HMAC SHA-1 to 96 bits according to NIST SP 800-107rev1.*
A3942	**KAS**[33] *NIST SP 800-56Arev3* *NIST SP 800-135rev1* *Compliant to IG D.F. Scenario 2, Path 2.*	KAS-ECC-SSC with SSH KDF	P-224, P-256, P-384, P-521	Key agreement *Key establishment methodology provides between 112 and 256 bits of encryption strength*
		KAS-ECC-SSC with TLS v1.0/v1.1 KDF	P-224, P-256, P-384, P-521	Key agreement *Key establishment methodology provides between 112 and 256 bits of encryption strength*
		KAS-FFC-SSC with IKE v1/v2 KDF	MODP-2048, MODP-3072, MODP-4096, MODP-6144	Key agreement *Key establishment methodology provides between 112 and 176 bits of encryption strength*

[24] CVL – Component Validation List
[25] IKE – Internet Key Exchange
[26] SSH – Secure Shell
[27] SNMP – Simple Network Management Protocol
[28] TLS – Transport Layer Security
[29] RFC – Request for Comments
[30] DRBG – Deterministic Random Bit Generator
[31] ECDSA – Elliptic Curve Digital Signature Algorithm
[32] HMAC – (keyed-) Hashed Message Authentication Code
[33] KAS – Key Agreement Scheme

CAVP Certificate[17]	Algorithm and Standard	Mode / Method	Description / Key Size(s) / Key Strengths	Use / Function
		KAS-FFC-SSC with SSH KDF	MODP-2048, MODP-4096	Key agreement *Key establishment methodology provides between 112 and 176 bits of encryption strength*
		KAS-FFC-SSC with TLS v1.0/v1.1 KDF	ffdhe2048, ffdhe3072, ffdhe4096, ffdhe6144	Key agreement *Key establishment methodology provides between 112 and 176 bits of encryption strength*
A3942	**KAS** *NIST SP 800-56Arev3* *RFC[34] 7627* *Compliant to IG D.F. Scenario 2, Path 2.*	KAS-ECC-SSC with TLS v1.2 KDF	P-224, P-256, P-384, P-521	Key agreement *Key establishment methodology provides between 112 and 256 bits of encryption strength*
		KAS-FFC-SSC with TLS v1.2 KDF	ffdhe2048, ffdhe3072, ffdhe4096, ffdhe6144	Key agreement *Key establishment methodology provides between 112 and 176 bits of encryption strength*
A3942	**KAS-ECC-SSC**[35] *NIST SP 800-56Arev3*	EphemeralUnified	P-224, P-256, P-384, P-521	Shared secret computation
A3942	**KAS-FFC-SSC**[36] *NIST SP 800-56Arev3*	dhEphem	MODP-2048, MODP-3072, MODP-4096, MODP-6144, ffdhe2048, ffdhe3072, ffdhe4096, ffdhe6144	Shared secret computation
A3942	**KTS-IFC**[37] *NIST SP 800-56Brev2* *Compliant to IG D.G.*	rsakpg1-basic	KTS-OAEP-basic	Key transport *Key establishment methodology provides 112 bits of encryption strength*
A3942	**PBKDF2**[38] *NIST SP 800-132*	Section 5.4, option 1a	HMAC SHA-1	Password-based key derivation
A3942	**RSA**[39] *FIPS PUB 186-4*	Key generation mode: B.3.3	2048, 3072	Key pair generation
		PKCS#1 v1.5	2048, 3072 (SHA2-256, SHA2-384, SHA2-512)	Digital signature generation
			2048, 3072 (SHA-1, SHA2-256, SHA2-384, SHA2-512)	Digital signature verification
A3942	**Safe Primes** *NIST SP 800-56Arev3, Appendix D*	-	MODP-2048, MODP-3072, MODP-4096, MODP-6144, ffdhe2048, ffdhe3072, ffdhe4096, ffdhe6144	Key generation

[34] RFC – Request for Comments
[35] KAS-ECC-SSC – Key Agreement Scheme - Elliptic Curve Cryptography - Shared Secret Computation
[36] KAS-FFC-SSC – Key Agreement Scheme - Finite Field Cryptography - Shared Secret Computation
[37] KTS-IFC – Key Transport Scheme - Integer Factorization Cryptography
[38] PBKDF2 – Password-Based Key Derivation Function 2
[39] RSA – Rivest Shamir Adleman

CAVP Certificate[17]	Algorithm and Standard	Mode / Method	Description / Key Size(s) / Key Strengths	Use / Function
		-	MODP-2048, MODP-3072, MODP-4096, MODP-6144, ffdhe2048, ffdhe3072, ffdhe4096, ffdhe6144	Key verification
A3942	**SHS**[40] *FIPS PUB 180-4*	SHA-1, SHA2-256, SHA2-384, SHA2-512	-	Message digest

The Netscaler Control Plane Cryptographic Library uses PBKDF option 1a for PEM[41] key establishment. The PBKDF takes an input salt that is 128 bits in length with a password/passphrase containing at least 8 characters and produces a random value of 256 bits for AES keys. A password length of 8 characters is enforced by the module (see section 11.2.2 Configure the Passphrase Requirements). In addition, the function has an iteration count of 2,048. The underlying pseudorandom function used in this derivation is HMAC SHA-1. The keys derived from these PBKDF functions are only used for storage applications.

The vendor affirms the following cryptographic security methods implemented by the Netscaler Control Plane Cryptographic Library:

- Cryptographic key generation – As per *NIST SP 800-133*, the module uses its Approved DRBG to generate cryptographic keys and seeds used for the generation of cryptographic keys. The resulting symmetric key or generated seed is an unmodified output from the DRBG. The module's DRBG is seeded via entropy generated from CPU Jitter. The module requests a minimum number of 256 bits of entropy per call, and generates symmetric SSPs with up to 256 bits of size and security strength and asymmetric SSPs with up to 6144 bits of size and 178 bits of security strength.

The module does not implement any non-approved algorithms allowed in the Approved mode of operation.

The Netscaler Control Plane Cryptographic Library, Netscaler Data Plane Cryptographic Library, and Intel Hardware Cryptographic Accelerator implement the non-Approved algorithms shown in Table 4. These algorithms are allowed for use in the Approved mode of operation, as there is no security claimed on their use.

Table 4 – Non-Approved Algorithms Allowed in the Approved Mode of Operation with No Security Claimed

Algorithm	Caveat	Use / Function
MD5	-	Message digest in TLS 1.0/1.1[42]

The Netscaler Control Plane Cryptographic Library does not include any non-Approved algorithms not allowed in the Approved mode of operation.

2.2.2 Netscaler Data Plane Cryptographic Library

Table 5 lists the Approved algorithms implemented in the Netscaler Data Plane Cryptographic Library.

[40] SHS – Secure Hash Standard
[41] PEM – Privacy-Enhanced Mail
[42] Per *FIPS 140-3 Implementation Guidance* 2.4.A, this hashing technique with TLS 1.0/1.1 is allowed in the Approved mode with no security claimed.

Table 5 – Approved Algorithms (Netscaler Data Plane Cryptographic Library)

CAVP Certificate[43]	Algorithm and Standard	Mode / Method	Description / Key Size(s) / Key Strengths	Use / Function
A3943	**AES** *FIPS PUB 197*	CBC	128, 192, 256	Encryption/decryption
A3943	**AES** *NIST SP 800-38D*	GCM	128, 256	Encryption/decryption
Vendor Affirmed	**CKG** *NIST SP 800-133rev2 Compliant to SP 800-133rev2 Section 4 and 6.3 method 3.*	-	-	Cryptographic key generation
A3943	**CVL** *NIST SP 800-56Arev3*	KDF (TLS v1.0/1.1)	-	Key derivation *No part of TLS protocol, other than the KDF, has been tested by the CAVP and CMVP.*
A3943	**CVL** *RFC 5246* *RFC 7627*	KDF (TLS v1.2)	-	Key derivation *No part of the TLS protocol, other than the KDF, has been tested by the CAVP and CMVP.*
A3943	**CVL** *RFC 8446*	KDF (TLS v1.3)	-	Key derivation *No part of TLS protocol, other than the KDF, has been tested by the CAVP and CMVP.*
A3943	**DRBG** *NIST SP 800-90Arev1*	Hash-based	-	Deterministic random bit generation
A3943	**ECDSA** *FIPS PUB 186-4*	Secret generation mode: Testing candidates	P-224, P-256, P-384, P-521	Key pair generation
		-	P-224, P-256, P-384, P-521	Public key validation
		-	P-224, P-256, P-384, P-521 (SHA2-224, SHA2-256, SHA2-384, SHA2-512)	Digital signature generation
		-	P-224, P-256, P-384, P-521 (SHA-1, SHA2-224, SHA2-256, SHA2-384, SHA2-512)	Digital signature verification
A3943	**HMAC** *FIPS PUB 198-1*	SHA-1, SHA2-224, SHA2-256, SHA2-384, SHA2-512	112 (minimum)	Message authentication *The cryptographic library supports the truncation of HMAC SHA-1 to 96 bits according to NIST SP 800-107rev1.*
A3943	**KAS-ECC-SSC** *NIST SP 800-56Arev3*	EphemeralUnified	P-224, P-256, P-384, P-521	Shared secret computation
A3943	**KBKDF** *NIST SP 800-108*	Counter	HMAC-SHA2-256	Key derivation

[43] This table includes vendor-affirmed algorithms that are approved but CAVP testing is not yet available.

CAVP Certificate[43]	Algorithm and Standard	Mode / Method	Description / Key Size(s) / Key Strengths	Use / Function
A3943	**KTS-IFC** *NIST SP 800-56Brev2 Compliant to IG D.G.*	rsakpg1-basic	KTS-OAEP-basic	Key transport *Key establishment methodology provides 112 bits of encryption strength*
A3943	**RSA** *FIPS PUB 186-2*	PKCS#1 v1.5	4096 (SHA-1, SHA2-224, SHA2-256, SHA2-384, SHA2-512)	Digital signature verification
A3943	**RSA** *FIPS PUB 186-4*	PKCS#1 v1.5	2048, 3072, 4096 (SHA2-224, SHA2-256, SHA2-384, SHA2-512)	Digital signature generation
			1024, 2048, 3072, 4096 (SHA-1, SHA2-224, SHA2-256, SHA2-384, SHA2-512)	Digital signature verification
A3943	**SHS** *FIPS PUB 180-4*	SHA-1, SHA2-224, SHA2-256, SHA2-384, SHA2-512	-	Message digest

**Not all tested algorithms/modes are used by the module.*

The vendor affirms the following cryptographic security methods implemented by the Netscaler Data Plane Cryptographic Library:

- Cryptographic key generation – *As per NIST SP 800-133*, the module uses its Approved DRBG to generate cryptographic keys and seeds used for the generation of cryptographic keys. The resulting symmetric key or generated seed is an unmodified output from the DRBG. The module's DRBG is seeded via entropy generated from CPU Jitter. The module requests a minimum number of 256 bits of entropy per call, and generates symmetric SSPs with up to 256 bits of size and security strength, and asymmetric SSPs with a maximum size of 2048 bits (RSA), and 256 bits of security strength (ECDSA).

The Netscaler Data Plane Cryptographic Library does not include any non-Approved algorithms allowed in the Approved mode of operations.

Please see Table 4 above and the preceding paragraph that specifies the non-Approved algorithms allowed in the Approved mode of operation with no security claimed for the Netscaler Data Plane Cryptographic Library.

The Netscaler Data Plane Cryptographic Library does not include any non-Approved algorithms not allowed in the Approved mode of operations.

2.2.3 Intel Hardware Cryptographic Accelerator

Table 6 lists the Approved algorithms implemented in the module's Intel Communication Chipset 8955 hardware cryptographic accelerator. Random values are provided by the NetScaler Data Plane Cryptographic Library to cryptographic functions requiring it.

Table 6 – Approved Algorithms (Intel Hardware Cryptographic Accelerator)

CAVP Certificate	Algorithm and Standard	Mode / Method	Description / Key Size(s) / Key Strengths	Use / Function
A3944	**AES** *FIPS PUB 197*	CBC	128, 192, 256	Encryption/decryption
A3944	**AES** *NIST SP 800-38D*	GCM	128, 256	Encryption/decryption
A3944	**CVL** *NIST SP 800-56Arev3*	KDF (TLS v1.0/1.1)	-	Key derivation *No part of TLS protocol, other than the KDF, has been tested by the CAVP and CMVP.*
A3944	**CVL** *RFC 5246* *RFC 7627*	KDF (TLS v1.2)	-	Key derivation *No part of the TLS protocol, other than the KDF, has been tested by the CAVP and CMVP.*
A3944	**ECDSA** *FIPS PUB 186-4*	Secret generation mode: Testing candidates	P-224, P-256, P-384, P-521	Key pair generation
		-	P-224, P-256, P-384, P-521	Public key validation
		-	P-224, P-256, P-384, P-521 (SHA2-224, SHA2-256, SHA2-384, SHA2-512)	Digital signature generation
		-	P-224, P-256, P-384, P-521 (SHA1, SHA2-224, SHA2-256, SHA2-384, SHA2-512)	Digital signature verification
A3944	**HMAC** *FIPS PUB 198-1*	SHA-1, SHA2-224, SHA2-256, SHA2-384, SHA2-512	160, 256, 384, 512	Message authentication *The cryptographic library supports the truncation of HMAC SHA-1 to 96 bits according to NIST SP 800-107rev1.*
A3944	**KAS-ECC-SSC** *NIST SP 800-56Arev3*	EphemeralUnified	P-224, P-256, P-384, P-521	Shared secret computation
A3944	**RSA** *FIPS PUB 186-4*	PKCS#1 v1.5	2048, 3072, 4096	Digital signature generation
			1024, 2048, 3072, 4096	Digital signature verification
A3944	**SHS** *FIPS PUB 180-4*	SHA-1, SHA2-224, SHA2-256, SHA2-384, SHA2-512	-	Message digest

**Not all tested algorithms/modes are used by the module.*

The Intel Hardware Cryptographic Accelerator does not include any non-Approved algorithms allowed in the Approved mode of operations.

Please see Table 4 above and the preceding paragraph that specifies the non-Approved algorithms allowed in the Approved mode of operation with no security claimed non-Approved algorithms allowed in the Approved mode of operation with no security claimed for the Intel Hardware Cryptographic Accelerator.

The Intel Hardware Cryptographic Accelerator does not include any non-Approved algorithms not allowed in the Approved mode of operations.

2.2.4 NetScaler CPU Jitter Entropy Source

Table 6 lists the Approved algorithms implemented in the module's CPU Jitter Entropy Source.

Table 7 – Approved Algorithms (NetScaler CPU Jitter Entropy Source)

CAVP Certificate	Algorithm and Standard	Mode / Method	Description / Key Size(s) / Key Strengths	Use / Function
A3513	**SHA** *FIPS PUB 202*	SHA3-256	-	Message digest

The NetScaler CPU Jitter Entropy Source does not include any non-Approved algorithms allowed in the Approved mode of operations.

The NetScaler CPU Jitter Entropy Source does not include any non-Approved algorithms allowed in the Approved mode of operation with no security claimed.

The NetScaler CPU Jitter Entropy Source does not include any non-Approved algorithms not allowed in the Approved mode of operations.

2.3 Cryptographic Boundary

The cryptographic boundary of the module is defined by the enclosure of each NetScaler MPX appliance chassis. This includes all ports, physical interfaces, and removable covers.

The NetScaler MPX 89xx FIPS appliance is illustrated in Figure 2 and Figure 3.

Figure 2 – NetScaler MPX 89xx FIPS Front Panel

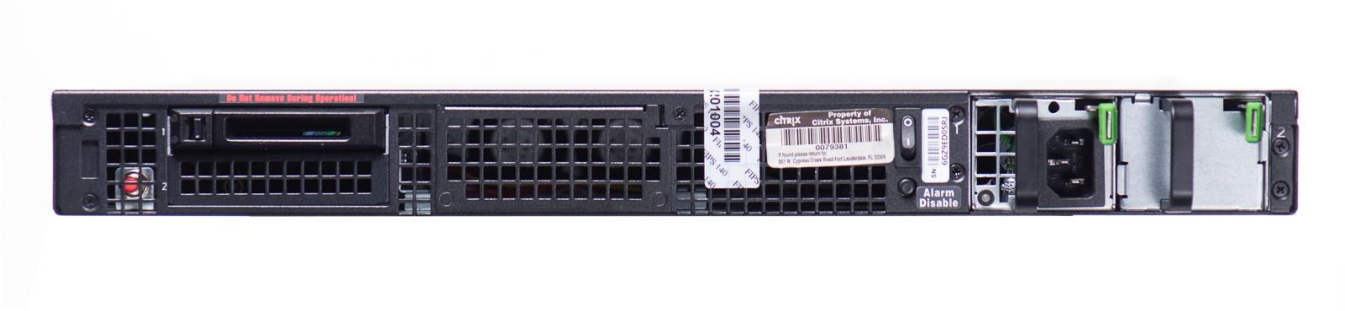

Figure 3 – NetScaler MPX 89xx FIPS Rear Panel

The NetScaler MPX 91xx FIPS appliance is illustrated in Figure 4 and Figure 5.

Figure 4 – NetScaler MPX 91xx FIPS Front Panel

Figure 5 – NetScaler MPX 91xx FIPS Rear Panel

The NetScaler MPX 15xxx-50G FIPS appliance is illustrated in Figure 6 and Figure 7.

Figure 6 – NetScaler MPX 15xxx-50G FIPS Front Panel

Figure 7 – NetScaler MPX 15xxx-50G FIPS Rear Panel

2.4 Excluded Components

There are no excluded components.

2.5 Modes of Operation

When installed, configured, and operated according to this Security Policy, the module supports the Approved mode of operation only; non-Approved operations are not supported.

3. Cryptographic Module Interfaces

FIPS 140-3 defines the following logical interfaces for cryptographic modules:

- Data Input
- Data Output
- Control Input
- Control Output
- Status Output

As a hardware appliance, the module's physical perimeter includes the physical ports, manual controls, physical indicators, and physical, logical, and electrical characteristics of the device. Each of the module's physical ports and manual controls maps to one of the defined FIPS 140-3 logical interfaces. A mapping of the interfaces, the host device's physical interfaces, and the module's logical interfaces can be found in Table 8.

Table 8 – Ports and Interfaces

Physical Port	Logical Interface	Data That Passes Over Port/Interface
10/100/1000Base-T copper RJ45 Ethernet port	Data Input	Network traffic (ingress)
	Data Output	Network traffic (egress)
	Control Input	Administrative data; Management data used to remotely manage the appliance independently of the firmware via the Lights-Out Management (LOM) feature
	Control Output	Control information is sent to remote machines supporting LDAP and RADIUS in order for the module to communicate with these machines.
	Status Output	Status information used to remotely monitor the appliance independently of the firmware via the Lights-Out Management (LOM) feature
LOM Port[44]	N/A	N/A
Management Port	Control Input	Ethernet Management ports used to connect directly to the appliance for CSG ADC administration functions
	Status Output	Ethernet Management ports used to connect directly to the appliance for CSG ADC administration functions
10G SFP+ Ethernet port*	Data Input	Network traffic (ingress)
	Data Output	Network traffic (egress
	Control Input	Administrative data; Management data used to remotely manage the appliance independently of the firmware via the Lights-Out Management (LOM) feature

[44] The LOM Port is disabled by default, the operator shall not enable this port. For more information see section 11.4.4 Additional Administrator Policies and Guidance.

Physical Port	Logical Interface	Data That Passes Over Port/Interface
	Control Output	Control information is sent to remote machines supporting LDAP and RADIUS in order for the module to communicate with these machines.
	Status Output	Status information used to remotely monitor the appliance independently of the firmware via the Lights-Out Management (LOM) feature
50G Ethernet port	Data Input	Network traffic (ingress)
	Data Output	Network traffic (egress)
	Control Input	Administrative data; Management data used to remotely manage the appliance independently of the firmware via the Lights-Out Management (LOM) feature
	Control Output	Control information is sent to remote machines supporting LDAP and RADIUS in order for the module to communicate with these machines.
	Status Output	Status information used to remotely monitor the appliance independently of the firmware via the Lights-Out Management (LOM) feature
RS-232 serial port	Control Input	Initial configuration data from a connected computer
	Status Output	Status information sent to a connected computer regarding initial configuration activities
LCD Keypad	Control Input	Initial configuration information from a connected computer; status information (available only on the 89xx FIPS & 15xxx-50G FIPS models)
	Status Output	IP information, system status updates, system information, current selection, or input information
Disable Alarm button**	Control Input	Button used to stop the power alarm from sounding.
NMI[45] button	Control Input	Button used (at the request of Technical Support) to initiate a core dump.
Power interface	Power	N/A

**1G copper transceivers are supported in 10G slots; 1G fiber transceivers are not supported.*

***The Disable Alarm button is functional only if a second power supply is installed.*

[45] NMI – Non-Maskable Interrupt

4. Roles, Services, and Authentication

The sections below describe the module's authorized roles, services, and operator authentication methods.

4.1 Authorized Roles

The module supports a Crypto Officer (CO) that authorized operators can assume. The CO role performs administrative services on the module, such as initialization, configuration, and monitoring of the module. The CO role includes the privileges listed under the read-only, operator, network, and sysadmin command policies.
The module also supports the following role(s):

- User – The User role can view the current status of the module and employ the services of the module (including IPsec[46], TLS, SSH, and SNMPv3 services). The User role includes the privileges listed under the read-only command policy.

Table 9 below lists the supported roles, along with the services (including input and output) available to each role.

Table 9 – Roles, Service Commands, Input and Output

Role	Service	Input	Output
CO, User	Show Status	Show Status Command	Module Status
CO	Perform self-tests on-demand	Reboot Command	Status output
CO	Perform initial network configuration	Command and parameters	Command response / status output
CO, User	Show versioning information	Show Hardware and Show Versions Command	Module name, version
CO	View system information	Show Info Command	Status output
CO	Configure system settings	Command and parameters	Command response / status output
CO	Configure HA[47]	Command and parameters	Status output / parameters accepted
CO	Manage NTP[48] servers	Command	Status output
CO	Zeroize	Reboot Command	Status output / system power on & off messages
CO	Configure system profiles	Command and parameters	Command response / status output
CO	Manage users	Command and user info	Status output
CO	Configure system auditing	Command and parameters	Command response / status output
CO	View audit logs	Command	Status output / system events
CO	Configure network settings	Command and parameters	Command response / status output
CO	Exchange routing information	Command	Status output / network ingo
CO	Configure SSH	Command and parameters	Command response / status output
CO, User	Establish SSH sessions	Command (CLI or Rest API)	Status output / connection success
CO	Configure CloudBridge	Command and parameters	Command response / status output
CO	Configure clustering	Command and parameters	Command response / status output

[46] IPsec – Internet Protocol Security
[47] HA – High Availability
[48] NTP – Network Time Protocol

Role	Service	Input	Output
CO, User	Establish IPsec session	Command	Status output / connection success
CO	Backup and restore	Command / backup files	Status output / backup files
CO	Manage encryption keys	Command	Status output
CO	Manage HMAC keys	Command	Status output
CO	Configure traffic management	Command and parameters	Command response / status output
CO, User	Establish TLS session	Command	Status output / connection success
CO, User	Resume TLS session	Command	Status output / connection success
CO	Apply data policies	Command	Status output
CO	Configure security	Command and parameters	Command response / status output
CO	Configure Gateway	Command and parameters	Command response / status output
CO	Establish Gateway connection	Command and parameters	Command response / status output / connection success
CO	Configure external servers for system, AAA, and Gateway authentication	Command and parameters	Command response / status output
CO	Configure SNMPv3	Command and parameters	Command response / status output
CO	SNMPv3 traps	None	Status output
CO	Zeroize KEK	Command	Status output (non-error message on success)
CO	Zeroize SSH private keys	Command	Status output (non-error message on success)
CO, User	Authenticate operators	Password or certificate	Status output / login success
CO	Firmware load	Command and firmware image	Status output / new firmware loaded and version

The module supports up to 10 concurrent connections. Operators connect to the module via an SSH connection (using the CLI or REST API) of via a TLS connection (using the Web GUI). Each operator authenticates using a username/password or a certificate associated with the correct protocol in order to set up secure communication channels. Each secure session for simultaneous operators is distinguished and kept separate by unique session information, which is provided by the session protocol and protected by the OS.

Each session remains active (logged in) and secured until the operator logs out or is automatically logged out from inactivity (inactivity default is 900 seconds).

4.2 Authentication Methods

The module supports *identity*-based authentication; operators explicitly assume their role based on the authentication credentials used. Each role determines the functionality available to the operator within the module.

Operators authenticate to the module using either:

- a username and password. Password complexity policies can be configured by an operator with the Crypto Officer role and are enforced by the module. All operators are required to follow the password policies.

- certificates associated with the selected protocol. The module supports RSA digital certificate authentication of users during Web GUI/HTTPS (TLS) access.

The strength objectives of the authentication mechanisms are as follows:

- For each attempt to use an authentication mechanism, the probability shall be less than one in 1,000,000 that a random attempt will succeed or a false acceptance will occur.

- For multiple attempts to use an authentication mechanism during a one-minute period, the probability shall be less than one in 100,000 that a random attempt will succeed or a false acceptance will occur.

To meet these objectives, the password policies shall be configured by the Crypto Officer such that all passwords shall require:

- A minimum of 8 total characters
- At least one lowercase letter
- At least one uppercase letter
- At least one digit
- At least one special character (~, `, !, @, #, $, %, ^, &, *, -, _, =, +, {, }, [,], |, \, :, <, >, /, ., ,, " ")

The strength calculations for each of the authentication mechanisms are provided in Table 10 below.

Table 10 – Authentication Mechanism Used by the Module

Authentication Mechanism	Strength
Password	The minimum length of the password is eight characters, with 89 different case-sensitive alphanumeric characters and symbols possible for usage. Adhering to the module password policies described in section 11.2.2, there are (26^1) * (26^1) * (10^1) * (27^1) * (89^4) = 11,451,713,827,320 possible passwords. Therefore, the chance of a random attempt falsely succeeding is 1:11,451,713,827,320, which meets the 1:1,000,000 authentication strength objective. The fastest network connection supported by the module is 1000 Mbps. At most ($1x10^9$ bits/second × 60 seconds) = $6x10^{10}$ = 60,000,000,000 bits of data can be transmitted in one minute. The minimum password is 64 bits (8 bits per character x 8 characters), meaning $9.375x10^8$ passwords can be passed to the module (assuming there is no overhead). This equates to a 1:4,591,650 chance of a random attempt will succeed, or a false acceptance will occur in a one-minute period, which is less than the required probability.
Certificate	Using conservative estimates and equating a 2048-bit RSA key to a 112-bit symmetric key, the probability for a random attempt to succeed is: • =1 per 2^{112} • =1 per 5.19×10^{33} which is a lesser probability than 1 per 1,000,000. Given that there can be 60,000,000,000 bits of data transmitted to the module in one minute and that a certificate contains a 2048-bit RSA key, then at most 60,000,000,000 / 2048 or $2.93x10^7$ certificates can be passed to the module in a one-minute period (assuming there is no overhead), meaning if one key has a 1:$5.19x10^{33}$ chance of succeeding then in a one minute period there is a $2.93x10^7$:$5.19x10^{33}$, or 1:$1.77x10^{26}$ chance of a random attempt succeeding, which is less than the required probability.

4.3 Services

Descriptions of the services available are provided in Table 11 below.

As allowed per section 2.4.C of *FIPS 140-3 Implementation Guidance*, the module provides indicators for the use of Approved services through a combination of an explicit indication (via a global Approved mode indicator) and an implicit indication (via the successful completion of the service).

Please note that the keys and Sensitive Security Parameters (SSPs) listed in the table indicate the access rights required using the following notation:

- G = Generate: The module generates or derives the SSP.
- R = Read: The SSP is read from the module (e.g., the SSP is output).
- W = Write: The SSP is updated, imported, or written to the module.
- E = Execute: The module uses the SSP in performing a cryptographic operation.
- Z = Zeroize: The module zeroizes the SSP.

Table 11 – Approved Services

Service	Description	Approved Security Function(s)	Keys and/or SSPs	Roles	Access Rights to Keys and/or SSPs	Indicator
Perform self-tests on-demand	Perform pre-operational self-tests	None	None	CO	None	Log File
Perform initial network configuration	Set up initial network configuration and licenses	None	None	CO	N/A	Success from CLI
View system information	View system info and statistics; view/end system sessions	None	None	CO	N/A	Console Output
Configure system settings	Configure modes and features, system settings, and cloud parameters	AES (Cert. A3942) HMAC (Cert. A3943) SHS (Cert. A3943)	AES Key KEK Hash DRBG Entropy Hash DRBG Seed Hash DRBG 'V' Value Hash DRBG 'C' Value	CO	AES Key – W KEK – E Hash DRBG Entropy – E Hash DRBG Seed –W/E Hash DRBG 'V' Value –W/E Hash DRBG 'C' Value –W/E	Command Line Interface
Configure HA[49]	Configure HA nodes, route monitors, failover interface set	None	None	CO	N/A	Command Line Interface and Traffic
Manage NTP[50] servers	Add, edit, delete NTP servers; configure NTP parameters and synchronization state	None	None	CO	N/A	Command Line Interface

[49] HA – High Availability
[50] NTP – Network Time Protocol

Service	Description	Approved Security Function(s)	Keys and/or SSPs	Roles	Access Rights to Keys and/or SSPs	Indicator
Configure system profiles	Add, edit, delete system profiles	KDF TLS (Cert. A3942) AES (Cert. A3942) HMAC (Cert. A3942) DRBG (Cert. A3942) SHS (Cert. A3942) MD5 (Allowed for TLS 1.0/1.1)	TLS Extended Master Secret TLS Ticket Encryption Key TLS Ticket Authentication Key CTR DRBG Entropy CTR DRBG Seed CTR DRBG 'V' Value CTR DRBG 'Key' Value KEK	CO	TLS Extended Master Secret –W/E TLS Ticket Encryption Key – R/W TLS Ticket Authentication Key – R/W CTR DRBG Entropy – E CTR DRBG Seed –W/E CTR DRBG 'V' Value –W/E CTR DRBG 'Key' Value –W/E KEK – E	Command Line Interface
Manage users	Add, edit delete users, groups, and command policies; view user/group partition bindings	None	None	CO	N/A	Command Line Interface
Zeroize	Reboot the module (same as power cycle)	None	PEM Passphrase PEM Key AES GCM Key AES GCM IV DH Public Key DH Private Key ECDH Public Key ECDH Private Key RSA Public Key RSA Private Key SSH Shared Secret SSH Session Key SSH Authentication Key IKE/IPsec Shared Secret IKE/IPsec Session Key IKE/IPsec Authentication Key TLS Pre-Master Secret TLS Extended Master Secret TLS Session Key TLS Authentication Key TLS Ticket Encryption Key TLS Ticket Authentication Key Hash DRBG Entropy Hash DRBG Seed Hash DRBG “V” Value” Hash DRBG “C” Value CTR DRBG Entropy CTR DRBG Seed CTR DRBG “V” Value CTR DRBG “Key” Value SNMPv3 Private Key SNMPv3 Authentication Key	CO	PEM Passphrase – Z PEM Key – Z AES GCM Key – Z AES GCM IV – Z DH Public Key – Z DH Private Key – Z ECDH Public Key – Z ECDH Private Key – Z RSA Public Key – Z RSA Private Key – Z SSH Shared Secret – Z SSH Session Key – Z SSH Authentication Key – Z IKE/IPsec Shared Secret – Z IKE/IPsec Session Key – Z IKE/IPsec Authentication Key – Z TLS Pre-Master Secret – Z TLS Extended Master Secret – Z TLS Session Key – Z TLS Authentication Key – Z TLS Ticket Encryption Key – Z TLS Ticket Authentication Key – Z Hash DRBG Entropy – Z Hash DRBG Seed – Z Hash DRBG “V” Value – Z Hash DRBG “C” Value – Z CTR DRBG Entropy – Z CTR DRBG Seed – Z CTR DRBG “V” Value – Z CTR DRBG “Key” Value – Z SNMPv3 Private Key – Z SNMPv3 Authentication Key – Z	N/A
Configure system auditing	Add, edit, delete syslog/nslog auditing policies and servers; bind classic/advanced global policies	None	None	CO	N/A	Command Line Interface
View audit logs	View authentication, system, and event logs	None	None	CO	N/A	N/A (Audit Logs)
Configure network settings	Configure network routing protocols	AES (Cert. A3942)	ZebOS Router Password KEK	CO	ZebOS Router Password – W KEK – E	Command Line Interface
Exchange routing information	Exchange routing update information using ZebOS, authenticate source of packets	AES (Cert. A3942)	ZebOS Router Password KEK	CO	ZebOS Router Password – E KEK – E	Show Command O/P and Traffic

Service	Description	Approved Security Function(s)	Keys and/or SSPs	Roles	Access Rights to Keys and/or SSPs	Indicator
Configure SSH	Configure SSH authentication settings; generate SSH keys	CKG (Vendor Affirmed) DRBG (Cert. A3942) ECDSA (Cert. A3942) RSA (Cert. A3942)	SSH Private Key SSH Public Key CTR DRBG Entropy CTR DRBG Seed CTR DRBG 'V' Value CTR DRBG 'Key' Value	CO	SSH Private Key – W/E SSH Public Key – W CTR DRBG Entropy –E CTR DRBG Seed –W/E CTR DRBG 'V' Value –W/E CTR DRBG 'Key' Value –W/E	Command Line Interface
Establish SSH sessions	Establish an SSH session	AES (Cert. A3942) CKG (Vendor Affirmed) DRBG (Cert. A3942) ECDSA (Cert. A3942) HMAC (Cert. A3942) KAS-ECC-SSC (Cert. A3942) KAS-FFC-SSC (Cert. A3942) KTS-IFC (Cert. A3942) RSA (Cert. A3942) Safe Primes Key Generation (Cert. A3942) SHS (Cert. A3942) SSH KDF (Cert. A3942)	SSH Public Key DH Private Key Component DH Public Key Component ECDH Private Key Component ECDH Public Key Component SSH Shared Secret SSH Session Key SSH Authentication Key CTR DRBG Entropy CTR DRBG Seed CTR DRBG 'V' Value CTR DRBG 'Key' Value	CO User	SSH Public Key – R/E DH Private Key Component – W/E DH Public Key Component – R/E ECDH Private Key Component – W/E ECDH Public Key Component – R/E SSH Shared Secret – W/E SSH Session Key – W/E SSH Authentication Key – W/E CTR DRBG Entropy – E CTR DRBG Seed –W/E CTR DRBG 'V' Value –W/E CTR DRBG 'Key' Value –W/E	Traffic
Configure CloudBridge	Configure IPsec profile; configure CloudBridge Connector settings, network bridges, and IP tunnels; view IP tunnel details	AES (Cert. A3942) KAS-FFC-SSC (Cert. A3942) Safe Primes Key Generation (Cert. A3942)	IKE/IPsec PSK[51] KEK	CO	IKE/IPsec PSK – W KEK – E	Command Line Interface
Configure clustering	Configure an appliance to either be the cluster coordinator or a node in the cluster	None	Cluster Password	CO	Cluster Password – W	Command Line Interface
Establish IPsec session	Establish an IPsec Session	KAS-FFC-SSC (Cert. A3942) AES (Cert. A3942) CKG (Vendor Affirmed) DRBG (Cert. A3942) HMAC (Cert. A3942) KDE IKEv1 (Cert. A3942) KDE IKEv2 (Cert. A3942) Safe Primes Key Generation (Cert. A3942) SHS (Cert. A3942)	DH Private Key Component DH Public Key Component IKE/IPsec Shared Secret IKE/IPsec PSK KEK IKE/IPsec Session Key IKE/IPsec Authentication Key CTR DRBG Entropy CTR DRBG Seed CTR DRBG 'V' Value CTR DRBG 'Key' Value	CO User	DH Private Key Component – W/E DH Public Key Component – R/E IKE/IPsec Shared Secret – W/XE IKE/IPsec PSK – E KEK – E IKE/IPsec Session Key – W/E IKE/IPsec Authentication Key – W/E CTR DRBG Entropy – E CTR DRBG Seed –W/E CTR DRBG 'V' Value –W/E CTR DRBG 'Key' Value –W/E	Traffic
Backup and restore	Backup/import system configuration files; download and delete backup files; restore	None	None	CO	N/A	N/A
Manage encryption keys	Add, edit, delete encryption keys	AES (Cert. A3943) DRBG (Cert. A3943)	AES Key KEK Hash DRBG Entropy Hash DRBG Seed Hash DRBG 'V' Value Hash DRBG 'C' Value	CO	AES Key – R/W KEK – E Hash DRBG Entropy – E Hash DRBG Seed –W/E Hash DRBG 'V' Value –W/E Hash DRBG 'C' Value –W/E	Command Line Interface
Manage HMAC keys	Add, edit, delete HMAC keys	AES (Cert. A3943) DRBG (Cert. A3943) HMAC (Cert. A3943) SHS (Cert. A3943)	HMAC Key KEK Hash DRBG Entropy Hash DRBG Seed Hash DRBG 'V' Value Hash DRBG 'C' Value	CO	HMAC Key – R/W KEK – E Hash DRBG Entropy – E Hash DRBG Seed –W/E Hash DRBG 'V' Value –W/E Hash DRBG 'C' Value –W/E	Command Line Interface

[51] PSK – Pre-shared Key

Service	Description	Approved Security Function(s)	Keys and/or SSPs	Roles	Access Rights to Keys and/or SSPs	Indicator
Configure traffic management	Configure TLS; Configure load balancing, priority load balancing, content switching, and cache redirection settings, DNS[52], GSLB[53], Subscriber, service chaining, and user protocol settings	AES (Certs. A3942, A3943) DRBG (Certs. A3942, A3943) ECDSA (Certs. A3942, A3943) PBKDF2 (Cert. A3942) RSA (Certs. A3942, A3943)	CA[54] Public Key TLS Private Key TLS Public Key Private DNS KSK[55] Public DNS KSK Private DNS ZSK[56] Public DNS ZSK SSH Private Key SSH Public Key PEM Passphrase PEM Key KEK CTR DRBG Entropy CTR DRBG Seed CTR DRBG 'V' Value CTR DRBG 'Key' Value Hash DRBG Entropy Hash DRBG Seed Hash DRBG 'V' Value Hash DRBG 'C' Value	CO	CA Public Key – R/W/E TLS Private Key – R/W/E TLS Public Key – R/W Private DNS KSK – R/W/E Public DNS KSK – R/W Private DNS ZSK – R/W/E Public DNS ZSK – R/W SSH Private Key – R/W/E SSH Public Key – R/W/E PEM Passphrase – R/W/E PEM Key – W/E KEK – E CTR DRBG Entropy – E CTR DRBG Seed – W/E CTR DRBG 'V' Value –W/E CTR DRBG 'Key' Value –W/E Hash DRBG Entropy – E Hash DRBG Seed –W/E Hash DRBG 'V' Value –W/E Hash DRBG 'C' Value –W/E	Command Line Interface
Establish TLS session	Establish a web session using TLS protocol	AES (Certs. A3942, A3943, A3944) CKG (Vendor Affirmed) DRBG (Certs. A3942, A3943, and A3944) ECDSA (Certs. A3942, A3943, and A3944) HMAC (Certs. A3942, A3943, and A3944) KAS-ECC-SSC (Certs. A3942, A3943, A3944) KAS-FFC-SSC (Cert. A3942) KDF TLS (Certs. A3942, A3943, A3944) KTS-IFC (Certs. A3942 and A3943) PBKDF2 (Cert. A3942) RSA (Certs. A3942, A3943, A3944) Safe Primes Key Generation (Cert. A3942) SHS (Certs. A3942, A3943, and A3944) TLS v1.2 KDF RFC7267 (Certs. A3942, A3943, A3944) TLS v1.3 KDF (Cert. A3943) MD5 (Allowed for TLS 1.0/1.1)	TLS Private Key TLS Public Key DH Private Key Component DH Public Key Component ECDH Private Key Component ECDH Public Key Component RSA Private Key Component RSA Public Key Component TLS Premaster Secret TLS Extended Master Secret TLS Session Key TLS Authentication Key AES GCM IV[57] AES GCM Key PEM Passphrase PEM Key KEK CTR DRBG Entropy CTR DRBG Seed CTR DRBG 'V' Value CTR DRBG 'Key' Value Hash DRBG Entropy Hash DRBG Seed Hash DRBG 'V' Value Hash DRBG 'C' Value	CO User	TLS Private Key –E TLS Public Key – R/EDH Private Key Component – W/E DH Public Key Component – R/E ECDH Private Key Component – W/E ECDH Public Key Component – R/E RSA Private Key Component – W/E RSA Public Key Component – R/E TLS Premaster Secret – R/W/E TLS Extended Master Secret – W/E TLS Session Key – W/E TLS Authentication Key – W/E AES GCM IV – W/E AES GCM Key – W/E PEM Passphrase –E PEM Key – W/E KEK – E CTR DRBG Entropy – E CTR DRBG Seed –W/E CTR DRBG 'V' Value –W/E CTR DRBG 'Key' Value –W/E Hash DRBG Entropy – E Hash DRBG Seed – W/E Hash DRBG 'V' Value – W/E Hash DRBG 'C' Value – W/E	Traffic
Resume TLS session	Resume a web session using TLS protocol	AES (Cert. A3943, A3944) DRBG (Cert. A3943, A3944) ECDSA (Cert. A3943, A3944) HMAC (Cert. A3943, A3944) KTS-IFC (Cert. A3943) RSA (Cert. A3943, A3944) SHS (Cert. A3943, A3944) MD5 (Allowed for TLS 1.0/1.1)	TLS Ticket Encryption Key TLS Ticket Authentication Key TLS Session Key TLS Authentication Key AES GCM IV AES GCM Key KEK Hash DRBG Entropy Hash DRBG Seed Hash DRBG 'V' Value Hash DRBG 'C' Value	CO User	TLS Ticket Encryption Key –W/E TLS Ticket Authentication Key –W/E TLS Session Key –E TLS Authentication Key –E AES GCM IV – W/E AES GCM Key – W/E KEK – E Hash DRBG Entropy –E Hash DRBG Seed –W/E Hash DRBG 'V' Value –W/E Hash DRBG 'C' Value –W/E	Traffic
Apply data policies	Apply data policies to user data in transit (according to configuration)	AES (Certs. A3942, A3943) HMAC (Certs. A3942, A3943) SHS (Certs. A3942, A3943)	AES Key HMAC Key KEK	CO	AES Key – E HMAC Key – E KEK – E	Traffic

[52] DNS – Domain Name System
[53] GSLB – Global Server Load Balancing
[54] CA – Certificate Authority
[55] KSK – Key Signing Key
[56] ZSK – Zone Signing Key
[57] IV – Initialization Vector

Service	Description	Approved Security Function(s)	Keys and/or SSPs	Roles	Access Rights to Keys and/or SSPs	Indicator
Configure security	Configure DNS security profiles, application firewall profiles and policies, reputation settings, protection features, and content inspection policies	None	None	CO	N/A	Command Line Interface
Configure Gateway	Configure Gateway global settings, virtual servers, portal themes, AAA[58] groups and users, policies, and resources	AES (Cert. A3942 KBKDF (Cert. A3943)	RDP[59] PSK KEK	CO	RDP PSK – W KEK – E	Command Line Interface
Establish Gateway connection	Establish Gateway connection based on global settings	AES (Cert. A3943)	RDP PSK RDP Session Key KEK	CO	RDP PSK – E RDP Session Key – E KEK – E	Traffic
Configure external servers for system, AAA, and Gateway authentication	Configure LDAP[60], Oauth, OpenID, DFA[61], and SAML[62] servers to be used in system, AAA, or Gateway authentication	AES (Cert. A3942) RSA (Cert. A3942)	LDAP Admin Password Oauth Client Secret DFA Shared Secret KEK	CO	LDAP Admin Password – W Oauth Client Secret – R/W DFA Shared Secret – R/W KEK – E	Command Line Interface
Radius Over TLS	Establish a TLS session with radius server	AES (Certs. A3942, A3943) CKG (Vendor Affirmed) DRBG (Certs. A3942, A3943) ECDSA (Certs. A3942, A3943) HMAC (Certs. A3942, A3943) KAS-ECC-SSC (Certs. A3942, A3943) KDF TLS (Certs. A3942, A3943, A3944) KAS-FFC-SSC (Cert. A3942) KTS-IFC (Certs. A3942, A3943) PBKDF2 (Cert. A3942) RSA (Certs. A3942, A3943) Safe Primes Key Generation (Cert. A3942) SHS (Certs. A3942, A3943) TLS v1.2 KDF RFC7267 (Certs. A3942, A3943, A3944) TLS v1.3 KDF (Cert. A3943) MD5 (Allowed for TLS 1.0/1.1)	TLS Private Key TLS Public Key DH Private Key Component DH Public Key Component ECDH Private Key Component ECDH Public Key Component RSA Private Key Component RSA Public Key Component TLS Premaster Secret TLS Extended Master Secret TLS Session Key TLS Authentication Key AES GCM IV[63] AES GCM Key PEM Passphrase PEM Key KEK CTR DRBG Entropy CTR DRBG Seed CTR DRBG 'V' Value CTR DRBG 'Key' Value Hash DRBG Entropy Hash DRBG Seed Hash DRBG 'V' Value Hash DRBG 'C' Value	CO User	TLS Private Key – E TLS Public Key – R/E DH Private Key Component – W/E DH Public Key Component – R/E ECDH Private Key Component – W/E ECDH Public Key Component – R/E RSA Private Key Component – W/E RSA Public Key Component – R/E TLS Premaster Secret –W/E TLS Extended Master Secret – W/E TLS Session Key – W/E TLS Authentication Key – W/E AES GCM IV – W/E AES GCM Key – W/E PEM Passphrase – R/E PEM Key – W/E KEK – E CTR DRBG Entropy – E CTR DRBG Seed – W/E CTR DRBG 'V' Value – W/E CTR DRBG 'Key' Value – W/E Hash DRBG Entropy – E Hash DRBG Seed – W/E Hash DRBG 'V' Value – W/E Hash DRBG 'C' Value – W/E	Traffic

[58] AAA – Authentication, Authorization, Accounting
[59] RDP – Remote Desktop Protocol
[60] LDAP – Lightweight Directory Access Protocol
[61] DFA – Delegated Form Authentication
[62] SAML – Security Assertion Markup Language
[63] IV – Initialization Vector

Service	Description	Approved Security Function(s)	Keys and/or SSPs	Roles	Access Rights to Keys and/or SSPs	Indicator
Configure SNMPv3	Configure SNMP communities, traps, managers, views, groups, users, alarms, and engine ID[64]; view SNMP OIDs[65]	AES (Cert. A3942) HMAC (Cert. A3942) SHS (Cert. A3942)	SNMPv3 Authentication Passphrase SNMPv3 Privacy Passphrase KEK	CO	SNMPv3 Authentication Passphrase – W SNMPv3 Privacy Passphrase – W KEK – E	Command Line Interface
SNMPv3 traps	Provides system condition information	AES (Cert. A3942) HMAC (Cert. A3942) SHS (Cert. A3942)	SNMPv3 Authentication Passphrase SNMPv3 Privacy Passphrase SNMPv3 Privacy Key SNMPv3 Authentication Key	CO	SNMPv3 Authentication Passphrase – E SNMPv3 Privacy Passphrase – E SNMPv3 Privacy Key – W/E SNMPv3 Authentication Key – W/E	Log files
Show status	Show the system status	None	None	CO	N/A	N/A
Zeroize KEK	Zeroize KEK	None	KEK KEK Fragment 1 KEK Fragment 2	CO	KEK – Z KEK Fragment 1 – Z KEK Fragment 2 – Z	API return value
Zeroize SSH private keys	Zeroize SSH private keys	None	SSH Private Key	CO	SSH Private Key – Z	API return value
Authenticate operators	Used for operator logins to the module	AES (Cert. A3942) ECDSA (Cert. A3942) RSA (Cert. A3942)	Operator Password LDAP Admin Password SSH Public Key Oauth Client Secret DFA Shared Secret DFA Session Key TLS Public Key AES Key AES GCM Key AES GCM IV KEK	None	Operator Password - W LDAP Admin Password – W/E SSH Public Key – E Oauth Client Secret – E DFA Shared Secret – E DFA Session Key – E TLS Public Key – E AES Key – E AES GCM Key – E AES GCM IV – E KEK – E	Traffic
Firmware Load	Update the module's firmware to a new version[66]	RSA (Cert. A3942)	Firmware Load Integrity Key	CO	Firmware Load Integrity Key - R	Log files

The module does not provide any non-Approved services.

[64] ID – Identifier
[65] OID – Object Identifier
[66] The operator shall be aware the new firmware version may not be a FIPS validated version.

5. Software/Firmware Security

All firmware within the cryptographic boundary is verified using an approved integrity technique implemented within the cryptographic module itself. The module implements a 2048-bit RSA digital signature verification with a SHA-512 hash to ensure the integrity of its firmware components.

The module's pre-operational integrity check is performed automatically at module power-up. This integrity check can also be performed on demand by the module operator by performing a reboot.

6. Operational Environment

The module employs a limited operational environment. The module does not provide access to a general-purpose operating system (OS). All services provided by the module are provided by the module's firmware and external interfaces. All firmware upgrades are digitally signed, and a conditional self-test (RSA signature verification) is performed with each upgrade. Therefore, per *ISO/IEC 19790:2021* section 7.6.1, requirements for this section are not applicable.

7. Physical Security

As a multi-chip standalone hardware module, the module includes an enclosure composed of hard, production-grade, metal components necessary to meet FIPS 140-3 level 2 physical security requirements. The module enclosure completely encloses all of its internal components, and all integrated circuits are coated with commercial standard passivation.

The MPX enclosure has removable front and back covers. Each cover is secured with screws and serialized tamper-evident seals. Tamper-evident seals are applied at the factory to the modules to protect against unauthorized access to the module. When the module is received, the operator must confirm placement of all tamper-evident seals.

Table 12 – Physical Security Inspection Guidelines

Physical Security Mechanism	Recommended Frequency of Inspection/Test	Inspection/Test Details
Tamper-evident seal	Every 3 months	Verify that each seal is in place and untampered

If there is an attempt to remove a cover, evidence of the attempt will be observable via the residue remaining from the torn label.

For additional guidance regarding the inspection of the seals upon receipt, please refer to section 11.1.1 of this document.

8. Non-Invasive Security

This section is not applicable. There are currently no approved non-invasive mitigation techniques references in *ISO/IEC 19790:2021* Annex F.

9. Sensitive Security Parameter Management

9.1 Keys and SSPs

The module supports the keys and other SSPs listed in Table 13 and Table 14 below.

Table 13 – SSPs

Key/SSP Name/Type	Strength	Security Function and Cert #	Generation	Import / Export	Establishment	Storage	Zeroization	Use & Related Keys
KEK Fragment 1 (CSP)	2048 bits	HMAC (Cert. A3942)	Generated internally via Approved DRBG	Never imported; never exported	-	Plaintext in non-volatile memory	CLI command	Hashed in combination with KEK Fragment 2 to derive KEK
KEK Fragment 2 (CSP)	2048 bits	HMAC (Cert. A3942)	Generated internally via Approved DRBG	Never imported; never exported	-	Plaintext in non-volatile memory	CLI command	Hashed in combination with KEK Fragment 1 to derive KEK
KEK (AES key) (CSP)	256 bits	AES (Cert. A3942)	-	Never imported; never exported	Derived internally using combined hashes of KEK Fragment 1 and KEK Fragment 2	Plaintext in volatile memory	Reboot; remove power	Encryption and decryption of passwords and passphrases
PEM Key (AES key) (CSP)	256 bits	PBKDF2 (Cert. A3942)	Generated internally via PBKDF	Never imported; never exported	Derived internally via PBKDF	Encrypted on disk (via KEK)	CLI command	Encryption and decryption of asymmetric private keys
AES key (CSP)	Between 128 and 256 bits	AES(Cert. A3943)	Generated internally via Approved DRBG	Imported in plaintext form via local console or in encrypted form via TLS or SSH session / exits the module in encrypted form as part of config backup file	-	Encrypted on disk (via KEK)	N/A[67]	Encryption and decryption
AES GCM key (CSP)	256 bits	AES (GCM mode) (Cert. A3943)	Generated internally via Approved DRBG	Never exits the module	-	Plaintext in volatile memory	Reboot; remove power	Encryption and decryption
HMAC Key (CSP)	Between 160 and 512 bits	HMAC (Cert. A3943)	Generated internally via Approved DRBG	Imported in plaintext form via local console or in encrypted form via TLS or SSH session / exits the module in encrypted form as part of config backup file	-	Encrypted on disk (via KEK)	N/A[67]	Message authentication with SHS

[67] Zeroization of KEK renders SSP permanently unrecoverable

Key/SSP Name/Type	Strength	Security Function and Cert #	Generation	Import / Export	Establishment	Storage	Zeroization	Use & Related Keys
CA Public Key (PSP)	[RSA public key] Between 80 and 150 bits [ECDSA public key] Between 112 and 256 bits	RSA (Cert. A3942) KTS-IFC (Cert. A3942)	-	Imported in plaintext form via local console or in encrypted form via TLS or SSH session / exits the module in plaintext form	-	Plaintext on disk	No[68]	TLS certificate authentication **1024-bit RSA public keys are used for signature verification only**
DH Private Key (CSP)	[for SSH sessions] Between 112 and 201 bits [for TLS sessions] Between 112 and 150 bits [for IKE sessions] 112 bits	KAS-FFC-SSC (Cert. A3943)	Generated internally via Approved DRBG	Never imported; never exported	-	Plaintext in volatile memory	Reboot; remove power; session termination	Generation of SSH, TLS, and IKE shared secrets
DH Public Key (PSP)	[for SSH sessions] Between 112 and 201 bits [for TLS sessions] Between 112 and 150 bits [for IKE sessions] 112 bits	KAS-FFC-SSC (Cert. A3943)	[for the module] Generated internally via Approved DRBG	[for the module] Exits the module in plaintext form [for a peer] Input in plaintext form / Never exits the module	-	Plaintext in volatile memory	Reboot; remove power; session termination	Generation of SSH, TLS, and IKE shared secrets
ECDH Private Key (CSP)	Between 112 and 256 bits	KAS-ECC-SSC (Certs. A3942, A3943)	Generated internally via Approved DRBG	Never imported; never exported	-	Plaintext in volatile memory	Reboot; remove power; session termination	Generation of SSH and TLS shared secrets
ECDH Public Key (PSP)	Between 112 and 256 bits	KAS-ECC-SSC (Certs. A3942, A3943, A3944)	[for the module] Generated internally via Approved DRBG	[for the module] Exits the module in plaintext form [for a peer] Input in plaintext form / Never exits the module	-	Plaintext in volatile memory	Reboot; remove power; session termination	Generation of SSH and TLS shared secrets
RSA Private Key (CSP)	112 or 128 bits	RSA (Cert. A3942)	Generated internally via Approved DRBG	Never imported; never exported	-	Encrypted on disk (via KEK)	N/A[67]	Generation of TLS shared secrets
RSA Public Key (PSP)	112 or 128 bits	RSA (Cert. A3942) KTS-IFC (Cert. A3942)	[for the module] Generated internally via Approved DRBG	[for the module] Exits the module in plaintext form [for a peer] Input in plaintext form / Never exits the module	-	Plaintext in volatile memory	No[68]	Generation of TLS shared secrets

[68] NetScaler MPX detects modification of Public Security Parameters listed in this table.

Key/SSP Name/Type	Strength	Security Function and Cert #	Generation	Import / Export	Establishment	Storage	Zeroization	Use & Related Keys
SSH Private Key (CSP)	[RSA private key] 112 or 128 bits [ECDSA private key] Between 112 and 256 bits	RSA (Cert. A3942) ECDSA (Cert. A3942)	Generated internally via Approved DRBG	Exits the module in encrypted form as part of config backup file	-	Plaintext on disk	CLI command	Authentication during SSH session negotiation; RBA[69] Authentication for LDAP; GSLB configuration sync
SSH Public Key (PSP)	[RSA public key] 112 or 128 bits [ECDSA public key] Between 112 and 256 bits	RSA (Cert. A3942) ECDSA (Cert. A3942)	Generated internally via Approved DRBG	Exits the module in encrypted form as part of config backup file	-	Plaintext in volatile memory	No[68]	Authentication during SSH session negotiation; RBA Authentication for LDAP; GSLB configuration sync
SSH Session Key AES key (CBC and CTR mode) (CSP)	Between 128 and 256 bits	AES (CBC, CTR modes) (Cert. A3942)	-	Never imported; never exported	Derived internally via SSH KDF	Plaintext in volatile memory	Reboot; remove power; session termination	Encryption and decryption of SSH session packets
SSH Authentication Key HMAC key (CSP)	Between 160 and 512 bits	HMAC (Cert. A3942)	-	Never imported; never exported	Derived internally via SSH KDF	Plaintext in volatile memory	Reboot; remove power; session termination	Authentication of SSH session packets
IKE/IPsec Pre-shared key (PSK) (CSP)	-	-	-	input in plaintext form via local console / Exits the module in encrypted form as part of config backup file	Derived internally via shared secret computation	Plaintext in volatile memory	Reboot; remove power; session termination	Authentication during IKE/IPsec session negotiation [IKEv1 Only] Derivation of the IKE/IPsec Session Keys and IKE/IPsec Authentication Keys
IKE/IPsec Session Key (AES key) (CSP)	Between 128 and 256 bits	AES (Cert. A3942)	Generated internally via IKE KDF	Never imported; never exported	-	Plaintext in volatile memory	Reboot; remove power; session termination	Encryption and decryption of IKE/IPsec session packets
IKE/IPsec Authentication Key (HMAC key) (CSP)	Between 160 and 512 bits	HMAC (Cert. A3943)	Derived internally via IKE KDF	Never imported; never exported	Derived internally via IKE KDF	Plaintext in volatile memory	Reboot; remove power; session termination	Authentication of IKE/IPsec session packets
RDP Session Key (CSP)	256 bits	AES (Cert. A3942)	-	Never exits the module	Key Derivation	Plaintext in volatile memory	Reboot; remove power; session termination	Encryption and decryption of RDP user and target information
DFA Session Key (CSP)	256 bits	AES (Cert. A3943)	-	Never exits the module	Key Derivation	Plaintext in volatile memory	Reboot; remove power; session termination	DFA authentication to the module

[69] RBA – Role-based Authentication

Key/SSP Name/Type	Strength	Security Function and Cert #	Generation	Import / Export	Establishment	Storage	Zeroization	Use & Related Keys
TLS Private Key (CSP)	[RSA private key] Between 112 and 150 bits [ECDSA private key] Between 112 and 256 bits	RSA (Cert. A3942) ECDSA (Cert. A3942)	Generated internally via Approved DRBG	Imported in plaintext form via local console or in encrypted form via TLS or SSH session / Exits the module in encrypted form as part of config backup file		Encrypted on disk (via PEM key)	N/A[67]	TLS authentication; SAML authentication (RSA only); OpenID authentication (RSA only)
TLS Session Key (CSP)	[AES key] 128 or 256 bits [AES GCM key] 128 or 256 bits	AES (Certs. A3942, A3943) AES (GCM mode) (Certs. A3942, A3943)	-	Never imported; never exported	Derived internally using the TLS Pre-Master Secret via TLS KDF	Plaintext in volatile memory	Reboot; remove power; session termination	Encryption and decryption of TLS session packets
TLS Authentication Key (HMAC key) (CSP)	Between 160 and 384 bits	HMAC (Certs. A3942, A3943)	-	Never imported; never exported	Derived internally using the TLS Pre-Master Secret via TLS KDF	Plaintext in volatile memory	Reboot; remove power; session termination	Authentication of TLS session packets
TLS Ticket Encryption Key (AES key) (CSP)	128 bits	AES (Cert. A3943)	Generated internally via Approved DRBG	Imported in encrypted form via TLS session / Never exits the module	-	Plaintext in volatile memory	Reboot; remove power; session termination	Encryption and decryption of TLS session tickets
TLS Ticket Authentication Key (HMAC key) (CSP)	256 bits	HMAC (Certs. A3942, A3943)	Generated internally via Approved DRBG	Imported in encrypted form via TLS session / Never exits the module	-	Plaintext in volatile memory	Reboot; remove power; session termination	Computes the digest of TLS session tickets
SNMPv3 Privacy Key (AES key) (CSP)	128 bits	AES (Cert. A3942)	-	Never imported; never exported	Derived internally via SNMP KDF	Plaintext in volatile memory	Reboot; remove power; session termination	Encryption and decryption of SNMPv3 packets
SNMPv3 Authentication Key (HMAC key) (CSP)	160 bits	HMAC (Cert. A3942)	-	Never imported; never exported	Derived internally via SNMP KDF	Plaintext in volatile memory	Reboot; remove power	Authentication of SNMPv3 packets
Public DNS KSK (RSA public key) (PSP)	Between 112 and 150 bits	RSA (Cert. A3942)	Generated internally via Approved DRBG	Imported in encrypted form via SSH session / Exits the module in plaintext form as part of config backup file	-	Plaintext on disk	No[68]	Public DNS ZSK authentication
Private DNS KSK (RSA private key) (CSP)	Between 112 and 150 bits	RSA (Cert. A3942)	Generated internally via Approved DRBG	Imported in encrypted form via SSH session / Exits the module in encrypted form as part of config backup file	-	Encrypted on disk (via PEM key)	N/A[67]	Public DNS ZSK signature generation
Public DNS ZSK (RSA public key) (PSP)	Between 112 and 150 bits	RSA (Cert. A3942)	Generated internally via Approved DRBG	Imported in encrypted form via SSH session / Exits the module in plaintext form as part of config backup file	-	Plaintext on disk	No[68]	DNS zone authentication

Key/SSP Name/Type	Strength	Security Function and Cert #	Generation	Import / Export	Establishment	Storage	Zeroization	Use & Related Keys
Private DNS ZSK (RSA private key) (CSP)	Between 112 and 150 bits	RSA (Cert. A3942)	Generated internally via Approved DRBG	Imported in encrypted form via SSH session / Exits the module in encrypted form as part of config backup file	-	Encrypted on disk (via PEM key)	N/A[67]	DNS zone signature generation

Keys derived from the PBKDF function are only used for storage applications.

Table 14 – Other SSPs

Key/SSP Name/Type	Strength	Security Function and Cert. Number	Generation	Import/Export	Establishment	Storage	Zeroization[70]	Use &Related Keys
PEM Passphrase (Alphanumeric string) (CSP)	-	-	-	Input in plaintext form via local console / Exits the module in encrypted form as part of config backup file	-	Plaintext in volatile memory or encrypted on disk (via KEK)	[for plaintext] Reboot; remove power	Derivation of PEM Key
AES GCM IV (96 and 128-bit IV) (CSP)	-	AES (GCM mode) (Cert. A3942)	Generated internally deterministically [71]	Never exits the module	-	Plaintext in volatile memory	Reboot; remove power	IV for AES GCM
SSH Shared Secret (CSP)	-	-	-	Never exits the module	Derived internally via SSH KDF	Plaintext in volatile memory	Reboot; remove power; session termination	Derivation of the SSH Session Key and SSH Authentication Key
IKE/IPsec Shared Secret (CSP)	-	-	-	Never exits the module	-	Plaintext in volatile memory	Reboot; remove power; session termination	Derivation of the IKE/IPsec Session Keys and IKE/IPsec Authentication Keys
TLS Pre-Master Secret (CSP)	-	KAS-ECC-SSC (Certs. A3942, A3943, A3944) KAS-FFC-SSC (Cert. A3943)	[for RSA cipher suites and module acting as client] Generated internally via Approved DRBG	[for RSA cipher suites and module acting as server] Imported in encrypted form via RSA key transport / Never exits the module [for RSA cipher suites and module acting as client] Exits the module in encrypted form via RSA key transport [for DH/ECDH cipher suites] Never exits the module	[for DH/ECDH cipher suites] Derived internally via DH/ECDH shared secret computation	Plaintext in volatile memory	Reboot; remove power; completion of TLS Session Key and TLS Authentication Key derivation	Derivation of the TLS Extended Master Secret

[70] The indicators provided by zeroization methods specified in this column are implicit as the normal, non-error, status output of the function performing zeroization.

[71] In compliance with TLS 1.2 GCM Cipher Suites for TLS and Section 8.2.1 of NIST SP 800-38D

Key/SSP Name/Type	Strength	Security Function and Cert. Number	Generation	Import/Export	Establishment	Storage	Zeroization[70]	Use &Related Keys
TLS Extended Master Secret (CSP)	-	TLS KDF (Certs. A3942, A3943)	-	Never exits the module	Derived internally via TLS KDF	Plaintext in volatile memory	Reboot; remove power; session termination	Derivation of the TLS Session Key and TLS Authentication Key
Hash DRBG Entropy (CSP)	-	DRBG (Cert. A3943)	-	Never exits the module	-	Plaintext in volatile memory	Reboot; remove power	Entropy input for Hash DRBG
Hash DRBG Seed (CSP)	-	DRBG (Cert. A3943)	Generated internally via Approved DRBG	Never exits the module	-	Plaintext in volatile memory	Reboot; remove power	Seed material for Hash DRBG
Hash DRBG 'V' Value (Internal state value) (CSP)	-	DRBG (Cert. A3943)	Generated internally via Approved DRBG	Never exits the module	-	Plaintext in volatile memory	Reboot; remove power	Internal state value used with Hash DRBG
Hash DRBG 'C' Value (Internal state value) (CSP)	-	DRBG (Cert. A3943)	Generated internally via Approved DRBG	Never exits the module	-	Plaintext in volatile memory	Reboot; remove power	Internal state value used with Hash DRBG
CTR DRBG Entropy (CSP)	-	DRBG (Cert. A3942)	Generated internally via CPU Jitter Entropy Source	Never exits the module	-	Plaintext in volatile memory	Reboot; remove power	Entropy input for CTR DRBG
CTR DRBG Seed (CSP)	-	DRBG (Cert. A3942)	Generated internally via Approved DRBG	Never exits the module	-	Plaintext in volatile memory	Reboot; remove power	Seed material for CTR DRBG
CTR DRBG 'V' Value (CSP)	-	DRBG (Cert. A3942)	Generated internally via Approved DRBG	Never exits the module	-	Plaintext in volatile memory	Reboot; remove power	Internal state value used with CTR DRBG
CTR DRBG 'Key' Value (AES key) (CSP)	-	DRBG (Cert. A3942)	Generated internally via Approved DRBG	Never exits the module	-	Plaintext in volatile memory	Reboot; remove power	Internal state value used with CTR DRBG
SNMPv3 Privacy Passphrase (Alphanumeric string) (CSP)	-	-	-	Input in plaintext form via local console or in encrypted form via TLS or SSH session / Exits the module in encrypted form as part of config backup file	-	Encrypted on disk (via KEK)	N/A[67]	Derivation of the SNMPv3 Privacy Key
SNMPv3 Authentication Passphrase (Alphanumeric string) (CSP)	-	-	-	Input in plaintext form via local console or in encrypted form via TLS or SSH session / Exits the module in encrypted form as part of config backup file	-	Encrypted on disk (via KEK)	N/A[67]	Derivation of the SNMPv3 Authentication Key
LDAP Admin Password (Alphanumeric string) (CSP)	-	-	-	Input in plaintext form via local console or in encrypted form via TLS or SSH session / Exits the module in encrypted form as part of config backup file	-	Encrypted on disk (via KEK)	N/A[67]	Used to bind to the LDAP server

Key/SSP Name/Type	Strength	Security Function and Cert. Number	Generation	Import/Export	Establishment	Storage	Zeroization[70]	Use &Related Keys
RDP PSK (Shared secret) (CSP)	-	KBKDF (Cert. A3943)	-	Input in plaintext form via local console or in encrypted form via TLS or SSH session / Exits the module in encrypted form as part of config backup file	-	Encrypted on disk (via KEK)	N/A[67]	Used as input to derive RDP Session Key
Oauth Client Secret (Shared secret) (CSP)	-	-	-	Input in plaintext form via local console or in encrypted form via TLS or SSH session / Exits the module in encrypted form as part of config backup file	-	Encrypted on disk (via KEK)	N/A[67]	Oauth and Oauth IDP[72] authentication to the module
DFA Shared Secret (CSP)	-	KBKDF (Cert. A3943)	-	Input in plaintext form via local console or in encrypted form via TLS or SSH session / Exits the module in encrypted form as part of config backup file	-	Encrypted on disk (via KEK)	N/A[67]	Used as input to derive DFA Session Key
ZebOS Router Password (Alphanumeric string) (CSP)	-	-	-	Input in plaintext form via local console or in encrypted form via TLS or SSH session / Exits the module in encrypted form as part of config backup file	Key Entry	Encrypted on disk (via KEK)	N/A[67]	Router authentication
Cluster Password (Alphanumeric string) (CSP)	-	-	-	Input in plaintext form via local console or in encrypted form via TLS or SSH session / Exits the module in encrypted form	Key Entry	Encrypted on disk (via KEK)	N/A[67]	Used to connect nodes to the cluster coordinator
Operator Password (Alphanumeric string) (CSP)	-	-	-	Input in plaintext form via TLS or SSH session / Exits the module in encrypted form	Key Entry	Plaintext in volatile memory	Reboot; remove power	Authenticate the operator to the module via an external authentication service
Firmware Load Integrity Key (RSA public key) (PSP)	2048 bits	RSA (Cert. A3942)	-	Input in plaintext	Key Entry	Plaintext in volatile memory	Reboot; remove power	Used to verify the new firmware load

All RSA and ECDSA keys at 2048 and 3072-bit modulus size are generated internally by the Netscaler Control Plane Cryptographic Library. All RSA and ECDSA keys at the 4096-bit modulus size are generated outside of the module and input either in plaintext form via local console or encrypted form via a TLS or SSH session.

[72] IDP – Identity Provider

AES GCM encryption is used in the context of the TLS 1.2 protocol. The module supports acceptable AES GCM cipher suites from section 3.3.1 of *NIST SP 800-52r2* and meets the (key/IV) pair uniqueness requirements from *NIST SP 800-38D*. The mechanism for IV generation is compliant with *RFC 5288* per scenario 1 in *FIPS 140-3 IG* C.H. The counter portion of the IV is strictly increasing.

The nonce explicit part of the IV does not exhaust the maximum number of possible values for a given session key. This condition is implicitly ensured by the design of the TLS protocol, in which the nonce_explicit is denied exhaustion by the control exerted by the protocol's (and hence also the module's) management logic (wherein the nonce_explicit is incremented per each TLS record). This management logic also implies that the probability of an exhaustion of all 2^{64} - 1 values of the nonce_explicit for the same TLS session in a realistic time frame is not significant.

9.2 RGB Entropy Sources

The following table specifies the module's entropy sources.

Table 15 – Non-Deterministic Random Number Generation Specification

Entropy Source(s)	Minimum Number of Bits of Entropy	Details
CPU Jitter (ESV Cert. E52) *Compliant to SP 800-90B.*	256 bits	The min-entropy (per 4 bits of data) of the tests for each device was: • MPX 89xx FIPS = 3.44 bits • MPX 91xx FIPS = 3.66 bits • MPX 15xxx-50G FIPS = 3.53 bits As long as there is at least one bit of entropy per four bits of raw noise data, the entropy provided by each call to CPU Jitter entropy can be considered to contain full entropy. When the DRBG requests 384 bits of entropy for seeding, the function is called four times and returns 384 bits of entropy, thus exceeding the FIPS requirement of at least 112 bits of entropy. This entropy source is used by all cryptographic libraries and algorithms of the module for generation of keys and random values used in key generation. Cloud Software Group NetScaler CPU Jitter Entropy Source SP 800-90B Non-Proprietary Public Use Document CPU Jitter (JENT) v3.4.0

10. Self-Tests

Both pre-operational and conditional self-tests are performed by the module. Pre-operational tests are performed between the time the cryptographic module is powered up and before the module transitions to the operational state. Conditional self-tests are performed by the module during module operation when certain conditions exist. The following sections list the self-tests performed by the module, their expected error status, and the error resolutions.

10.1 Pre-Operational Self-Tests

The module performs the following pre-operational self-test(s):

- Firmware integrity test (using RSA 2048 digital signature verification with SHA-512)

10.2 Conditional Self-Tests

The module performs the following conditional self-tests:

- Conditional cryptographic algorithm self-tests (CASTs)
  - Netscaler Control Plane Cryptographic Library
    - AES encrypt KAT[73]
    - AES decrypt KAT
    - AES GCM encrypt KAT
    - AES GCM decrypt KAT
    - CTR DRBG KAT
    - CTR DRBG instantiate/generate/reseed KAT
    - DH primitive “Z” computation test
    - ECDH primitive “Z” computation test
    - ECDSA sign KAT (P-256)
    - ECDSA verify KAT (P-256)
    - HMAC KATs (SHA-1, SHA2-256, SHA2-512)
    - PBKDF2 KAT (SHA-1)
    - RSA sign KAT
    - RSA verify KAT
    - SHA KATs (SHA-1, SHA2-256, SHA2-512, SHA3-256)
    - IKE KDF KAT
    - SSH KDF KAT
    - TLS v1.0/1.1 KDF KAT
    - TLS v1.2 KDF KAT
  - Netscaler Data Plane Cryptographic Library
    - AES encrypt KAT
    - AES decrypt KAT

[73] KAT – Known Answer Test

        - AES GCM encrypt KAT
        - AES GCM decrypt KAT
        - ECDH Primitive “Z” computation test
        - ECDSA sign KAT (P-256)
        - ECDSA verify KAT (P-256)
        - Hash DRBG KAT
        - Hash DRBG instantiate/generate/reseed KAT (AES, 256-bit, with derivation function)
        - HMAC KATs (SHA-1, SHA2-256, SHA2-512)
        - KBKDF KAT
        - RSA sign KAT
        - RSA verify KAT
        - SHA KATs (SHA-1, SHA2-256, SHA2-512)
        - TLS v1.0/1.1 KDF KAT
        - TLS v1.2 KDF KAT
        - TLS v1.3 KDF KAT

    - Intel Hardware Cryptographic Accelerator
        - AES encrypt KAT
        - AES decrypt KAT
        - AES GCM encrypt KAT
        - AES GCM decrypt KAT
        - ECDH Primitive “Z” computation test
        - ECDSA sign KAT (P-256)
        - ECDSA verify KAT (P-256)
        - HMAC KATs (SHA-1, SHA2-256, SHA2-512)
        - RSA sign KAT
        - RSA verify KAT
        - SHA KATs (SHA-1, SHA2-256, SHA2-512)
        - TLS v1.0/1.1 KDF KAT
        - TLS v1.2 KDF KAT
        - Continuous Health Tests on the entropy source:
            - Adaptive Proportion Test on entropy source
            - Repetition Count Test on entropy source

    To ensure all conditional CASTs are performed prior to the first operational use of the associated algorithm, all CASTs are performed during the module’s initial power-up sequence. The CASTs for algorithms used in the pre-operational firmware integrity test are performed prior to the integrity test itself; all other CASTs are executed immediately after the successful completion of the firmware integrity test.

- Conditional pair-wise consistency tests (PCTs)
    - Netscaler Control Plane Cryptographic Library
        - ECDSA sign/verify PCT (upon generation of a key pair for ECDSA signature functions)
        - KAS-FFC PCT (upon generation of a key pair for DH Key Agreement functions)
        - RSA sign/verify PCT (upon generation of a key pair for RSA signature functions)
        - RSA encrypt/decrypt PCT (upon generation of a key pair for RSA key transport functions)

- Other conditional self-tests
    - Firmware Load Test (using RSA 2048 digital signature verification with SHA-256)

10.3 Self-Test Failure Handling

If the module fails the pre-operational integrity test, the module enters a critical error state and logs an error message. In this state, the boot sequence and entire system is halted. The only action available from this state is to reboot the module to trigger the re-execution of the integrity test. The error condition is considered to have been cleared if the module successfully passes the pre-operational integrity test. If the module continues to return to a halted state, the module is considered to be malfunctioning or compromised, and Cloud Customer Support must be contacted.

If the module enters the critical error state due to a failure of any of the conditional CASTs, cryptographic operations are halted, and the module inhibits all data output from the module. The module logs an error message and automatically reboots to clear the error state. The CO must contact Cloud Software Group if this error occurs.

The successful completion or failure of the pre-operational self-tests and conditional CASTs can be verified by checking the log files.

- Netscaler Control Plane Cryptographic Library – Successful completion of the self-tests is indicated by "POST Success" in `/var/log/FIPS-post.log`. Failure is indicated by "POST Failed" in `/var/log/FIPS-post.log`.

- Netscaler Data Plane Cryptographic Library – Successful completion of the self-tests is indicated by "FIPS POST Successful" in `/var/log/ns.log`. Failure is indicated by "FIPS Post Failed" in `/var/log/ns.log`.

Intel Hardware Cryptographic Accelerator – Successful completion of the self-tests is indicated by "FIPS POST Successful" in `/var/log/ns.log`. Failure is indicated by "FIPS Post Failed" in `/var/log/ns.log`.
If any of the remaining conditional self-tests fail, the module goes through a soft error state and the following message is displayed:

```
"Internal failure in SSL cert/key generation tool"
```

For these failures, the module returns to an operational state once the message is displayed (and the error is logged). The user may retry the service (which calls the conditional self-test again) or move to other operations. Successful completion of the conditional self-test is indicated by the absence of an error message.

11. Life-Cycle Assurance

The sections below describe how to ensure the module is operating in its validated configuration, including the following:

- Procedures for secure installation, initialization, startup, and operation of the module
- Maintenance requirements
- Administrator and non-Administrator guidance

Operating the module without following the guidance herein (including the use of undocumented services) will result in non-compliant behavior and is outside the scope of this Security Policy.

11.1 Secure Installation

The module is shipped to the customer in a non-configured state. The CO is responsible for all initial setup activities, including installing and configuring the module firmware. Prior to the installation, the CO should read the document entries within the Citrix ADC 13.1 – Getting Started with Citrix ADC webpage on Citrix's online product documentation portal.

The following sections provide references to step-by-step instructions for the setup and installation of the module, as well as the steps necessary to configure the module for its Approved mode of operation.

11.1.1 Initial Tamper-Evident Seal Inspection

Tamper-evident seals are applied at the factory to the modules to protect against unauthorized access to the module. When the module is received, the operator must confirm placement of all tamper-evident seals.

The MPX 89xx FIPS will have a total of four (4) tamper-evident seals installed.

- One seal is placed on the front cover, connecting the front and top of the enclosure (Figure 8).
- One seal is placed on the back of the enclosure, connecting the back to the top. (Figure 9).
- One seal is placed on the left rear side of the enclosure, connecting the side to the top (Figure 10).
- One seal is placed on the right rear side of the enclosure, connecting the side to the top (Figure 11).

Figure 8 – Front Cover of the MPX 89xx FIPS

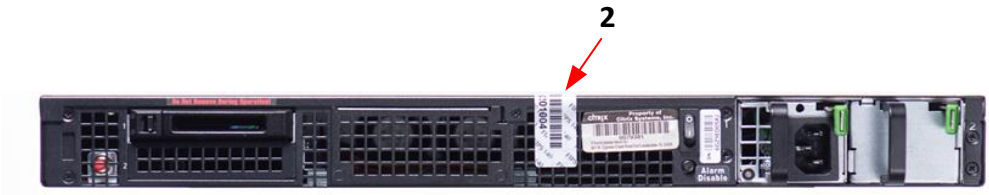

Figure 9 – Back Panel of the MPX 89xx FIPS

Figure 10 – Left Side of the MPX 89xx FIPS

Figure 11 – Right Side of the MPX 89xx FIPS

The MPX 91xx FIPS will have a total of four (4) tamper-evident seals installed.

- One seal is placed on the front cover, connecting the front and top of the enclosure (Figure 12).
- One seal is placed on the back of the enclosure, connecting the back to the top. (Figure 9).
- One seal is placed on the left rear side of the enclosure, connecting the side to the top (Figure 14).
- One seal is placed on the right rear side of the enclosure, connecting the side to the top (Figure 15).

Figure 12 – Front Cover of the MPX 91xx FIPS

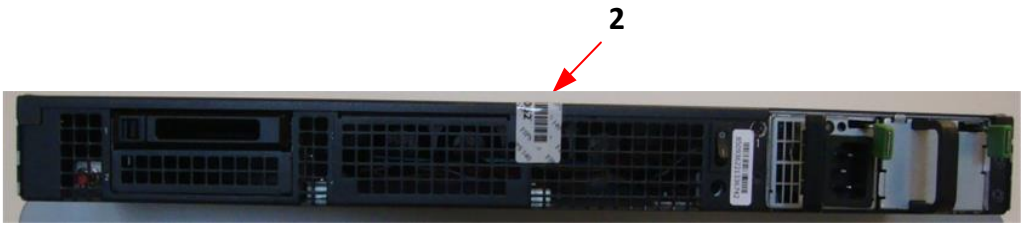

Figure 13 – Back Panel of the MPX 91xx FIPS

Figure 14 – Left Side of the MPX 91xx FIPS

Figure 15 – Right Side of the MPX 91xx FIPS

The MPX 15xxx-50G FIPS will have a total of four (4) tamper-evident seals installed.

- One seal is placed on the front cover, connecting the front and top of the enclosure (Figure 16).
- One seal is placed on the back of the enclosure, connecting the back to the top. (Figure 17).
- One seal is placed on the left rear side of the enclosure, connecting the side to the top (Figure 18).
- One seal is placed on the right rear side of the enclosure, connecting the side to the top (Figure 19).

Figure 16 – Front Cover of the MPX 15xxx-50G FIPS

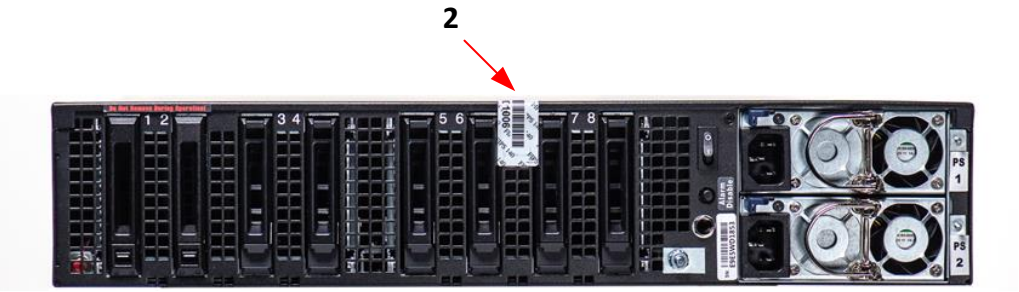

Figure 17 – Back Panel of the MPX 15xxx-50G FIPS

Figure 18 – Left Side of the MPX 15xxx-50G FIPS

Figure 19 – Right Side of the MPX 15xxx-50G FIPS

All tamper-evident seals are required for the module to be considered operating in a Approved mode of operation. If any seals show signs of tampering, the CO must contact Cloud Customer Support immediately.

11.1.2 Installation

For detailed guidance regarding the installation of the module, please see the Citrix ADC 13.1 – Getting Started with Citrix ADC webpage on the online product documentation portal and refer to the following entries in that document:

- Citrix ADC MPX hardware-software compatibility matrix
- Prepare for Installation
- Install the Hardware

The above entries include the MPX support matrix and usage guidelines, prerequisites for setting up the appliance, and installation instructions. To install the required license files, the CO must follow the instructions on the Citrix

ADC licensing overview webpage on Citrix's online product documentation portal. Once the license files are installed, reboot the module so all licenses are applied.

11.2 Initialization

After the appliance has been setup, the CO is responsible for the general configuration of the module. The Web GUI or CLI can be used for the general configuration of the module. All general configuration must be complete before performing configuration necessary to place the module in a Approved mode of operation.

The general configuration requirements and instructions are described in the "Quick Start Installation and Configuration" section of the Citrix ADC Deployment Guide found on Citrix's online product documentation portal.

11.2.1 Approved Mode Configuration and Status

The CO is responsible for the security-relevant configuration of the module. To initialize the module for Approved mode of operation, the CO must:

- Configure the passphrase requirements
- Replace the default TLS certificate
- Disable HTTP access to the Web GUI
- Disable local authentication after initial configuration

To accomplish these tasks, the CO must follow the procedures detailed in the sections below (for more information, please see the "Configuration Guidelines" section of the document entry Citrix ADC Deployment Guide.

11.2.2 Configure the Passphrase Requirements

Passphrases are used to derive keys using PBKDF. The CO must configure strong passphrase requirements. This is accomplished with the following steps from the Web GUI:

1. In the Configuration navigation pane, go to **System** and click the **Settings** node.
2. In the **Settings** section, click the **Change Global System Settings** link.
3. In the **Strong Password** field, select **Enable All**.
4. In the **Min Password Length** field, type "8".
5. Click **OK**.

11.2.3 Replace the Default TLS Certificate

By default, the module includes a factory-provisioned RSA certificate for TLS connections (`ns-server.cert` and `ns-server.key`). This certificate is not intended for use in production deployments and must be replaced. The CO must replace the default certificate with a newly-generated certificate after the initial installation.

To replace the default TLS certificate, the CO must follow these steps:

1. Run the following CLI command to set the hostname of the module: `set ns hostName [hostname]`
2. From the Web GUI, complete the following procedure to create a Certificate Signing Request (CSR):
   - In the Configuration navigation pane, go to **Traffic Management** and click the **SSL** node.

- In the **SSL Certificates** section, click the **Create Certificate Request** link.
- Make sure to provide values for all the required fields marked with an "*" and then click **Create**. Note that the **Common Name** field will contain the value of `hostname` created in step 1 above.

3. Submit the CSR file to a trusted CA. The CSR file is available in the `/nsconfig/ssl` directory.
4. After receiving the certificate from the trusted CA, copy the file to the `/nsconfig/ssl` directory.
5. From the Web GUI, navigate to **Traffic Management** > **SSL** and choose **ns-server-certificate**.
6. Click **Update**.
7. In the **Certificate File Name** field, choose the certificate file that was received from the CA. Use the **Browse** option to choose the file that you have received from CA after signing**.** Choose the **Browse > Local** option if the file is saved on your workstation/local drive.
8. In the **Private Key File Name** field, specify the default private key file name (`ns-server.key`).
9. Select the **No Domain Check** option.
10. Click **OK**.

For more information, please refer to the Citrix Support Knowledge Center article CTX122521) on Citrix's online product documentation portal.

11.2.4 Disable HTTP Access to the Web GUI

The CO protects traffic to the administrative interface and Web GUI, by configuring the module to use HTTPS[74]. Once the module has been configured to use new TLS and SSH certificates, disable HTTP access to the GUI management interface with the following CLI command: `set ns ip <NSIP> -gui SECUREONLY`

11.2.5 Disable Local Authentication

The nsroot account is a default account with root CLI access (superuser) privileges that is required for initial configuration. During initial configuration, the CO shall disable local system authentication to block access to all local accounts (including the nsroot account), and the CO must ensure that superuser privileges are not assigned to any user account. To disable local system authentication and enable external system authentication, the CO must run the following CLI command:

```
set system parameter -localauth disabled
```

11.2.6 Enable External Authentication

Once the module is configured in Approved mode and the `nsroot` account is disabled, then external authentication must be configured. Follow the instructions on the Citrix ADC 13.1 – Configuring external user authentication webpage found on the Cloud online product documentation portal to configure external system authentication.

The CO must ensure the following before enabling external authentication:

- A secure connection is established with the external authentication service.
- Shell access is disabled for all profiles on the external authentication service.

[74] HTTPS – Hypertext Transfer Protocol Secure

11.3 Startup

No additional startup steps are required to be performed by end-users.

11.4 Administrator Guidance

Once installed and configured, the Crypto Officer is responsible for maintaining and monitoring the status of the module to ensure that it is running in its Approved mode. Please refer to this section for guidance that the Crypto Officer must follow to ensure that the module is operating in a Approved manner.

11.4.1 On-Demand Self-Tests

Although pre-operational self-tests are performed automatically during module power up, they can also be manually launched on demand. Self-tests can be executed by:

- power-cycling the module
- using the reset button on the platform (if applicable)
- the `reboot` CLI command
- the `reboot` API method
- via the Web GUI by navigating to **Configuration > System > System Information** and clicking the **Reboot** button

11.4.2 Zeroization

There are many CSPs within the module's cryptographic boundary including symmetric keys, private keys, public keys, and passphrases. CSPs reside in multiple storage media including the RAM and system memory. All ephemeral keys are zeroized on module reboot, power removal, or session termination.

The KEK is stored as plaintext in non-volatile memory. Zeroizing the KEK renders all passphrases and passwords stored in the non-volatile memory unrecoverable, effectively zeroizing them. The KEK is zeroized via the following CLI command:

```
rm system csps -type KEK
```

SSH private keys are stored as plaintext in non-volatile memory. SSH private keys are zeroized via the following CLI command:

```
rm system csps -type SSH_HOST_KEYS
```

The output (indicator) of both zeroization commands above is successful return from the command line without any error showing on the console. If the commands fails, an error will show on the console before returning control to the user.

After the module's integrity test is complete the firmware clears out all values when the signature verification operation is complete (zeroizes temporary values used in the integrity test).

11.4.3 Status and Versioning Information

The CO shall be responsible for regularly monitoring the module's status for the Approved mode of operation. When configured according to the CO's guidance, the module only operates in the Approved mode. Thus, the current status of the module when operational is always in the Approved mode.

An operator can view the versioning information by:

- using the following CLI commands:

`show ns info`	shows details about the firmware, including firmware version, enabled and disabled features, and configured network information
`show ns version`	shows version and build number of the appliance
`show ns hardware`	shows details of the appliance hardware and information such as the host ID[75] and serial number

- using the RESTful Nitro API with the GET method:

```
https://module-ip-address>/nitro/v5/config/nshardware
https://module-ip-address>/nitro/v5/config/nsversion
```

- using the Web GUI by navigating to **Configuration > System > System Information**

This will display general system and hardware information about the device, including the platform version, CPU information, and appliance serial number. Additionally, the Web GUI's dashboard includes a system overview section with information such as system HA state, system master state, and system uptime.

If any irregular activity is noticed or the module is consistently reporting errors, then Cloud Customer Support should be contacted.

11.4.4 Additional Administrator Policies and Guidance

This section notes additional policies below that must be followed by COs:

- All private keys (except for SSH private keys) must be stored as PEM files in encrypted format using one of the Approved encryption algorithms listed in Table 3 or Table 5.

- Upon successful bootup of the module, the module is configured by default to use only *NIST SP 800-52rev2* recommended cipher suites for TLS connections. If modified, the CO must ensure that only Approved cipher suites are configured while in the Approved mode. It is recommended to use the list of approved TLS cipher suites in section 3.3 of NIST SP 800-52*rev2* as guidance.

- The module must be configured to use PSK-based authentication for IPsec connections. The CO must provide a PSK value when configuring IPsec profiles via the GUI, CLI, or API. Configuring digital certificate-based authentication for IPsec connections is **prohibited** while in the Approved mode of operation.

[75] ID – Identifier

- Kerberos traffic management/SSO shall not be configured or used in the Approved mode of operation.
- The module supports clustering, and it may act as either the cluster coordinator or the cluster node. Once appliances are clustered together, all configuration is done on the cluster coordinator and pushed to nodes within the cluster. For details on configuring clusters, refer to Citrix ADC 13.1 – Clustering.
- The CO must ensure that the "Key" and "AutoKey" authentication parameters are not set when adding NTP servers via the GUI, CLI, or API.
- If the module's power is lost and then restored, the CO shall establish a new key for AES GCM encryption.
- The module has built-in CA tools used to create self-signed certificates for testing purposes. While the feature does include the generation of keys, those keys are not considered CSPs (as they are not being used for production purposes). The CO must ensure that all certificates are signed using a trusted CA and not by a self-signed certificate.
- When performing a firmware update the following steps must be performed:
    - Load firmware load integrity key
    - Load firmware package
    - Zeroize SSH keys using `rm system csps -type SSH_HOST_KEYS`
    - Run the installation script
- The operator shall not enable the LOM port via ADC configuration.
- The operator shall perform the zeroization commands as specified in section 11.4.2 Zeroization prior to invoking the "Firmware Load" service.

11.5 Non-Administrator Guidance

Operators with the User role do not have the ability to configure sensitive information on the module. They must be diligent to select strong passwords and must not reveal their password to anyone. Additionally, they must be careful to protect any secret or private keys in their possession.

12. Mitigation of Other Attacks

The module does not claim to mitigate any attacks beyond the FIPS 140-3 Level 2 requirements for this validation. Therefore, per ISO/IEC 19790:2021 section 7.12, requirements for this section are not applicable.

Appendix A. Acronyms and Abbreviations

Table 16 provides definitions for the acronyms and abbreviations used in this document.

Table 16 – Acronyms and Abbreviations

Term	Definition
AAA	Authentication, Authorization, Accounting
ADC	Application Delivery Controller
AES	Advanced Encryption Standard
API	Application Programming Interface
CA	Certificate Authority
CAST	Cryptographic Algorithm Self-Test
CBC	Cipher Block Chaining
CCCS	Canadian Centre for Cyber Security
CCM	Counter with Cipher Block Chaining - Message Authentication Code
CFB	Cipher Feedback
CKG	Cryptographic Key Generation
CLI	Command Line Interface
CMVP	Cryptographic Module Validation Program
CO	Cryptographic Officer
CPU	Central Processing Unit
CSP	Critical Security Parameter
CTR	Counter
CVL	Component Validation List
DEP	Default Entry Point
DFA	Delegated Form Authentication
DH	Diffie-Hellman
DNS	Domain Name Service
DRBG	Deterministic Random Bit Generator
DSA	Digital Signature Algorithm
ECB	Electronic Code Book
ECC	Elliptic Curve Cryptography
ECC CDH	Elliptic Curve Cryptography Cofactor Diffie-Hellman
ECDH	Elliptic Curve Diffie-Hellman
ECDSA	Elliptic Curve Digital Signature Algorithm
EFT	Environmental Failure Testing

Term	Definition
FFC	Finite Field Cryptography
FIPS	Federal Information Processing Standard
GCM	Galois/Counter Mode
GSLB	Global Server Load Balancing
GMAC	Galois Message Authentication Code
GPC	General-Purpose Computer
GUI	Graphical User Interface
HMAC	(keyed-) Hash Message Authentication Code
HTML	Hypertext Markup Language
HTTP	Hypertext Transfer Protocol
IKE	Internet Key Exchange
KAS	Key Agreement Scheme
KAS-SSC	Key Agreement Scheme-Shared Secret Computation
KAT	Known Answer Test
KDF	Key Derivation Function
KEK	Key Encryption Key
KTS	Key Transport Scheme
KW	Key Wrap
KWP	Key Wrap with Padding
LDAP	Lightweight Directory Access Protocol
LOM	Lights Out Management
MD5	Message Digest 5
MLE	Medium and Large Enterprise
MODP	Modular Exponentiation
NDRNG	Non-Deterministic Random Number Generator
NIST	National Institute of Standards and Technology
NTP	Network Time Protocol
OID	Object Identifier
OS	Operating System
PBKDF	Password Based Key Derivation Function
PCT	Pairwise Consistency Test
PEM	Privacy-Enhanced Mail
PKCS	Public Key Cryptography Standard
PSK	Pre-shared Key
PSS	Probabilistic Signature Scheme
PUB	Publication

Term	Definition
RBA	Role Based Authentication
RDP	Remote Desktop Protocol
REST	Representational State Transfer
RNG	Random Number Generator
RSA	Rivest, Shamir, and Adleman
SAML	Security Assurance Markup Language
SHA	Secure Hash Algorithm
SME	Small and Medium Enterprise
SHS	Secure Hash Standard
SNMP	Simple Network Management Protocol
SP	Special Publication
SQL	Structured Query Language
SSL	Secure Sockets Layer
TCP	Transmission Control Protocol
TGS	Ticket Granting Service
TLS	Transport Layer Security
UDP	User Datagram Protocol
URL	Uniform Resource Locator
XML	eXtensible Markup Language

Prepared by:
Corsec Security, Inc.

12600 Fair Lakes Circle, Suite 210
Fairfax, VA 22033
United States of America

Phone: +1 703 267 6050
Email: info@corsec.com
http://www.corsec.com