Citrix Systems, Inc.

Secure Deployment Guide for NetScaler MPX, VPX, and SDX Appliances

March 2018

CITRIX®

Copyright and Trademark Notice and Disclaimers

The following information is for FCC compliance of Class A devices: This equipment has been tested and found to comply with the limits for a Class A digital device, pursuant to part 15 of the FCC rules. These limits are designed to provide reasonable protection against harmful interference when the equipment is operated in a commercial environment. This equipment generates, uses, and can radiate radio-frequency energy and, if not installed and used in accordance with the instruction manual, may cause harmful interference to radio communications. Operation of this equipment in a residential area is likely to cause harmful interference, in which case users will be required to correct the interference at their own expense.

Modifying the equipment without Citrix' written authorization may result in the equipment no longer complying with FCC requirements for Class A digital devices. In that event, your right to use the equipment may be limited by FCC regulations, and you may be required to correct any interference to radio or television communications at your own expense.

You can determine whether your equipment is causing interference by turning it off. If the interference stops, it was probably caused by the NetScaler Request Switch™ 9000 Series equipment. If the NetScaler equipment causes interference, try to correct the interference by using one or more of the following measures:

Move the NetScaler equipment to one side or the other of your equipment.

Move the NetScaler equipment farther away from your equipment.

Plug the NetScaler equipment into an outlet on a different circuit from your equipment. (Make sure the NetScaler equipment and your equipment are on circuits controlled by different circuit breakers or fuses.)

Modifications to this product not authorized by Citrix Systems, Inc., could void the FCC approval and negate your authority to operate the product.

BroadCom is a registered trademark of BroadCom Corporation. Fast Ramp, NetScaler, and NetScaler Request Switch are trademarks of Citrix Systems, Inc. Linux is a registered trademark of Linus Torvalds. Internet Explorer, Microsoft, PowerPoint, Windows and Windows product names such as Windows NT are trademarks or registered trademarks of the Microsoft Corporation. NetScape is a registered trademark of Netscape Communications Corporation. Red Hat is a trademark of Red Hat, Inc. Sun and Sun Microsystems are registered trademarks of Sun Microsystems, Inc. Other brand and product names may be registered trademarks or trademarks of their respective holders.

The license to Citrix and third-party software delivered as part of Product(s) is identified in the relevant Product documentation as delivered with the Product(s).

Last Updated: March 2018

Table of Contents

Introduction to Best Practices for NetScaler MPX, VPX, and SDX Security

A Citrix® NetScaler® MPX™ appliance is an application delivery controller that accelerates web sites, provides L4-7 traffic management, offers an integrated application firewall, and offloads servers. A Citrix® NetScaler® VPX™ instance is a virtual appliance that has all the features of a NetScaler MPX appliance, runs on standard servers, and provides higher availability for web applications including Citrix XenDesktop and XenApp. A Citrix® NetScaler® SDX appliance provides advanced virtualization for all the flexibility of VPX with the performance of MPX. Using MPX, VPX, and SDX, an organization can deploy the flex or true-multitenancy solution that optimizes your web-application delivery infrastructure by separating high-volume shared network services from processor-intensive, application-specific services. A NetScaler appliance also provides the seamless integration with Citrix OpenCloud Access that can extend the datacenter with the power of the Cloud.

To maintain security through the deployment lifecycle, Citrix recommends reviewing the following considerations for:

- Physical Security
- Appliance Security
- Network Security
- Administration and Management

Note that different deployments might require different security considerations. This document provides general security guidance to help you decide on an appropriate secure deployment based on your specific security requirements.

Deployment Guidelines

When deploying a Citrix NetScaler, you should consider the following physical and appliance security best practices:

Physical Security Best Practice

Deploy the NetScaler appliance in a secure location

The NetScaler appliances should be deployed in a secure location with sufficient physical access controls to protect the appliances from unauthorized access. At the minimum, access to the server room should be controlled with a lock, electronic card reader, or other similar physical methods.

Additional measures can include the use of an electronic surveillance system, for example CCTV, to continuously monitor the activity of the room. In the event of an unauthorized intrusion, the output from this system should notify security personnel. In the case of CCTV, the recorded footage will be available for audit purposes.

Secure access to the appliance front panel and console port

The NetScaler appliance or VPX hosting server should be deployed in a rack or cage that can be locked with a suitable key, or other physical methods. This will prevent access to the physical ports of the NetScaler appliance or, in the case of a VPX deployment, the virtualization host console.

Power Supply Protection

The NetScaler appliance (or hosting server) should be protected with a suitable uninterruptible power supply (UPS). In the event of a power outage, this will ensure continued operation of the appliance, or allow controlled shutdown of physical or virtual NetScalers. The use of a UPS will also aid in the protection against power spikes.

Cryptographic key protection

If additional protection is required for the cryptographic keys in your deployment, consider use of a FIPS 140-2 Level 2 compliant appliance. The FIPS platform uses a hardware security module to protect critical cryptographic keys in the appliance from unauthorized access.

NetScaler Appliance Security Best Practice

Perform appliance software updates
Citrix strongly recommends that, prior to deployment, customers ensure their appliances have been updated with the latest firmware versions. When carried out remotely, Citrix recommends that customers use a secure protocol, such as SFTP or HTTPS, to upgrade the appliance.

Customers are also strongly advised to review security bulletins that relate to their Citrix products. For information on new and updated security bulletins, please refer to the Citrix Security Bulletins web page (https://support.citrix.com/securitybulletins) and consider signing up for alerts on new and updated bulletins.

Secure the operating system of servers hosting a NetScaler VPX appliance
A NetScaler VPX appliance can run either a virtual appliance on a standard virtualization server or as a virtual appliance on a NetScaler SDX.

In addition to applying normal physical security procedures, you should protect access to the virtualization host with role-based access control and strong password management. Additionally, the server should be updated with the latest security patches for the operating system when they become available, and deploy up-to-date antivirus software on the server, if applicable to the type of virtualization. Customers using the NetScaler SDX platform to host NetScaler VPX should ensure that they are using the latest firmware version for their NetScaler SDX.

Reset the NetScaler Lights Out Management (LOM)
Citrix recommends that, before configuring the LOM for use in a production deployment, you perform a factory reset of the LOM to restore the default settings.

1. At the NetScaler shell prompt, run the following command:

   ```
   >ipmitool raw 0x30 0x41 0x1
   ```

   Note: Running the above command resets the LOM to the factory default settings and deletes all the SSL certificates. For instructions on how to reconfigure the LOM port, please refer to the following documentation:

   http://docs.citrix.com/en-us/netscaler-hardware-platforms/mpx/netscaler-mpx-lights-out-management-port-lom.html

2. In the LOM GUI, navigate to **Configuration > SSL Certification**, and add a new certificate and private key.

Additionally, Citrix strongly recommends that the following user configuration is carried out. Using the LOM GUI:

- Navigate to **Configuration > Users > Modify User** and change the password of the nsroot superuser account.
- Navigate to **Configuration > Users > Modify User** and create policies for, or bind existing policies to, the users.
- Navigate to **Configuration > IP Access Control > Add** and configure the IP access control to allow access to the known range of IP addresses.
- Navigate to **Configuration > Users > Modify User**, create an alternative superuser account and bind policies to this account.

For more details about LOM configuration, see LOM Configuration.

Maintenance and removal of persistent data
In the event that a NetScaler is redeployed to another environment, decommissioned, or returned to Citrix under RMA, you should ensure that persistent data is correctly removed from the appliance.

For more information about this process, see the following FAQ: https://www.citrix.com/support/programs/faqs.html.

Configuration Guidelines

Network Security

When deploying a NetScaler appliance to a production environment, Citrix strongly recommends that the following key configuration changes are made:

- The NetScaler administrator interface (NSIP) should not be exposed to the Internet.
- The NetScaler default SSL certificate should be replaced.
- HTTPS (HTTP over TLS) should be used when accessing the GUI and the default HTTP interface disabled.

The following section provides more information on these key considerations, in addition to further changes that are recommended.

Key Network Security Considerations

Do not expose the NSIP to the Internet

Citrix strongly recommends that the NetScaler Management IP (NSIP) is not exposed to the public Internet and is deployed behind an appropriate stateful Packet Inspection (SPI) firewall.

Replace the NetScaler Default TLS Certificate

During the initial configuration of a NetScaler appliance, default TLS certificates are created. These are not intended for use in production deployments and should be replaced.

Citrix recommends that customers configure the NetScaler appliance to use certificates either from a reputable Certificate Authority (CA) or appropriate certificates from your enterprise CA.

When bound to a public-facing virtual server, a valid TLS certificate from a reputable CA simplifies the user experience for Internet-facing web applications; user web browsers require no user interaction when initiating secure communication with the web server. To replace the default NetScaler certificate with a trusted CA certificate, see Knowledge Center article CTX122521: "How to Replace the Default Certificate of a NetScaler Appliance with a Trusted CA Certificate that Matches the Hostname of the Appliance."

Alternatively, it is possible to create and use custom TLS certificates and private keys. While this can provide an equivalent level of transport layer security, it requires the TLS certificates to be distributed to users and will require user interaction when initiating connections to the web server. For more information on how to create custom certificates, see Knowledge Center article CTX121617: "How to Create and Install Self-Signed Certificates on NetScaler Appliance"

More information on TLS certificate management and configuration can be found in the "NetScaler TLS Recommendations" section of this guide.

Disable HTTP access to the Administrator Interface

To protect traffic to the NetScaler administrative interface and GUI, the NetScaler appliance should be configured to use HTTPS. This can be accomplished with the following steps:

- Create a 2048-bit or greater RSA private and public key pair and use the keys for HTTPS and SSH to access NetScaler IP address, replacing the factory provisioned 512-bit RSA private and public key pair.

- Configure the appliance to use only strong cipher suites and change the 'DEFAULT' set of cipher suites to reflect this on the appliance. It is recommended that you use the list of approved TLS CipherSuites in section 3.3 of NIST Special Publication 800-52 (Revision 1) as a guidance. This document can be found on the NIST website at the following

address: https://www.nist.gov/publications/guidelines-selection-configuration-and-use-transport-layer-security-tls-implementations?pub_id=915295

- Configure the appliance to use SSH public key authentication to access the administrator interface. **Do not use the NetScaler default keys**. Create and use your own 2048-bit RSA private and public key pair. For more information, see Knowledge Center article CTX109011: How to Secure SSH Access to the NetScaler Appliance with Public Key Authentication.

- Once the NetScaler has been configured to use these new certificates, HTTP access to the GUI management interface can be disabled with the following command:

```
> set ns ip <NSIP> -gui SECUREONLY
```

For more information on how to configure secure access to the Administration GUI, see the Knowledge Center article CTX111531: "How to Enable Secure Access to NetScaler GUI Using the SNIP/MIP Address of the Appliance."

Additional Network Security Considerations:

The following additional network-related security considerations should also be taken into account when deploying your NetScaler appliances:

Disable SSH Port Forwarding
SSH Port Forwarding is not required by the NetScaler appliance. If you do not wish to use this functionality, then Citrix recommends that you disable it using the following steps:

1. Edit the /etc/sshd_config file by adding the following line.

```
AllowTcpForwarding no
```

2. Save the file and copy it to `/nsconfig` to make the changes are persistent in case you reboot during the tests.

Kill the process by using the `kill -SIGHUP <sshdpid>` command, or restart the system.

Configure the NetScaler appliance with High Availability
In deployments where continuous operation is required, the NetScaler appliances can be deployed in a high availability setup. Such a setup provides continued operation if one of the appliances stops functioning or requires an offline upgrade.

For information on how to configure high availability setup, see High Availability > Configuring High Availability topic on the Citrix Docs and Knowledge Center article CTX116748: How to Set Up a High Availability Pair on NetScaler.

In deployments where high availability is not required, this feature should be disabled.

Set up secure communication between peer appliances
If you have configured your NetScaler appliances in a high availability or GSLB setup, secure the communication between the appliances.

To secure communication between the appliances, perform the following procedure on each appliance:

1. In the configuration utility's navigation pane, expand the **Network** node.
2. Select the **RPC** node.
3. On the RPC page, select the IP address.
4. Click **Open**.
5. Type the password in the **Password** and **Confirm Password** fields.
6. Select the **Secure** option on the Configure RPC node dialog box.

The NetScaler appliance features can also use SSH key based authentication for internal communication when the internal user is disabled. In such cases, the key name must be set as "ns_comm_key". For more information, see Accessing a NetScaler by Using SSH Keys and No Password.

Note: It is recommended that you disable the **internal** user account (by using the `set ns param -internaluserlogin disabled` command).

Configure Network Security Domains and VLANs
Citrix strongly recommends that network traffic to the NetScaler appliance's management interface is separated, either physically or logically, from normal network traffic. The recommended best practice is to have three VLANs:

- Outside Internet VLAN
- Management VLAN
- Inside server VLAN

Citrix recommends configuring the network to make the LOM port part of the management VLAN.

When deploying a NetScaler appliance in two-arm mode, dedicate a specific port to a specific network. If VLAN tagging and binding two networks to one port is required, you should ensure that the two networks have the same, or similar, security levels.

If the two networks have significantly different security levels, VLAN tagging should not be used. Instead, consider dedicating a port for each specific network and use independent VLANs distributed over the ports on the appliance.

Note: The NetScaler VPX appliances do not support tagged VLANs.

Consider Using the Application Firewall
A NetScaler platinum edition licensed appliance provides a built-in application firewall that uses a positive security model and automatically learns proper application behavior for protection against threats such as command injection, SQL injection, and Cross Site Scripting.

When you use the application firewall, users can add additional security to the web application without code changes and with little change in configuration. For more information, see the NetScaler Application Firewall web page.

Restrict non-management applications access
Run the following command to restrict the ability of non-management applications to access a NetScaler appliance.

```
> set ns ip <NSIP> -restrictAccess enabled
```

Secure Cluster Deployment
If NetScaler cluster nodes are distributed outside the data center, Citrix strongly recommends the use of secure RPC for Node to Node Messaging (NNM), AppNNM and the setup of high availability.

To enable the Secure RPC feature for all NetScaler IP address in a NetScaler Cluster and a high availability setup, run the following command:

```
> set rpcnode <ip> -secure on
```

Note: Additional configuration may be required. For more information, see the Clustering topics on the Citrix Docs site.

When deployed in an L3 cluster deployment, packets between NetScaler nodes are exchanged over an unencrypted GRE tunnel that uses the NSIP addresses of the source and destination nodes for routing. When this exchange occurs over the

internet, in the absence of an IPSec tunnel, the NSIPs will be exposed on the internet. This is not recommended as it does not comply with the security best practices for the NetScaler ADC.

Citrix strongly recommends that customers establish their own IPSec solution to use the cluster over L3 feature.

If the IP forwarding feature is not in use, use the following command to disable L3 mode:

```
> disable ns mode L3
```

Use Secure MEP for Global Server Load Balancing (GSLB)
To encrypt the MEP between NetScaler appliances for GSLB, run the following command from the NSCLI:

```
> set rpcNode <GSLB Site IP> -secure yes
```

Securing Pass-through Traffic on the NetScaler Appliance by using the Infrastructure Mode Settings

Citrix NetScaler Web Application Firewall infrastructure mode settings can be used to secure pass-through traffic on the NetScaler appliance. These infrastructure mode settings provide a basic level of security without breaking any applications. The following list summarizes the available infrastructure mode settings.

- Session state protection
- Session fixation protection (enable HTTP Only)
- HSTS (enable HTTP Strict Transport Security (HSTS))
- Strong Authentication
- End-to-end SSL preferred (TLS 1.2 and TLS 1.1)
- Proxy HTTPS / Deny all other traffic

Session state protection

Recommendation: Enabled
NetScaler: Enabled by default for most entities

The Session state protection setting is enabled by default and requires no specific configuration. When the NetScaler appliance is configured to proxy a connection; for example, when flow hits a configured virtual server or service of type TCP or above, the NetScaler appliance creates a stateful session. The NetScaler appliance continues to maintain the state of these connections and only packets that fall in to this state machine are processed. Other packets are either dropped or reset.

The following service type entities achieve this stateful behavior on a NetScaler appliance.

- ADNS_TCP
- DIAMETER, DNS_TCP
- FTP-c
- GRE-c
- HTTP
- MYSQL, MSSQL
- NNTP
- ORACLE
- PUSH, PPTP
- RTSP, RDP
- SIP_SSL , SIP_TCP
- SMPP
- SSL, SSL_BRIDGE, SSL_DIAMETER, SSL_PUSH
- SSL_TCP, SYSLOG_TCP
- TCP
- ADNS_TCP
- RNAT (rnat_tcpproxy is ENABLED)

Session fixation protection (by enabling the HttpOnly flag or by adding a rewrite policy)

Recommendation: To enable HttpOnly for cookies set by the NetScaler appliance or backend server
NetScaler: Enabled by Default for the NetScaler inserted cookies, possible via Rewrite for cookies set by backend server.

HttpOnly: When you tag a cookie with the HttpOnly flag, it indicates to the browser that this cookie should only be accessed by the server. Any attempt to access the cookie from client script is strictly forbidden. HttpOnly cookies, if properly implemented, makes huge classes of common XSS attacks much harder to pull off.
The following is an example of a cookie with the HttpOnly flag set:

```
Set-Cookie: ASP.NET_SessionId=ig2fac55; path=/; HttpOnly
```

- The cookies inserted by NetScaler for Cookie Insert persistence, by default, sets the HttpOnly flag to indicate that the cookie is nonscriptable and should not be revealed to the client application. Therefore, a client-side script cannot access the cookie, and the client is not susceptible to cross-site scripting.

  To enable the HttpOnly flag setting by using the command line interface
  At the command prompt, type:

  ```
  set lb parameter -HttpOnlyCookieFlag (ENABLED)
  ```

Using rewrite policy to insert Secure and HttpOnly for cookies

- The rewrite policy inserts Secure and HTTP only for cookies sent by the backend server.

  Note: Secure and HttpOnly cookies together can be done for SSL VIPs. For non-SSL VIPs one could just insert the HttpOnly flag.

  With NetScaler, one can include HTTP only and Secure flags for cookies set by the server.
  - **HttpOnly** - This option on a cookie causes the web browsers to return the cookie using the http (or https) protocol only; the non-http methods such as JavaScript document.cookie references cannot access the Cookie. This option assists in preventing Cookie theft due to cross-site scripting.
  - **Secure** - This option on a cookie causes the web browsers to return only the cookie value when the transmission is encrypted by SSL. This option can be used to prevent cookie theft through connection eavesdropping.

  To create a rewrite policy by using the command line interface

  1. Enable the Rewrite feature, if not already enabled.
     ```
     enable feature REWRITE
     ```

  2. Create a rewrite action (this example is configured to set both Secure and HttpOnly flags. If either one is missing, modify it as necessary for other combinations).
     ```
     add rewrite action <action name> replace_all http.RES.full_Header
     "\"path=/; Secure; HttpOnly\"" -search "regex(re!(path=/\\; Secure;
     HttpOnly)|(path=/\\; Secure)|(path=/\\; HttpOnly)|(path=/)!)" -bypassSafetyCheck
     YES
     ```
     Example
     ```
     add rewrite action act_cookie_Secure replace_all http.RES.full_Header
     "\"path=/; Secure; HttpOnly\"" -search "regex(re!(path=/\\; Secure;
     HttpOnly)|(path=/\\; Secure)|(path=/\\; HttpOnly)|(path=/)!)" -bypassSafetyCheck
     YES
     ```

  3. Create a rewrite policy to trigger the action.
     ```
     add rewrite policy <policy name> "http.RES.HEADER(\"Set-Cookie\").EXISTS" <action
     name>
     ```

Example

```
add rewrite policy rw_force_secure_cookie "http.RES.HEADER(\"Set-Cookie\").EXISTS"
act_cookie_Secure
```

4. Bind the rewrite policy to the VServer to be secured (if Secure option is used, an SSL VServer should be used).

```
bind lb vserver <vserver name> - <policy name> -priority <priority number> -
gotoPriorityExpression NEXT -type RESPONSE
```

Example

```
bind lb vserver mySSLVServer -policyName rw_force_secure_cookie -priority 100 -
gotoPriorityExpression NEXT -type RESPONSE
```

For more information, see https://support.citrix.com/article/CTX138055

HSTS (enable HTTP Strict Transport Security (HSTS))

Recommendation: Enabled
NetScaler: In NetScaler software version 12.0, this setting can be enabled by using the CLI. In NetScaler software versions 11.1 and earlier, this setting can be enabled by using the rewrite policy.

- In NetScaler Software version 12.0, NetScaler appliances support HTTP strict transport security (HSTS) as an inbuilt option in SSL profiles and SSL virtual servers.

  To enable HSTS by using the NetScaler command line
  At the command prompt, type:

  ```
  add ssl vserver <vServerName> -HSTS ( ENABLED ) maxage <positive_integer> -
  IncludeSubdomains ( YES | NO)
  ```

  OR

  ```
  add ssl profile <name> -HSTS ( ENABLED ) -maxage <positive_integer> -
  IncludeSubdomains ( YES | NO )
  ```

  For more information, see https://docs.citrix.com/en-us/netscaler/12/ssl/ssl-support-for-hsts.html

- In NetScaler software versions 11.1 and earlier, HTTP strict transport security (HSTS) can be enabled by creating a rewrite policy and binding it globally or to the vserver in question.
  At the command prompt, type:

  - `add rewrite action <action name> insert_http_header Strict-Transport-Security "\"max-age=157680000\""`
    Example
    `add rewrite action insert_STS_header insert_http_header Strict-Transport-Security "\"max-age=157680000\""`

  - `add rewrite policy <policy name> "true" <action name>`
    Example
    `add rewrite policy enforce_STS "true" insert_STS_header`

  - `bind lb vserver <vserver name> - <policy name> -priority <priority number> END -type RESPONSE`

Example

```
bind lb vserver vs1 -policyName enforce_STS -priority 100 -
gotoPriorityExpression END -type RESPONSE
```

For more information, see the following topics:

https://support.citrix.com/article/CTX205221
https://www.citrix.com/blogs/2010/09/10/strict-transport-security-sts-or-hsts-with-citrix-netscaler-and-access-gateway-enterprise/

Strong Authentication

Strong Authentication (or multifactor authentication – MFA) should be enabled for all access to sensitive data, apps and administration.

For details on how sensitive apps can be set up for multi factor authentication, see https://docs.citrix.com/en-us/netscaler/11-1/aaa-tm/multi-factor-nfactor-authentication.html

End-to-end SSL preferred (TLS 1.2 and TLS 1.1)

It is recommended to have SSL both on the frontend and backend. SSLv3 and TLS v1.0 can be disabled on SSL entities as there have been security vulnerabilities reported against these. You can only have TLS 1.1 and TLS 1.2 enabled. If possible, have only TLS 1.2 version on the client facing VIPs. It can either be done at the SSL entity level or at the profile level and all of the SSL entities inherit the SSL settings from the profile.

To disable SSL entities by using the command line interface

At the command prompt, type:

```
set ssl vserver <vServerName> -ssl2 DISABLED   -ssl3  DISABLED   -tls1   DISABLED

set ssl service <vServiceName> -ssl2 DISABLED   -ssl3  DISABLED   -tls1   DISABLED
```

NetScaler Recommended Ciphersuites

The following ciphers are supported by NetScaler that do not include any components on the "mandatory discard" list. These are organized by key-exchange (RSA, DHE and ECDHE) then by placing the higher performing ones at the top with the higher security ones at the bottom:

Recommend RSA Key Exchange Ciphersuites

- TLS1-AES-128-CBC-SHA
- TLS1-AES-256-CBC-SHA
- TLS1.2-AES-128-SHA256
- TLS1.2-AES-256-SHA256
- TLS1.2-AES128-GCM-SHA256
- TLS1.2-AES256-GCM-SHA384

Recommend DHE Key Exchange Ciphersuites

- TLS1-DHE-RSA-AES-128-CBC-SHA
- TLS1-DHE-RSA-AES-256-CBC-SHA
- TLS1.2-DHE-RSA-AES-128-SHA256
- TLS1.2-DHE-RSA-AES-256-SHA256
- TLS1.2-DHE-RSA-AES128-GCM-SHA256

- TLS1.2-DHE-RSA-AES256-GCM-SHA384

Recommend ECDHE Key Exchange Ciphersuites

- TLS1-ECDHE-RSA-AES128-SHA
- TLS1-ECDHE-RSA-AES256-SHA
- TLS1.2-ECDHE-RSA-AES-128-SHA256
- TLS1.2-ECDHE-RSA-AES-256-SHA384
- TLS1.2-ECDHE-RSA-AES128-GCM-SHA256
- TLS1.2-ECDHE-RSA-AES256-GCM-SHA384

Recommend Ciphersuites in the order of preference

The following list of ciphers include RSA, DHE and ECDHE key exchanges. It provides the best compromise between security, performance, and compatibility.

1. TLS1.2-AES128-GCM-SHA256
2. TLS1.2-AES-128-SHA256
3. TLS1.2-ECDHE-RSA-AES128-GCM-SHA256
4. TLS1.2-ECDHE-RSA-AES-128-SHA256
5. TLS1-ECDHE-RSA-AES128-SHA
6. TLS1.2-DHE-RSA-AES128-GCM-SHA256
7. TLS1.2-DHE-RSA-AES-128-SHA256
8. TLS1-DHE-RSA-AES-128-CBC-SHA
9. TLS1-AES-128-CBC-SHA

Proxy HTTPS / Deny all other traffic

Wherever feasible have SSL VIPs for better encryption of data, by using secure SSL versions (TLSv1.1 and TLSv1.2) and secure ciphers. The SSL TPS and SSL throughput should be considered while enabling SSL for the VIPs and backend SSL services.

Administration and Management

This section provides examples of specific configuration changes that can be applied to increase the security of the NetScaler and NetScaler SDX appliances. Additional guidance on NetScaler configuration best practices can be found in Knowledge Center article CTX121149, "Recommended Settings and Best Practices for a Generic Implementation of a NetScaler Appliance."

System and User Accounts

Change Password for the nsroot Super User Account

You cannot delete the built-in nsroot superuser. Therefore, change the default password for the nsroot account to a secure password. To change the default password for the nsroot user, perform the following procedure:

1. Log on as the superuser and open the configuration utility.
2. In the navigation pane, expand the **Systems** node.
3. Select the **Users** node.
4. On the System Users page, select the **nsroot** user.
5. Select **Change Password**.
6. Type the required password in the **Password** and **Confirm Password** fields.
7. Click **OK**.

Create an Alternative Superuser Account
To create a superuser account, run the following commands:

```
> add system user <newuser> <password>
> bind system user <newuser> superuser 0
```

Use this superuser account instead of the default nsroot superuser account.

For NetScaler SDX deployments, an administrator must change the default credentials for the NetScaler SDX appliance and its GUI management console after the initial set up. To change the password for the default user, perform the following steps:

1. Log on as the superuser and open the configuration utility.
2. In the navigation pane, expand the **Systems** node.
3. Select the **Users** node.
4. On the **System Users** page, select the default user.
5. Select **Modify**.
6. Type the required password in the **Password** and **Confirm Password** fields.
7. Click **OK**.

Note: From NetScaler release 11.0 and later, local users and administrators must choose strong passwords. Examples of password complexity requirements are as follows:

- The password must have a minimum length of eight characters.
- The password must not contain dictionary words or a combination of dictionary words.
- The password must at least include one uppercase letter, one lowercase letter, one number, and one special character.

Strong passwords can be enforced by setting two parameters, one for the minimum length of passwords and the other to enforce password complexity:

```
> set system parameter -localAuth ( ENABLED | DISABLED ) -minpasswordlen
<positive_integer> -natPcbForceFlushLimit <positive_integer> -natPcbRstOnTimeout (
ENABLED | DISABLED )
-strongpassword ( ENABLED | DISABLED ) -promptString <string> -rbaOnResponse (
ENABLED | DISABLED ) -timeout <secs>
```

In deployments where multiple administrators are required, consider using an external authentication method to authenticate users, for example RADIUS, TACACS+, or LDAP(S).

Access the NetScaler Using SSH Keys and No Password
In deployments where there is a requirement to administer a large number of NetScaler appliances, consider using SSH Keys and No Password. For information on how to configure this feature, see the following article: Accessing a NetScaler by Using SSH Keys and No Password.

Create the system master key for data protection
From NetScaler 11.0 release, it is necessary to create a system master key to protect certain security parameters, such as service accounts passwords required for LDAP authentication and locally stored AAA User Accounts.

To create the system master key:

1. Using the command line interface, log in as a system administrator.
2. Enter the following command:
   ```
   > create kek <file name>
   ```

Note:

- After the create system kek command is executed, KEK is used for all password encryptions.
- You cannot delete the KEK file. If you have shell access and you delete the key fragment files by mistake, then this might result in configuration loss, synchronization failure, logon failure. Following are some of the points to note:
    - Always use an older configuration file matching to the build being installed when downgrading; else logon, source configuration, synchronization, failover might fail.
    - If any of the key fragment files are lost or corrupted, the encryption /decryption of sensitive data results in failure which might in turn result in configuration loss, synchronization failure, logon failure.
- The Pass Phrase must be at least 8 characters long.

Use Access Control Lists

By default, all protocols and ports, including GUI and SSH, are accessible on a NetScaler appliance. Access control lists (ACLs) can help you to manage the appliance securely by allowing only explicitly specified users to access ports and protocols.

Recommendations for controlling access to the appliance:

- Consider using NetScaler Gateway to limit access to the appliance to the GUI only. For administrators who require methods of access in addition to the GUI, the NetScaler Gateway should be configured with a default 'DENY' ACL for ports 80, 443, and 3010, but with an explicit 'ALLOW' for trusted IP addresses to access these ports.

  This policy can be extended for use with a range of trusted IP addresses with the following NSCLI command:

  ```
  > add acl local_access allow -srcip 192.168.0.1-192.168.0.3 -destip 192.168.0.1-
  192.168.0.3
  > apply acls
  ```

- If you use SNMP, explicitly allow SNMP traffic with ACL. Following is a set of sample commands:

  ```
  >add acl snmp1-ssh ALLOW -srcip 10.0.0.1-10.0.0.20 -destip 192.168.0.2-192.168.0.3 -
  destport 161 -protocol udp
  >add acl snmp2-ssh ALLOW -srcip 172.16.0.1-172.16.0.20 -destip 192.168.0.2-
  192.168.0.3 –destport 161 -protocol udp
  >apply acls
  ```

  In the preceding example, the command provides access for all SNMP queries to the two defined subnets, even if the queries are to the appropriately defined community.

  You can enable management functions on NSIP, SNIP, and MIP addresses. If any of these are enabled, provide access to the NSIP, SNIP, or MIP addresses with ACLs for protecting the access to the management functions. The administrator can also configure the appliance such that it is not accessible with the ping command.

- Open Shortest Path First (OSPF) and IPSEC are not a TCP or UDP based protocol. Therefore, if you need the appliance to support these protocols, explicitly allow the traffic using these protocols by using an ACL. Run the following command for defining an ACL to specify OSPF and IPSEC by protocol numbers:

  ```
  >add acl allow_ospf allow -protocolnumber 89
  >add acl allow_ipsec allow –protocolnumber 50
  ```

- If XML-API Web service is used, complete the following tasks to secure the API interface:
- Provide permission to the host for accessing the interface by using an ACL. For example, run the following commands to enable the hosts in the 10.0.0.1-20 and 172.16.0.1-20 IP address range to access the XML-API interface:

  ```
  > add acl xml-api1 ALLOW -srcip 10.0.0.1-10.0.0.20 -destip 192.168.0.2-192.168.0.3 -
  destport 80 -protocol tcp
  ```

```
> add acl xml-api2 ALLOW -srcip 172.16.0.1-172.16.0.20 -destip 192.168.0.2-
192.168.0.3 -destport 80 -protocol tcp
> apply acls
```

- Specify secure transport for the XML-API Web Service by configuring an HTTPS front-end server on the appliance with an appropriate responder policy. This is applicable to the appliance running NetScaler software release 8.0 or later. Following is a set of sample commands:

```
> enable ns feature responder
> add responder policy allow_soap 'HTTP.REQ.URL.STARTSWITH("/soap").NOT' RESET
> add lb vserver xml-https ssl 192.168.0.4 443
> add server localhost 127.0.0.1
> add service xml-service localhost HTTP 80
> bind lb vserver xml-https xml-service
> bind lb vserver xml-https -policyName allow_soap -type REQUEST -priority 1
> add ssl certkey xml-certificate -cert testcert.cert -key testcert.key
> bind ssl certkey xml-https xml-certificate
```

- You can achieve additional security by using a client-side certificate. For more information about client-side certificates and client authentication, see the SSL Offload and Acceleration > Configuring Client Authentication topic on Citrix Docs or Knowledge Center article CTX214874: "How to Create and Use Client Certificates on NetScaler Appliance with Firmware 10.1 and Above".

- If you use SNMP, explicitly allow SNMP traffic with ACL. Following is a set of sample commands:

```
>add acl snmp1-ssh ALLOW -srcip 10.0.0.1-10.0.0.20 -destip 192.168.0.2-192.168.0.3 -
destport 161 -protocol udp
>add acl snmp2-ssh ALLOW -srcip 172.16.0.1-172.16.0.20 -destip 192.168.0.2-
192.168.0.3 –destport 161 -protocol udp
>apply acls
```

  In the preceding example, the command provides access for all SNMP queries to the two defined subnets, even if the queries are to the appropriately defined community.
  You can enable management functions on SIP, SNIP, and MIP addresses. If any of these are enabled, provide access to the SIP, SNIP, or MIP addresses with ACLs for protecting the access to the management functions. The administrator can also configure the appliance such that it is not accessible with the ping command.

- Open Shortest Path First (OSPF) and IPSEC are not TCP or UDP based protocols. Therefore, if you need the appliance to support these protocols, explicitly allow the traffic using these protocols by using an ACL. Run the following command for defining an ACL to specify OSPF and IPSEC by protocol numbers:

```
> add acl allow_ospf allow -protocolnumber 89
> add acl allow_ipsec allow –protocolnumber 50
```

- Add the default deny action for NetScaler IP and MIP addresses. This ACL ensures that all ports and protocols are denied except those that are explicitly allowed in the list. You must add this ACL as the last ACL in the list. Do not put this ACL in the list until you have added all the ACLs that explicitly allow access to the protocols and ports. The default deny ACL should have low priority. Run the following command to add the default deny action:

```
> add acl default_deny deny –destip 192.168.0.1-192.168.0.3
> apply acls
```

- Use Role-Based Access Control for Administrative Users
  The NetScaler appliance includes four command policies or roles such as operator, read-only, network, and superuser. Additionally, you can define command policies, create different administration accounts for different roles, and assign the command policies that are necessary for the role to the accounts. The following is a set of sample commands to restrict read-only access to the read-only user:

  ```
  > add system user readonlyuser
  > bind system user readonlyuser read-only 0
  ```

  For further information on configuring users, user groups or command policies, see the Citrix Docs:

Configure system session timeout

A session timeout interval is provided to restrict the time duration for which a session (GUI, CLI, or API) remains active when not in use. For the NetScaler appliance, the system session timeout can be configured at the following levels:

- **User level timeout.** Applicable to the specific user.
  GUI: Navigate to **System > User Administration > Users**, select a user, and edit the user's timeout setting.
  CLI: At the command prompt, enter the following command:

  ```
  > set system user <name> -timeout <secs>
  ```

- **User group level timeout.** Applicable to all users in the group.

  GUI: Navigate to **System > User Administration > Groups**, select a group, and edit the group's timeout setting.
  CLI: At the command prompt, enter the following command:

  ```
  > set system group <groupName> -timeout <secs>
  ```

- **Global system timeout.** Applicable to all users and users from groups who do not have a timeout configured.

  GUI: Navigate to **System > Settings**, click **Set global system parameters**, and set the **ANY Client Idle Timeout (secs)** parameter.
  CLI: At the command prompt, enter the following command:

  ```
  > set system parameter -timeout <secs>
  ```

The timeout value specified for a user has the highest priority. If timeout is not configured for the user, the timeout configured for a member group is considered. If timeout is not specified for a group (or the user does not belong to a group), the globally configured timeout value is considered. If timeout is not configured at any level, the default value of 900 seconds is set as the system session timeout.

You can also restrict the timeout value so that the session timeout value cannot be configured beyond the timeout value configured by the administrator. You can restrict the timeout value between 5 minutes to 1 day. To restrict the timeout value:

- **GUI:** Navigate to **System > Settings**, click **Set global system parameters**, and select the **Restricted Timeout** field.
- **CLI:** At the command prompt, enter the following command:

  ```
  > set system parameter -restrictedtimeout <ENABLED/DISABLED>
  ```

After the user enables restrictedTimeout parameter, If the timeout value is already configured to a value larger than 1 day or less than 5 minutes, user will be notified to change the timeout value. If the user does not the change the timeout value then, by default, the timeout value will be reconfigured to 900 secs (15 minutes) during the next reboot.

Additionally, you can specify timeout durations for each of the interfaces you are accessing. However, the timeout value specified for a specific interface is restricted to the timeout value configured for the user that is accessing the interface. For example, consider a user "publicadmin" has a timeout value of 20 minutes. Now, when accessing an interface, the user must specify a timeout value that is within 20 minutes.

To configure the timeout duration at each interface:

- **CLI:** Specify the timeout value on the command prompt by using the following command:

```
> set cli mode -timeout <secs>
```

- **API:** Specify the timeout value in the login payload.

Logging and Monitoring

Configure NTP

Citrix recommends that Network Time Protocol (NTP) is enabled on the appliance and configured to use a trusted network time server. This ensures that times recorded for the log entries and system events are accurate and synchronized with other network resources.

When configuring NTP, the ntp.conf file must be modified to restrict the NTP server from disclosing the information in sensitive packets.

You can run the following commands to configure NTP on the appliance:

```
> add ntp server <IP_address> 10
> enable ntp sync
```

Modify the ntp.conf file for each trusted NTP server that you add. There should be a corresponding restrict entry for every server entry. You can locate the ntp.conf file by running the "**find . –name ntp.conf"** command from the appliance's shell prompt.

Configure SNMP

The NetScaler appliance supports version 3 of the SNMP protocol. SNMPv3 incorporates administration and security capabilities such as authentication, access control and data integrity checks. For more information, see System > SNMP topics on the Citrix Docs.

Note that, if you do not configure at least one SNMP manager, the appliance will accept and respond to SNMP queries from all IP addresses in the network. Run the following command to add an SNMP manager and restrict this behavior:

```
> add snmp manager <IP_address>
```

In deployments where SNMP is not required, the functionality should be disabled with the following command:

```
> set ns ip <IP_Address> -snmp disabled
```

Configure Logging to External NetScaler Log Host

The NetScaler Audit Server logs all states and status information collected by different modules in the kernel as well as in the user-level daemons. The Audit Server enables an administrator to refer to the event history in a chronological order.

The Audit Server is similar to the SYSLOG server that collects logs from the appliance. The Audit Server uses the nsroot credentials to fetch logs from the appliance(s).

- **Local Audit Server Configuration**
  Run the following command to configure logging to the local Audit Server in the NetScaler appliance:
  ```
  > set audit nslogparams –serverip <hostname> -serverport <port>
  ```

- **Remote Audit Server Configuration**
  To configure logging to the Audit Server in a remote computer, install the Audit Server on that computer. Following are sample Audit Server options:

  ./audserver -help
  usage : audserver -[cmds] [cmd arguments]
  cmds cmd arguments: -f <filename> -d debug
  -help - detail help
  -start - cmd arguements,[starts audit server]
  -stop - stop audit server
  -verify - cmd arguments [verifies config file]
  -addns - cmd arguments [add a netscaler to conf file]
  -version - prints the version info

  Note that this provides functionality for logging audit messages generated by the appliance's ns.log file only. To log all syslog messages, perform the following steps:

  1. Remove the log file specifications from the /nsconfig/syslog.conf file for the local facilities.
  2. Replace the log file specifications with the log host name or IP address of the remote syslog host, similar to the following entries:

     local0.* @10.100.3.53
     local1.* @10.100.3.53

  3. Configure the syslog server to accept log entries from the above logging facilities. To determine how to do this, see the syslog server documentation.
  4. For most UNIX-based servers using the standard syslog software, you must add a local facility configuration entry for the messages and nsvpn.log files to the syslog.conf configuration file. The facility values must correspond to those configured on the appliance.
  5. The remote syslog server in any UNIX-based computer by default does not listen for remote logs. Therefore, run the following command to start the remote syslog server:

     ```
     syslogd -m 0 –r
     ```

     Note: Refer to the equivalent options of the syslog variant that is deployed in the audit server.

LOM Configuration

Citrix strongly recommends that the following measures are taken to secure the LOM interface:

- Do not expose the LOM port to the Internet.
- Deploy the LOM behind an SPI firewall.
- Deploy the LOM onto a network segment that is separated either logically (separate VLAN) or physically (separate LAN) from untrusted network traffic.
- Set different user name, password, SSL-certificate and SSL-key values for the LOM and the NetScaler management ports.

- Ensure that devices used to access the LOM management interface are exclusively dedicated to a network-management purpose and placed on a management network segment that is in the same physical LAN or VLAN as other management device ports.
- To easily identify and isolate LOM IP addresses, reserve special IP addresses (private subnets) for LOM management interfaces and management servers. Do not use reserved IP subnets with LAN interfaces of the managed appliances. Dynamic IP addresses assigned by DHCP are not recommended, because they make it difficult to implement firewall Access Control Lists based on a MAC address outside of the LAN segment.
- Set the password for a minimum of 8 characters, with a combination of alphanumeric and special characters. Change the password frequently.

Applications and Services

Configure NetScaler to drop invalid HTTP requests
Citrix strongly recommends that the NetScaler appliance is configured with strict checking and enforcement of HTTP requests to prevent invalid HTTP requests passing through virtual servers. This can be done by binding an in-built HTTP profile, *nshttp_default_strict_validation*, to the virtual server(s) using the following command on the NSCLI:

```
> show ns httpProfile (Shows the available http profile (default+user configured
profiles))
> set lb vserver <vserver name> -httpProfileName nshttp_default_strict_validation
```

Citrix recommends that customers using this option test the changes in a staging environment before releasing it to production.

Configure protection against HTTP Denial of Service attacks
The NetScaler appliance firmware supports limited countermeasures against HTTP Denial of Service attacks, including 'slow-read' type attacks. You can configure these features by using the *nsapimgr* utility from the shell prompt of the appliance:

- small_window_threshold (default=1)
- small_window_idle_timeout (default=7 sec)
- small_window_cleanthresh (default=100)
- small_window_protection (default=Enabled)

The default settings are adequate for preventing the HTTP Denial of Service attacks, including slow-read attacks, however, some tuning of the parameters may be required for other attacks.

To protect against such attacks, adjust the *small_window_threshold* property upward by using the following *nsapimgr* command from the appliance's shell prompt:

```
$ nsapimgr -ys small_window_threshold=<desired value>
```

You can verify the protection against HTTP Denial of Service attacks by monitoring the following counters with `nsconmsg -d stats` command from the shell prompt of the appliance:

- nstcp_cur_zero_win_pcbs: This counter tracks the number of PCBs that currently have a low Window value.
- nstcp_err_conndrop_at_pass: This counter is incremented when the appliance detects that, while passing packets through from one side to other, it has exceeded the nscfg_small_window_idletimeout value.
- nstcp_err_conndrop_at_retx: This counter is incremented when the time that lapses during retransmission exceeds the nscfg_small_window_idletimeout value.
- nstcp_cur_pcbs_probed_withKA: This counter tracks the number of PCBs in the surge queue that are probed with a KA probe.

Citrix recommends that customers using this option test the changes in a staging environment before releasing it to production.

Configure NetScaler to defend against TCP spoofing attacks
The following commands can be used to help protect back-end servers against TCP spoofing attacks:

```
> set ns tcpProfile profile1 -rstWindowAttenuate ENABLED -spoofSynDrop ENABLED
 Done
> set lb vserver lbvserver1 -tcpProfileName profile1
 Done
```

Citrix recommends that customers using this option test the changes in a staging environment before releasing it to production.

Configure NetScaler to accept specific HTTP Headers
It is possible to configure NetScaler to accept only specific HTTP headers. This can be accomplished by adding a rewrite action to restrict network traffic with specific, defined HTTP headers from being passed to back-end server.

The following global rewrite action sends only network traffic with headers such as Host, Accept, and test to the server:

```
> add rewrite action act1 replace_all q/HTTP.REQ.FULL_HEADER.after_str("\r\n")/
q{TARGET.REGEX_SELECT(re/(iu)^(Host|Accept|test):.*\r\n/) ALT ""} -pattern
q{re/(U).+:.+r\n/}
> add rewrite policy pol1 HTTP.REQ.IS_VALID act1
> bind rewrite global pol1 100
```

Note: These commands are only supported in NetScaler release 10.5 and later.

Configuring Close Notify
A close-notify is a secure message that indicates the end of SSL data transmission. In compliance with RFC 5246: The client and the server must share knowledge that the connection is ending in order to avoid a truncation attack. Either party may initiate the exchange of closing messages. Either party may initiate a close by sending a close_notify alert. Any data received after a closure alert is ignored, unless some other fatal alert has been transmitted, each party is required to send a close_notify alert before closing the write side of the connection.

In order to ensure that audit events are captured for TLS termination events log on to the CLI as a *superuser* or *sysadmin* and execute the following commands:

```
> set ssl parameter -sendCloseNotify y
> save ns config
```

DNSSec Security Recommendations

Citrix recommends that the following recommendations are applied for customers using DNSSec:

Use RSA 1024 Bits or Higher for KSK/ZSK Private Keys
NIST recommends that DNS administrators maintain 1024-bit RSA/SHA-1 and/or RSA/SHA-256 ZSKs until 01 October, 2015.

Enable SNMP Alarm for DNSSEC Key Expiration
By default, the SNMP alarm for DNSSEC key expiration is enabled on a NetScaler appliance. The key expiry notification is sent through an SNMP trap called *dnskeyExpiry*. Three MIB variables, *dnskeyName, dnskeyTimeToExpire* and

dnskeyUnitsOfExpiry, are sent along with the *dnskeyExpiry* SNMP trap. For more information, see the Citrix NetScaler SNMP OID Reference.

Roll Over KSK/ZSK Private Keys before the x.509 Certificates Expire
On a NetScaler appliance, you can use the pre-publish and double signature methods to perform a rollover of the Zone Signing Key and Key Signing Key. For more information, see Domain Name System > Configuring DNSSEC topic on the Citrix Docs.

Secure DNSSec ADNS Server
If the appliance is configured in DNSSEC proxy mode, it caches the responses from the backend ADNS server and forwards the cached responses to the DNS clients.

When NetScaler is authoritative for a given zone, all the resource records in the zone are configured on the NetScaler. To sign the authoritative zone, you must create keys (the Zone Signing Key and the Key Signing Key) for the zone, add the keys to the ADC, and then sign the zone

To configure NetScaler as an authoritative server, perform the following steps:

1. Add an ADNS service.
   For example: `add service s1 <ip address> adns 53`

2. Create DNS keys.
   For example, to act as an authoritative server for "com" domain:
   ```
   create dns key -zoneName com -keytype ksK -algorithm rsASHA1 -keysize 3000 -
   fileNamePrefix com.ksk.rsasha1.3000
   create dns key -zoneName com -keytype zsk -algorithm rsASHA1 -keysize 3000 -
   fileNamePrefix com.zsk.rsasha1.3000
   ```

   Note: You have to create the DNS keys once and they are saved in /nsconfig/dns.

3. Add DNS keys.
   For example,
   ```
   add dns key com.zsk.3000 /nsconfig/dns/com.zsk.rsasha1.3000.key
   /nsconfig/dns/com.zsk.rsasha1.3000.private
   add dns key com.ksk.3000 /nsconfig/dns/com.ksk.rsasha1.3000.key
   /nsconfig/dns/com.ksk.rsasha1.3000.private
   ```

4. Add NS and SOA records for "com" zone and then sign the zone.
   ```
   add dns soaRec com -originServer n1.com -contact citrix
   add dns nsrec com n1.com
   add dns zone com -proxyMode no
   add dns addRec n1.com 1.1.1.1
   sign dns zone com
   ```

   Note: In addition, you must also enable the **DNSEC Extension** parameter in DNS global parameters.

For more information on configuring the NetScaler as an authoritative domain name server, see Domain Name System > Configuring the NetScaler as an ADNS Server topic on the Citrix Docs.

Legacy configuration

Configure NetScaler to disable SSLv2 redirect

If you enable the SSL v2 Redirect feature on a NetScaler appliance, the appliance performs the SSL handshake and redirects the client to the configured URL. If this feature is disabled, the appliance denies performing the SSL handshake process with SSL v2 clients.

Run the following command to disable the SSLv2 redirect:

```
> set ssl vserver <vserver_name> -sslv2redirect DISABLED -cipherredirect DISABLED
```

Note: Starting with NetScaler software release 9.2, SSLv2 redirect and cipher redirect features are disabled by default.

Configure NetScaler version 10.0 and earlier to use secure SSL renegotiation
To configure NetScaler to prevent non-secure SSL renegotiation for NetScaler software release 9.3e or 10.0, run the following command:

```
> set ssl parameter -denySSLReneg NONSECURE
```

For earlier releases of the NetScaler software, run the following command to disable SSL Renegotiation:

```
> set ssl parameter -denySSLReneg ALL
```

The following command allows renegotiation for secure clients and servers only:

```
> set ssl parameter -denySSLReneg NONSECURE
```

For more information, see Knowledge Center article CTX123680, "How to Configure and Use the -denySSLReneg Parameter."

NetScaler Cryptographic Recommendations

This section details a number of key steps that should be followed to ensure that cryptographic material is correctly secured on the NetScaler appliance. It also provides information on how to configure appliances to use this material to protect both the appliance itself, backend servers and end users.

Managing TLS Certificates and Keys:

Configuring TLS Cipher Suites for NDPP deployments
For the list of TLS cipher suites that are supported for NDPP deployments, see https://www.citrix.com/content/dam/citrix/en_us/documents/downloads/netscaler-adc/Common-criteria-documents-for-NetScaler-10.5.zip.

To ensure that only the approved cipher suites are configured on the appliance, complete the following configuration steps from the CLI:

1. Unbind all ciphers from the virtual server
   ```
   > unbind ssl vs v1 –cipherName FIPS
   ```

2. Bind only TLS1-AES-256-CBC-SHA and then TLS1-AES-128-CBC-SHA with the command:
   ```
   > bind ssl vs v1 –cipherName <cipher>
   > bind ssl vs v1 -cipherName TLS1-AES-256-CBC-SHA
   ```

Importing a Trusted Root CA Certificate

1. Using a secure file transfer utility, such as scp or WinSCP, transfer the server issuer (root) certificate to the /nsconfig/ssl directory of the NetScaler appliance.

   Note: You must authenticate as a super user through SCP or winSCP to complete this step.

2. Log on to the NetScaler appliance as a system administrator or super user and type the following command:
   ```
   > add ssl certkey <Certificate_Name> –cert <Cert_File_Name>
   ```

Note: Only install root CA certificates from certificate authorities that are known to be trustworthy. You must remove all other certificates.

- **Importing a PKCS#12 (.PFX) Certificate and Key File**
  Detailed information on how certificate and key files can be imported into the NetScaler appliance can be found in SSL Offload and Acceleration > Importing Existing Certificates and Keys topics on the Citrix Docs.

1. Transfer the .pfx file to the /nsconfig/ssl directory, as mentioned in *step 1* in the preceding section.
2. Authenticate to the NetScaler appliance through the CLI as a *sysadmin* or *superuser* and execute the following command:
   ```
   > convert ssl pkcs12 Cert-Client-1.pfx -export -certFile Cert-Client-1 -keyFile Key-Client-1
   ```
3. Add the certificate to the NetScaler appliance as follows:
   ```
   > add ssl certkey Clent-Cert-1 –cert Cert-Client-1
   ```
4. Save the current configuration.
   ```
   > save ns config
   ```

Note: From NetScaler 11.0 release onwards, the PKCS#12 (.PFX) file is automatically converted to PEM and all the certificates are added and linked to the CA automatically.

Installing Certificates and Key Pairs Using a Trusted CA

To obtain a certificate from a public or enterprise certificate authority (CA) you must first generate a private key and certificate signing request (CSR). This is done as follows:

1. Authenticate to the NetScaler CLI as a *sysadmin* or *superuser*.
2. Create an RSA private key.
   ```
   > create fipsKey m1 -modulus 2048
   ```
3. Create the certificate signing request (CSR):
   ```
   > create certreq csr_1 -fipsKeyName m1 -countryName IN -stateName BA -organizationName citrix
   ```
4. Submit the CSR to the CA.
   For most commercial and enterprise CAs, this is usually done in an email request. However, the method of submission may vary across enterprise CA environments. The CA returns a valid certificate by email, but this too may vary among enterprise CAs. After you receive the certificate from the CA, securely copy it to the /nsconfig/ssl directory.

   Log in as a *superuser* or *sysadmin* and run the following command from the CLI:
   ```
   > add ssl certKey ck_1 -cert cert1_1 -fipsKey m1
   ```

NetScaler-FIPS Recommendations

Configuring NetScaler SDX in a FIPS-based Deployment
If you are an existing FIPS customer and using a NetScaler SDX appliance for true multitenancy, use the FIPS certified NetScaler MPX appliance for terminating TLS and forwarding traffic to the NetScaler SDX appliance. Alternatively, it is possible to use a Thales external HSM.

Change FIPS crypto card passwords
When using a FIPS certified version of NetScaler with a Hardware Security Module (HSM), change the default Security officer (SO) and set a new user password as shown below. If you don't know the default SO password of an FIPS-enabled NetScaler appliance, contact Citrix Technical Support.

Note: Only a super user or sysadmin can carry out this task.

```
> set ssl fips -initHSM Level-2 <soPassword> <oldSoPassword> <user-Password> [-
hsmLabel <string>]
> save configuration
> initHSM
```

FIPS initialization level. The appliance currently supports Level-2 (FIPS 140-2).
This is a mandatory argument.
Possible values: Level-2
hsmLabel
Label to identify the Hardware Security Module (HSM).
Maximum Length: 31

Note: All data on the FIPS card will be erased with the above command.

Store the HSM password in a secure location
The password to the HSM should be stored in a secure location in accordance with your company's operating procedures.

Note: The HSM is locked after three unsuccessful login attempts. When locked, it becomes nonoperational and you cannot alter its configuration.

Additional Features: App Firewall and Gateway

This section provides examples of configuration changes that can be applied to both the Application Firewall and NetScaler Gateway to improve the security of the deployed appliances. This section also contains information on building multiple tiers or security.

Application Firewall Security Recommendations

Deploy the Appliance in the Two-Arm Mode
With a two-arm mode installation, the appliance is physically located between the users and web servers that the appliance protects. Connections must pass through the appliance. This arrangement minimizes the chances of finding a route around the appliance.

Use a 'Default Deny' policy
Citrix recommends that administrators configure the Application Firewall with a deny all policy at the global level to block all requests that do not match an Application Firewall policy. The following is a sample set of commands to configure a 'deny all' policy at the global level:

```
> add appfw profile default_deny_profile –defaults advanced
```

```
> add appfw policy default_deny_policy NS_TRUE default_deny_profile
> bind appfw global default_deny_policy <PRIORITY>
```

Note: The PRIORITY setting should ensure that the default policy gets evaluated last (only if the request does not match any other configured policies).

NetScaler software release 9.2 includes default profiles, such as appfw_block, which when configured block requests that do not match the Application Firewall policies. Run the following command to set the default profile:

```
> set appfw settings -defaultProfile appfw_block
```

Application Firewall – Building Multiple Tiers of Security

The following guidelines help you build multiple tiers of security depending on your environment and the applications that are supported.

First tier of security
To build the first tier of security, perform the following:

- Enable Buffer Overflow, SQL injection, and Cross Site scripting.
- Start URL is needed when the application is very particular on which URLs need to be accessed and have to protect against forceful browsing.
- Enable Field Format Checks if your application is expecting inputs in a form field.
  XSS check could generate false positives as many companies have a large installed base of JavaScript-enhanced web content that violates the same origin rule. If you enable the HTML Cross-Site Scripting check on such a site, you have to generate the appropriate exceptions so that the check does not block legitimate activity.

It is recommended to roll out the first tier, look for false positives, deploy the exceptions and then move on to the next tier. A staged implementation helps in managing the AppFw deployment.

Second tier of security
To build the second tier of security, perform the following:

Enable Signatures on the profile in addition to Buffer Overflow, SQL injection, and Cross Site scripting. There are 1300 + signatures. Try to enable only those signatures that are applicable for protecting your application, rather than enabling all signature rules.

It is recommended to roll out the second tier, look for false positives, deploy the exceptions and then move on to the next tier. A staged implementation helps in managing the Application Firewall deployment.

Third tier of security
To build the third tier of security, perform the following:

- Based on the application needs, enable Advanced Profile Security checks like CSRF tagging, Cookie Consistency. Form Field consistency on parts of applications that need it.
- Advanced security checks require more processing and can affect performance. Unless your application needs advanced security, you might want to start with a basic profile and tighten the security as required for your application.

The security checks disabled in the basic Application Firewall profile all operate on objects in the HTTP response. Therefore, these security checks are more resource intensive. When the Application Firewall performs response side

protections, it needs to remember information sent to each individual client. For example, if a form is protected by the Application Firewall, form field information sent in the response is retained in memory. When the client submits the form in the next subsequent request, it is checked for inconsistencies before the information is sent to the Web Server. This concept is referred to as Sessionization. Security checks such as URL Enclosure within Start URL, Cookie Consistency, Form Field Consistency, and CSRF Form Tagging all imply Sessionization. The amount of CPU and memory resources utilized by these security checks increments linearly with the number of requests sent through the Application Firewall.

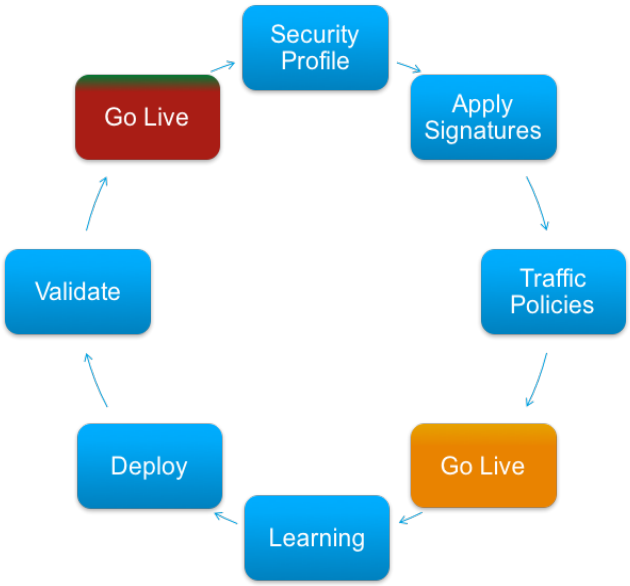
For example:

- **Enable Form Field Consistency check**: This check is required to verify if the web forms were not modified inappropriately by the client. An application that serves and hosts critical information in forms would need the check.

- **CSRF Form tagging check**: This is another check for forms. The Cross Site Request Forgery (CSRF) Form Tagging check tags each web form sent by a protected web site to users with a unique and unpredictable FormID, and then examines the web forms returned by users to ensure that the supplied FormID is correct. This check protects against cross-site request forgery attacks. This check needs to be enabled if application has web based forms. This check requires relatively little CPU processing capacity compared to certain other security checks that analyze web forms in depth. It is therefore able to handle high volume attacks without seriously degrading the performance of the protected web site or the application firewall itself.

Application Firewall Workflow Steps

The following diagram illustrates the Application Firewall workflow steps:



The following are the high-level steps involved in the Application Firewall Workflow:

1. Configure the security profile.
2. Apply signatures for all known threats - the negative model.
3. Configure traffic policies that can detect the correct traffic flow where this security profile needs to be activated. You are ready for the production traffic to pass-through the system. First level of flow is completed. Further, configure the learning infrastructure. Many times, customers want to do learning in production traffic thus having the signatures applied will avoid any risk. Perform the following steps:

a. Configure the learning infrastructure.
b. Deploy the learnt rules for protection.
c. Validate the learning data along with the signatures applied before going live.

NetScaler Gateway Security Recommendations

Use a 'Default Deny' policy
Citrix recommends that administrators configure the NetScaler Gateway with a 'deny all' policy at the global level, in addition to the use of authorization policies to selectively enable access to resources on a group basis.

By default, the defaultAuthorizationAction parameter is set to DENY. Verify this setting and grant explicit access to each user. You can use the `show defaultAuthorizationAction` command on the CLI to verify the setting. To set the parameter to deny all resources at the global level, run the following command from the CLI:

```
> set vpn parameter -defaultAuthorizationAction DENY
```

Use TLS1.1/1.2 Communication Between Servers
Citrix strongly recommends that TLS1.1/1.2 is used for the links between NetScaler Gateway appliance and other services, such as LDAP and Web Interface servers.
The use of older versions of this protocol, 1.0, and SSLv3 and earlier is not recommended.

Use the 'Intranet Applications' feature
Use Intranet Applications to define which networks are intercepted by the NetScaler Gateway plug-in and sent to the gateway. Following is a sample set commands to define interception:

```
> add vpn intranetApplication intra1 ANY 10.217.0.0 -netmask 255.255.0.0 -destPort 1-
65535 -interception TRANSPARENT
> bind vpn vserver v1 –intranetapp intra1
```

Additional Information Resources

See the following resources for additional security information about the NetScaler and NetScaler Gateway appliances:

- Citrix Security Portal: http://www.citrix.com/security
- NetScaler Documentation, including documentation for NetScaler Application Firewall and NetScaler Gateway http://docs.citrix.com/en-us/netscaler.html

For further assistance with configuration of your Citrix NetScaler, you can submit a support request at: https://www.citrix.com/support.html