Citrix Systems, Inc.

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

NetScaler 9.3-10.5
V6

November 2014

CiTRIX®

Copyright and Trademark Notice and Disclaimers

ALTHOUGH THE MATERIAL PRESENTED IN THIS DOCUMENT IS BELIEVED TO BE ACCURATE, IT IS PRESENTED WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED. USERS MUST TAKE ALL RESPONSIBILITY FOR THE USE OR APPLICATION OF THE PRODUCT(S) DESCRIBED IN THIS MANUAL. THE EXCLUSIVE PRODUCT WARRANTIES ARE SET FORTH IN THE RELEVANT PRODUCT DOCUMENTATION AS DELIVERED WITH THE PRODUCT(S).

CITRIX SYSTEMS, INC. OR ITS SUPPLIERS DO NOT ASSUME ANY LIABILITY THAT MAY OCCUR DUE TO THE USE OR APPLICATION OF THE PRODUCT(S) DESCRIBED IN THIS DOCUMENT. INFORMATION IN THIS DOCUMENT IS SUBJECT TO CHANGE WITHOUT NOTICE. COMPANIES, NAMES, AND DATA USED IN EXAMPLES ARE FICTITIOUS UNLESS OTHERWISE NOTED.

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, 2013

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 the following security considerations:

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

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 security requirements.

Deployment Guidelines

In addition to the recommendations for physical security, appliance security, network security, and administration and management, consider the Citrix recommendations for NetScaler FIPS, NetScaler Gateway Enterprise Edition security, application firewall security, and DNSSEC security.

Physical Security

For physical security, deploy a NetScaler appliance in a secure server room and protect the front panel, console port, and power supply.

Deploy NetScaler Appliance in Secure Server Room—The appliance should be placed in the secure server room, which protects the appliance from unauthorized access. At the minimum, access to the server room should be controlled by an electronic card reader. The server room should be monitored by CCTV that continuously records the activity of the room for audits. In the event of a break-in to the server room, the electronic surveillance system should send an alarm to the security personnel for immediate response. For additional protection, consider upgrading to a FIPS 140-2 Level 2 compliant MPX appliance. The FIPS platform uses a hardware security module to protect critical cryptographic keys in the appliance from unauthorized access.

Protect Front Panel and Console Port from Unauthorized Access—Secure the appliance in a locked cage or rack with physical-key access control.
Protect Power Supply—Make sure that the appliance is protected with an uninterruptable power supply (UPS).

Appliance Security

For appliance security, secure the operating system of any server hosting a NetScaler VPX appliance, perform remote software updates, and follow secure lifecycle management practices:

Secure the Operating System of Server Hosting a NetScaler VPX Appliance—A NetScaler VPX appliance runs as a virtual appliance on a standard server. You should protect the access to the standard server with role based access control and strong password management. Additionally, you should periodically update the server with the latest security patch for the operating system, and deploy up-to-date antivirus software on the server.

Perform Remote Software Updates—Install all security updates to resolve any known issue. When you update the NetScaler software, use a secure protocol, such as SFTP or HTTPS. Refer to the Security Bulletins web page to sign up for receiving security alerts.

Follow Secure Lifecycle Management Practices—To manage an appliance when redeploying, initiating RMA, and decommissioning sensitive data, complete the data-reminisce countermeasures by removing the persistent data from the appliance.

Network Security

For network security, do not use the NetScaler default SSL certificate. Use Transport Layer Security (TLS) when accessing the administrator interface, protect the appliance's non-routable management IP address, configure a high availability setup, use a stateful firewall, and implement other safeguards as appropriate for your deployment. SSH forwarding is not required. You can disable it.

Also consider using Citrix OpenCloud Access.

Do not use the NetScaler Default SSL Certificate—During the pilot installation, he NetScaler appliance uses the default certificate for SSL with the administrator and NetScaler SDX administrator graphical user interface (GUI). After the pilot configuration, do not use the default certificates. They are not intended for production deployment. Configure the NetScaler appliance either to use certificates from a reputable Certificate Authority or with custom certificates with your own private and public SSL key pairs. Do not use the default certificates for any Internet-facing web application or for accessing the administrator GUI and/or SDX administrator GUI. Create and use custom SSL certificates and private keys. To create a custom certificate, expand the SSL tab in the Navigation Pane of the GUI and launch the Create Certificate Wizard.

An SSL certificate from a reputable Certificate Authority simplifies the user experience for Internet-facing Web applications. Unlike the situation with a self-signed certificate or a certificate from a private Certificate Authority, web browsers do not require users to install the certificate from the reputable Certificate Authority to initiate secure communication with the Web server. To replace the default NetScaler certificate with a trusted Certificate Authority 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."

Use Transport Layer Security when Accessing Administrator Interface—Using Transport Layer Security with encryption protects the access to the administrator interface and GUI. Do the following:

- Use HTTPS to access the GUI management interface.
- Create a 2048-bit RSA private and public key pair and use the keys for HTTPS and SSH to access NetScaler IP address, instead of using the factory provisioned 512-bit RSA private and public key pair.
- Configure the appliance to use only strong Cipher Suites. Use the list of approved TLS CipherSuites in table 3 of NIST Special Publication 800-52 as a guidance. You should always change the default set of cipher suites, if possible.
- 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."
- Disable the HTTP access to the GUI management interface. To do so, run the following command:

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

Use and Protect a Non-routable Management IP Address—Make sure that the management IP address is not accessible from the Internet and is secured by a firewall.

Configure a High Availability Setup—Deploy NetScaler appliances in a high availability setup. Such a setup provides continued operation if one of the appliances stops functioning or requires an offline upgrade.

Configure Network Security Domains—When deploying in two-arm mode, dedicate a specific port to a specific network. If VLAN tagging and binding two networks to one port is required, the two networks should have the same or similar security levels. If the two networks have different security levels, do not use a tag. Instead, dedicate a port for each specific network and use independent VLANs distributed over the ports on the appliance. Tagged VLANs are not supported by a NetScaler VPX appliance.

Disable HTTP access to the Administrator Interface—Run the following command to disable the HTTP access to the NetScaler administrator interface:

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

If NTP is not used, use the following command to close the NTP port 123:

```
> disable ntp sync
```

Secure Cluster Deployment—Use secure RPC for Node to Node Messaging (NNM), AppNNM, and high availability setup. This is highly recommended if NetScaler cluster nodes are distributed outside the data center. Enabling secure RPC might significantly affect the performance of a NetScaler appliance. Therefore, you must carefully plan and verify secure RPC for a NetScaler Cluster. 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
```

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

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

Use Stateful Firewall Protection—Deploy the NetScaler appliance behind a stateful firewall application.

SDX in FIPS based Deployment—If you are an existing FIPS customer and have to use NetScaler SDX appliance for true multitenancy, use the FIPS certified NetScaler MPX appliance for terminating SSL and forwarding traffic to the NetScaler SDX appliance.

Disable SSH Port Forwarding—SSH Port Forwarding does not have to be enabled on NetScaler Appliance. To disable it:

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

LOM—Citrix recommends that, before reconfiguring the LOM, you perform a factory reset of the LOM to restore the factory 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, see http://support.citrix.com/proddocs/topic/netscaler-hrdwre-installation-10-5/ns-hardware-lom-intro-wrapper-con.html.

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

Administration and Management

For secure administration and management:

- Create an alternative superuser account
- Change the default password for the nsroot superuser and nsrecover user accounts
- Change the default user account password for the NetScaler SDX appliance,
- Follow best practices for configuring a NetScaler appliance
- Use access control lists (ACLs)
- Use secure transport for the XML-API Web Service, consider using a client-side certificate
- Use role-based access control for administrative users
- Set up secure communication between peer appliances
- Configure logging to an external NetScaler log host
- Add snmp managers
- Use SNMP v3 security features
- Configure NTP
- Restrict information packets from the remote NTP host
- Disable SSLv2 redirect
- Drop invalid http requests
- Protect against HTTP denial of service attacks
- Use secure SSL Renegotiation, whitelist HTTP headers
- Disable Layer 3 mode, consider using the NetScaler built-in application firewall
- Access the NetScaler by using SSH keys and no password
- Configure system session timeout
- Enable the NetScaler to defend TCP against spoof attacks.
- Change FIPS crypto card passwords
- Store the HSM password in a secure location.

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

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

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

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**.

Change the Default User Account Password for NetScaler SDX Appliance—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 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 default user.
5. Select **Modify**.
6. Type the required password in the **Password** and **Confirm Password** fields.
7. Click **OK**.

Follow Best Practices for Configuring a NetScaler Appliance—See Knowledge Center article CTX121149, “Recommended Settings and Best Practices for a Generic Implementation of a NetScaler Appliance.”

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. Consider the following recommendations for controlling access to the appliance:

- Use NetScaler Gateway Enterprise Edition to allow only GUI access to the appliance. For administrators who do not want to access the GUI through an NetScaler Gateway Enterprise Edition appliance, configure a default deny ACL for ports 80, 443, and 3010. Then, explicitly allow trusted IP addresses to access these ports.
  - Allow access to the appliance’s NetScaler IP (NSIP) address from only a specific set of IP addresses. Run the following commands to enable a range of IP addresses to access the NetScaler IP address:

```
> 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 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, see Knowledge Center article CTX128674, "NetScaler Application Security Guide."

- 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 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
```

- 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 more information about the Role-Based Access Control of the appliance, refer to CTX128667 - Citrix NetScaler Administration Guide.

Set up Secure Communication Between Peer Appliances—If you have configured NetScaler appliances in a high availability setup 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.

NetScaler features can also use SSH key based authentication for internal communication when the internal user is disabled (by using the **set ns config -internaluserlogin disabled** command). 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 config -internaluserlogin disabled** command)**.**

Configure Other Accounts Remotely—Consider configuring externally authenticated administrative accounts to use RADIUS, TACACS+, or LDAP(S).

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 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
  ```

  See Knowledge Center article CTX112893, “Installation and Configuration Guide,” for remote side configuration on various operating systems, such as Windows and Linux. This works only for logging audit messages generated by the appliance’s ns.log file. To log all syslog messages, perform the following procedure:

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.

Add SNMP Managers—If you do not configure at least one SNMP manager, the appliance accepts and responds to SNMP queries from all IP addresses in the network. Run the following command to add an SNMP manager:

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

If you want to disable an SNMP Manager, run the following command:

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

Use SNMP v3 Security Features—The NetScaler appliance supports SNMP protocol version 3. SNMPv3 incorporates administration and security capabilities such as authentication, access control, and data integrity checks.

Note: For more information about SNMP v3 security features, see Knowledge Center article CTX121813, “NetScaler Administration Guide.”

Configure NTP—Configuring Network Time Protocol (NTP) on the appliance ensures that times recorded for the log entries and system events are accurate, assuming that the time server is also secured. When you configure NTP, modify the ntp.conf file 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 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.

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.

Drop Invalid HTTP Requests—For increased availability of the back-end servers, consider allowing only valid HTTP requests to reach them. To do so, run the following command:

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

Protect Against HTTP Denial of Service Attacks—The NetScaler appliance supports countermeasures against HTTP Denial of Service attacks, including the latest slow-read attack. 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 generally adequate for preventing the HTTP Denial of Service attacks, including the slow-read attacks. If a malicious client sends a window with a maximum segment size (MSS) value of 1 or greater and slowly reads the response data, the NetScaler appliance treats the client as a legitimate client. To protect against such an attack, 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 elapses 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.

Use Secure SSL Renegotiation—To specify 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.”

Whitelist HTTP Headers—Consider adding the rewrite action such that only network traffic with certain headers is sent to the server. For example, the following 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
```

Disable Layer 3 Mode—If you do not use IP forwarding feature, un the following command to disable L3 mode:

```
> disable ns mode L3
```

Consider Using the Application Firewall on a NetScaler Platinum Edition Appliance—A NetScaler platinum edition 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.

LOM—In the LOM GUI, do the following:

- 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.

Access the NetScaler by Using SSH Keys and No Password—If you administer a large number of NetScaler appliances, storing and looking up passwords for logging on to individual appliances can be cumbersome. To avoid being prompted for passwords, you can set up secure shell access with public key encryption on each appliance. For more information, see Accessing a NetScaler by Using SSH Keys and No Password.

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, 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 Time-out (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 and 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, let us consider a user "publicadmin" who 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.

Defend against TCP spoofing attacks—Enable NetScaler to defend against TCP spoof attacks. Use the following commands:

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

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

NetScaler-FIPS Recommendations

Change FIPS crypto card password and store the Hardware Security Module (HSM) password in a secure location:
Change FIPS Crypto Card Passwords—If you are using a FIPS certified version of the NetScaler appliance with an HSM, change the default Security Officer (SO) password. Run the following command to set a new SO password:

```
> set ssl fips -initHSM Level-2
Enter soPassword:
Enter oldSoPassword:
Enter userPassword:
> save config
```

Note: The preceding command erases all data on the FIPS card.

Store the HSM Password in a Secure Location—The HSM module of the appliance is locked after three unsuccessful login attempts. After the HSM module is locked, the appliance ceases to operate, and you cannot alter its configuration. To avoid such a condition, store the HSM password in a secure location.

NetScaler Gateway Enterprise Edition Security Recommendations

To secure an NetScaler Gateway Enterprise Edition appliance, use Default Deny, use SSL communication between servers, and use Intranet application feature:

Use Default Deny—Consider denying all resources at the global level and using 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 each user. You can use the show defaultAuthorizationAction command to verify the setting. To set the parameter to deny all resources at the global level, run the following command:

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

Use SSLv3/TLS Communication Between Servers—Use SSLv3/TLS for the links between NetScaler Gateway Enterprise Edition appliance and other services, such as LDAP and Web interface servers.

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
```

Application Firewall Security Recommendations

Deploy the NetScaler appliance in the Two-Arm Mode and use Default Deny.

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 Default Deny—Consider configuring 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
```

DNSSec Security Recommendations

For DNSSec security, use RSA 1024 bits or higher for DNSSEC KSK/ZSK keys, enable SNMP alarm for DNSSEC key expiration, roll over the KSK/ZSK private keys before their x.509 certificates expire, and secure the ADNS server inside the corporate network if the NetScaler appliance is used in proxy mode.

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 Knowledge Center article CTX128676, “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 instructions, see Knowledge Center article CTX12870, “Citrix NetScaler Traffic Management Guide.”

Secure DNSSec ADNS Server—If the appliance is configured in DNSSEC proxy mode, it caches the responses from the back-end ADNS server and forwards the cached responses to the DNS Clients.

LOM Recommendations

Citrix recommends that you take the following measures for LOM security:

- Make the LOM port accessible from only an isolated network segment that is physically (separate LAN) or logically (separate VLAN) air gapped from untrusted networks (including the Internet)·
  The recommended best practice is to have three VLANs:
  - Outside Internet VLAN
  - Management VLAN
  - Inside server VLAN
- Make the LOM port part of the management VLAN used for management ports 0/1 and 0/2, because it also operates as a management port.
- Set different user-name, password, SSL-certificate, and SSL-key values for the LOM and the NetScaler management ports.
- Make sure 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.
- Deploy the LOM behind a stateful firewall application.
- Set the password for a minimum of 8 characters, with a combination of alphabetic, numeric, and special characters. Change the password frequently.
- Set the LOM IP address to a static IP address. Static IP addresses can be manually or automatically assigned by DHCP, based on the MAC addresses of the LOM. Automatic assignment of a static IP address by DHCP enables automatic configuration upon first bootup during initial commissioning. 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. Using a zero configuration, remotely scripted solution also reduces the attack-window time during first boot to about a couple of minutes.

More Information

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

- Citrix Security Site: http://www.citrix.com/security
- NetScaler Documentation: http://support.citrix.com/product/nsad/v10/#tab-doc
- Citrix Application Firewall Users Guide: http://support.citrix.com/article/CTX132360
- NetScaler Command Reference Guide: http://support.citrix.com/article/CTX132384

Additionally, you can submit your queries at: http://www.citrix.com/support.html