NetScaler secure deployment guide

Contents

Best practices for NetScaler MPX, VPX, and SDX security

July 4, 2024

NetScaler MPX is an application delivery controller that accelerates websites, provides L4-L7 traffic management, offers an integrated NetScaler Web App Firewall, and offloads servers. NetScaler VPX instance is a virtual appliance that has all the features of NetScaler MPX, runs on standard servers, and provides a higher availability for web applications including Citrix Virtual Apps and Desktops. NetScaler SDX 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. NetScaler also provides the seamless integration with Citrix OpenCloud Access that can extend the data center with the power of the Cloud.

To maintain security through the deployment lifecycle, we recommend you to review the following considerations for:

- 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 specific security requirements.

Additional information resources

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

- Security Portal
- Product Documentation

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

Deployment guidelines

August 20, 2024

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

Physical security best practices

Deploy the NetScaler appliance in a secure location

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

Other 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 must notify security personnel. If there is CCTV, the recorded footage is available for audit purposes.

Secure access to NetScaler front panel and console port

NetScaler or VPX hosting server must be deployed in a rack or cage that can be locked with a suitable key, or other physical methods. The locking prevents access to the physical ports of the NetScaler or, in a VPX deployment, the virtualization host console.

Power supply protection

NetScaler (or hosting server) must be protected with a suitable uninterruptible power supply. In the event of a power outage, the uninterruptible power supply ensures continued operation of NetScaler, or allows a controlled shutdown of a physical or virtual NetScaler. The use of an uninterruptible power supply also aids in the protection against power spikes.

Cryptographic key protection

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

NetScaler security best practice

Perform NetScaler software updates

We recommend that, before deployment, customers ensure that their NetScaler has been updated with the latest firmware versions. When carried out remotely, we recommend that customers use a

secure protocol, such as SFTP or HTTPS, to upgrade NetScaler.

Customers are also advised reviewing security bulletins that relate to their NetScaler products. For information about new and updated security bulletins, see the NetScaler Security Bulletins webpage https://support.citrix.com/knowledge-center/search#/ and consider signing up for alerts for new and updated bulletins https://support.citrix.com/user/alerts.

Secure the operating system of servers hosting NetScaler VPX

NetScaler VPX can run either a virtual appliance on a standard virtualization server or as a virtual appliance on NetScaler SDX.

In addition to applying normal physical security procedures, you must protect access to the virtualization host with a role-based access control and strong password management. Also, the server must be updated with the latest security patches for the operating system when they become available, and deploy an 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 must ensure that they are using the latest firmware version for their NetScaler SDX.

Reset the NetScaler lights out management (LOM)

We recommend 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 this 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 Lights out management port of the NetScaler MPX appliance.

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

   Also, we recommend 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**, and 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

If a NetScaler is redeployed to another environment, decommissioned, or returned under RMA, ensure that persistent data is correctly removed from NetScaler.

For more information about this process, see Wiping your data before sending the ADC appliance to Citrix.

Configuration guidelines

June 19, 2024

While configuring a NetScaler, consider the following configuration guidelines:

- Network security
- Securing the pass-through traffic on NetScaler

Network security

August 20, 2024

When deploying NetScaler in a production environment, we recommend that the following key configuration changes are made:

- Do not expose the NetScaler administrator interface (NSIP) to the Internet.
- The NetScaler default SSL certificate must be replaced.
- HTTPS (HTTP over TLS) must 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 the further changes that are recommended.

Key network security considerations

Do not expose the NSIP and Management Service IP address to the Internet:

We recommend that the NetScaler Management IP (NSIP) address and Management Service IP address of SDX 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 NetScaler, the default TLS certificates are created. These certificates are not intended for use in production deployments and must be replaced.

We recommend that customers configure NetScaler to use certificates either from a reputable Certificate Authority (CA) or appropriate certificates from your enterprise Certificate Authority.

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 host name of the appliance."

Alternatively, it is possible to create and use custom TLS certificates and private keys. While this action can provide an equivalent level of transport layer security, it requires the TLS certificates to be distributed to users and requires a 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, NetScaler must be configured to use HTTPS. Perform 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 the NetScaler IP address, replacing the factory provisioned 512-bit RSA private and public key pair.
- Configure NetScaler to use only strong cipher suites and change the 'DEFAULT'set of cipher suites to strong cipher suites on NetScaler. We recommend that you use the list of approved TLS Cipher suites in section 3.3 of NIST Special Publication 800-52 (Revision 1). 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 NetScaler 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 and the NetScaler product documentation: SSH key-based authentication for local system users
- 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.

Other network security considerations

Limit VPX shell access of VPX administrators who are not trusted to manage the SDX:

In situations where it is desirable to have a different person administer a VPX to that of the Management Service, the Management Service administrator must create a VPX admin user which has limited shell access on the VPX and only provide the restricted admin user account to the VPX administrator.

Some operations might require shell access (such as administering SSL certificates). However, only individuals who are trusted to administer the SVM must be granted access to the VPX instance shell. RBAC level commands, listed later in this section, can be assigned to those accounts. These recommendations are applicable for all SVM-IP/VPX-NSIP (L2/L3) management workflows and must be followed for secure access auditing purposes.

The following steps can be used to remove shell access from a VPX admin.

Securing an existing VPX instance:

1. Log in to the VPX CLI as `nsroot` or superuser.

   We recommend not to use the `nsroot` account and instead create a superuser account. When using the `nsroot` account, ensure that the passwords are strong with special characters. For details on strong passwords, see Administration and management.

   - Create a user and an RBAC policy in a VPX instance on NetScaler SDX.
   - Bind that user to the policy.

   ```
   > add system user userabc
   Enter password:
   Confirm password:
   Done
   ```



```
    > bind system user userabc superuser 2
    Done
    > add system cmdpolicy shell deny (shell)
    Done
    > bind system user userabc shell 1
    Done
```

> **Note:**
>
> In this example, the system `cmdpolicy` (ex: `cmdpolicy` name: shell) is created to deny shell access. This policy is bound to the user `userabc` with priority high. Default superuser `cmdpolicy` is also bound as lower priority to the system user. With this configuration, the new system user has superuser RBAC policies but shell access is denied.

2. Log in as the new system user and perform the following actions:

   - Verify that the current user has applied the RBAC policies.
   - Run any commands that the user is authorized to. (for example, `show system cmdpolicy`)
   - Run the `shell` command to verify that shell access is restricted.

   login as: `userabc`

   Pre-authentication banner message from server:

```
|
    ############################################################################

> ##
| #
>  #
| #        WARNING: Access to this system is for authorized users
    only
>  #
| #         Disconnect IMMEDIATELY if you are not an authorized
    user!
>  #
| #
>  #
|
    ############################################################################

> ##
|
End of banner message from server
Keyboard-interactive authentication prompts from server:
| Password:
End of keyboard-interactive prompts from server
Last login: Thu May 13 04:11:15 2021 from 10.10.1.1
Done
```



```
> whoami
    UserName:  userabc        LoggedIn:  "Thu May 13 04:18:50 2021
       "
Done
```

3. In the console of that VPX, log in as that user and make sure that the shell access is not allowed for this user:

```
> shell
ERROR: Not authorized to execute this command [shell]
```

4. Log in as regular admin user (`nsroot`) and make sure that shell access is allowed:

```
> shell
Copyright (c) 1992-2013 The FreeBSD Project.
Copyright (c) 1979, 1980, 1983, 1986, 1988, 1989, 1991, 1992,
   1993, 1994
The Regents of the University of California. All rights reserved.

root@Zela-40G-10#
```

Securing a new VPX instance:

1. When a new VPX instance is created from the Management Service GUI, create an INSTANCE ADMIN user, and clear the **Shell/SFTP/SCP Access** checkbox. On disabling shell access, `svm_access_policy` (action DENY) is bound explicitly to the specified instance admin user.
2. Provide this user information to the VPX admin. The SDX admin must retain this `nsroot` admin password and must not share it with the VPX admin.

> **Notes**:
>
> - To change the `nsroot` password, log on to Management Service, select the instance, and change the password. Never change the `nsroot` password from the VPX CLI.
> - For details about RBAC users, see User, user groups, and command policies.
> - For modifying the password of NetScaler from SVM, see Modify a NetScaler instance.
> - For provisioning NetScaler with instance administration, see Add a NetScaler instance.

Disable SSH port forwarding:

SSH port forwarding is not required by NetScaler. If you do not want to use this functionality, then we recommend that you disable it by 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 the `/nsconfig` directory to ensure that the changes are persistent in case you reboot during the tests.

3. Restart the `sshd` process by using the following command:

```
kill -HUP `cat /var/run/sshd.pid`
```

Configure NetScaler with high availability:

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

For information on how to configure a high availability setup, see Configuring high availability.

Set up secure communication between peer appliances:

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

To secure communication, we recommend that you change the internal user account or RPC node password, and enable the **Secure** option. RPC nodes are internal system entities used for system-to-system communication of configuration and session information.

NetScaler features can also use an SSH key-based authentication for internal communication when the internal user account is disabled. In such cases, the key name must be set as "ns_comm_key". For more information, see Access a NetScaler appliance by using SSH keys and no password.

Change the default passwords:

For enhanced security, we recommend that you change the administrator, and internal user account or RPC node passwords for both on-premises and cloud deployments. Frequently changing the passwords is advisable.

- Administrator password: See Change administrator password.
- Internal user account or RPC node password: See Change an RPC node password.

> **Note**
>
> We also recommend that you disable the internal user account and instead use the key-based authentication.

Configure network security domains and VLANs:

We recommend that network traffic to NetScaler 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

We recommend configuring the network to make the LOM port part of the management VLAN.

When deploying NetScaler 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 must ensure that the two networks have the same, or similar, security levels.

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

Consider using NetScaler Web App Firewall:
A Premium edition licensed NetScaler provides a built-in NetScaler Web App Firewall that uses a positive security model and automatically learns the proper application behavior for protection against threats such as command injection, SQL injection, and Cross Site Scripting.

When you use NetScaler Web App Firewall, users can add extra security to the web application without code changes and with minimal change in configuration. For more information, see Introduction to NetScaler Web Application Firewall.

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

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

Secure cluster deployment:
If NetScaler cluster nodes are distributed outside the data center, we recommend that you use secure RPC for Node to Node Messaging (NNM), AppNNM, and a high availability setup.

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

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

Note: Other configurations might be required. For more information, see the **Clustering** topics on the Product Documentation.

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 the exchange occurs over the internet, in the absence of an IPsec tunnel, the NSIPs are exposed on the internet, which is not recommended as it doesn't comply with the security best practices for NetScaler.

We recommend that customers establish their own IPsec solution to use the cluster over the 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 for GSLB, run the following command from the NSCLI:

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

Secure the load balancing persistence cookie:

We recommend encrypting the load balancing persistence cookie in addition to the SSL/TLS channel. For more information, see HTTP cookie persistence.

Helloverifyrequest parameter to mitigate the DTLS DDoS amplification attack:

Starting from NetScaler release 12.1 build 62.x and release 13.0 build 79.x, the `helloverifyrequest` parameter is enabled by default. Enabling the `helloverifyrequest` parameter on the DTLS profile helps mitigate the risk of an attacker or bots overwhelming the network throughput, potentially leading to outbound bandwidth exhaustion. That is, it helps mitigate the DTLS DDoS amplification attack.

To view the `helloverifyrequest` parameter status, at the CLI prompt, type:

```
show dtlsProfile
```

Securing the pass-through traffic on NetScaler

August 20, 2024

Infrastructure mode settings can be used to the secure pass-through traffic on NetScaler. 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
- 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 NetScaler is configured to proxy a connection. For example, when the flow selects a configured virtual server or service of type TCP or above, NetScaler creates a stateful session. NetScaler 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 NetScaler.

- 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 NetScaler or back-end server
NetScaler: Enabled by Default for the NetScaler inserted cookies, possible via Rewrite for cookies set by the back-end server.

HttpOnly: When you tag a cookie with the HttpOnly flag, it indicates to the browser that this cookie must be accessed only by the server. Any attempt to access the cookie from the client script is strictly forbidden. HttpOnly cookies, if properly implemented, makes huge classes of common cross-site scripting attacks much harder to pull off.

The following is an example of a cookie with the HttpOnly flag set:

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

The cookies inserted by NetScaler for Cookie Insert persistence, by default, set the HttpOnly flag to indicate that the cookie is nonscriptable and must 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 back-end server.

Note: Secure and HttpOnly cookies together can be done for SSL VIPs. For non-SSL VIPs one can 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 helps 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.

Create a rewrite policy by using the CLI

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=/)!)"

   or

   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
   ```


> **Note:**
>
> Starting from NetScaler release 13.1, the `bypassSafetyCheck` parameter is not applicable. However, for releases before 13.1, this parameter is supported.

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 virtual server to be secured (if the Secure option is used, an SSL virtual server must 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)):

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 the following topics.

- Configure support for HTTP strict transport security (HSTS).
- https://support.citrix.com/article/CTX205221

Strong authentication:

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

For details on how sensitive apps can be set up for multifactor authentication, see Multi-Factor (nFactor) authentication.

End-to-end SSL preferred:

It is recommended to have SSL both on the front end and back end. Older unsecure protocol versions, such as SSLv3, TLS 1.0, and TLS 1.1 can be disabled on SSL entities. You can only have TLS 1.2 and TLS 1.3 enabled. It can either be done at the SSL entity level or at the profile level and all the SSL entities inherit the SSL settings from the profile.

Disable unsecure and enable secure protocol versions on SSL entities by using the CLI

At the command prompt, type:

```
set ssl vserver <vServerName> -ssl2 DISABLED -ssl3 DISABLED -tls1
    DISABLED -tls11 DISABLED -tls12 ENABLED -tls13
    ENABLED

set ssl service <vServiceName> -ssl2 DISABLED -ssl3 DISABLED -tls1
    DISABLED -tls11 DISABLED -tls12 ENABLED -tls13
    ENABLED
```

If SSL profile is enabled, use the following command:

```
set ssl profile <frontend profile> -ssl3 DISABLED -tls1 DISABLED
    -tls11 DISABLED -tls12 ENABLED -tls13 ENABLED

set ssl profile <backend profile> -ssl3 DISABLED -tls1 DISABLED -
    tls11 DISABLED -tls12 ENABLED -tls13 ENABLED
```

> **Note:
>
> We recommend enabling TLS 1.3 using the profile instead of enabling it on virtual server entities. For more information, see Support for TLS 1.3 protocol.

NetScaler recommended cipher suites:

The following ciphers supported by NetScaler do not include any components on the "mandatory discard"list. These ciphers 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 Cipher suites:

- 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 Cipher suites:

- 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 Cipher suites:

- 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 Cipher suites in the order of preference:

The following list of ciphers includes 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

SSL secure profile and secure ciphers:

We recommend that you bind the secure front-end profile (ns_default_ssl_profile_secure_frontend) to your SSL virtual server. A secure cipher alias is added and bound to the secure front-end profile. To list the ciphers that are part of this alias, at the command prompt type:

```
show cipher SECURE

    1) Cipher Name: TLS1.2-ECDHE-RSA-AES256-GCM-SHA384 Priority : 1
           Description: TLS 1.2 Kx=ECC-DHE  Au=RSA  Enc=AES-GCM(256)
              Mac=AEAD   HexCode=0xc030
    2) Cipher Name: TLS1.2-ECDHE-RSA-AES128-GCM-SHA256 Priority : 2
```



```
            Description: TLS 1.2 Kx=ECC-DHE  Au=RSA  Enc=AES-GCM(128)
               Mac=AEAD   HexCode=0xc02f
     3) Cipher Name: TLS1.2-ECDHE-ECDSA-AES256-GCM-SHA384
        Priority : 3
            Description: TLS 1.2 Kx=ECC-DHE  Au=ECDSA Enc=AES-GCM(256)
               Mac=AEAD   HexCode=0xc02c
     4) Cipher Name: TLS1.2-ECDHE-ECDSA-AES128-GCM-SHA256
        Priority : 4
            Description: TLS 1.2 Kx=ECC-DHE  Au=ECDSA Enc=AES-GCM(128)
               Mac=AEAD   HexCode=0xc02b
Done
```

For more information about the secure front-end profile, see Secure front-end profile.

Protocols lower than TLS 1.2 are disabled on the SSL internal services. If the default (enhanced) profile is enabled, then the ns_default_ssl_profile_internal_frontend_service profile is bound to the SSL internal services and SSLv3, TLS 1.0, TLS 1.1, and TLS 1.3 protocols are disabled in the profile.

Proxy HTTPS / deny all other traffic:

Wherever feasible have SSL VIPs for better encryption of data, by using secure SSL versions (TLS 1.2 or TLS 1.3) and secure ciphers. The SSL TPS and SSL throughput must be considered while enabling SSL for the VIPs and back-end SSL services.

Administration and management

July 25, 2024

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

See the following topics for more information.

- System and user accounts
- Logging and monitoring
- LOM configuration
- Applications and services
- DNSSEC security recommendations
- Legacy configuration
- Configure NDCPP compliance certificate check

System and user accounts

August 20, 2024

Change password for the super user account:
You cannot delete the built-in administrator superuser (`nsroot`). Therefore, change the default password for that account to a secure password. To change the default password for the admin 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 `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 and its GUI management console after the initial setup. 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.

Strong password for system user:

We recommend using a strong password for system users accounts created in NetScaler. 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 -minpasswordlen <positive_integer> -
-strongpassword ( ENABLED | DISABLED )
```

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

Lock system user account for management access:
NetScaler enables you to lock a system user for 24 hours and deny access to the user. NetScaler supports the configuration for both system user and external users. At the command prompt type:

```
set aaa parameter –persistentLoginAttempts DISABLED
```

Now, to lock a user account, at the command prompt, type:

```
lock aaa user test
```

For information on how to configure this feature by using the GUI, see User account and password management.

Unlock a locked system user account for management access:
System users and external users can be locked for 24 hours using the lock authentication, authorization, and auditing user command. The NetScaler enables you to unlock the locked system user. At the command prompt, type:

```
unlock aaa user test
```

For information on how to configure this feature by using the GUI, see User account and password management.

Disable management access for system user account:
When external authentication is configured on NetScaler and as an admin that you prefer to deny access to system users to log on to management access, you must disable the localAuth option in the system parameter.

> **Note:**
>
> External server must be configured.

At the command prompt, type the following:

```
set system parameter localAuth <ENABLED|DISABLED>
```


Example:

```
set system parameter localAuth DISABLED
```

For information on how to configure this feature by using the GUI, see User account and password management.

Force password change for administrative users:

For `nsroot` secured authentication, NetScaler prompts the user to change the default password to a new one if the `forcePasswordChange` option is enabled in the system parameter. You can change your `nsroot` password either from CLI or GUI, on your first login with the default credentials. At the command prompt, type:

```
set system parameter -forcePasswordChange ( ENABLED | DISABLED )
```

For example of how to configure this feature, see User account and password management.

Access the NetScaler Using SSH Keys and No Password:

In deployments where there is a requirement to administer many NetScaler appliances, consider using SSH Keys and No Password. For information on how to configure this feature, see Access a NetScaler appliance by using SSH keys and no password.

Create the system main key for data protection: From Citrix ADC 12.1 to Citrix 13.0–71.44, it is necessary to create a system main key to protect certain security parameters, such as service accounts passwords required for the LDAP authentication and locally stored authentication, authorization, and auditing User Accounts.

> **Note:**
>
> From Citrix 13.0 build 76.31 and later, a random system main key is created by default automatically with the upgrade process. Ensure to update KEK frequently in accordance with the organization's password policy.

To create the system main key:

1. Using the CLI, log in as a system administrator.
2. Enter the following command:

```
1 create kek <passphrase>
```

Note:

- After the `create kek` command is run, KEK is used for most password encryptions (local user passwords do not get encrypted with KEK).
- You must not delete the KEK file. If you have shell access and you delete the key fragment files by mistake, it might result in configuration loss, synchronization failure, logon failure. Note the following.

  - 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.

Update key encryption key on a deployed NetScaler:

NetScaler supports updating the KEK on a deployed ADC. Use the following command to update the KEK.

```
update kek -level <basic | extended>
```

The update KEK command is supported only on the NSIP interface. The command supports the following two options.

- **Basic**: Backs up old keys, creates keys, and responds. If any of the file updates fail, the system reports an error and reverts to the original state.
- **Extended**: Backs up old keys and creates keys. Updates config files such as ns.conf and ns.conf.0 under the default and non-default partitions. During the update, blocks all configuration changes. After the update is done, NetScaler responds. If any of these file updates fail, the system reports an error and reverts to the original state.

Previously, NetScaler only supported the default per node KEK. There was no option to update the KEK.

As a security best practice, KEK must be changed frequently in accordance with the organization's password policy.

Use access control lists:

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

Recommendations for controlling access to NetScaler:

- Consider using NetScaler Gateway to limit access to NetScaler to the GUI only. For administrators who require methods of access in addition to the GUI, the NetScaler Gateway must 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 the 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. The 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 and SNIP addresses. If enabled, provide access to the NSIP, SNIP, addresses with ACLs for protecting the access to the management functions. The administrator can also configure NetScaler 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 NetScaler 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 an 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
```

- To apply ACLs for the internal ports, use the following command:


```
set l3param -implicitACLAllow DISABLED
```

> **Note:**
>
> The default value for the *implicitACLAllow* command is **ENABLED**.

- To remove ACLs from the internal ports, use the following command:

```
set l3param -implicitACLAllow ENABLED
```

- You can achieve extra security by using a client-side certificate. For more information about client-side certificates and client authentication, see Client authentication or Knowledge Center article CTX214874: How to Create and Use Client Certificates on NetScaler Appliance with Firmware 10.1 and Above.

Use role-based access control for administrative users:

NetScaler includes four command policies or roles such as operator, read-only, network, and superuser. You can also 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 the 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 User, user groups, and command policies.

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 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 a 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 a 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 parameter**s, 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 the restrictedTimeout parameter, and if the timeout value is already configured to a value larger than 1 day or less than 5 minutes, the user is 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.

You can also 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 timeout value of 20 minutes. Now, when accessing an interface, the user must specify the 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

August 20, 2024

Configure Network Time Protocol

We recommend that the Network Time Protocol (NTP) is enabled on NetScaler and configured to use a trusted network time server. Enabling NTP 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 NetScaler:

```
add ntp server <IP_address> 10

enable ntp sync
```

Modify the ntp.conf file for each trusted NTP server that you add. There must 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 NetScaler shell prompt.

Configure SNMP

NetScaler 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 Configuring NetScaler for SNMPv3 queries.

> **Note:**
>
> We recommend that you use SNMPv3 instead of SNMPv1 and SNMPv2.

If you do not configure at least one SNMP manager, NetScaler accepts and responds 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 must 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 and in the user-level daemons. The Audit Server enables an administrator to see the event history in a chronological order. The Audit Server is similar to the SYSLOG server that collects logs from NetScaler. The Audit Server uses the administrator credentials to fetch logs from one or more appliances.

- Local Audit Server Configuration

Run the following command to configure logging to the local Audit Server in NetScaler:

```
> 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. The following are the 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
```

These options provide functionality for logging audit messages generated by the NetScaler 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 preceding logging facilities. For more information, 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 values configured on NetScaler.
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: See the equivalent options of the syslog variant that is deployed in the audit server.

LOM configuration

June 19, 2024

We recommend 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 an 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 NetScaler. 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

August 20, 2024

Configure NetScaler to delete or pass the upgrade header

A new parameter `passProtocolUpgrade` is added to the HTTP profile to prevent attacks on the back-end servers. Depending on the state of this parameter, the upgrade header is passed in the request sent to the back-end or deleted before sending the request.

- If the `passProtocolUpgrade` parameter is enabled, then the upgrade header is passed to the back end. The server accepts the upgrade request and notifies it in its response.
- If this parameter is disabled, then the upgrade header is deleted and the remaining request is sent to the back end.

The `passProtocolUpgrade` parameter is added to the following profiles.

- nshttp_default_profile - enabled by default
- nshttp_default_strict_validation - disabled by default
- nshttp_default_internal_apps - disabled by default
- nshttp_default_http_quic_profile - enabled by default

We recommend that you set the `passProtocolUpgrade` parameter to disabled.

Set the `passProtocolUpgrade` parameter by using the CLI:

At the command prompt, type the following:

```
set ns httpProfile <name> [-passProtocolUpgrade ( ENABLED | DISABLED )]
```

Set the `passProtocolUpgrade` parameter by using the GUI:

1. Navigate to **System -> Profiles -> HTTP Profiles**.
2. Create or edit an HTTP profile.
3. Select the **Pass Protocol Upgrade** checkbox.

Configure NetScaler to drop invalid HTTP requests

We recommend that NetScaler is configured with strict checking and enforcement of HTTP requests to prevent invalid HTTP requests passing through virtual servers. To do so, bind an in-built HTTP profile, *nshttp_default_strict_validation*, to one or more virtual servers using the following command on the CLI:

```
1 show ns httpProfile (Shows the available http profile (default+user
      configured profiles))
2
3 set lb vserver <vserver name> -httpProfileName
      nshttp_default_strict_validation
```

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

Protection against the HTTP desync attacks is enabled by default on the strict HTTP validation profile (nshttp_default_strict_validation). Use the strict profile for all the client-facing entities.

For more information on HTTP request smuggling attacks and its mitigation, see the support article NetScaler - HTTP Request Smuggling Reference Guide.

Configure protection against HTTP Denial of Service attacks

The NetScaler 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 NetScaler shell prompt:

- 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 might 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 NetScaler shell prompt:

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

> **Note:**
>
> The `small_window_threshold` desired value can be set based on the incoming traffic pattern in the deployment. The acceptable range is from 0 to 2^32.

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

- 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 NetScaler detects that, while passing packets through from one side to the 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.

We recommend 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
```

We recommend 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 the 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 the 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
```

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 to avoid the truncation attack. Either party can initiate the exchange of closing messages 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. To ensure that audit events are captured for TLS termination events log on to the CLI as a superuser or sysadmin and run the following commands:

```
set ssl parameter -sendCloseNotify y

save ns config
```


Secure Management GUI, NITRO API, and RPC communication

To secure the management GUI, NITRO API, and RPC communication on NetScaler and NetScaler Gateway, the setting `maxclientForHttpdInternalService` is added in NetScaler. This setting is disabled by default. You must enable the parameter to secure the management GUI, NITRO API, and RPC communication.

It is also recommended that you set `maxclientForHttpdInternalService` to match the MaxClients value in /etc/httpd.conf by using the following shell command. The default value of MaxClients is 30.

```
1 nsapimgr_wr.sh -ys maxclientForHttpdInternalService=<val>
```

For more information on setting the `maxclientForHttpdInternalService` value and the NetScaler versions that support this setting, see https://support.citrix.com/article/CTX331588.

DNSSEC security recommendations

August 20, 2024

We recommend 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 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 NetScaler. The key expiry notification is sent through an SNMP trap called dnskeyExpiry. Three MIB variables, `dnskeyName`, and `dnskeyUnitsOfExpiry`, are sent along with the `dnskeyExpiry` SNMP trap. For more information, see the NetScaler SNMP OID Reference.

Roll over KSK/ZSK private keys before the x.509 certificate expires

On NetScaler, 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 the **Domain Name System > Configuring DNSSEC** topic on the NetScaler Docs.

Secure DNSSEC ADNS server

If NetScaler 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.

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

   ```
   create dns key -zoneName com -keytype ksK -algorithm rsASHA512 -
       keysize 3000 -fileNamePrefix com.ksk.rsasha1.3000

   create dns key -zoneName com -keytype zsk -algorithm rsASHA512 -
       keysize 3000 -fileNamePrefix com.zsk.rsasha1.3000
   ```

   > **Note:**
   >
   > You must 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 the 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 the DNS global parameters.

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

Legacy configuration

June 19, 2024

Configure NetScaler to disable SSLv2 redirect

If you enable the SSL v2 Redirect feature on NetScaler, it performs the SSL handshake and redirects the client to the configured URL. If this feature is disabled, NetScaler 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
```

Configure NetScaler to prevent non-secure SSL renegotiation

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 How to Configure and Use the -denySSLReneg Parameter.

Configure NDcPP compliance certificate check

July 5, 2024

NDcPP compliance certificate check applies when NetScaler acts as a client (back-end connection). During certificate verification, ignore the common name if SAN is present in the SSL certificate.

At the command prompt, type the following commands to configure the "ndcppComplianceCertCheck"attribute in the SSL parameter:


```
set ssl parameter [-quantumSize <quantumSize>] [-crlMemorySizeMB <
    positive_integer>] [-strictCAChecks (YES | NO)] [-sslTriggerTimeout
    <positive_integer>] [-sendCloseNotify (YES | NO)] [-
    encryptTriggerPktCount <positive_integer>] [-denySSLReneg <
    denySSLReneg>] [-insertionEncoding (Unicode|UTF-8)] [-ocspCacheSize
    <positive_integer>][- pushFlag <positive_integer>] [-
    dropReqWithNoHostHeader (YES | NO)] [-pushEncTriggerTimeout <
    positive_integer>] [-ndcppComplianceCertCheck ( YES | NO)] [-
    heterogeneousSSLHW (ENABLED | DISABLED )]
```

Example:

```
set ssl parameter -quantumSize 8 -crlMemorySizeMB 256 -strictCAChecks
    no -ssltriggerTimeout 100 -sendClosenotify no -
    encryptTriggerPktCount 45 -denySSLReneg NONSECURE -insertionEncoding
     unicode -ocspCacheSize 10 -pushFlag 3 -dropReqWithNoHostHeader YES
     -pushEncTriggerTimeout 100 ms -ndcppComplianceCertCheck YES
```

NetScaler cryptographic recommendations

August 20, 2024

This section details some key steps that must be followed to ensure that cryptographic material is correctly secured on the NetScaler. It also provides information on how to configure NetScaler to use this material to protect NetScaler, back-end servers, and end users.

Managing TLS certificates and keys

Configuring TLS cipher suites for FIPS and NDcPP deployments

The following TLS cipher suites are supported for FIPS and NDcPP deployments.

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

- TLS1.2-ECDHE-RSA-AES256-GCM-SHA384
- TLS1.2-ECDHE-RSA-AES128-GCM-SHA256
- TLS1.2-AES-256-SHA256
- TLS1.2-AES-128-SHA256
- TLS1-ECDHE-ECDSA-AES256-SHA
- TLS1-ECDHE-ECDSA-AES128-SHA
- TLS1.2-ECDHE-ECDSA-AES256-SHA384
- TLS1.2-ECDHE-ECDSA-AES128-SHA256
- TLS1.2-ECDHE-ECDSA-AES256-GCM-SHA384
- TLS1.2-ECDHE-ECDSA-AES128-GCM-SHA256
- TLS1.3-AES256-GCM-SHA384
- TLS1.3-AES128-GCM-SHA256

  For the list of ciphers supported on MPX 14000 FIPS, see https://docs.netscaler.com/en-us/citrix-adc/downloads/cipher-support-on-netscaler-mpx-sdx-14000-fips.pdf.

To ensure that only the approved cipher suites are configured on NetScaler, 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
```

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). Perform the following steps:

1. Authenticate to the NetScaler CLI as a sysadmin or superuser.
2. Create an RSA private key.

```
create fipsKey m1 -keytype RSA -modulus 2048 -exponent F4
```

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 Certificate Authority.

For most commercial and enterprise CAs, the CSR is sent in an email request. However, the method of submission can vary across enterprise CA environments. The CA returns a valid certificate by email, but this action too can 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 NetScaler SDX for true multitenancy, use the FIPS certified NetScaler MPX for terminating TLS and forwarding traffic to the NetScaler SDX. 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 follows. If you don't know the default SO password of a FIPS-enabled NetScaler, contact NetScaler 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. NetScaler currently supports Level-2 (FIPS 140-2).
This argument is mandatory.
Possible values: Level-2

hsmLabel

Label to identify the Hardware Security Module (HSM).

Maximum Length: 31

Note: All data on the FIPS card is erased with the preceding command.

Store the HSM password in a secure location

The password to the HSM must 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.

Other features

July 25, 2024

This section provides examples of configuration changes that can be applied to both the NetScaler Web App Firewall and NetScaler Gateway to improve the security of the deployed appliances and information on building multiple tiers or security. This section also contains information on configuration details when using NetScaler or NetScaler Gateway as SAML SP or SAML IdP or both.

See the following topics for more information.

- NetScaler Web App Firewall security recommendations
- NetScaler Gateway security recommendations

NetScaler Web App Firewall security recommendations

August 20, 2024

- For RFC compliance checks, it is recommended to keep 'APPFW_RFC_BLOCK'as the default `rfcprofile` for the WAF profile.
- WAF supports inserting `Samesite` cookie attribute value and the cookie can be restricted to the same-site or cross-site context by selecting 'Strict'or 'Lax'values.

Deploy NetScaler in the two-arm mode

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

Use a 'Default Deny'policy

We recommend that administrators configure NetScaler Web App Firewall with a deny all policy at the global level to block all requests that do not match a NetScaler Web App 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 true default_deny_profile

bind appfw global default_deny_policy <PRIORITY>
```

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

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

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

NetScaler Web App 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.

Configure a different value for the **sessionCookieName** parameter in each tier.

```
set appfw settings -sessionCookieName "citrix_ns_id_1"
```

First tier of security

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

- Enable Buffer Overflow, SQL injection, and Cross Site scripting.
- A start URL is needed when the application is particular on which URLs must be accessed and have to protect against forceful browsing.
- Enable Field Format Checks if your application is expecting inputs in a form field.

Cross-site scripting check might 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.

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, do 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.

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 NetScaler Web App Firewall deployment.

Third tier of security

To build the third tier of security, do 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 the 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 NetScaler Web App Firewall profile all operate on objects in the HTTP response. Therefore, these security checks are more resource intensive. When the NetScaler Web App Firewall performs response side protections, it needs to remember the information sent to each individual client. For example, if a form is protected by the NetScaler Web App 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 used by these security checks increments linearly with the number of requests sent through the NetScaler Web App 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 needs the check.

- CSRF Form tagging check: This check is for forms. The Cross Site Request Forgery (CSRF) Form Tagging check tags each web form sent by a protected website 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 must be enabled if the 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 website or the NetScaler Web App Firewall itself.

NetScaler Web App Firewall workflow steps

Perform the following steps in the NetScaler Web App 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 must be activated.

You are ready for the production traffic to pass-through the system. The 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 avoids any risk. Perform the following steps:

1. Configure the learning infrastructure.
2. Deploy the learned rules for protection.
3. Validate the learning data along with the signatures applied before going live.

NetScaler Gateway security recommendations

July 25, 2024

Use a 'Default Deny'policy

We recommend 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 the 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 TLS1.2 communication between servers

We recommend that TLS1.2 or TLS 1.3 be used for the links between NetScaler Gateway and other services, such as LDAP and Web Interface servers.
The use of older versions of this protocol, TLS 1.1, TLS 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. The following is a sample set of 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
```

Authentication, authorization, and auditing security recommendations

If a NetScaler or a NetScaler Gateway appliance is configured as SAML SP or SAML IdP or both, see the article https://support.citrix.com/article/CTX316577 for recommended configuration details.

For details about SAML authentication, see SAML authentication.

Enable encryption of NetScaler Gateway login information for nFactor authentication

A NetScaler Gateway appliance with nFactor authentication can encrypt the login request fields submitted by a client (browser or SSO apps) during the authentication process. The encrypted login request fields provide an extra layer of security to protect the user's sensitive data from being disclosed.

To enable the login encryption by using the CLI, run the following command.

```
set aaa parameter [-loginEncryption (ENABLED | DISABLED)]
```

To enable the login encryption by using the GUI

1. Navigate to **Security > AAA –Application Traffic**.
2. Click **Change authentication AAA settings** under the Authentication Settings section.
3. On the **Configure AAA Parameter** page, in **Login Encryption** click **Enabled**.

For more details on login encryption, see Encryption of NetScaler Gateway login information for nFactor authentication.

Best practices for NetScaler Console security

July 5, 2024

NetScaler Console is a centralized management solution that simplifies operations by providing administrators with enterprise-wide visibility and automating management jobs that need to be run across multiple instances. You can manage and monitor NetScaler products that include NetScaler MPX, NetScaler VPX, NetScaler SDX, NetScaler CPX, and NetScaler Gateway. You can use NetScaler Console to manage, monitor, and troubleshoot the entire global application delivery infrastructure from a single, unified console.

NetScaler Console is a virtual appliance that runs on Citrix XenServer, VMware ESXi, and Linux KVM. NetScaler Console addresses the application visibility challenge by collecting the following detailed information about web-application and virtual-desktop traffic:

- User-session-level information
- Webpage performance data
- Database information flowing through the NetScaler instances at your site and provides actionable reports.

NetScaler Console enables IT administrators to troubleshoot and proactively monitor customer issues in a matter of minutes.

To maintain security through the deployment lifecycle, we recommend the following considerations:

Do not expose the NetScaler Console IP address and NetScaler agent IP address to the Internet

We recommend that the NetScaler Console IP address and NetScaler agent IP address is not exposed to the public Internet and is deployed behind an appropriate stateful Packet Inspection (SPI) firewall.

Strong password for system user

We recommend using a strong password for system users accounts created in NetScaler Console. 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 include at least one uppercase letter, one lowercase letter, one number, and one special character.

To set a minimum password length using NetScaler Console:

1. Navigate to **Settings > Users & Roles**.
2. In the **User Administration** page, click **Settings** on the right.
3. Select **Enable Password Complexity**.
4. In the **Password Policy** page, specify the minimum password length as 8.
5. Click **OK**.

Change the default certificate

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

We recommend that you configure NetScaler Console to use certificates either from a reputable Certificate Authority (CA) or appropriate certificates from your enterprise Certificate Authority. For more information, see Install SSL certificates.

To install an SSL certificate on NetScaler Console:

1. Navigate to **Settings > Administration**.
2. Under **SSL Settings**, click **Install SSL Certificate**.
3. In the **Install SSL Certificate on Console** page, select the certificate and key files and optionally specify a password if the private key is encrypted.
4. Click **OK**.

Disable local authentication

When external authentication is configured on NetScaler Console and as an admin you prefer to deny access to local system users to log on to management access, you must disable local authentication. For more information see, Enable external authentication.

> **Note:**
>
> External server must be configured.

To disable local authentication:

1. Navigate to **Settings > Authentication**.
2. On the **Authentication** page, click **Settings**.
3. On the **Authentication Settings** page, in **Server Type** select EXTERNAL.

4. Click **Insert**, and on the **External Servers** page, select one or multiple authentication servers to cascade.
5. Clear **Enable fallback local authentication** to disable local authentication.
6. Click **OK**.