Citrix Systems, Inc.

NetScaler MAS Secure Deployment Guide

December 2017

Copyright and Trademark Notice and Disclaimers

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

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

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

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

Move the NetScaler equipment farther away from your equipment.

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

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

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

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

Last Updated: December 2017

Introduction to Best Practices for NetScaler MAS Security

NetScaler Management and Analytics System (MAS) is a centralized management solution. NetScaler MAS simplifies operations by providing administrators with enterprise-wide visibility and by automating the management jobs that must be executed across multiple instances. You can use NetScaler MAS to manage, monitor, and troubleshoot the entire global application delivery infrastructure from a single, unified console.

You can manage and monitor Citrix application networking products such as those listed as follows:

- Citrix NetScaler MPX
- Citrix NetScaler VPX
- Citrix NetScaler Gateway
- Citrix NetScaler SDX
- Citrix NetScaler CPX
- Citrix NetScaler SD-WAN.

NetScaler MAS is a virtual appliance that runs on Citrix XenServer, VMware ESXi, Hyper-V, and Linux KVM. NetScaler MAS addresses the application visibility challenge by collecting detailed information on web-application and virtual-desktop traffic, such as flow, user-session-level information, webpage performance data. NetScaler MAS also analyzes database information flowing through the NetScaler appliances, NetScaler Gateway appliances, or NetScaler SD-WAN appliances at your site and provides actionable reports. NetScaler MAS enables IT administrators to troubleshoot and proactively monitors customer issues.

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

- Physical Security
- NetScaler MAS Security
- Network Security
- Administration and Management
- Additional Features

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

Deployment Guidelines

When you are deploying Citrix NetScaler MAS, consider the following physical and server security best practices:

Physical Security Best Practice

Deploy the NetScaler MAS server in a secure location

Deploy NetScaler MAS servers in a secure location with sufficient physical access controls to protect the servers from unauthorized access. Control access to the server room with a lock, an electronic card reader, or any other similar physical methods.

Additional measures can include the use of an electronic surveillance system. For example, you can use CCTV, to monitor the activity of the room. If there is an unauthorized intrusion, the security personnel can be notified. Ensure that the recorded tape from the CCTV is always available for audit purposes.

Secure access to the appliance front panel and console port

Deploy the NetScaler MAS hosting server (hypervisor) in a rack or cage that can be locked securely. You can also use other physical methods to secure the server. Securing the server prevents access to the physical ports of the virtualization host console.

Power Supply Protection

Protect the hosting server by using a suitable uninterruptible power supply (UPS). If there is a power outage a UPS ensures a continued operation of the NetScaler MAS server, or allows controlled shutdown of NetScaler MAS. The use of a UPS also helps in providing protection against power spikes.

NetScaler MAS Security Best Practice

Perform appliance software updates

Citrix recommends that you make sure the NetScaler MAS servers are always updated to the latest version.

- When you are upgrading NetScaler MAS remotely, use a secure protocol, such as HTTPS, to upgrade the server.
- Periodically review security bulletins related to Citrix products.

Note: For information on new and updated security bulletins, see Citrix Security Bulletins webpage. You can also consider signing up for alerts on new and updated bulletins.

Secure the operating system of servers hosting NetScaler MAS

A NetScaler MAS server runs as a virtual appliance on any virtualization server. Apart from applying normal physical security procedures, you must also protect access to the virtualization host by using role-based access control and strong password management. Update the server with the latest security patches for the operating system whenever they are available. Deploy up-to-date antivirus software on the server, if applicable to the type of virtualization.

Configuration Guidelines

Network Security

When deploying a NetScaler MAS server to a production environment, Citrix strongly recommends that you make the following key configuration changes:

- Enable SSL Cipher settings.
- Replace NetScaler MAS default SSL certificate.
- Use HTTPS (HTTP over TLS) when accessing the NetScaler MAS GUI and disable the default HTTP interface.
- Use HTTPS protocol for NetScaler MAS and NetScaler API communication.
- Use HTTPS for two-way communication between Cisco APIC and NetScaler MAS deployed in service manager mode.
- You can use HTTP and HTTPS for communication between NetScaler MAS and OpenStack, but use only HTTPS for communication between NetScaler MAS and VMware NSX Manager.
- Use HTTPS for all communication between NetScaler MAS and NetScaler instances.
- Use HTTPS or SSH to configure NetScaler instances from NetScaler MAS Analytics.
- Configure ports other than HTTPS for NetScaler MAS to receive AppFlow/LogStream from NetScaler instances.

The following section provides more changes that are recommended.

Do not expose the Management IP to the Internet

Citrix strongly recommends that you do not expose NetScaler MAS Management IP address to the public internet. Deploy NetScaler MAS behind an appropriate Stateful Packet Inspection (SPI) firewall.

But if you configure NetScaler MAS for the following two features, you might expose the NetScaler MAS Management IP address as both these configurations need access to the internet:

- Configure NetScaler MAS to act as a proxy license server to allow NetScaler instances to fetch license files from Citrix website.
- Configure NetScaler MAS so that it can fetch license files from Citrix website using Jazz.

Replace the NetScaler MAS Default TLS Certificate

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

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

When bound to a public-facing virtual server, a valid TLS certificate from a reputable CA simplifies the user experience for internet-facing web applications.

Disable HTTP access to NetScaler MAS

To protect NetScaler traffic coming into NetScaler MAS, configure the NetScaler to use HTTPS. Do the following steps:

1. Log on to NetScaler MAS.
2. Navigate to **System** > **System Administration**.
3. Under **System Settings**, click **Change System Settings**.
4. Select the check box **Secure Access Only**.

Administration and Management

This section provides examples of specific configuration changes that can be applied to increase the security of the NetScaler MAS.

System and User Accounts

Change Password for the nsroot Super User Account

You cannot delete the built-in nsroot super user. So, change the default password for the nsroot account to a secure password.

To change the default password for the nsroot user, do the following procedure:

1. Log on to NetScaler MAS as the super user.
2. Navigate to **System** > **User Administration** > **Users**.
3. Select "nsroot" and click **Edit**.
4. Select **Change Password** and specify a new password.
5. Click **OK**.

Create an Alternative Superuser Account

To create a super user account, see: https://docs.citrix.com/en-us/netscaler-mas/12/authentication-and-rbac/role-based-access-control.html

Enforce Password Complexity

Local users and administrators must select strong passwords. Examples of password complexity requirements are as follows:

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

Strong passwords are enforced by setting two parameters; one for password complexity and the other for the minimum length of passwords

1. Log on to NetScaler MAS.
2. Navigate to **System** > **User Administration**.
3. Under **User Configuration**, click **Password Policy**.
4. Select **Enable Password Complexity**.
5. In **Minimum Password Length**, specify a number to set the minimum length of the password.

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

Use Role-Based Access Control

NetScaler MAS provides fine-grained, role-based access control (RBAC). You can grant access permissions that are based on the roles of individual users within your enterprise. In this context, access is the ability to perform a specific task, such as view, create, modify, or delete a file. Define roles according to the authority and responsibility of the users within the enterprise. For example, one user might be allowed to perform all network operations, while another user can observe the traffic flow in applications and help in creating configuration templates.

For details, see: https://docs.citrix.com/en-us/netscaler-mas/12/authentication-and-rbac/role-based-access-control.html

Logging and Monitoring

Configure NTP

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

It is important that you enable NTP on the NetScaler MAS server when you are using NetScaler MAS based licensing for NetScaler instances.

Configuring an NTP server ensures that the NetScaler MAS clock has the same date and time settings as the other servers on the network.

To configure an NTP server on NetScaler MAS:

1. Navigate to **System** > **NTP Servers**, and then click **Add**.
2. On the **Create NTP Server** page, enter the following details:
    a. **Server Name/IP Address** – Type the domain name or IP address of the NTP server. The name or IP address cannot be changed after you have added the NTP server.
    b. **Minimum Poll Interval** – Specify the minimum value for the interval between transmitted NTP messages, in seconds as a power of 2. For example, if you want the minimum poll interval to be 64 seconds, which can be expressed as 2^6, enter 6
    c. **Maximum Poll Interval** – Specify the maximum value for the interval between transmitted NTP messages, in seconds as a power of 2. For example, if you want the maximum poll interval to be 256 seconds, which can be expressed as 2^8, enter 8.
    d. **Key Identifier** - Type the key identifier that can be used for symmetric key authentication with the NTP server. Do not add a key identifier if you selected Autokey.
    e. **Autokey** - Select **Autokey** if you want to use public key authentication with the NTP server. Do not select if you want to add a key identifier.
    f. **Preferred** – Select this option if you want to specify this NTP server as the preferred server for clock synchronization. This applies only if more than one server is configured.
3. Click **Create**.

To enable NTP synchronization on NetScaler MAS:

1. Navigate to **System** > **NTP Servers**.
2. Click **NTP Synchronization** and select the **Enable NTP Synchronization** check box.

3. Click **OK**.

Additional Features

This section provides examples of configuration changes to improve the security of the deployed servers.

Use TLS 1.2 Communication Between Servers

Citrix strongly recommends that you use TLS 1.2 for all communication links between NetScaler MAS and other services, such as LDAP and web interface servers. Citrix also recommends disabling earlier cipher suites and compression.

- Do not use earlier versions of TLS protocol.
- Do not use SSLv3 and earlier versions.

Set Up System Health Notifications

Citrix recommends setting up system health notifications. For example, SNMP trap and email notifications so that you can get notified if something goes wrong.

- For additional information on how to create SNMP traps on NetScaler MAS, see How to Create SNMP Traps, Managers, and Users on NetScaler MAS.
- For more information on how to configure system notification settings, see How to Configure System Notification Settings of NetScaler MAS.

Additional Information Resources

See the following resources for more security information about NetScaler MAS:

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

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