Security and System administrator best practices

Ver.1.5 | July 2020

This section describes a collection of changes you can implement to make administrative access to the GUI more secure.

1. Install the NetXGATE unit in a physically secure location

A good place to start with is physical security. Install your NetXGATE in a secure location, such as a locked room or one with restricted access. A restricted location prevents unauthorized users from getting physical access to the device.

If unauthorized users have physical access, they can disrupt your entire network by disconnecting your NetXGATE (either by accident or on purpose). They could also connect a console cable and attempt to log into the CLI. Also, when a NetXGATE unit reboots, a person with physical access can interrupt the boot process and install different firmware.

2. Register your product with NetXGATE NetXCARE

You need to register your NetXGATE product with NetXGATE Support /NetXCARE to receive customer services, such as firmware updates , Hot-Fixes and Customer support. You must also register your product for NetXCARE services, such as up-to-date AV , Geo-IP and IPS signatures. To register your product the contact NetXGATE Support.

3. Keep your NetXGATE Firmware up to date

Always keep NetXGATE Firmware up to date. The most recent version is the most stable and has the most bugs fixed and vulnerabilities removed. NetXGATE periodically updates the NetXGATE firmware to include new features and resolve important issues.

After you register your NetXGATE or Renewed , you can receive notifications on NetXGATE GUI about firmware updates. You can update the firmware directly from the GUI or by downloading firmware updates from the NetXGATE website (offline Mode).

Before you install any new firmware, be sure to follow these steps:

.Review the release notes for the latest firmware release.

.Back up the current configuration.

.Only NetXGATE administrators who have read and write privileges can upgrade the NetXGATE firmware or New Patches.

4. Restrict Local Service Access Control

Where possible, remove ALL services from the WAN and other custom 'External' zones.

Some firewalls are located in secure areas and external datacentres. Should the firewall not be reachable from a trusted source, administrators should avoid opening up direct device access (Web-Admin) on untrusted, external interfaces.

Note: Where external firewall management is required, consider managing the firewall via secure connection e.g. SSL remote access VPN.

5. Get your firewall and NAT rules in order

Once again, the purpose of this guide is to provide practical best practice guidance to secure your NG firewall, before attempting to use the firewall to protect internal network nodes/resources. Firewall rules can be utilized to aid the security of the firewall itself and thwart additional attack vectors.

NetXGATE recommends that administrators check the following firewall rule best practice criteria and modify it as appropriate to your firewall environment.

- **Ensure that your firewall rules are ordered correctly.** Firewall rules are matched from the top down, and as a rule of thumb, more specific rules will precede general rules.

- **Audit your firewall rules regularly**: Ensure unused rules are deleted and remove redundant host definitions.

  Tip: Reset your data transfer count periodically, any unused rule will then be easily identifiable. Rules that should be required, yet do not show use, may indicate a higher firewall rule match.

- **Where possible, ensure firewall rule traffic is logged.**

  TIP: As NetXGATE support on-Appliance Log and report up-to 3+ Month **.** In addition to Local log storage, Logs should be saved to an external destination such as a Syslog Server or Secure FTP Server for the preservation of data for Incident Response (IR), audit, and in case of hardware failure.

- **Reduce the threat landscape** – Enable GEO-IP filter rule to block countries of origin by using it.

  Note: Customers should also note that hackers may utilize local country 'Pivot points' to launch attacks, therefore Geo-IP filtering should be considered as an aid to security and not relied upon.

- If appropriate, ensure a firewall rule is created to **restrict DNS**, allowing DNS queries to sanctioned servers and sanctioned hosts only to prevent pharming/DNS poisoning attacks and ensure correct DNS resolution.

  To Enable DNS Security , go to *Configuration > Firewall /NAT > DNS Security* , Enable the DNS Security Service . Here admin can force its users to use Built in DNS Servers.

- Create your firewall rules with as much granularity as possible. E.g. refrain from creating rules that allow traffic from an entire zone or network where a specific host could be defined.

  •Under Firewall Filter ,Group similar firewall rules from LAN to WAN and Under Port Forward rule in case of WAN 2 LAN (DNAT). Organizing rules in this way simplifies administration and minimizes human error.

- Pay attention to WAN to LAN rules (Port Forward Rule Specially): Make sure the rule is necessary – what specific business function does it serve? Can this function be achieved through another mechanism?

- Reverse Proxy traffic from WAN to DMZ (if possible) instead of NAT'ing traffic to specific internal hosts.

6. Changing the Admin Password (with Public Key authentication or Two factor Authentication*)

ALWAYS CHANGE THE DEFAULT ADMINISTRATOR PASSWORD BEFORE DEPLOYING A FIREWALL TO PRODUCTION !

The ways to change the NetXGATE Admin password:

Navigate to *Administration > Admin User Management > Change password settings* Change the password ,Click **Submit**

(*Presently Not available under GUI)

7. Disable administrative access to the external (Internet-facing) interface

When possible, don't allow administration access on the external (Internet-facing) interface.
To disable administrative access, From the GUI go to *Configuration > Firewall /NAT > System Security* , edit the Remote Management via WAN and disable HTTPS, PING, HTTP.

8. Allow only HTTPS access to the GUI

For greater security never allow HTTP administrative access Via GUI to a NetXGATE, only allow only HTTPS .

9. Ensure HTTPS access ports should be non-standard ports only .

By Default , NetXGATE can be access via non-standard HTTPS port only (HTTPS administrative access for added security) .
For example: https://<ip-address>:4433.
If Admin want to change the HTTPS port different to 4433, he may do it from *Configuration > Firewall /NAT > System Security*.

10. Maintain short login timeouts

As per best practice NetXGATE keep the default time of 5 minutes.
Suggest to set the idle timeout to a short time to avoid the possibility of an administrator walking away from their management computer and leaving it exposed to unauthorized personnel.

11. Restrict logins from trusted hosts

Setting up trusted hosts for an administrator limits the addresses from where they can log into NetXGATE . The trusted hosts configuration applies to most forms of administrative access including HTTPS. When you identify a trusted host for an administrator account, NetXGATE accepts that administrator's login only from one of the trusted hosts. A login, even with proper credentials, from a non-trusted host is dropped.
Even if you have configured trusted hosts, if you have enabled ping administrative access on a NetXGATE interface, it will respond to ping requests from any IP address.

To identify trusted hosts, go to *Configuration > Firewall /NAT > System Security*, edit the Allow remote Management Via WAN by , Select "All" to *"Specify IP"*, and add up to ten trusted host IP addresses.

Trusted host IP addresses can identify individual hosts or subnets. Just like firewall policies, NetXGATE searches through the list of trusted hosts in order and acts on the first match it finds. When you configure trusted hosts, start by adding specific addresses at the top of the list.

12. Create multiple administrator accounts

Rather than allowing all administrators to access NetXGATE with the same administrator account, you can create accounts for each person or each role that requires administrative access. This configuration allows you to track the activities of each administrator or administrative role.
If you want administrators to have different functions you can add different administrator profiles. Go to *Administration > Admin user Management* and Add New Unique *"Account Type" and "Page Access Control"* .

13. Modify administrator account lockout duration and threshold values

By default, the NetXGATE sets the number of password retries at three, allowing the administrator a maximum of three attempts to log into their account before locking the account for a set amount of time .

Both the number of attempts (admin-lockout-threshold) and the wait time before the administrator can try to enter a password again (admin-lockout-duration)

14. Rename the admin administrator account

You can improve security by renaming /disable the default admin account. To do this, create a new administrator account with the "Administrator" Account type and log in as that Unique administrator. Then go to *Administrators>Admin User management* and disable the current/Default "admin" administrator and create a new Admin profile /Account type with New name . Renaming the admin account makes it more difficult for an attacker to log into NetXGATE.

15. Set system time by synchronizing with an NTP server

For accurate time, by Default NetXGATE use an NTP server to set system time. Synchronized time facilitates auditing and consistency between expiry dates used in expiration of certificates and security protocols.

From the GUI go to *Administrator* > *System Management* > *NTP Setting* and select *Synchronize with NTP Server*. By default, this causes NetXGATE to synchronize with secure NTP servers (e.g pool.ntp.org).

16. View auditing and logging.

From NetXGATE On-Appliance Log &Reports , you can view reports or system event log messages to look for system events that may indicate potential problems.
Establish an auditing schedule to routinely inspect logs for signs of intrusion and probing.

17. Disable unused interfaces

To disable an interface from the GUI, go to Configuration >*Network Setting* > Edit the interface to be disabled under WAN/LAN connection Type .