About the NetScaler Gateway MPX Appliance

May 11, 2015

The hardware platform (appliance) used for NetScaler Gateway is the MPX that runs on the NetScaler platform. This appliance supports classic and nCore NetScaler Gateway software deployments. The MPX appliance supports NetScaler Gateway 10.1 and later, Access Gateway 10, Access Gateway 9.3, Enterprise Edition, and Access Gateway 9.2, Enterprise Edition.

Note: NetScaler Gateway 10.5. NetScaler Gateway 10.1, and Access Gateway 10 must run on an nCore version of the appliance.

The following table shows the versions of the NetScaler Gateway and Access Gateway software that are supported on the MPX appliance.

NetScaler Gateway version	MPX support
9.2 Classic	Yes
9.2 nCore You must install a minimum of Build 55.5 to use nCore on a 9.2 appliance.	Yes
9.3 nCore	Yes
10 nCore	Yes
10.1 nCore and newer	Yes

The preconfigured IP address of NetScaler Gateway is 192.168.100.1 and the subnet mask is 255.255.0.0. To change the IP address, you can use a serial cable and a terminal emulation program, or you can connect NetScaler Gateway by using network cables and the configuration utility.

You can install the NetScaler Gateway appliances in the DMZ or the secure network. For more information about deployment scenarios, see Deploying NetScaler Gateway.

For information about setting up the MPX appliance in a rack, see section Installing the Model MPX Appliance in a Rack. This section discusses the MPX specifications and how to install and configure the MPX appliance.
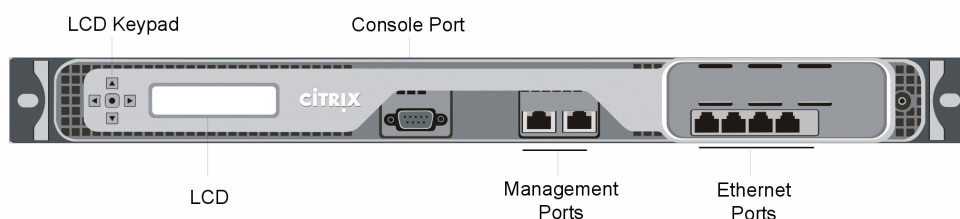
Model MPX Specifications

Jul 15, 2013

The Model MPX is a single dual-core processor, 1U appliance that ships with 4 gigabytes (GB) of memory.

The following figure shows the front panel of the MPX.

Figure 1. MPX front panel

The MPX has the following ports:

- One RS232 serial console port.
- Two 10/100/1000Base-T copper Ethernet management ports, numbered 0/1 and 0/2 from left to right. You can use these ports to connect directly to the appliance to enable system administration functions.
- Four 10/100/1000Base-T copper Ethernet ports numbered 1/1, 1/2, 1/3, and 1/4 from left to right.

Note: The network port numbers on all appliances consist of two numbers separated by a forward slash. The first number is the port adapter slot number. The second number is the interface port number. Ports on appliances are numbered sequentially starting with 1.

The following figure shows the back panel of the MPX.

Figure 2. MPX back panel
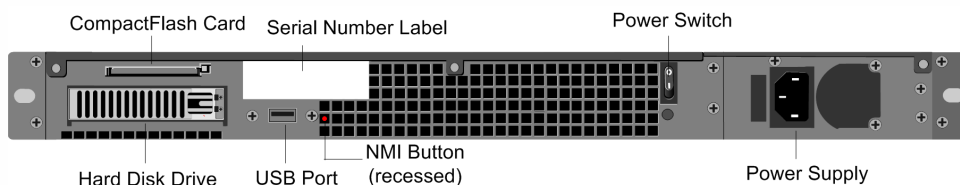
The following components are visible on the back panel of the MPX:

- A 4-GB removable CompactFlash card that is used to store the operating system.
- A power switch that turns off power to the MPX, as if you were to unplug the power supply. Press the switch for five seconds to turn off the power.
- A removable hard disk drive that is used to store user data. Appliances shipped before February, 2012 store user data on a hard disk drive. In appliances shipped after February, 2012, a solid-state drive replaces the hard disk drive. Both types of drive have the same functionality and support the same software releases.
- One USB port (not functional in this release; reserved for a future release).
- A non-maskable interrupt (NMI) button that is used at the request of Technical Support and produces a core dump on the appliance. You must use a pen, pencil, or other pointed object to press this red button, which is recessed to prevent unintentional activation.
- A single 300 watt, 110–220 volt power supply with fan. The power-supply fan is designed to turn on when the internal temperature of the power supply reaches a certain value. You cannot see the fan turning on the back panel. You can see the fixed part of the fan that holds the spinning motor.

Front and Back Panel Components

Nov 02, 2012

The front panel of the appliance has an LCD display and various ports, including an RS232 serial console port, copper Ethernet ports, and copper and fiber Small Form Factor Pluggable (SFP) ports. The number, type, and location of ports vary by hardware platform. The back panel of the appliance provides access to the power supply, fan, CompactFlash card, and hard disk drive.

Power Supply and Fan. Appliances are configured with either a single power supply or, for higher capacity fault-tolerant models, a dual-power supply configuration. The power supply on the MPX appliance is configured with a single fan. Each unit ships with a standard power cord that plugs into the appliance's power supply and an NEMA 5-15 plug on the other end for connecting to the power outlet on the rack or in the wall.

CompactFlash Card. The CompactFlash drive in all appliances contains the operating system for the unit. It is mounted as /flash.

Hard Disk Drive. The hard disk drive on all appliances contains logs and other data files. It is mounted as /var.

Ports

Jul 15, 2013

Ports are used to connect the appliance to external devices. NetScaler Gateway appliances support RS232 serial ports, 10/100/1000Base-T copper Ethernet ports, 1-gigabit copper and fiber Small Form Factor Pluggable (SFP) ports, and 10-gigabit fiber SFP+ ports. All appliances have a combination of some or all of these ports. For details on the type and number of ports available on your appliance, see the specific topic that describes your appliance.

RS232 Serial Console Port

The RS232 serial console port on the front of each appliance provides a direct connection between the appliance and a workstation or laptop, allowing direct access to the appliance for initial configuration or troubleshooting.

All hardware platforms ship with an appropriate serial cable that you can use to connect your workstation or laptop computer to the appliance. For instructions on connecting your workstation or laptop to the appliance, see section Setting Up the Model MPX Appliance.

Copper Ethernet Ports

The copper Ethernet ports installed on many models of the appliance are standard RJ45 ports.

The following two types of copper Ethernet ports may be installed on your appliance:
- 10/100BASE-T port. This type of port has a maximum transmission speed of 100 megabits per second (Mbps). The MPX appliance has a single 10/100BASE-T port.
- 10/100/1000BASE-T port. This type of port has a maximum transmission speed of 1 GB, which is 10 times faster than the other type of copper Ethernet port. The MPX has six copper Ethernet ports.

To connect any of these ports to your network, you plug one end of a standard Ethernet cable into the port and plug the other end into the appropriate network connector.

SFP Ports

An SFP port can operate at speeds of up to 1 gigabit per second. The port accepts either a copper SFP transceiver for operation as a copper Ethernet port or a fiber SFP transceiver for operation as a fiberoptic port.

The following tables list the maximum distance specifications for NetScaler Gateway pluggable media (1G SFP and XFP transceivers). The1G Pluggable Media table has the following columns:

- SKU: Citrix maintains multiple SKUs for the same part.
- Description: The price list description of the part.
- Transmit Wavelength: The nominal transmit wavelength.
- Cable/Fiber Type: Fiber characteristics affect the maximum transmit distance achievable. This is especially true with 10G on multi-mode fiber (MMF), where various dispersion components become dominant.
- Typical Reach: Maximum transmit distance.
- Products: Some chassis are available with different media options. Use the appropriate data sheet to confirm that your particular chassis type supports the media.

1G Pluggable Media

The following table lists the maximum distance specifications for 1G transceivers.

Table 1. Copper 1G SFP Distance Specifications

SKU	Description	Transmitter Wavelength (nm)	Cable Type	Typical Reach (m)	Products
EW3A0000235, EW3B0000235, EW3C0000235, EW3D0000235, EW3E0000235, EW3F0000235, EW3P0000143, EW3X0000235, EW3Z0000087	Citrix NetScaler 1G SFP Ethernet Copper (100m) - 4 Pack	n/a	Category 5 (Cat-5) Copper Cable	100 m	MPX

Table 2. Short Reach Fiber 1G SFP Distance Specifications

SKU	Description	Transmitter Wavelength (nm)	Fiber Type	Typical Reach (m)	Products
EW3A0000234, EW3B0000234, EW3C0000234, EW3D0000234, EW3E0000234, EW3F0000234, EW3P0000142, EW3X0000234, EW3Z0000086	Citrix NetScaler 1G SFP Ethernet SX (300m) - 4 Pack	850nm (nominal)	50/125um MMF, 2000MHz-km (OM3)	550 m	MPX
			50/125um MMF, 500MHz-km (OM2)	550 m	
			50/125um MMF, 400MHz-km	550 m	
			62.5/125um MMF, 200MHz-km (OM1)	300 m	
			62.5/125um MMF, 160MHz-km	300 m	

LED Port-Status Indicators

Note: This section applies to the MPX appliance.
The port LEDs show whether the link is established and traffic is flowing through the port. The following table describes the LED indicators for each port. There are two LED indicators for each port type.

Table 3. LED port-status indicators

Port Type	LED Location	LED Function	LED Color	LED Indicates
10G SFP+ (10 Gbps)	Left	Link/Activity	Off	No link.
			Solid Color	Link is established but no traffic is passing through the port.
			Blinking green	Traffic is passing through the port.
	Right	Speed	Off	No connection.
			Solid green	Traffic rate of 10 gigabits per second.
1G SFP (1 Gbps)	Left	Link/Activity	Off	No link.
			Solid green	Link is established but no traffic is passing through the port.
			Blinking green	Traffic is passing through the port.
	Right	Speed	Off	No connection.
			Yellow	Traffic rate of 1 gigabit per second.
Ethernet (RJ45)	Left	Speed	Off	No connection, or a traffic rate of 10 megabits per second (Mbps).
			Green	Traffic rate of 100 Mbps.
			Yellow	Traffic rate of 1 gigabit per second.
	Right	Link/Activity	Off	No link.
			Solid green	Link is established but no traffic is passing through the port.
			Blinking green	Traffic is passing through the port.
Management	Left	Speed	Off	No connection, or a traffic rate of 10 Mbps.

(RJ45)			Green	Traffic rate of 100 Mbps.
			Amber	Traffic rate of 1 gigabit per second.
	Right	Link/Activity	Off	No link.
			Solid yellow	Link is established but no traffic is passing through the port.
			Blinking yellow	Traffic is passing through the port.

Plan

Jul 15, 2013

Before you install your new MPX appliance, carefully unpack the appliance and make sure that you received all of the parts according to the appliance you ordered. Next, verify that the location where you will install the appliance meets temperature and power requirements. Also, verify that the server cabinet or floor-to-ceiling cabinet is securely bolted to the floor and has sufficient airflow.

Only trained and qualified personnel should install, maintain, or replace the appliance and should be sure to follow all cautions and warnings.

Unpacking the Model MPX Appliance

Jul 15, 2013

Your appliance comes with hardware accessories, such as cables, adapters, and rail kit, will vary depending on the hardware platform you order. Unpack the box that contains your new appliance on a sturdy table with plenty of space and inspect the contents.

Use the following list to verify that you received everything that should be in the box:

- The appliance you ordered.
- One RJ-45 to DB-9 adapter.
- One 6 ft RJ-45/DB-9 cable.
- One power cable.
- One mounting rail kit with all the models.

In addition to the items included in the box with your new appliance, you will need the following items to complete the installation and initial configuration process:
- Ethernet cables for each additional Ethernet port that you will connect to your network.
- One available Ethernet port on your network switch or hub for each Ethernet port you want to connect to your network.
  Note: Transceiver modules are sold separately. Please contact your Citrix sales representative to order transceiver modules for your appliance. Only transceivers supplied by Citrix are supported on the appliance.
- A computer to serve as a management workstation.

Preparing the Site and Rack

Jul 15, 2013

The NetScaler Gateway appliance has specific site and rack requirements. You must make sure that adequate environmental control and power density are available. Racks must be bolted to the ground and have sufficient airflow. Preparing the site and rack are important steps in the installation process and will help ensure a smooth installation.

Site Requirements

The appliance should be installed in a server room or server cabinet with the following features:

- **Environment control**. An air conditioner, preferably a dedicated computer room air conditioner (CRAC), capable of maintaining the cabinet or server room at a temperature of no more than 21°C/70°F at altitudes up to 2100 m/7000 ft, or 15°C/60°F at higher altitudes, a humidity level no greater than 45 percent, and a dust-free environment.
- **Power density**. Wiring capable of handling at least 4000 W per rack unit in addition to power needs for the CRAC.

Rack Requirements

The rack on which you install your appliance should meet the following criteria:

- **Rack characteristics**. Racks should be either integrated into a purpose-designed server cabinet or be the floor-to-ceiling type, bolted down at both top and bottom to ensure stability. If you have a cabinet, you should install the cabinet perpendicular to a load-bearing wall for stability and sufficient airflow. If you have a server room, you should install your racks in rows spaced at least 1 meter/3 feet apart for sufficient airflow. Your rack must give your IT personnel the ability to access the front and back of each appliance and all power and network connections.
- **Power connections**. At minimum, two standard power outlets per unit.
- **Network connections**. At minimum, four Ethernet connections per rack unit.
- **Space requirements**. One empty rack unit.

Cautions and Warnings

May 03, 2012

The installation instructions for the appliance provide instructions for carefully connecting the appliance to a power source. Heed all cautions and warnings regarding safety practices when working with power sources and supplies. To help ensure secure rack installation, sufficient airflow, and appliance stability, follow all prescribed precautions.

Important: Only trained and qualified personnel should install, maintain, or replace the appliance.

Power Supply Precautions

- Remove all jewelry and other metal objects that might come into contact with power sources or wires before installing or repairing the appliance. When you touch both a live power source or wire and ground, any metal objects can heat up rapidly and may cause burns, set clothing on fire, or fuse the metal object to an exposed terminal.
- Never stack the appliance on top of any other server or electronic equipment.
- Do not block access to the power socket or power sockets where your appliance is plugged in. In emergencies, unplugging the appliance is the fallback disconnection method.
- All appliances are designed to be installed on power systems that use TN earthing. Do not install your device on a power system that uses either TT or IT earthing.
- Ensure that the appliance has a direct physical connection to the earth during normal use. When installing or repairing an appliance, always ensure that the ground circuit is connected first and is disconnected last.
- Ensure that a fuse or circuit breaker no larger than 120 VAC, 15 A U.S. (240 VAC, 16 A international) is used on all current-carrying conductors on the power system to which your appliances are connected.
- Always unplug any appliance before performing repairs or upgrades.
- Do not overload the wiring in your server cabinet or on your server room rack.
- During thunderstorms, or anticipated thunderstorms located in the vicinity of the building where your appliance is located, avoid performing any repairs or upgrades until the danger of lightning has passed.
- Never touch a power supply when the power cord is plugged in. As long as the power cord is plugged in, line voltages are present in the power supply even when the power switch is off.
- Ensure the stability of your appliance by installing it as follows:
    - If the appliance is the only unit in the rack, mount it at the bottom of the rack.
    - When mounting the appliance in a partially filled rack, load the rack from the bottom to the top with the heaviest server at the bottom of the rack.
    - If the rack has stabilizing devices available, install them before mounting or servicing the appliance in the rack.
- When you dispose of an old appliance or any components, follow any local and national laws on disposal of electronic waste.
- To prevent possible explosions, replace expired batteries with the same model or a manufacturer-recommended substitute and follow the manufacturer's instructions on battery replacement.
- Never remove a power supply cover or any sealed part that has a label that reads: Hazardous voltage, current, and energy levels are present inside any component that has this label attached. There are no user-serviceable parts inside these components. If you suspect a problem with none of these parts, contact Citrix Technical Support.

Appliance Precautions

- Determine the placement of each component in the rack before you install the rail.
- Install the heaviest appliance on the bottom of the rack first, and then work up. Equipment should be mounted into a rack so that a hazardous condition does not arise due to uneven mechanical loading.
- Allow the power supply units and hot plug hard drives to cool before touching them.

- To maintain proper cooling, always keep the rack's front door, panels, and appliance components closed.
- Install the equipment near a socket outlet for easy access.
- If installed in a closed or multi-unit rack assembly, the ambient operating temperature of the rack environment may be greater than the ambient temperature of the room. Therefore, consideration should be given to installing the equipment in an environment compatible with the manufacturer's maximum rated ambient temperature (Tmra).

Clearance Precautions

- Mount equipment into a rack with airflow sufficient for safe operation.
- Leave enough clearance in front of the rack to open the front door completely (25 inches).
- Leave approximately 30 inches of clearance behind the rack to allow for sufficient airflow and ease in servicing.
- This product is for installation only in Restricted Access Locations (RALs) such as dedicated equipment rooms and service closets.

Rack Precautions

- Ensure that the leveling jackets on the bottom of the rack are fully extended to the floor with the full weight of the rack resting on them.
- In a single rack installation, attach a stabilizer to the rack.
- In multiple rack installations, couple (attach) the racks together.
- Always make sure the rack is stable before extending a component from the rack.
- Extend only one component at a time. Extending two or more simultaneously may cause the rack to become unstable.

Install and Setup

Jul 15, 2013

When you receive your MPX appliance, you unpack the appliance and prepare the site and rack. After you determine that the location where you will install your appliance meets the environmental standards and the server rack is in place according to the instructions, you install the hardware. After you mount the appliance, you connect it to the network, to a power source, and to the console terminal that you use for the initial configuration of NetScaler Gateway. After you turn on the appliance, you perform the initial configuration, and assign management and network IP addresses. Be sure to observe the cautions and warnings listed with the installation instructions.

Getting Ready to Install the Model MPX Appliance

Jul 15, 2013

To install the Model MPX appliance, verify that the contents of the box match the packing list. If an item on the packing list is missing from the box, contact Citrix Customer Care.

Before installing NetScaler Gateway, collect materials for the initial configuration and for the connection to your network.

For initial configuration, use one of the following setups:

- A cross-over cable and Windows-based computer
- Two network cables, a network switch, and a Windows-based computer
- A serial cable and a computer with terminal emulation software

For a connection to a local area network, use the following items:

- One network cable to connect NetScaler Gateway inside a firewall or to a server load balancer
- Two network cables to connect NetScaler Gateway located in the DMZ to the Internet and secure network

Citrix recommends that you use a pre-installation checklist for the Model MPX. For more information, see section NetScaler Gateway Pre-Installation Checklist. You can use the checklist to collect the following network information for appliances that are located in the secure network and in the DMZ:

- The NetScaler Gateway internal IP address and subnet mask.
- The NetScaler Gateway external IP address and subnet mask.
- The NetScaler Gateway fully qualified domain name (FQDN) for network address translation (NAT).
- The IP address of the default gateway device.
- The port to be used for connections. The default is 443.

If connecting NetScaler Gateway to a server load balancer, you need the following information:

- The NetScaler Gateway IP address and subnet mask.
- The settings of the server load balancer as the default gateway device (if required). See the load balancer manufacturer's documentation for more information.
- The FQDN of the server load balancer to be used as the external public address of NetScaler Gateway.
- The port to be used for connections. The default is 443.

Note: NetScaler Gateway requires the use of static IP addresses and does not support Dynamic Host Configuration Protocol (DHCP).

Selecting a Location for the Appliance

Jul 15, 2013

When selecting where to put the NetScaler Gateway appliance, consider the following:

- Leave enough clearance in front of the rack so that you can access the LCD and various ports on the front panel of the appliance.
- Leave approximately 30 inches of clearance in the back of the rack to allow for sufficient airflow and easy servicing.
- Install the NetScaler Gateway appliance in a restricted area, such as a dedicated lab or service closet.
- Ground the rack to ensure that a reliable ground is maintained at all times.
- Leave enough clearance in front of the rack to enable you to open the front bezel completely.

Setting Up the Model MPX Appliance

Jul 15, 2013

The following procedure describes how to set up the NetScaler Gateway Model MPX appliance for the first time.

To physically connect the NetScaler Gateway appliance

1. Install NetScaler Gateway in a rack if it is rack-mounted.
2. Connect the power cord to the AC power receptacle.
3. Connect either the serial cable to a Windows-based computer, a cross-over cable to a Windows-based computer, or an RJ-45 network cable to a network switch and NetScaler Gateway.
4. Configure the TCP/IP settings by following the instructions in **section** Configuring Initial Settings by Using the Serial Console.

Installing the Model MPX Appliance in a Rack

Jul 15, 2013

Most appliances can be installed in standard server racks. The appliances ship with a set of rails, which you must install before you mount the appliance. The only tool you will need to install an appliance is a Phillips screwdriver.

Caution: If you are installing the appliance as the only unit in the rack, mount it at the bottom. If the rack contains other units, make sure that the heaviest unit is at the bottom. If the rack has stabilizing devices available, install them before mounting the appliance.

The MPX appliance requires one rack unit. Each unit ships with a mounting rail kit that contains two rail assemblies, one for the left side and the other for the right side of the appliance, as well as screws to attach the rails. You must install the assemblies before mounting the appliance in the rack.

To mount the appliance, you must first install the rails and then install the appliance in the rack.

Perform the following tasks to install the rails:

- Remove the inner rails from the rail assembly.
- Attach the inner rails to the appliance.
- Adjust the length of the rack rails.
- Install the rack rails on the server cabinet or rack.

The following figure illustrates the steps to attach the inner rails to the appliance, attach the outer rails to the rack, and then slide the appliance out of the rack to ensure that it is locked in place.
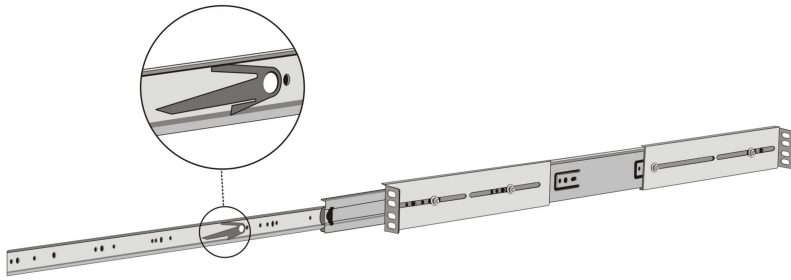
Figure 1. Rack mounting the appliance
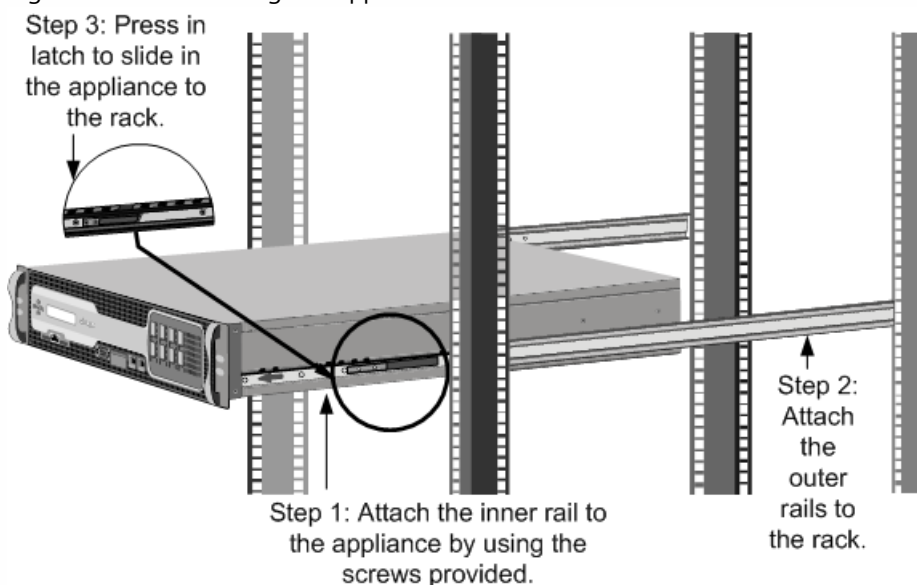
To remove the inner rails from the rail assembly

1. Place the rail assembly on a flat surface.
2. Slide out the inner rail toward the front of the assembly.
3. Depress the locking tabs until the inner rail comes all the way out of the rail assembly, as shown in the following figure.
   Figure 2. Removing inner rails

4. Repeat steps 1 through 3 to remove the second inner rail.

To attach the inner rails to the appliance

1. Position the right inner rail behind the ear bracket on the right side of the appliance.
2. Align the holes on the rail with the corresponding holes on the side of the appliance.
3. Attach the rail to the appliance with screws, as shown in the following figure.

   Figure 3. Attaching inner rails

4. Repeat steps 1 through 3 to install the left inner rail on the left side of the appliance.

To install the rack rails

1. Position the rack rails at the desired location in the rack, keeping the sliding rail guide facing inward.
2. Snap the tool-less rails to the rack.

   Note: Make sure that both rack rails are at same height and that the rail guides are facing inward.

To install the appliance in a rack

1. Align the inner rails, attached to the appliance, with the rack rails.
2. Slide the appliance into the rack rails, keeping the pressure even on both sides.
3. Verify that the appliance is locked in place by pulling it all the way out from the rack.

Connecting the Cables to the MPX Appliance

Nov 18, 2013

When the NetScaler Gateway appliance is securely mounted on the rack, you are ready to connect the cables. Ethernet cables and console cables are connected first. Connect the power cable last.
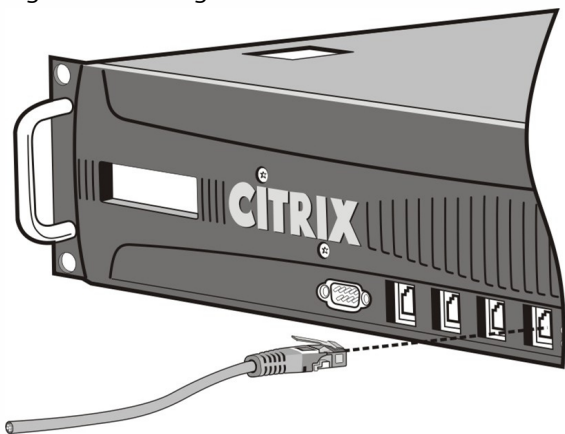
Connecting the Ethernet Cables

Ethernet cables connect your appliance to the network. The type of cable you need depends on the type of port used to connect to the network. Use a category 5e or category 6 Ethernet cable with a standard RJ-45 connector on the 10/100/1000BASE-T port or 1-gigabit SFP copper transceiver. Use a fiber-optic cable with an LC duplex connector with SFP transceivers. The type of connector at the other end of the fiber-optic cable depends on the port of the device that you are connecting to.

To connect an Ethernet cable to a 10/100/1000BASE-T port or 1-gigabit SFP copper transceiver

1. Insert the RJ-45 connector on one end of your Ethernet cable into an appropriate port on the front panel of the appliance as shown in the following figure.

   Figure 1. Inserting an Ethernet cable

2. Insert the RJ-45 connector on the other end into the target device, such as a router or switch.
3. Verify that the LED glows amber when the connection is established.

To connect the Ethernet cable to an SFP fiber transceiver

1. Remove the dust caps from the transceiver and cable.
2. Insert the LC connector on one end of the fiber-optic cable into the appropriate port on the front panel of the appliance.
3. Insert the connector on the other end into the target device, such as a router or switch.
4. Verify that the LED glows amber when the connection is established.

Connecting the Console Cable

You can use the console cable to connect your appliance to a computer or terminal from which you will configure the appliance. Alternatively, you can use a computer connected to the network. Before connecting the console cable, you can accept the following default settings:

- Computer or terminal supports VT100 terminal emulation

- 9600 baud
- 8 data bits
- 1 stop bit
- Parity set to none
- Flow control set to none

Connect one end of the console cable to the RS232 serial port on the appliance and the other end to the computer or terminal.

To connect the console cable to a computer or terminal

1. Insert the DB-9 connector at the end of the cable into the console port that is located on the front panel of the appliance, as shown in the following figure.

   Figure 2. Inserting a console cable
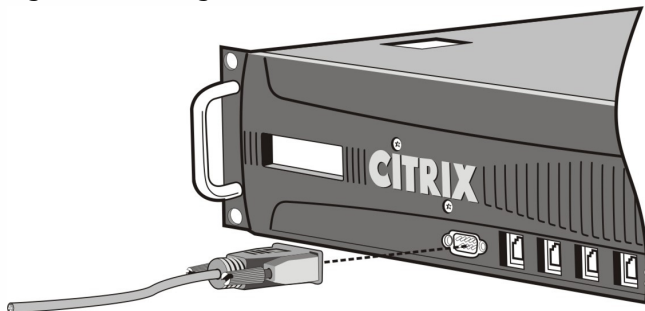
   Note: To use a cable with an RJ-45 converter, insert the optional converter provided into the console port and attach the cable to it.
2. Insert the RJ-45 connector at the other end of the cable into the serial port of the computer or terminal.
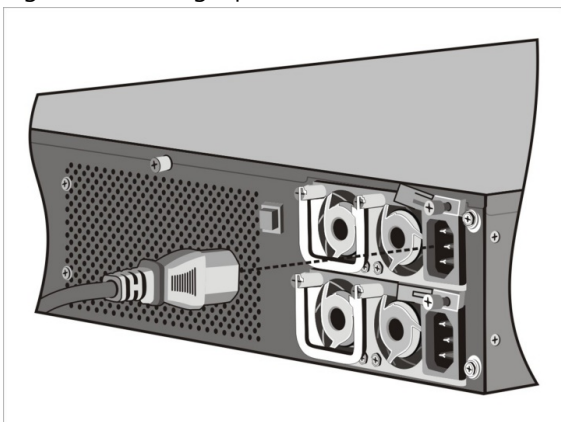
Connecting the Power Cable

The MPX 5500 appliances has one power cable. A separate ground cable is not required because grounding is provided by the three-prong plug.

To connect the appliance to the power source

1. Connect one end of the power cable to the power outlet on the back panel of the appliance, next to the power supply and fan, as shown in the following figure.

   Figure 3. Inserting a power cable

2. Connect the other end of the power cable to a standard 110V/220V power outlet.
3. If a second power supply is provided, repeat steps 1 and 2 to connect the second power supply.

Turning on the Model MPX Appliance

Jul 15, 2013

After you install the NetScaler Gateway appliance in a rack and connect the cables, you are ready to turn on the appliance. Before you turn on the appliance, verify that you connected the power cable properly. When two power supplies are present, make sure the second cable is connected to an outlet for a different circuit than the first.

1. Verify that you are connected to the appliance through a console or Ethernet port. This step will ensure that you can configure the appliance after you turn it on.
2. Press the ON/OFF toggle power switch on the back panel of the appliance, as shown in the following figure.
   Figure 1. Power switch on back panel
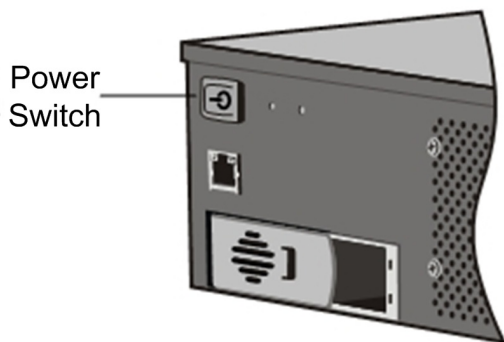
3. Verify that the LCD on the front panel is backlit and the start message appears, as shown in the following figure.
   Figure 2. LCD startup screen
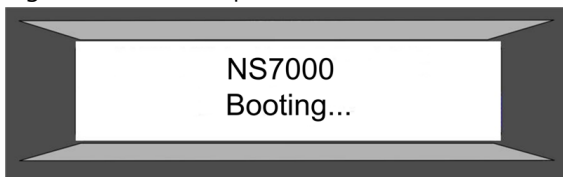
Caution: Be aware of the location of the emergency power off (EPO) switch so that you can quickly turn off power to the appliance if an electrical accident occurs. (The EPO can be located anywhere, including on the rack, the data center, or the lab.)

Performing the Initial Configuration of the MPX Appliance

Feb 20, 2014

After you have installed the MPX appliance in a rack, you are ready to perform the initial configuration. When the initial configuration is complete, you can then configure NetScaler Gateway to work in your network.

To perform the initial configuration, you can use the LCD keypad on the front panel of the appliance, the serial console, or the Setup Wizard. You can access the Setup Wizard from any computer that is on the same network as the new NetScaler Gateway appliance. However, because this method uses the default IP address for NetScaler Gateway, you must install and configure one appliance at a time.

If you want to configure a new NetScaler Gateway appliance from a remote network, or if you want to install multiple appliances and then configure them without using the console port, you can use Dynamic Host Configuration Protocol (DHCP) to assign each new appliance an IP address at which you can access the appliance for remote configuration.

When you finish installing and configuring the initial settings on the NetScaler Gateway 10.1 appliance by using the command-line interface, when you log on to the configuration utility for the first time, the First-time configuration appears if the following is true:

- You did not install a license on the appliance.
- You did not configure a subnet or mapped IP address.
- You left the default IP address of the appliances as 192.168.100.1.

For more information about the first time configuration, see **section** Configuring NetScaler Gateway with the First Time Use Configuration.

You can also use the Setup Wizard to configure the NetScaler Gateway appliance. For more information about available wizards, see **section** Configuring the NetScaler Gateway by Using Wizards.

Configuring the Model MPX Appliance

Jul 15, 2013

You can perform the initial configuration of NetScaler Gateway by using a serial console, the Setup Wizard in the configuration utility, or Dynamic Host Configuration Protocol (DHCP). You can also perform the initial configuration by using the LCD keypad on the front panel of the appliance.

You can access the Setup Wizard from any computer that is on the same network as the new NetScaler Gateway appliance. However, because this method uses the default IP address for NetScaler Gateway, you must install and configure one appliance at a time. If you want to configure a new appliance from a remote network, or if you want to install multiple appliances and then configure them without using the console port, you can use DHCP to assign each new NetScaler Gateway appliance a unique IP address at which you can access the appliance for remote configuration.

Configuring the MPX Appliance by Using the LCD Keyboard

Jul 15, 2013

When you first install the MPX appliance, you can configure the initial settings by using the LCD keypad on the front panel of the appliance. The keypad interacts with the LCD display module, which also appears on the front panel of these appliances.

Note: You can use the LCD keypad for initial configuration on a new appliance with the default configuration. The configuration file (ns.conf) should contain the following command and default values:

set ns config -IPAddress 192.168.100.1 -netmask 255.255.0.0

The functions of the different keys are explained in the following table.

Table 1. LCD Key Functions

Key	Function
<	Moves the cursor one digit to the left.
>	Moves the cursor one digit to the right.
^	Increments the digit under the cursor.
v	Decrements the digit under the cursor.
.	Processes the information or terminates the configuration, if none of the values is changed. This key is also known as the ENTER key.

You are prompted to enter the subnet mask, NetScaler Gateway IP address, and default gateway, in that order. The subnet mask is associated with both the NetScaler Gateway IP address and default gateway IP address. The NetScaler Gateway IP address is the IP address of the appliance. The default gateway is the IP address for the router, which handles external IP traffic that NetScaler Gateway cannot otherwise route. The NetScaler Gateway IP address and the default gateway should be on the same subnet.

If you enter a valid value for the subnet mask, such as 255.255.255.224, you are prompted to enter the IP address. Similarly, if you enter a valid value for the IP address, you are prompted to enter the gateway address. If the value you entered is invalid, the following error message appears for three seconds, where xxx.xxx.xxx.xxx is the IP address you entered, followed by a request to reenter the value.

Invalid addr!

xxx.xxx.xxx.xxx

If you press the ENTER (.) key without changing any of the digits, the software interprets this keystroke as a user exit request. The following message appears for three seconds.

Exiting menu...

xxx.xxx.xxx.xxx

If all of the values you enter are valid, when you press the ENTER (.) key, the following message appears.

Values accepted,
Rebooting...
The subnet mask, NetScaler Gateway IP address, and gateway values are saved in the configuration file.

Configuring Initial Settings by Using the Serial Console

Jul 11, 2013

When you first install the appliance, you can configure the initial settings by using the serial console. With the serial console, you can change the system IP address, create a mapped IP address, configure advanced network settings, and change the time zone.

Note: To locate the serial console port on your appliance, see **section** Ports.

1. Connect the console cable into your appliance. For more information, see **section** Connecting the Cables to the MPX Appliance.

2. Run the terminal emulation program on your computed to connect to the appliance.
   - For Microsoft Windows, you can use the HyperTerminal.
     Note: HyperTerminal is not automatically installed on Windows 2000 Server, Windows Server 2003, or Windows Server 2008. To install HyperTerminal, use Add or Remove Programs in Control Panel.
   - For Apple Macintosh OS X, you can use the Terminal program or the shell-based telnet client.
     Note: Mac OS X is based on the FreeBSD UNIX platform. Most standard UNIX shell programs are available from the OSX command line.
   - For UNIX-based workstations, you can use the shell-based telnet client or any supported terminal emulation program.

3. Press ENTER. The terminal screen displays the logon prompt.
   Note: You might have to press ENTER two or three times, depending on the terminal program you are using.

4. Log on to the appliance by using the administrator credentials.
   The default user name and password is nsroot.

5. At the command prompt, type config ns to run the configuration script.

6. To complete the initial configuration of your appliance, follow the prompts.
   Note: To prevent an attacker from breaching your ability to send packets to the appliance, choose a non-routable IP address on your organization's LAN as your appliance IP address.

Instead of step 5 and 6, you can directly enter the commands for the initial configuration. Log on to the appliance and at the command prompt, type:

set ns config - **ipaddress** <IPAddress> -netmask <Netmask>

add ns ip <IPAddress> <Netmask> -type <Type>

add route <Network> <Netmask> <Gateway>

set system user nsroot <Password>

save ns config

reboot

Example

set ns config - ipaddress 10.102.29.60 - netmask 255.255.255.0

add ns ip 10.102.29.61 255.255.255.0 -type snip

add route 0.0.0.0 0.0.0.0 10.102.29.1

set system user nsroot administrator

save ns config

reboot

The initial configuration of your appliance is complete. To continue configuring the appliance, see **section** NetScaler Gateway. Note: For information about deploying a high availability pair, see **section** Configuring High Availability on NetScaler Gateway.

Configuring Initial Settings by Using the Setup Wizard

Jul 15, 2013

To configure the NetScaler Gateway appliance by using the Setup Wizard in the configuration utility, you need a computer that is configured on the same network as the appliance. You also need a minimum of Java Runtime Environment (JRE) version 1.6. You can use the Setup Wizard to configure the following initial settings on the appliance:

- System IP address and subnet mask
- Mapped IP address and subnet mask
- Host name
- Default gateway
- Licenses

Important: Before running the Setup Wizard, you should download your licenses from the Citrix web site and put them in a location on your computer or another device where you can access them from your web browser during configuration. Note: When you finish installing and configuring the initial settings on the NetScaler Gateway appliance by using the command-line interface, when you log on to the configuration utility for the first time, the First-time configuration appears if the following conditions are not met:

- You did not install a license on the appliance.
- You did not configure a subnet or mapped IP address.
- If the default IP address of the appliances is 192.168.100.1.

For more information about the first time configuration, see section Configuring NetScaler Gateway with the First Time Use Configuration.

To run the Setup Wizard

1. In a Web browser, type http://192.168.100.1
   Note: NetScaler Gateway is preconfigured with a default IP address of 192.168.100.1 and associated subnet mask of 255.255.0.0.
2. In User Name and Password, type the administrator credentials and then click Login.
   The default user name and password is nsroot.

3. In the configuration utility, in the navigation pane, click System.
4. In the details pane, click Setup Wizard.
5. In the Setup Wizard, click Next, and then follow the instructions in the wizard.
   Note: On the Choose Application page, click Skip this step. The Choose Application page is used primarily for appliances that are licensed to use NetScaler features.

Note: To prevent an attacker from breaching your ability to send packets to the appliance, choose a non-routable IP address on your organization's LAN as your appliance IP address.
The initial configuration of your appliance is complete. To continue configuring the appliance, see NetScaler Gateway 10.1 , Access Gateway 10, or Access Gateway 9.3, Enterprise Edition.
Note: For information about deploying a high availability pair, see section Configuring High Availability on NetScaler Gateway.

Using DHCP for Initial Access

Jul 15, 2013

For the initial configuration of a NetScaler Gateway appliance, Dynamic Host Configuration Protocol (DHCP) can eliminate dependency on the console by providing an IP address at which you can access the appliance to configure it remotely. You can also use DHCP after the initial configuration if, for example, you want to move an appliance to a different subnet.

To use DHCP, you must first specify the NetScaler Gateway vendor class identifier on a DHCP server. Optionally, you can also specify the pool of IP addresses from which your appliance can acquire an IP address. If a pool is not specified, the address is acquired from the general pool.

A new NetScaler Gateway appliance does not have a configuration file. When you connect a NetScaler Gateway appliance without a configuration file to the network, its DHCP client automatically polls the DHCP server for an IP address. If you have specified the vendor class identifier on the DHCP server, the server returns an address. You can also enable the DHCP client on a previously configured NetScaler Gateway appliance.

Prerequisites

To use DHCP, you must:
1. Note the system ID (sysid) on the serial number sticker on the back panel of the appliance.
2. Set up a DHCP server and configure it with the vendor class identifier.

To configure a Linux or UNIX DHCP server for NetScaler Gateway

1. Specify "citrix-NS" as the vendor class identifier for the appliance by adding the following configuration to the server's dhcpd.conf file:
   subclass "citrix-1" "citrix-NS"{
   vendor-option-space auto;
   option auto.key "citrix-NS";
   Note: The location of the dhcpd.conf file can be different in different versions and flavors of the Linux/UNIX-based operating system (for example, in FreeBSD 6.3 the file is present in the /etc/ folder). For the location, see the dhcpd man page of the DHCP server.
2. If you do not want NetScaler Gateway to use IP addresses from the general pool, specify a pool of addresses for the appliance. For example, adding the following configuration to the dhcpd.conf file specifies a pool of IP addresses ranging from 10.102.33.246 to 10.102.33.249.
   pool {
   allow members of "citrix-1";
   range 10.102.33.246 10.102.33.249;
   option subnet-mask 255.255.255.0;
   }
3. Terminate the DHCP process and restart it to reflect the change to the configuration file. At the shell command prompt, type:
   killall dhcpd

   dhcpd&

Implementing an Initial NetScaler Gateway Configuration from a Remote Computer

When a new NetScaler Gateway (or any appliance that does not have a configuration file) starts, it automatically polls the

DHCP server for an IP address and provides the DHCP server with its sysid. The DHCP server includes this sysid with the IP address that it assigns to the appliance in the server's dhcpd.leases file. To find the IP address currently assigned to your NetScaler Gateway, look in the dhcpd.leases file for the last entry with the sysid of your appliance in the uid or client-hostname field. Verify that the binding state in this entry is active. If the binding state is not active but free, the IP address is not yet associated with the appliance.

You can use this address to connect to NetScaler Gateway and remotely configure the initial settings. For example, you can change the IP address, subnet mask, and gateway settings that were fetched from the DHCP server. After completing the initial configuration, you can manually return the DHCP IP address to the server pool. Alternatively, restarting the appliance automatically releases the DHCP IP address back to the server pool. A restart also saves the NetScaler Gateway configuration file.

Example

The following code example shows an entry in a DHCP server's dhcpd.leases file. This entry verifies the binding state of the appliance with a sysid of 45eae1a8157e89b9314f.

```
lease 10.102.33.248 {
  starts 3 2009/08/19 00:40:37;
  ends 3 2009/08/19 06:40:37;
  cltt 3 2009/08/19 00:40:37;
  binding state active;
  next binding state free;
  hardware ethernet 00:d0:68:11:f4:d6;
  uid "45eae1a8157e89b9314f";
  client-hostname "45eae1a8157e89b9314f";
```
In the preceding example, the binding state is ACTIVE and the IP address assigned to the NetScaler is 10.102.33.248.

The following table describes DHCP-related command-line interface commands that you might want to use when configuring a new NetScaler Gateway.

Table 1. Command-line interface commands for using DHCP with a new NetScaler Gateway

Task	At the command prompt, type:
To verify the DHCP fetched details, such as IP address, subnet mask, and gateway on the appliance.	> sh dhcpParams
To release the DHCP IP address and return it to the IP address pool on the DHCP server when the appliance configuration is complete.	> release dhcpIP

Using DHCP When a Configuration File Is Present

If you need to move a NetScaler Gateway appliance to a different subnet, such as from a testing environment to a production environment, you can use DHCP to access a NetScaler Gateway that already has a configuration file. Before

moving the appliance, enable its DHCP client and save the configuration. As a result, when the appliance restarts, it automatically polls the DHCP server for an IP address. If you did not enable the DHCP client and save the configuration before shutting down the appliance, you will need to connect to the appliance through the console and dynamically run the DHCP client on the appliance. The DHCP server will then provide an IP address, a gateway, and a subnet mask. You can use the IP address to access the appliance and configure the other settings remotely.

If the DHCP client is enabled in the configuration file, you should disable it and then save the configuration file. If the DHCP client is enabled, the appliance will poll the DHCP server again for an IP address when it restarts.

The following table lists the command-line interface commands associated with each task.

Table 2. Command-line interface commands for using DHCP with a previously configured NetScaler Gateway

Task	At the command prompt, type:
To dynamically run the DHCP client to fetch an IP address from the DHCP server	> set dhcpParams dhcpClient on
To configure the DHCP client to run when the appliance restarts	> set dhcpParams dhcpClient on > save config
To prevent the DHCP client from running when the appliance restarts	> set dhcpParams dhcpClient off > save config Note: This is required only if the ON setting was saved.

The initial configuration of your appliance is complete.

Accessing an Appliance by Using SSH Keys and No Password

Apr 16, 2013

In a setup where you have a large number of appliances in a network, you need to store and look up passwords for each appliance before you can log on to the appliance. You can set up Secure Shell (SSH) access with public key encryption on the appliances so that you are not prompted for the password. To do this, generate the public/private key on the Linux client and then copy the public key to the appliance.

To generate the public/private key on a Linux client

1. Change the directory to /root/.ssh.
2. Generate the public and private key pair. At the command prompt, type [root@localhost .ssh]# ssh-keygen -t rsa
3. Press Enter when prompted for a file name to save the key.
4. Press Enter when prompted for a passphrase.

To copy the public key (id_rsa.pub) to the remote appliance

1. Log on to the remote appliance from the Linux client.
2. Change the directory to /nsconfig/ssh. At the command prompt, type: cd /nsconfig/ssh
3. Change to binary mode and copy the public key to this directory. At the command prompt, type:
   bin
   put id_rsa.pub

To set up SSH access with public key encryption on the appliance

1. Open a connection to the appliance using a telnet/SSH client, such as PuTTY.
2. Log on to the appliance using the administrator credentials.
3. At the shell prompt, change the directory to /nsconfig/ssh.
4. Append the public key to the authorized_keys file and change permissions. At the command prompt, type:
   cat id_rsa.pub >> authorized_keys
   chmod 755 authorized_keys
5. Remove the public key (optional). At the command prompt, type rm id_rsa.pub
6. At the prompt type the following command to complete the configuration:
   * cp authorized_keys /root/.ssh/authorized_keys2
7. Change the directory to /nsconfig. At the prompt type:
   cd /nsconfig

8. To prevent your changes from being lost if the appliance is restarted, add the following line to the rc.netscaler file:
   * cp /nsconfig/ssh/authorized_keys /root/.ssh/authorized_keys2
   Important: If the /nsconfig directory does not contain a rc.netscaler file, you must create one.

To verify SSH access with public key encryption on the appliance

On the Linux client, verify that you can connect to the remote appliance using SSH, without entering the password.

At the prompt, type:

ssh nsroot@<NSIPaddress>

You should not receive a prompt for a password.

Example

ssh nsroot@10.102.96.50

NetScaler Gateway Virtual Appliances

Jul 18, 2013

Citrix NetScaler Gateway VPX is a virtual appliance that delivers the same features and functionality as the physical appliance. You can deploy NetScaler Gateway VPX as a virtual workload on your own hardware, in addition to or as an alternative to using a physical appliance.

Like the NetScaler Gateway physical appliance, NetScaler Gateway VPX is a secure application access solution that provides administrators granular application-level control while empowering users with access from anywhere. It gives IT administrators a single point of control to manage access and actions based on both the user and the endpoint device, providing better risk, security, and compliance management.

NetScaler Gateway VPX supports the following versions:

- NetScaler Gateway 10.1
- Access Gateway 10
- Access Gateway 9.3, Enterprise Edition
- Access Gateway 5.0

You can install the software on your hypervisor of choice and receive the same granular configuration as with the physical appliance. User connections work the same as with the virtual appliance and you can use the same settings that you configure on the physical appliance.

In This Section

This section of eDocs contains information about installing, setting up, and configuring the basic settings for NetScaler Gateway VPX.

Introducing NetScaler Gateway VPX	Contains information about the NetScaler Gateway VPX architecture and hypervisor management tools.
System Requirements for NetScaler Gateway VPX	Contains information about specific hardware, virtual computer, and operating system requirements for the hypervisor management consoles and virtual appliances.
Downloading the Virtual Image for NetScaler Gateway VPX	Contains information about downloading and installing NetScaler Gateway VPX on Citrix XenServer, VMware ESX, or Microsoft Hyper-V. It also includes information about upgrading NetScaler Gateway VPX for 10.1, 10, or 9.3 .
Configuring NetScaler Gateway VPX for the First Time	Contains instructions for configuring basic settings for NetScaler Gateway VPX for the first time.

Introducing NetScaler Gateway VPX

Jul 18, 2013

NetScaler Gateway VPX is a virtual NetScaler Gateway appliance that is hosted on a hypervisor, such as Citrix XenServer. NetScaler Gateway VPX supports all the features and functionality of the physical NetScaler Gateway appliance.

You install the NetScaler Gateway VPX into your network where it functions as if you installed the physical appliance. NetScaler Gateway 10.1, and Access Gateway VPX 9.3 or 10 are virtual machine images that you can install and run on any hardware device that support the following minimum versions:

- XenServer 5 Update 3
- VMware ESX Version 3.5
- VMware ESXi Version 3.5
- Windows Server 2008 R2 with Hyper-V role

Access Gateway VPX 5.0 is supported on the following hypervisors:

- XenServer Version 5.5 and Version 5.6
- VMware ESX Version 4.1 and Version 4.1
- VMware ESXi Version 4.0 and Version 4.1

For more information about XenServer, see XenServer documentation. For more information about VMware ESX or vSphere, or Microsoft Hyper-V, see the manufacturer's documentation.

Each supported hypervisor also has management software that you use to install and manage virtual appliances. The software includes:

- XenCenter that is the management console for XenServer
- vSphere that is the management console for VMware ESX and ESXi
- Hyper-V Manager that is the management console for Windows Server 2008 R with the Hyper-V role enabled

These requirements are for the NetScaler Gateway virtual appliance and are in addition to the hypervisor requirements.

Before you begin installing NetScaler Gateway VPX, do the following:

- Obtain the NetScaler Gateway license files from the Citrix web site.
- Install XenServer, VMware ESX, VMware ESXi, or Microsoft Hyper-V on hardware that meets the minimum requirements.
- Install XenCenter or vSphere on a management computer (or server) that meets the minimum system requirements. For details about the hardware requirements, see section Prerequisites for Installing NetScaler Gateway VPX on XenServer or VMware ESX.

This section discusses the NetScaler Gateway VPX architecture and the management consoles you can use to install and manage the virtual appliance.

NetScaler Gateway VPX Architecture

Jul 18, 2013

NetScaler Gateway VPX runs on a server virtualization platform that offers the same functionality as the physical appliance.

The following figureshows the architecture of NetScaler Gateway VPX:
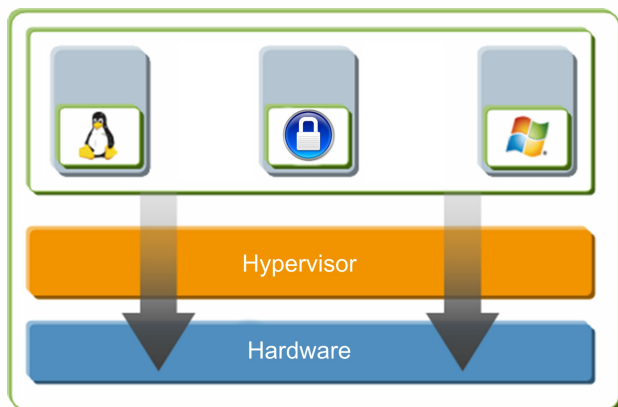
The solution architecture has the following components:

Hardware or physical layer:

Physical hardware components, including memory, CPU, network cards, and disk drives.

Hypervisor:

The hypervisor is a thin layer of software that runs on top of the hardware. The XenServer hypervisor, for example, gives each virtual machine a dedicated view of the hardware.

Virtual computer:

The operating system hosted on the hypervisor that appears to the user as a separate physical machine. The machine, however, shares physical resources with other virtual machines. The virtual machine is portable because it is abstracted from the physical hardware.

For example, you install NetScaler Gateway VPX on the hypervisor. The virtual appliance then uses drivers to access storage and network resources. NetScaler Gateway VPX appears to users as an independent NetScaler Gateway appliance with its own network identity, user authorization and authentication capabilities, configuration, and data. The virtual computers use the paravirtualization technique, which presents a software interface to virtual computers that is similar but not identical to that of the underlying hardware. This technique enables the virtual computers and the hypervisor to work together to achieve high performance for I/O and for CPU and memory virtualization.

About XenCenter

Jul 18, 2013

XenCenter is a graphical virtualization-management interface for XenServer that enables you to manage servers, resource pools, and shared storage, and to deploy, manage, and monitor virtual machines from your Windows-based desktop computer.

You use XenCenter to install NetScaler Gateway VPX on XenServer.

For more information about XenCenter, see the XenServer documentation.

Example of a NetScaler Gateway VPX Setup on XenServer

A NetScaler Gateway VPX setup provides secure remote access to applications and data.

The following figure shows how you can use NetScaler Gateway VPX with XenServer to deliver secure virtual application access.
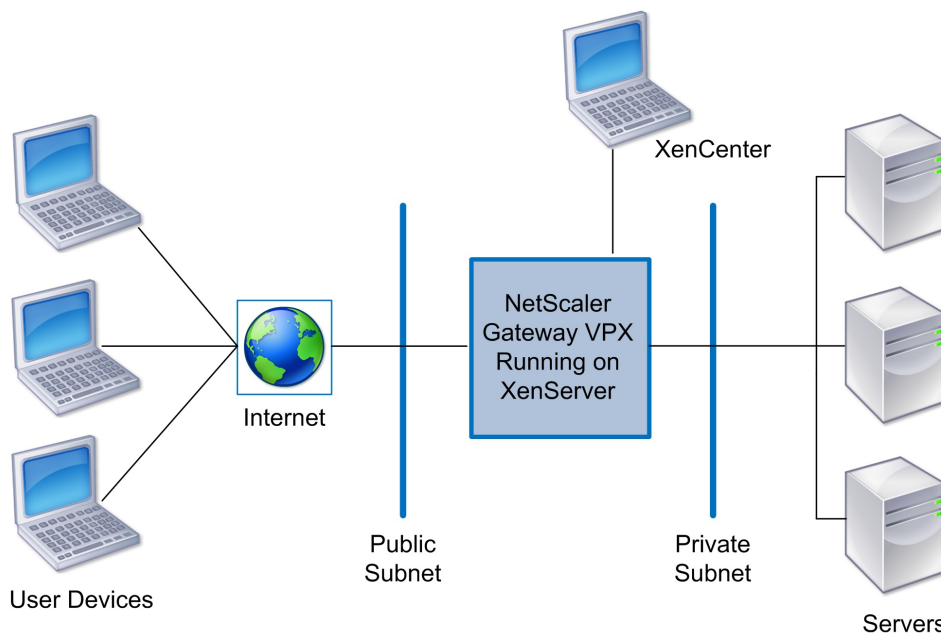
As shown in the preceding figure, NetScaler Gateway VPX, when deployed in front of application servers, acts as a secure entry point in the internal network for authenticated users.

About vSphere

Jul 18, 2013

vSphere is the management tool that you need to install to use and manage VMware ESX and VMware ESXi.

You use vSphere to install the virtual image file (.ova) for NetScaler Gateway on VMware. You also use vSphere to configure the basic settings of the virtual appliance. For details, see **section** Configuring NetScaler Gateway VPX for the First Time.

For more information about vSphere, see the vSphere documentation.

About Microsoft Hyper-V

Jul 18, 2013

The NetScaler Gateway VPX setup for the Microsoft Hyper-V platform requires Windows Server 2008 R2 with the Hyper-V role installed. Like all virtualization systems, Hyper-V enables you to create a virtualized computing environment that results in better usage of your hardware resources.

Hyper-V is a type 1 hypervisor that comes preinstalled with Windows Server 2008 R2. It needs to be enabled as a role on the Windows Server.

For more information about Hyper-V, see the Microsoft web site.

Note: Only Access Gateway VPX Versions 9.3 and 10 and NetScaler Gateway 10.1 support Microsoft Hyper-V.

System Requirements for NetScaler Gateway VPX

Jul 18, 2013

NetScaler Gateway VPX has specific hardware, virtual computer, and operating system requirements for the hypervisor management consoles. These requirements differ depending on the version of NetScaler Gateway VPX that you install.

This section contains the specifications for installing NetScaler Gateway VPX on XenServer, VMware ESX or ESXi, and Microsoft Hyper-V.

Prerequisites for Installing NetScaler Gateway VPX on XenServer or VMware ESX

Jul 18, 2013

NetScaler Gateway VPX is supported on the following minimum versions of XenServer and VMware hypervisors:

- XenServer 5 with Update 3
- VMWare ESX or ESXi 3.5

The following table describes the minimum specifications for the hardware on which the hypervisor—XenServer, VMware ESX, or VMware ESXi—runs Access Gateway VPX Versions 9.3 or 10, and NetScaler Gateway VPX 10.1.

For VMware system requirements, see the VMware web site.

Minimum requirements for the physical host server include:

Table 1. Minimum Hardware Requirements for the Hypervisor Host

CPU	Two or more 64-bit x86 CPUs with virtual assist enabled.
RAM	At least 4 gigabytes (GB).
Disk space	Locally attached storage (PATA, SATA, SCSI) with minimum of 20 GB of disk space.
Network	One 1 Gbps network adapter required; Recommended: Two network adapters of 1 Gbps each. For NetScaler Gateway VPX installed on VMware, the network adapter should be E1000.

Important Notes

- To run NetScaler Gateway VPX, you must enable hardware support for virtualization on the XenServer or VMware ESX host. Make sure that the BIOS option for virtualization support is enabled. Consult your BIOS documentation for more details.
- XenServer installation creates a 4-GB partition for the XenServer host control domain; the remaining space is available for NetScaler Gateway VPX and other virtual machines.

XenServer and VMware must provide adequate virtual computing resources to the NetScaler Gateway VPX as listed in the following table.

Table 2. Virtual Computing Resources of NetScaler Gateway VPX

Memory	2 GB for NetScaler Gateway VPX
Virtual CPU (VCPU)	Two VCPUs minimum for NetScaler Gateway VPX

Virtual Network Interfaces	For NetScaler Gateway, two virtual network interfaces
Minimum storage requirement	12 GB

Important Note

- If the virtual appliance is installed on ESX 3.5 or ESXi 3.5, you can install a maximum of 4 virtual network interfaces. If the virtual appliance is installed on ESX 4.0, the maximum is 10.

XenCenter System Requirements

XenCenter is a Windows-based application. The application cannot run on the same computer as the XenServer host. The following table describes the system requirements for XenCenter.

Table 3. System Requirements for XenCenter Installation

Operating system	Windows XP, Windows Server 2003, Windows Vista, or Windows 7
.NET Framework	Version 2.0, 3.0, 3.5, or 4
CPU	750 MHz minimum, 1 GHz or faster recommended
RAM	1 GB minimum, 2 GB recommended
Network	100 Mbps or faster network adapter

Prerequisites for Installing NetScaler Gateway VPX on Windows Server 2012 and Windows Server 2008 R2

Dec 23, 2013

You can install Access Gateway VPX 9.3 or 10, and NetScaler Gateway VPX 10.1 on Windows Server 2008 R2 or Windows Server 2012 with Hyper-V enabled.

Before you begin installing a virtual appliance, do the following:

- Enable the Hyper-V role. For more information about this task for Windows Server 2008 R2, see Hyper-V Installation on the Microsoft website. For more information for Windows Server 2012, see Install the Hyper-V Role and Configure a Virtual Machine on the Microsoft website.
- Download the VPX setup files.
- Obtain NetScaler Gateway VPX license files.

Windows Server 2008 R2 Hardware Requirements

The following table describes the minimum system requirements for Windows Server 2008 R2.

For more information about Windows Server 2008 R2 system requirements, see Windows Server 2008 System Requirements.

For information about installing Windows Server 2008 R2, see Installing Windows Server 2008 R2 in the Microsoft Technet Library.

The following table lists the virtual computing resources for each NetScaler Gateway VPX running on Hyper-V.

Table 1. Minimum Virtual Computing Resources Required for Running NetScaler Gateway VPX

Component	Requirement
RAM	4 GB
Virtual CPU	2
Disk space	20 GB
Virtual Network Interfaces	1

Downloading the Virtual Image for NetScaler Gateway VPX

Aug 26, 2013

The virtual image contains the package that you need in order to install NetScaler Gateway VPX on XenServer, VMware, or Hyper-V.

For the XenServer installation, the virtual image is a file with the file name extension of .xva.

For the VMware installation, the virtual image is a file with the file name extension of .ova.

For the Hyper-V installation on Microsoft Server 2008 R2, the virtual image is a file name with the file name extension of .vhd.

You can get the virtual image from the Citrix web site after you purchase NetScaler Gateway VPX.

To download NetScaler Gateway VPX

1. Go to the Citrix web site.
2. Click My Account and log on.
3. Click Downloads.
4. Under Find Downloads, select NetScaler Gateway.
5. In Select Download Type, select Virtual Appliances and then click Find.
6. On the NetScaler Gateway page, expand NetScaler Gateway or Access Gateway.
7. Click the appliance software version you want to download.
8. On the appliance software page for the version you want to download, select the virtual appliance and then click Download.
9. Follow the instructions on your screen to download the software.

To install NetScaler Gateway VPX by Using XenCenter

May 11, 2015

To install NetScaler Gateway VPX on XenServer, you must first install XenServer on a computer with adequate hardware resources. To perform the NetScaler Gateway VPX installation, you use XenCenter, which you must install on a remote computer that can connect to the XenServer host through the network. After you install NetScaler Gateway VPX, you can create virtual hardware components on XenServer. You can then use XenCenter to allocate the components to NetScaler Gateway VPX.

To use the virtual image of the NetScaler Gateway software, you need to obtain the exported virtual image file (.xva) and use XenCenter to import it to XenServer.

After you have installed and configured XenServer and XenCenter, you can use XenCenter to install NetScaler Gateway VPX on XenServer. Each instance of NetScaler Gateway VPX is a virtual NetScaler Gateway appliance running the same firmware as a physical appliance.

You can install XenCenter on any Windows-based computer in your network. You can download XenCenter from the XenServer download page on My Citrix. When you go to the download page, select your version of XenServer and then select the XenCenter Windows Management Console for your version to download and install XenCenter.

1. Click Start > All Programs > Citrix XenCenter.
2. In the navigation pane, click the name of the XenServer on which you want to install NetScaler Gateway VPX.
3. On the File menu, click Import.
4. In the Import dialog box, in Import file name, browse to the location to which you saved the NetScaler Gateway VPX .xva image file, click Open and then click Next.
5. On the Home server page, select the XenServer on which you want to install NetScaler Gateway VPX and then click Next.
6. On the Storage page, select the local storage repository in which to place the NetScaler Gateway VPX and then click Import to begin the import process.
7. On the Network page, click Add to add one or more virtual network interfaces and then click Next.
   Note: NetScaler Gateway VPX requires two network interfaces—one for the public (Internet) network and the second for the internal network.
   Caution: You must attach at least one network interface. If you do not attach a network interface, the virtual appliance automatically restarts and enters recovery mode. Subsequent logon attempts will fail. You will then need to delete the virtual appliance and reinstall it.
8. Click Finish to complete the import process.
   Note: You can click the Logs tab to view the status of the import process.

When importing the NetScaler Gateway virtual image is complete, you can then configure the basic settings for the appliance. For more information, see section Configuring NetScaler Gateway VPX for the First Time.

Installing NetScaler Gateway VPX by Using vSphere

May 11, 2015

To install NetScaler Gateway VPX on VMware ESX or VMware ESXi, you must first install VMware on a computer with adequate hardware resources. To perform the NetScaler Gateway VPX installation, you use vSphere, which you must install on a remote computer that can connect to the VMware host through the network. After you install NetScaler Gateway VPX, you can create virtual hardware components on VMware and then use vSphere to allocate them to NetScaler Gateway VPX.

To use the virtual image of the NetScaler Gateway software, you need to obtain the exported virtual image file (.ova) and import it to VMware by using vSphere.

After you install and configure VMware ESX and vSphere, you can use vSphere to install NetScaler Gateway VPX on VMware. Each instance of NetScaler Gateway VPX is a virtual NetScaler Gateway appliance running the same firmware as a physical appliance. NetScaler Gateway VPX and Access Gateway VPX Versions 10 and 9.3 support the VMware hypervisor and vSphere management tool.

Caution: During installation, you must attach at least one network interface. If you do not attach a network interface, the virtual appliance will automatically restart and enter recovery mode. Subsequent logon attempts will fail. You will then need to delete the virtual appliance and reinstall it.

To import the virtual image file to the vSphere Client

Make sure that the VMware computer or server is running.

1. Open the VMware vSphere Client. Click Start > VMware > VMware Vsphere Client.
2. Log on with your vSphere credentials.
3. Click File and then click Deploy OVF Template. The Deploy OVF Wizard opens.
4. In Source, select Deploy from file, browse to the .ova file on your computer, select the file and then click Next.
5. In OVF Template Details, click Next.
6. In Name and Location, type a name for the template, such as Citrix Access Gateway and then click Next.
7. In Ready to Complete, confirm the deployment settings, such as the host and cluster name, datastore, and network mapping and then click Finish.

Expand the IP address and the virtual appliance appears. If you want to install another NetScaler Gateway VPX image file, repeat Steps 3 through 7.

To turn on the virtual appliance

-   In the navigation pane, right-click the Citrix NetScaler Gateway VPX virtual image, click Power and then click Power On.

Installing NetScaler Gateway VPX on Microsoft Server 2008 R2

Jul 18, 2013

To install the NetScaler Gateway virtual appliance on Microsoft Windows Server 2008 R2, you must first install Windows Server 2008 R2, with the Hyper-V role enabled, on a computer with adequate system resources. While installing the Hyper-V role, make sure you specify the network adapters on the server that Hyper-V will use to create the virtual networks. You can reserve some network adapters for the host. You can use Hyper-V Manager to perform the NetScaler Gateway VPX installation.

Note: This functionality is only available in NetScaler Gateway 10.1 and Access Gateway Versions 9.3 and 10. NetScaler Gateway VPX for Hyper-V is delivered in virtual hard disk (VHD) format. It includes the default configuration for elements, such as CPU, network interfaces, and hard-disk size, and format.

After you install NetScaler Gateway VPX, you can configure the network adapters on NetScaler Gateway VPX and add virtual network adapters. Next, you assign the NetScaler Gateway IP address, subnet mask, and default gateway, and then you complete the basic configuration of the virtual appliance.

After you enable the Hyper-V role on Microsoft Server 2008 R2 and extracted the VPX files, you can use Hyper-V Manager to install NetScaler Gateway VPX. After you import the virtual appliance, you need to configure the virtual network adapters by associating them to the virtual networks created by Hyper-V.

You can configure a maximum of eight virtual network adapters. Even if the physical network adapter is down, the virtual appliance assumes that the virtual network adapter is up, because it can still communicate with the other virtual appliances on the same host (server).
Note: You cannot change any settings while the virtual appliance is running. Shut down the virtual appliance and then make changes.

To install NetScaler Gateway VPX by using Hyper-V Manager

1. To start Hyper-V Manager, click Start, point to Administrative Tools, and then click Hyper-V Managers.
2. In the navigation pane, under Hyper-V Manager, select the server on which you want to install NetScaler Gateway VPX.
3. On the Action menu, click Import Virtual Machine.
4. In the Import Virtual Machine dialog box, in Location, specify the path of the folder that contains the NetScaler Gateway VPX software files and then select Copy the virtual machine (create a new unique ID). This folder is the parent folder that contains the Snapshots, Virtual Hard Disks, and Virtual Machines folders.
   Note: If you received a compressed file, make sure that you extract the files into a folder before you specify the path to the folder.
5. Click Import.
6. Verify that the virtual appliance that you imported is listed under Virtual Machines.
7. To install another virtual appliance, repeat steps 2 through 6.
   Important: Make sure that you extract the files to a different folder in step 4.

To configure virtual network adapters for NetScaler Gateway VPX

1. Select the virtual appliance that you imported, and then on the Action menu, select Settings.
2. In the Settings for <virtual appliance name> dialog box, click Add Hardware in the left pane.
3. In the right pane, from the list of devices, select Network Adapter.

4. Click Add.
5. Verify that Network Adapter (not connected) appears in the left pane.
6. Select the network adapter in the left pane.
7. In the right pane, from the Network drop-down list, select the virtual network to connect the adapter to.
8. To select the virtual network for additional network adapters that you want to use, repeat steps 6 and 7.
9. Click Apply, and then click OK.

To configure NetScaler Gateway VPX

1. Right-click the virtual appliance that you previously installed and then click Start.
2. Access the console by double-clicking the virtual appliance.
3. Type the NetScaler Gateway IP address, subnet mask, and default gateway for your virtual appliance.

You have completed the basic configuration of your virtual appliance. Type the IP address in a Web browser to access the configuration utility for the virtual appliance.

Configuring NetScaler Gateway VPX for the First Time

After you import the virtual appliance to your hypervisor of choice, you can then configure the initial settings for the virtual appliance.

Configuring Basic Settings for NetScaler Gateway VPX

On NetScaler Gateway VPX 10.1 and Access Gateway VPX 9.3 or 10, you can configure the initial settings by either running a script in the command line or by using the Setup Wizard in the configuration utility. If you are using XenCenter or VMWare ESX or ESXi, you can click the Console tab, log on to NetScaler Gateway and then run the script.

To access the configuration utility for the first time to configure basic settings, type the NetScaler Gateway IP address default IP address into the address field of any web browser. You must be running a minimum of Java RunTime Environment (JRE) Version 1.6.

Configuring Basic Settings for Access Gateway VPX 5.0

After installing an instance of the Access Gateway VPX 5.0, you need to access the virtual appliance to configure the basic settings. When the installation is complete, you configure settings on the Console tab in the XenCenter Console or in vSphere. You configure the basic settings of the Access Gateway VPX as you would for a physical appliance that you connect using a serial cable and the serial console.

For details on using t he command line to configure initial network settings, see **section** Defining Network Settings on the Access Gateway Appliance by Using Express Set up.

You can use the XenCenter or vSphere serial console to set the IP address and subnet of the network adapter that is called eth0, as well as the IP address of the default gateway device. For Access Gateway VPX 5.0, you use the management console. You can also use the XenCenter or vSphere console to test a connection by using the PING command.

Access Gateway VPX requires two network interfaces—one for the public (Internet) network and the second for the internal network. For Access Gateway VPX 5.0, you can configure up to four network interfaces.

Caution: You must attached at least one network interface. If you do not attach a network interface, the virtual appliance will automatically restart and enter recovery mode. Subsequent logon attempts will fail. You will then need to delete the virtual appliance and reinstall it.

In Access Gateway VPX 5.0, you can select a management role for a **network** adapter that administrators use to connect to the management console and, optionally, t o connect wit h Secure Shell (SSH) t o the appliance. For details, see **section** Designating Network Adapters for Specific Uses. On the same Networking panel in t he management console, you can configure two Access Gateway appliances as a failover pair. You must designate an appliance failover role for a **network** adapter on each appliance in t he pair to support healthy monitoring traffic and to synchronize session information. For details, see How Appliance Failover Works on Access Gateway 5 .0.

Configuring Basic Settings for Access Gateway VPX 4.6

After installing an instance of the Access Gateway VPX 4.6, you need to access the virtual appliance to configure the basic settings. When the installation is complete, you configure settings on the Console tab in the XenCenter console. You configure the basic settings of Access Gateway VPX as you would for a physical appliance that you connect using a serial cable and the serial console.

For details on using the command line to configure initial network settings, see Access Gateway 4.6 Standard Edition documentation in the eDocs archive.

You can use the XenCenter serial console to set the IP address and subnet of the network adapter that is called eth0, as well as the IP address of the default gateway device. For Access Gateway VPX 4.6, you use the Administration Tool to configure all other settings. You can also use the XenCenter console to test a connection by using the PING command.

Access Gateway VPX requires two network interfaces—one for the public (Internet) network and the second for the internal network. For Access Gateway VPX 4.6, you cannot configure more than two network interfaces.

Access Gateway VPX 4.6 and 5.0 supports both one-arm and two-arm modes:

- One-arm mode uses one virtual network interface for inbound and outbound connections. In one-arm mode, a single IP address is assigned to Access Gateway. The default configuration of Access Gateway is one-arm mode.
- Two-arm mode uses two virtual network interfaces, one for external and one for internal connections. In two-arm mode, two IP addresses are assigned to Access Gateway—one for the external interface and one for the internal interface.

Upgrading NetScaler Gateway VPX

Jul 18, 2013

After you install NetScaler Gateway VPX on your hypervisor, you can then upgrade to new versions of the software by using the same method that you use for the physical appliance.

You can upgrade the software that resides on NetScaler Gateway when new releases are made available. You can check for updates on the Citrix Web site. You can upgrade to a new release only if your NetScaler Gateway licenses are under the Subscription Advantage program when the update is released. You can renew Subscription Advantage at any time. For more information, see the Citrix Web site.

When a new version is released, you download the .tgz file to your computer, copy the file to the NetScaler Gateway virtual appliance, and then upgrade by using either the command line or the configuration utility.

For the most recent Access Gateway 9.3, Enterprise Edition maintenance release readme, see article CTX129345 in the Citrix Knowledge Center.

For the most recent Access Gateway 10 maintenance release readme, see article CTX133966 in the Citrix Knowledge Center.

To download the VPX software for your NetScaler Gateway version, see section Downloading the Virtual Image for NetScaler Gateway VPX.

To upgrade NetScaler Gateway by using the Upgrade Wizard

1. In the configuration utility, in the navigation pane, click System.
2. In the details pane, click Upgrade Wizard.
3. Click Next and then follow the directions in the wizard.

To upgrade NetScaler Gateway by using a command prompt

1. Upload the software to NetScaler Gateway by using a secure FTP client, such as WinSCP, to connect to the appliance.
2. Copy the software from your computer to the /var/nsinstall directory on the appliance.
3. Use a Secure Shell (SSH) client, such as PuTTY, to open an SSH connection to the appliance.
4. Log on to NetScaler Gateway.
5. At a command prompt, type: shell
6. To change to the nsinstall directory, at a command prompt, type: cd /var/nsinstall
7. To view the contents of the directory, type: ls
8. To unpack the software, type: tar –xvzf build_X_XX.tgz
   where build_X_XX.tgz is the name of the build to which you want to upgrade.

9. To start the installation, at a command prompt, type: ./installns
10. When the installation is complete, restart NetScaler Gateway.

After NetScaler Gateway restarts, to verify successful installation, start the configuration utility. The NetScaler Gateway version that is on the appliance appears in the upper-right corner.

Deleting the NetScaler Gateway Virtual Image

Jul 09, 2013

If a virtual image is no longer required, you can use XenCenter or vSphere to delete the virtual image. Deleting a virtual image is the same as disconnecting the physical appliance from your network and removing it from the rack.

Note: When you delete the virtual appliance from XenCenter, if you do not delete the attached virtual disks, the virtual disks consume disk space in the XenServer resource pool.

To delete the virtual image in XenCenter

1. Start XenCenter on your computer.
2. In the navigation pane, right-click a NetScaler Gateway virtual image and then click Shut Down.
3. WhenNetScaler Gateway is shut down, right-click the virtual image and then click Delete.
4. Select Delete attached virtual disks and then click OK.

To delete the virtual image in vSphere

1. Open the VMware vSphere Client.
2. In the navigation pane, right-click the NetScaler Gateway virtual image, click Power and then click Power Off.
3. When NetScaler Gateway is shut down, right-click the virtual image and then click Delete from Disk.

To delete the virtual image in Microsoft Hyper-V

To delete the virtual image from Microsoft Hyper-V, you use the Hyper-V Manager. You can use the following guidelines:

- Remove all snapshots from the virtual image.
- Shut down the virtual image.

1. Remove all snapshots from the virtual image.
2. Shut down the virtual image.
3. Right-click the virtual image and click Delete.
4. Click Delete again.

This procedure removes the virtual image, but does not remove the virtual image files. To remove all the files, browse to the location where the virtual image is stored and delete the parent folder.

Importing NetScaler Gateway VPX to VMware

To install NetScaler Gateway VPX on VMware ESX or VMware ESXi, you must first install VMware on a computer with adequate hardware resources. To perform the NetScaler Gateway VPX installation, you use vSphere, which you must install on a remote computer that can connect to the VMware host through the network. After you install NetScaler Gateway VPX, you can create virtual hardware components on VMware and then use vSphere to allocate them to NetScaler Gateway VPX.

To use the virtual image of the NetScaler Gateway software, you need to obtain the exported virtual image file (.ova) and import it to VMware by using vSphere.

Former Access Gateway Appliance

Apr 18, 2013

The Model 2010 appliance supports Access Gateway 5.0. You can install the model 2010 in the DMZ or the secure network.

The preconfigured IP address of Access Gateway 5.0 on the Model 2010 is 10.20.30.40. To change the IP address, you can use a serial cable and a terminal emulation program, or you can connect Access Gateway by using network cables and the Access Gateway Management Console in Access Gateway 5.0.

Model 2010 Specifications

Sep 16, 2010

The Model 2010 appliance is a standard 1U 19 inch rack-mountable appliance that supports up to 500 concurrent users.

The 2010 appliance has the following ports:

- Two front-mounted 10/100/1000 Ethernet ports
- One RS232 front-mounted serial console port
- One rear-facing USB port

Prerequisites for Installing Access Gateway VPX Version 5.0 or 4.6

Sep 18, 2012

The following table describes the minimum specifications for the hardware on which the hypervisor—XenServer, VMware ESX, or VMware ESXi—runs Access Gateway VPX.

Table 1. Minimum Hardware Requirements for the Hypervisor Host

CPU	One or more 64-bit x86 CPUs
RAM	At least 2 gigabytes (GB)
Disk space	Locally attached storage (PATA, SATA, SCSI) with minimum of 40 GB of disk space. General disk space requirements for Access Gateway VPX: XenServer installation creates a 4-GB partition for the XenServer host control domain; remaining space is available for Access Gateway VPX and other virtual machines.
Network	One 1 Gbps network adapter required; Recommended: Two network adapters of 1 Gbps each

To install XenServer, see the XenServer Installation Guide on the Citrix Support Web site.

To install VMware, see the manufacturer's documentation.

XenServer and VMware must provide adequate virtual computing resources to the Access Gateway VPX as listed in the following table.

Table 2. Virtual Computing Resources of Access Gateway VPX

Memory	1 GB for Access Gateway VPX 4.6 From 1 up to 4 GB for Access Gateway VPX 5.0
Virtual CPU (VCPU)	One VCPU minimum, two VCPUs recommended for better performance. Access Gateway VPX can support up to eight cores.
Virtual Network Interfaces	For Access Gateway VPX 4.6, you can use one or two virtual network interfaces. For Access Gateway VPX 5.0, you can use up to four virtual network interfaces.
Minimum Storage Requirement	12 GB

XenCenter System Requirements

XenCenter is a Windows-based application. The application cannot run on the same computer as the XenServer host. The following table describes the system requirements for XenCenter:

Table 3. System Requirements for XenCenter Installation

Operating system	Windows XP, Windows Server 2003, Windows Vista, or Windows 7
.NET Framework	Version 2.0, 3.0, 3.5, or 4
CPU	750 MHz minimum, 1 GHz or faster recommended
RAM	1 GB minimum, 2 GB recommended
Network	100 Mbps or faster network adapter

For VMware system requirements, see the VMware Web site.

Setting Up the Model 2010 Appliance

May 16, 2011

The following procedures describe how to set up the Access Gateway Model 2010 appliance for the first time.

To physically connect the Access Gateway appliance

1. Install Access Gateway in a rack if it is rack-mounted.
2. Connect the power cord to the AC power receptacle.
3. Connect either the serial cable to a Windows-based computer, a cross-over cable to a Windows-based computer, or an RJ-45 network cable to a network switch and Access Gateway.
4. Configure the TCP/IP settings by following the instructions in **section** Configuring the Model 2010 Appliance.

Figure 1. Access Gateway connection options using a cross-over cable, a network switch, or terminal emulation

© 1999-2017 Citrix Systems, Inc. All rights reserved.
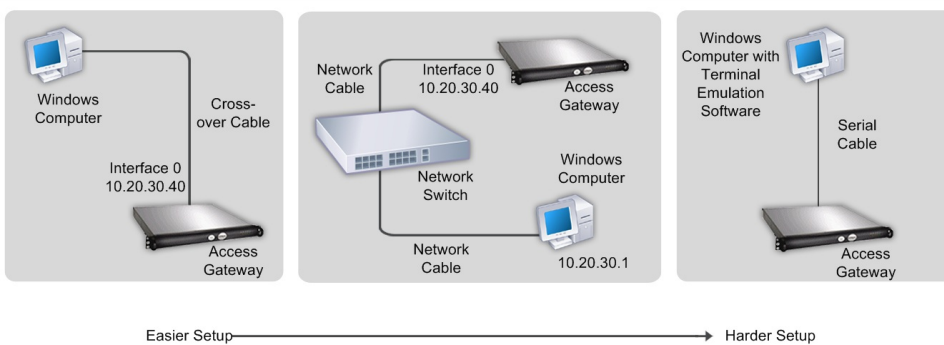
Installing the Model 2010 Appliance in a Rack

May 16, 2011

The following sections explain how to install the Access Gateway Model 2010 appliance in a rack:

- Identifying the Sections of the Rack Rails for the 2010 Appliance
- Installing the 2010 Appliance in a Four-Post Rack

Identifying the Sections of the Rack Rails for the 2010 Appliance

The 2010 appliance is delivered with a set of inner rails in two sections: inner rails and inner rail extensions. The inner rails are attached to the appliance and do not interfere with normal use of the appliance if you choose not to install the appliance in a rack.

The following illustration shows the sections of the outer rails for the Model 2010 appliance and how you should attach them to the rack.

Figure 1. Access Gateway Model 2010 rails
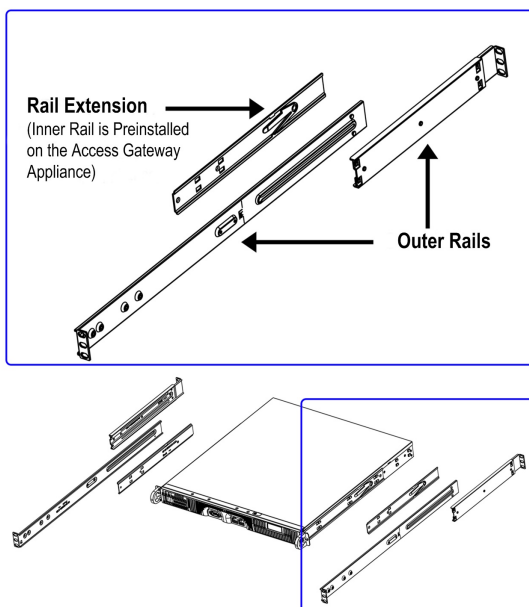
To identify the sections of the rack rails for the 2010 appliance

- Attach the inner rail extension to stabilize the appliance within the rack.

Installing the 2010 Appliance in a Four-Post Rack

The steps for installing the 2010 appliance in a four-post rack are:
- Installing the inner rail extensions on the appliance
- Installing the outer rails to the rack
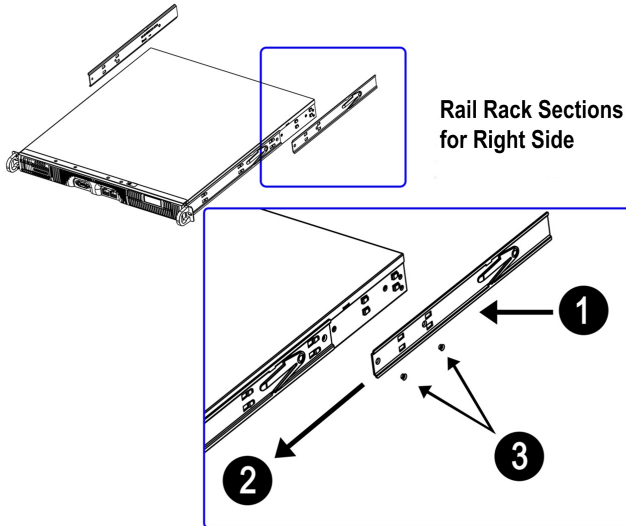- Installing the appliance in the rack

To install the inner rail extension

1. Place the inner rack extensions on the side of the appliance, aligning the hooks of the appliance with the rail extension

holes. Make sure the extension faces outward like the preattached inner rail.

2. Slide the extension toward the front of the chassis.
3. Secure the chassis with the two screws.
4. Repeat the above steps to mount the rack on the other side of the appliance.

The following illustration shows how you should attach the right-side rail rack sections to the appliance.

Figure 2. Attaching the rail rack sections to the right side of the appliance

When the rails are attached to the appliance, install the outer rails to the rack.

To install the outer rails to the rack

1. Attach the short bracket to the outside of the long bracket. The pins must be aligned with the slides. Both bracket ends must face the same direction.
2. Adjust both the short and long brackets to the correct distance so the rail fits tightly into the rack.
3. Secure the long bracket to the front side of the outer rail with two M5 screws and the short bracket to the rear side of the outer rail with three M5 screws.
4. Repeat the above steps for the second rail.
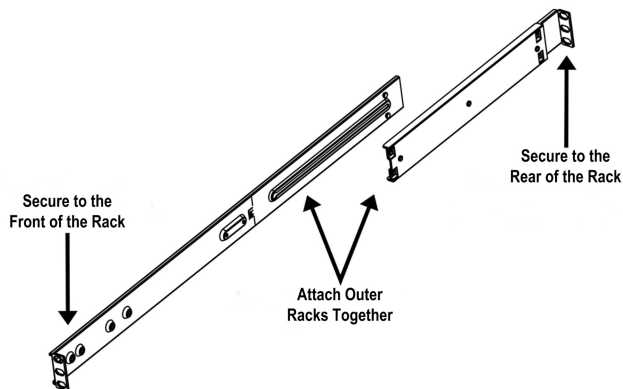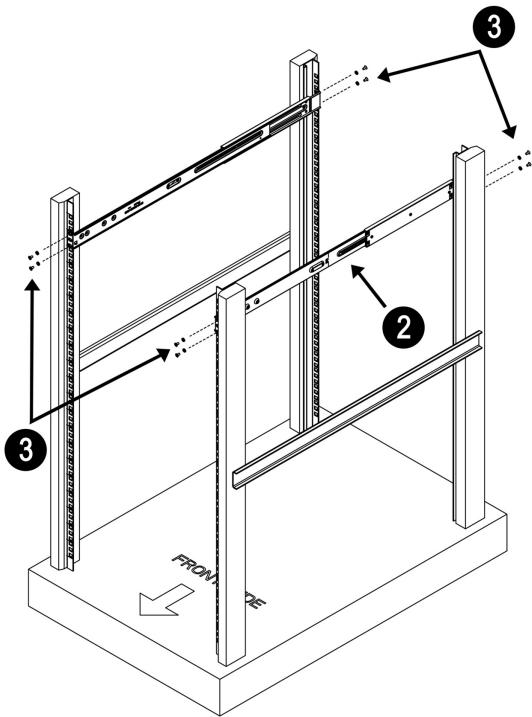
Figure 3. Assembling the outer rails to the rack

Figure 4. Installing the outer rails to the server rack

When the rails are installed in the rack, you can install Access Gateway.

To install the appliance in the rack

1. Confirm that the appliance includes the inner rails (A) and rail extensions (B). Confirm that the outer rails (C) are installed on the rack.
2. Line up the rails on the appliance (A and B) with the front of the rack rails (C).
3. Slide the appliance rails into the rack rails, keeping the pressure even on both sides. You might have to depress the locking tabs during insertion. When the appliance is pushed completely into the rack, you should hear the locking tabs click.
4. (Optional) Insert and tighten the thumbscrews that hold the front of the appliance to the rack.

Figure 5. Installing the Access Gateway into the rack
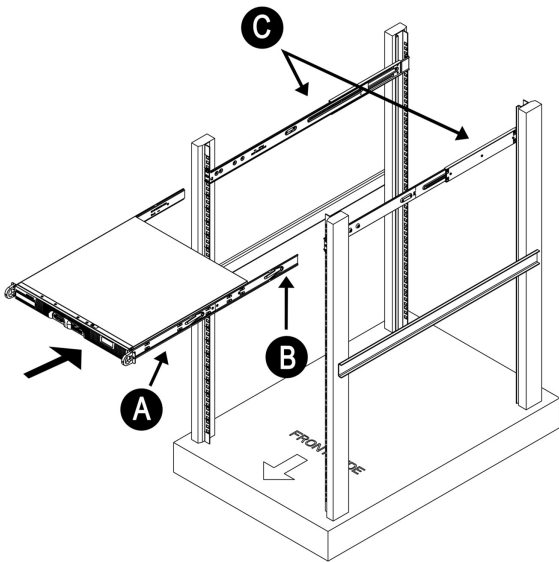
Installing the 2010 Appliance in a Two-Post Rack

If you are installing the appliance in a two-post (Telco) rack, follow the directions given on the previous pages for rack installation. The only difference in the installation procedure is the positioning of the rack brackets to the rack. Space them apart just enough to accommodate the width of the Telco rack, as shown in the following illustration.

Figure 6. Installing the Access Gateway in a two-post (Telco) rack
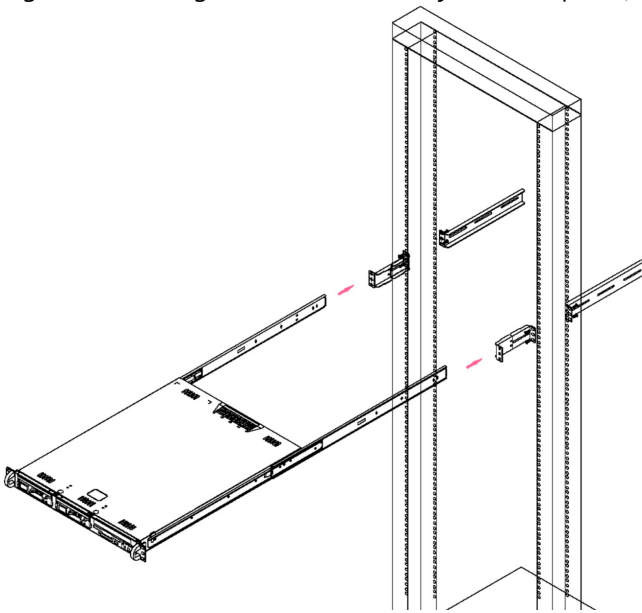
Turning on the Model 2010 Appliance

Jan 25, 2011

After you install the Access Gateway appliance in a rack and connect the cables, you are ready to turn on the appliance.

1. Verify that you are connected to the appliance through a console or Ethernet port.

   This step will ensure that you can configure the appliance after you turn it on.

2. Plug in the power cable.

   Note: The model 2010 appliance does not have a power switch, so the appliance turns on when you plug it in.

As it turns on, the appliance hums, and various lights on the surface flash. After a few seconds, the rapid changes in sound and lights become a steady hum.

Configuring the Model 2010 Appliance

Nov 12, 2012

You can use a serial console to configure the initial settings of Access Gateway. You can use the serial console to set the IP address and subnet of the network adapter that is called Interface 0, as well as the IP address of the default gateway device. You configure subsequent settings using the Management Console in Access Gateway 5.0 or the Administration Tool in Access Gateway 4.6.

For more information about configuring Access Gateway to work in your network, see the following:

- If you are using Access Gateway 5.0, see Access Gateway 5.0.
- If you are using Access Gateway 4.6, download the Access Gateway 4.6, Standard Edition PDF.

Replacing the Secure Gateway with NetScaler Gateway

Jul 15, 2013

If you currently use the Secure Gateway to enable remote access to servers running Citrix XenApp or Citrix XenDesktop, you can replace the Secure Gateway with Citrix NetScaler Gateway.

One of the benefits of choosing the appliance-based NetScaler Gateway includes support for additional applications and protocols. The software-based Secure Gateway is limited to support traffic on computers running XenApp or XenDesktop. Therefore, organizations that use the Secure Gateway might also deploy a remote access solution for other types of internal resources, adding more expense and work for administrators.

NetScaler Gateway can handle your organization's remote access needs by securing traffic to applications hosted by XenApp, desktops hosted by XenDesktop, as well as access to internal resources, such as email, internal Web applications, and network file shares. NetScaler Gateway, like the Secure Gateway, supports connections between Citrix online plug-ins, Desktop Receiver, and published resources in single-hop and double-hop DMZ deployments.

Note: When NetScaler Gateway is deployed in a double-hop DMZ, only connections between online plug-ins and published applications are supported. In this scenario, NetScaler Gateway does not support connections to additional internal resources by using the NetScaler Gateway Plug-in.
The benefits of replacing the Secure Gateway with NetScaler Gateway include:
- Replacing one or two Windows servers in the DMZ.
- Allowing for additional VPN functionality while maintaining the ability to access published applications and desktops.
- Allowing a broad range of user devices to connect to published applications in the secure network using Citrix online plug-ins.

The following figure shows a Secure Gateway deployment with the Web Interface in the DMZ with connections to computers running XenApp.

Figure 1. Secure Gateway deployment
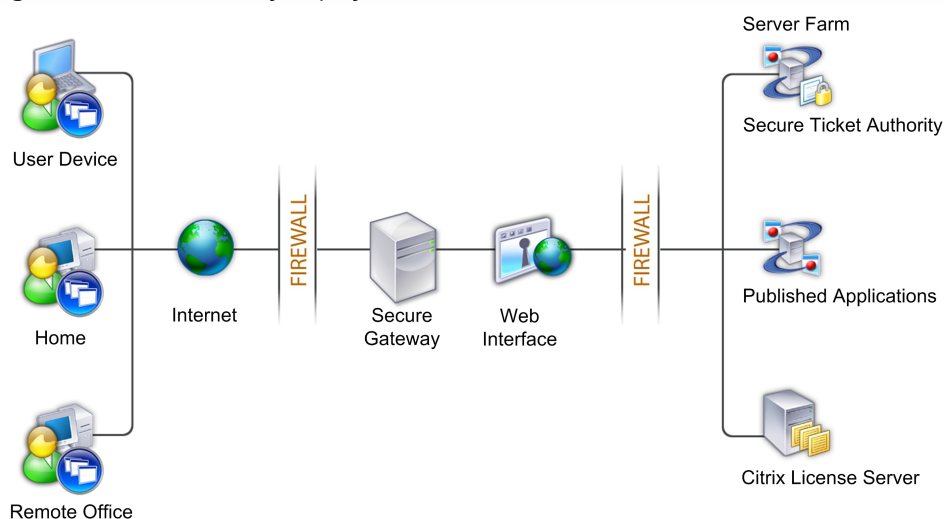
In this deployment, the Secure Gateway is running on a Windows server in the DMZ. The Web Interface is also deployed in the DMZ. XenApp or XenDesktop is running in the secure network. The Secure Ticket Authority (STA) is installed and configured automatically on XenApp and XenDesktop. If you have multiple servers running XenApp, you can receive

ticketing information from the STA on one server and published applications or desktops from another server.

The following figure shows the NetScaler Gateway deployment in the DMZ with the Web Interface located in the secure network:

Figure 2. NetScaler Gateway deployment
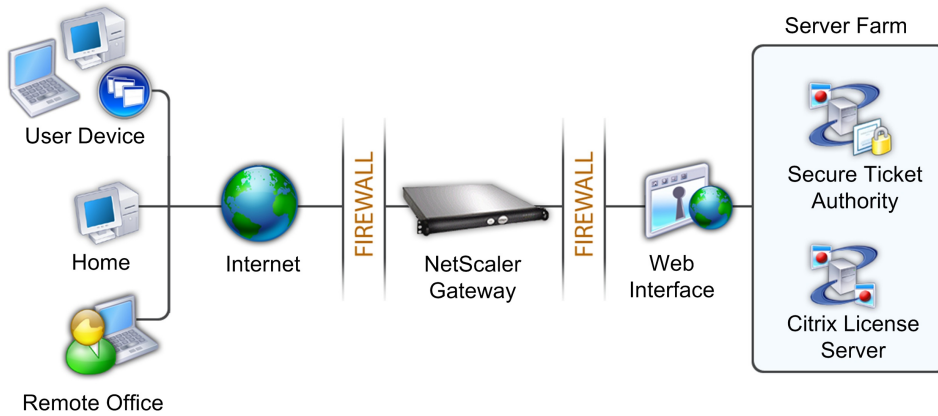
When the Secure Gateway is removed from the DMZ and replaced with NetScaler Gateway, you have the option of moving the Web Interface to the secure network. NetScaler Gateway authenticates and authorizes users and then connects to the Web Interface. This scenario provides greater security because there are two fewer Windows servers in the DMZ.

Important: When the Web Interface is placed in the secure network, you must configure authentication and authorization on NetScaler Gateway.

Migrating from the Secure Gateway to NetScaler Gateway

Jul 15, 2013

This topic discusses how to prepare to migrate from the Secure Gateway to NetScaler Gateway, and the two migration options you can choose: In-place migration or parallel migration.

Preparing to Migrate

Before migrating from the Secure Gateway to NetScaler Gateway, consider the following:

- Make sure that user devices meet system requirements. For more information about system requirements, see the appropriate guide for the Citrix online plug-in.
- Make sure port 443, the default security port on the firewall is open between the Internet and NetScaler Gateway. This requirement is identical in a Secure Gateway deployment.
- Install NetScaler Gateway. For details, see the installation instructions for your NetScaler Gateway appliance.
- Acquire and install the appropriate certificates on NetScaler Gateway. These include:
  - Server certificate for NetScaler Gateway
  - Root certificates for NetScaler Gateway, Secure Ticket Authority (STA), and user devices
- Configure the networks that users can connect to through NetScaler Gateway.

Migrating Options

You can choose from the following two options for migrating from the Secure Gateway to NetScaler Gateway:

- In-place migration, in which you transfer the certificate and fully qualified domain name (FQDN) on the Secure Gateway to NetScaler Gateway
- Parallel migration, in which you obtain a new signed certificate and FQDN for NetScaler Gateway

Each option is valid; however, the in-place migration has the potential to temporarily disrupt access to internal resources when compared with a new installation.

After the migration is complete, users can log on with their current credentials and do not have to perform any configuration to their device. Each option requires minimal user support.

Performing an In-Place Migration

When you choose an in-place migration from the Secure Gateway to NetScaler Gateway, you export the Secure Gateway certificate, upload it to NetScaler Gateway and bind it to a virtual server.

The certificate must be in PEM format before you can install it on NetScaler Gateway. If you are unfamiliar with the process of converting certificates, Citrix recommends a new installation of NetScaler Gateway and the use of a new certificate.
Important: If you are transferring a certificate from the Secure Gateway to Access Gateway Enterprise Edition, the FQDN of the certificate installed on the virtual server must match the FQDN of the Secure Gateway. With this option, you cannot take a phased approach because two identical FQDNs cannot reside on the same network.
An in-place migration is identical to a new installation of NetScaler Gateway, except for the following items:

- You use the Secure Gateway certificate on NetScaler Gateway

- The FQDN on the NetScaler Gateway certificate must match the FQDN of the Secure Gateway

Although in-place migration results in the least amount of user support (users do not need to be notified of a new Web address), if any mistakes are made in the configuration of the NetScaler Gateway that were not identified by proper testing procedures, all of your users are directly impacted. Mistakes could prevent users from logging on or connecting to published applications or desktops in the server farm.

Performing a Parallel Migration

Citrix recommends as a best practice that you run Secure Gateway parallel to NetScaler Gateway until all users are properly migrated to the appliance. To perform a parallel migration, you need to do the following:

- Obtain a new FQDN and certificate.
- Provide users with a new Web address for accessing resources to users.
- Provide users with a date when they will start using NetScaler Gateway.

A parallel migration gives you a greater level of control over configuration. You can undertake a phased migration approach, rather than transferring all users at one time as you would do during an in-place migration. You can migrate users to NetScaler Gateway in groups, thereby preventing downtime for connections.

Performing a parallel migration is identical to a new installation of NetScaler Gateway. You follow the steps to install the appliance, licenses, and certificates, in addition to configuring authentication and other settings on the appliance. Users continue to connect to the Secure Gateway until configuration of NetScaler Gateway is complete. The Secure Gateway runs parallel to NetScalter Gateway until you migrate all users successfully to the new environment. This option requires you to purchase or generate a new server certificate. A significant benefit, however, is that users do not experience a disruption in their access to internal resources.

To perform a parallel migration to NetScaler Gateway, complete the following steps:

1. Install NetScaler Gateway.
   This step configures the basic TCP/IP settings for NetScaler Gateway.

2. Configure the STA settings on NetScaler Gateway to connect to resources on computers running XenApp.
   Note: You can add more than one server running the STA to the list. The list of servers must be identical to the servers configured for the Web Interface.
3. Install a server certificate on NetScaler Gateway to secure client connections.
   Note: To use names that you can resolve for the STA and Web Interface, configure your Domain Name System (DNS) servers.
4. Configure the settings in the Web Interface for user access.
5. Remove the Web Interface from the DMZ and place it in the secure network.
   Note: You can also remove the server running the Secure Gateway from the DMZ and the server can be repurposed for another role.
6. After NetScaler Gateway is installed in your network, create a test user on NetScaler Gateway to test the connection.

If you have configured single sign-on to the Web Interface, users are logged on automatically and have access to published applications and desktops. If not, users log on to the Web Interface and can then can access their published applications or desktops.