SONICWALL®

Secure Mobile Access 10.2

Deployment Planning Guide

Contents

1

Deployment Scenarios Overview

Welcome to the SonicWall SMA Deployment Guide. SonicWall® Secure Mobile Access 210/410 and 500v provides a unified secure gateway to access all network and cloud resources. This guide contains configuration guidelines for deployment scenarios involving new DMZ, existing DMZ, and LAN deployments, along with basic configuration settings for those scenarios.

Topics:

Selecting a Deployment Scenario

The deployment scenarios described in this guide are based on actual customer deployments and are SonicWall-recommended deployment best practices for SMA appliances.

An SMA appliance is commonly deployed in one-arm mode over the DMZ interface on an accompanying gateway appliance, such as a SonicWall NSa 3600. This method of deployment offers additional layers of security control, plus the ability to use SonicWall's security services, including Gateway Anti-Virus, Anti-Spyware, Content Filtering, Intrusion Prevention Service, and Comprehensive Anti-Spam Service, to scan all incoming and outgoing traffic.

The primary interface (X0) on the SonicWall SMA connects to an available segment on the gateway device. The encrypted user session is passed through the gateway to the SMA appliance. The SonicWall SMA appliance decrypts the session and determines the requested resource.

The session traffic then traverses the gateway appliance to reach the internal network resources. The gateway appliance applies security services as data traverses the gateway. The internal network resource then returns the requested content to the SonicWall SMA appliance through the gateway, where it is encrypted and sent to the client.

SMA 210/410 and 500v Deployment Scenarios

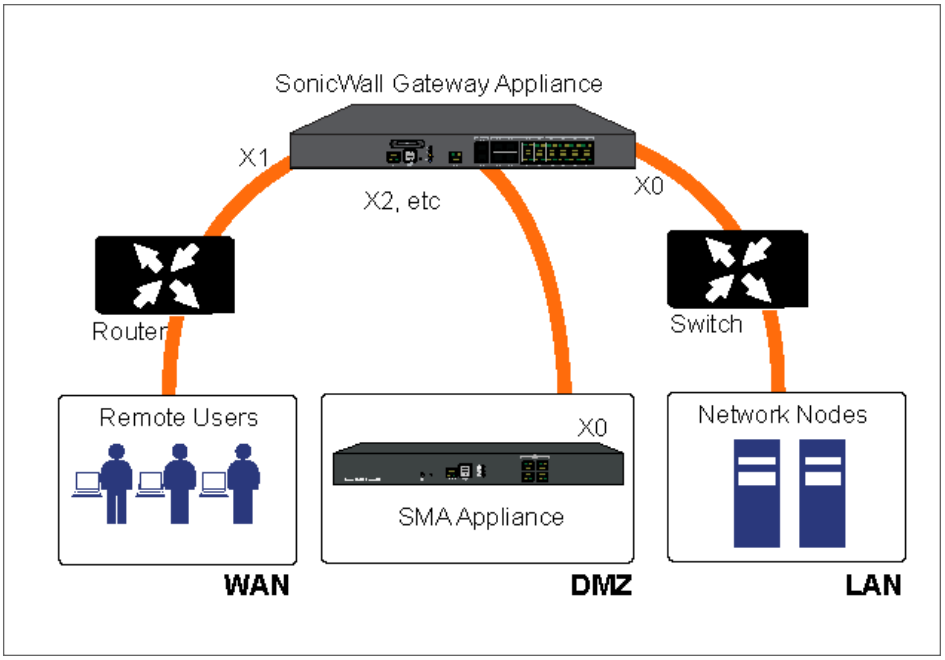
Gateway Appliance	Deployment Scenario	Requirements on Gateway Appliance
SonicOS 7 or higher: • TZ Series • NSa Series • NSsp Series • NSv Series	SMA on new DMZ	• An unused interface • NEW DMZ configured for NAT or Transparent Mode
	SMA on existing DMZ	• One dedicated interface in use as an existing DMZ
	SMA on LAN	• None

For a full list of the supported SonicWall firewall and firmware versions, see https://www.sonicwall.com/support/product-lifecycle-tables/

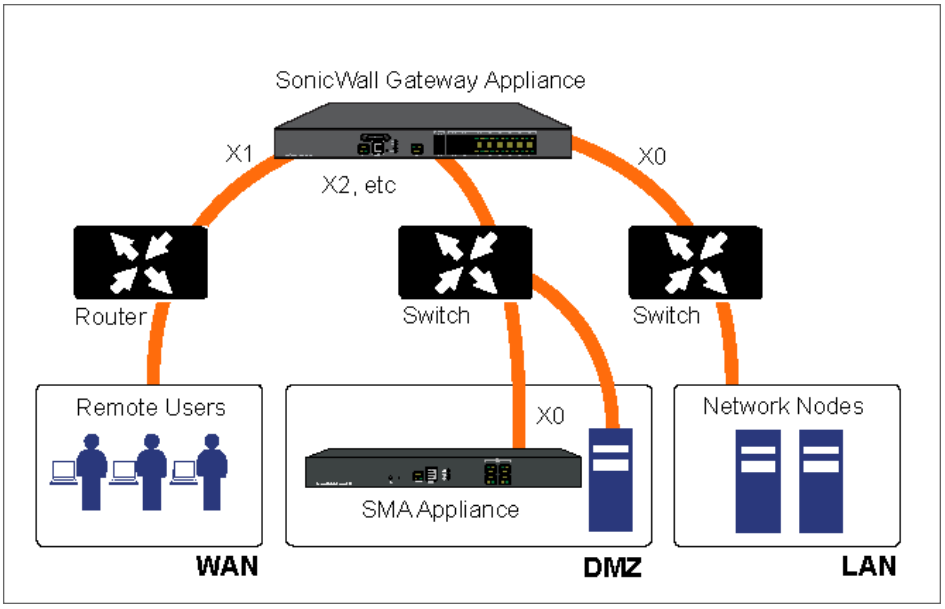
The following illustrations provide an overview of each deployment scenario:

- Overview of Scenario A: SMA on a New DMZ
- Overview of Scenario B: SMA on an Existing DMZ
- Overview of Scenario C: SMA on the LAN

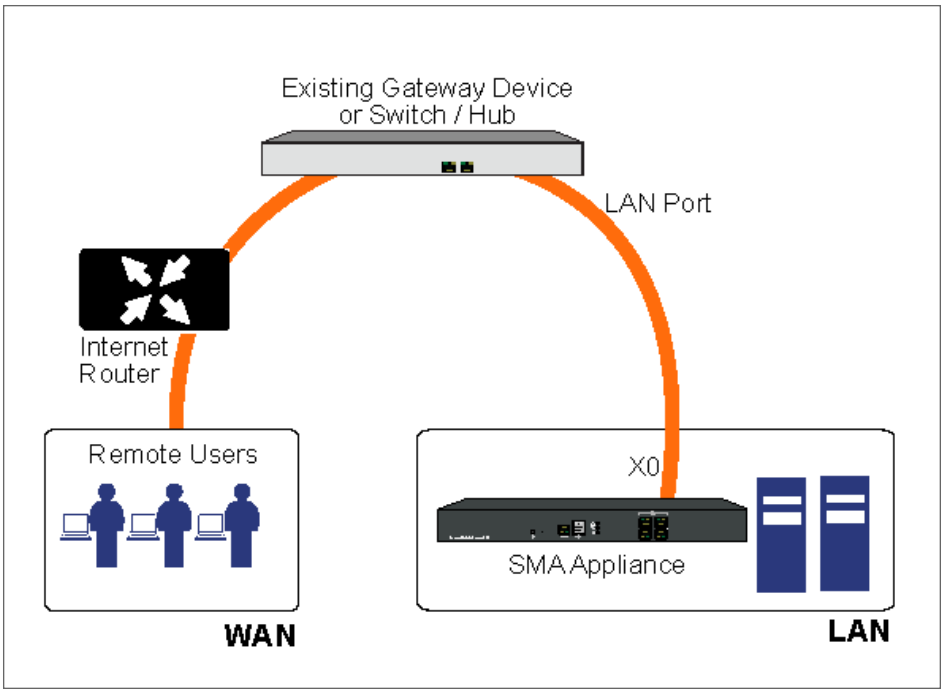
Overview of Scenario A: SMA on a New DMZ



Overview of Scenario B: SMA on an Existing DMZ



Overview of Scenario C: SMA on the LAN



2

Connecting the SMA on a New DMZ

The following procedures explain how to configure your gateway appliance on a new DMZ:

- Connecting the SMA to the Gateway
- Allowing a WAN to SMA Connection
- Allowing an SMA to LAN Connection

Connecting the SMA to the Gateway

To connect the SMA 210/410 and 500v using Scenario A:

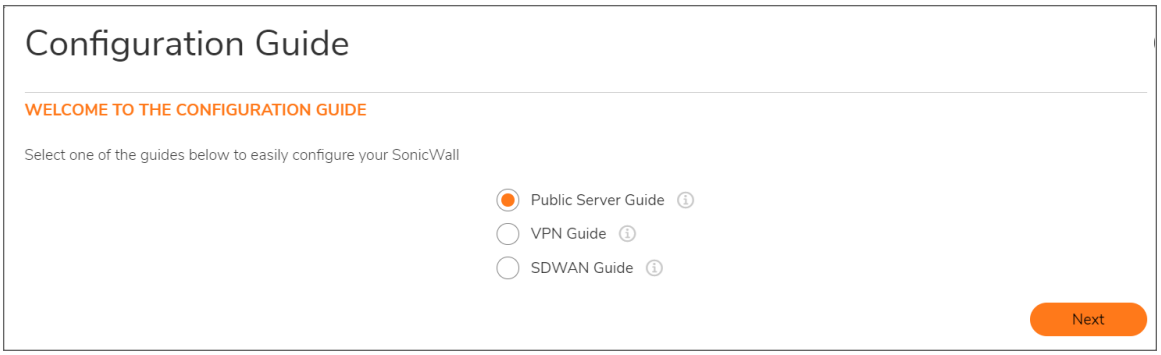
1. Connect one end of an Ethernet cable to an unused port on your SonicWall gateway appliance.
2. Connect the other end of the Ethernet cable to the X0 port on the front of your SonicWall Secure Mobile Access 210/410 and 500v. The X0 Port LED lights up indicating an active connection.
3. Configure the SMA X0 IP address. Refer to *Configuring the X0 IP Address*.

Allowing a WAN to SMA Connection

ⓘ **NOTE:** Before continuing, you must add a new SMA custom zone. Refer to *Adding a New SMA Custom Zone* for more information.

To allow a WAN to SMA connection:

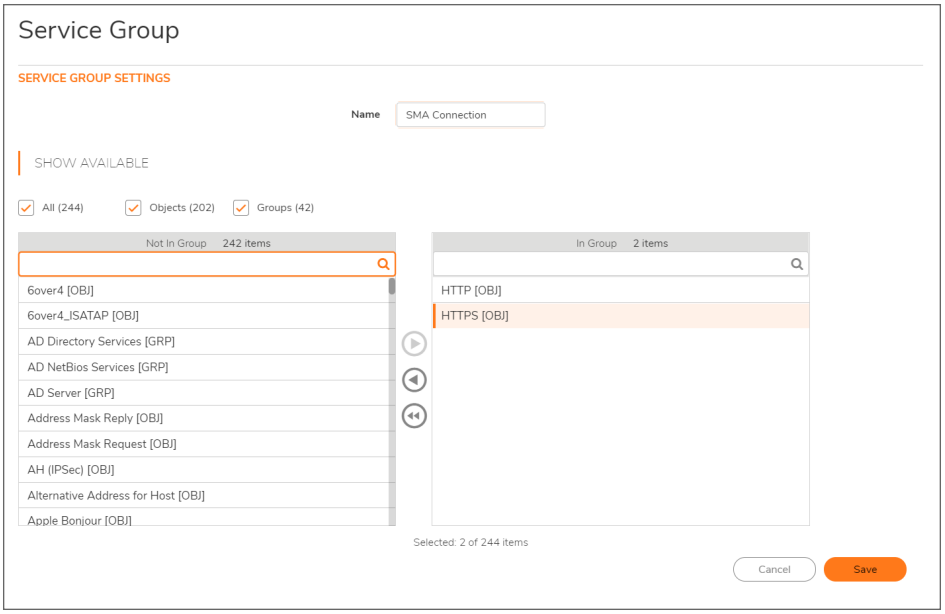
1. Using SonicOS, click the **Wizards** icon in the top right corner of the gateway appliance management interface.
2. On the **Configuration Guide** page, select the **Public Server Guide**, and then click **Next**.



3. On the **Public Server Guide**, select these options:

Service Type	Other
Services	Create new group

4. In the **Service Group** dialog box, create a service group for HTTP and HTTPS:
   - Enter a **Name** for the service.
   - Select both **HTTP** and **HTTPS** and click the arrow button to move them to the right column.
   - Click **Save**.



5. On the **Server Private Network Configuration** page, enter the following server and SMA information, and then click **Next**:

Server Name	Specify the name for the SMA appliance
Server Private IP Address	SMA appliance X0 IP address
Server Comment	Brief description of the server

6. On the **Server Public Information** page, accept the default IP address, or enter an IP address in your allowed public IP range. Click **Next**.

   NOTE: The default IP address is the WAN IP address of your SonicWall security appliance. If you accept this default, all HTTP and HTTPS traffic to this IP address will be routed to your SMA appliance.

7. The **Public Server Configuration Summary** page displays all the configuration actions that are performed. Click **Apply** to create the configuration and allow access from the WAN to the SMA on the DMZ.

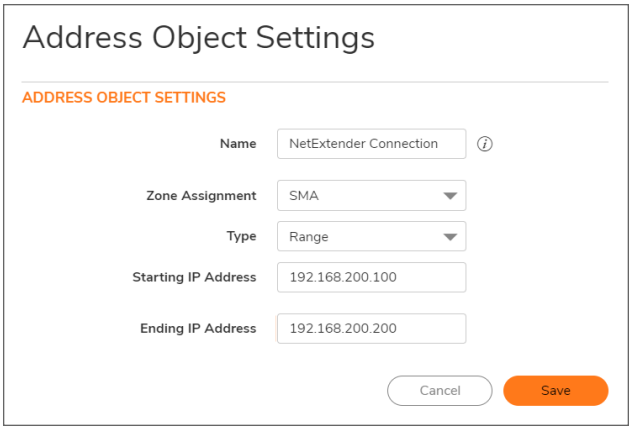
Allowing an SMA to LAN Connection

When users have connected to the SMA, they need to be able to connect to resources on the LAN.

To allow an SMA to LAN connection:

1. Using SonicOS, navigate to the **OBJECT | Match Objects > Addresses** page on the gateway appliance.
2. In the **Address Objects** tab, click **+Add**.
3. In the **Address Object Settings** dialog box, create an address object for the X0 interface IP address of your SMA appliance:

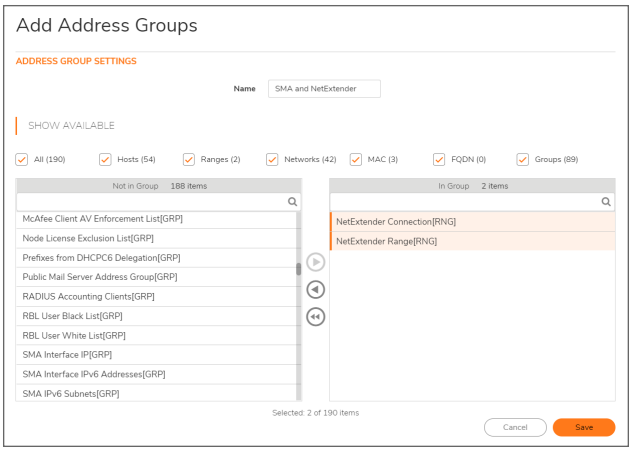
Name	Name of the SMA appliance
Zone Assignment	SMA
Type	Host
IP Address	SMA appliance X0 IP address (default 192.168.200.1)



4. Click **Save** to create the object. Once done, click **Close**.
5. Click **Add** again to create an address object for the NetExtender range.
6. In the **Add Address Object** dialog box, create an address object for the NetExtender range:

Name	Name for NetExtender range
Zone Assignment	SMA
Type	Range
Starting IP Address	Start of the NetExtender IP address range (default 192.168.200.100)
Ending IP Address	End of the NetExtender IP address range (default 192.168.200.200)

7. Click **Save** to create the object. Once added, click **Close**.
8. On the **OBJECT | Match Objects > Addresses** page, click the **Address Groups** tab.
9. Click **+Add**.
10. In the **Add Address Groups** dialog box, create a group for the X0 interface IP address of your SMA appliance and the NetExtender IP range:
    - Enter a name for the group.
    - In the left column, select the address objects you created and click the right arrow button.
    - Click **Save** to create the group when both objects are in the right column.



11. Navigate to the **POLICY | Rules and Policies > Access Rules** page, and select the **Matrix** view style.
12. Click the **SMA > LAN** icon.
13. On the page that displays for SMA to LAN, click **+Add**.

14. In the **Add Rule** window, create a rule to allow access to the LAN for the address group you just created:

Source Zone/Interface	SMA
Source Destination	LAN
Source Port	Any
Service	Any
Source	The address group you just created, such as SMA and NetExtender.
Destination	Any
Users Allowed	All
Users Excluded	None
Schedule	Always on
Select the following check box (es)	• Enable Logging • Allow Fragmented Packets

15. Click **OK** to create the rule.

This completes Scenario A.

ⓘ **NOTE:** Some gateway appliances have a default zone named SSLVPN. Do not select this zone when configuring for the SMA appliance. The SSLVPN zone is intended for use with the more limited SSLVPN features that are included in the firewall products.

Continue to *Additional Configuration* and *Testing and Troubleshooting Your Remote Connection*.

3

Connecting the SMA on an Existing DMZ

The following procedures explain how to configure your gateway on an existing DMZ:

- Connecting the SMA to the Gateway
- Allowing WAN to DMZ Connection
- Allowing DMZ to LAN Connection

Connecting the SMA to the Gateway

To connect the SMA using Scenario B:

1. Connect one end of an Ethernet cable to your DMZ, either directly to the corresponding port on your existing SonicWall gateway appliance, to a hub, or to a switch on your DMZ.
2. Connect the other end of the Ethernet cable to the X0 port on your SonicWall SMA 210/410 and 500v. The X0 Port LED lights up indicating an active connection.
3. Configure the SMA X0 with an IP address in the DMZ subnet. Refer to *Configuring the X0 IP Address* for more information.

Allowing WAN to LAN Connection

If you are already forwarding HTTP or HTTPS to an internal server and you only have a single public IP address, you need to select different (unique) ports of operation for either the existing servers or for the SMA appliance, because both cannot concurrently use the same IP address and port combinations.

To allow a WAN to LAN connection:

1. Using SonicOS, log into your gateway appliance as an administrator and click the **Wizards** icon at the top right of the interface.
2. On the **Configuration Guide** page, select the **Public Server Guide**, and then click **Next**.
3. On the **Public Server Guide** page of the **Wizard**, select:

Server Type	Other
Service	Create new group

The **Service Group** dialog box is displayed.

4. In the **Service Group** dialog box, create a service group for HTTP and HTTPS:
   - Enter a **Name** for the service group.
   - Select both **HTTP** and **HTTPS** and click the arrow button to move to the right column.
   - Click **OK**.
5. On the **Server Private Network Configuration** page, enter the following server information and click **Next**:

Server Name	Name for the SMA appliance
Server Private IP Address	The X0 IP address of the SMA appliance within your LAN range, such as `10.1.1.10/24`.
Server Comment	Brief description of the server

6. On the **Server Public Information** page, accept the default IP address or enter a new IP address in your allowed public IP range. Click **Next**.

   NOTE: The default IP address is the WAN IP address of your SonicWall firewall. If you accept this default, all HTTP and HTTPS traffic to this IP address is routed to your SMA appliance.
7. The **Public Server Configuration Summary** page displays all configuration actions that are performed. Click **Apply** to create the configuration and allow access from the WAN to the SMA appliance on the LAN.

Allowing DMZ to LAN Connection

When users have connected to the SMA, they need to be able to connect to resources on the LAN.

To allow a DMZ to LAN connection:

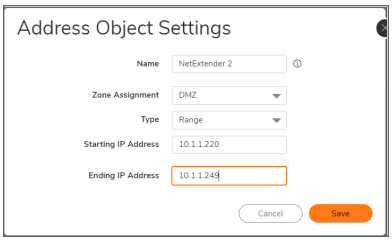
1. Using SonicOS, navigate to the **OBJECT | Match Objects > Addresses** page on the gateway appliance.
2. In the **Address Objects** tab, click **+Add**.
3. In the **Address Object Settings** dialog box, create an address object for the X0 interface IP address of your SMA appliance:

Name	Name of the SMA appliance
Zone Assignment	DMZ
Type	Host
IP Address	X0 IP address of the SMA appliance within your DMZ range, such as 10.1.1.10.

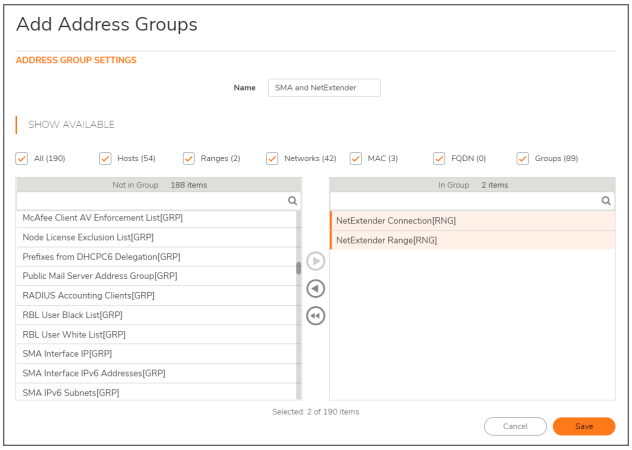
4. Click **OK** to create the object. Once added, click **Close**.

5. Click **+Add** again to create an address object for the NetExtender range.
6. In the **Add Object** dialog box, create an address object for the NetExtender range using the following options, then click **Add**:

Name	Name for NetExtender
Zone Assignment	DMZ
Type	Range
Starting IP address	Start of the NetExtender IP address range within your DMZ range, such as `10.1.1.220`.
Ending IP address	End of the NetExtender IP address range within your DMZ range, for example `10.1.1.249`.



7. On the **OBJECT | Match Objects > Addresses** page, click the **Address Groups** tab.
8. Click **+Add**.
9. In the **Add Address Groups** dialog box, create a group for the X0 interface IP address of your SMA appliance and the NetExtender IP range:
    - Enter a name for the group.
    - In the left column, select the address objects you created and click the right arrow button.
    - Click **Save** to create the group when both objects are in the right column.



10. Navigate to the **POLICY | Rules and Policies > Access Rules** page, and select the **Matrix** view style.

11. Click the **DMZ > LAN** icon.
12. On the page that displays for SMA to LAN, click **+Add**.
13. In the **Add Rule** window, create a rule to allow access to the LAN for the address group you just created:

Source Zone/Interface	SMA
Source Destination	LAN
Source Port	Any
Service	Any
Source	The address group you just created, such as SMA and NetExtender.
Destination	Any
Users Allowed	All
Users Excluded	None
Schedule	Always on
Select the following check box (es)	• Enable Logging • Allow Fragmented Packets

14. Click **OK** to create the rule.

This completes Scenario B.

ⓘ **NOTE:** Some gateway appliances have a default zone named SSLVPN. Do not select this zone when configuring for the SMA appliance. The SSLVPN zone is intended for use with the more limited SSLVPN features that are included in the firewall products.

Continue to *Additional Configuration* and *Testing and Troubleshooting Your Remote Connection*.

4

Deploying SMA on the LAN

The following procedures explain how to configure your gateway appliance on the LAN:

- Connecting the SMA to the Gateway
- Configuring SMA to LAN Connectivity

Connecting the SMA to the Gateway

To connect the SMA on the LAN:

1. Connect one end of an Ethernet cable to an unused port on your LAN hub or switch.
2. Connect the other end of the Ethernet cable to the X0 port on the front of your SonicWall SMA 210/410 and 500v.

   The X0 Port LED lights up indicating an active connection.
3. Configure the SMA X0 IP address. Refer to *Configuring the X0 IP Address* for more information.

Configuring SMA to LAN Connectivity

ⓘ **NOTE:** Before continuing, you must add a new SMA custom zone. Refer to *Adding a New SMA Custom Zone* for more information.

For users to access local resources through the SMA appliance, you must configure your gateway device to allow an outside connection through the SMA into your LAN.

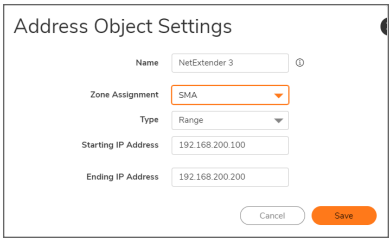
To allow an SMA to LAN connection:

1. Using SonicOS, navigate to the **OBJECT | Match Objects > Addresses** page on the gateway appliance.
2. In the **Address Objects** tab, click **+Add**.
3. In the **Address Object Settings** dialog box, create an address object for the X0 interface IP address of your SMA appliance:

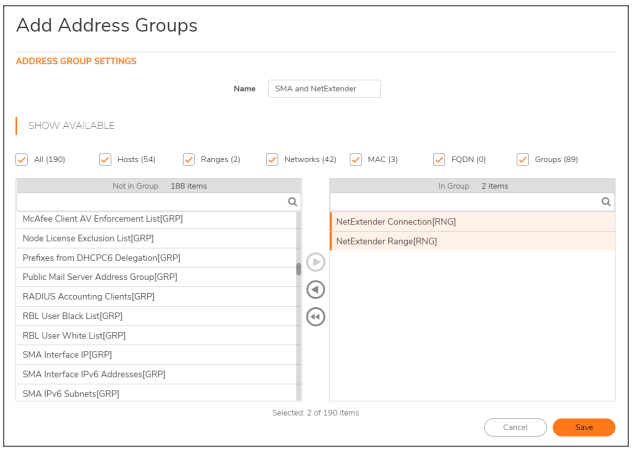
Name	Name for the SMA appliance
Zone Assignment	SMA
Type	Host
IP Address	SMA appliance X0 IP address (default `192.168.200.1`)

4. Click **+Add** to create the object. After adding, click **Close**.
5. Click **+Add** again to create an address object for the NetExtender range.
6. In the **Add Address Object** dialog box, create an address object for the NetExtender range, using the following options:

Name	Name for NetExtender range
Zone Assignment	SMA
Type	Range
Starting IP Address	Start of the NetExtender IP address range (default `192.168.200.100`)
Ending IP Address	End of the NetExtender IP address range (default `192.168.200.200`)



7. Click **Save** to create the object. Once added, click **Close**.
8. On the **OBJECT | Match Objects > Addresses** page, click the **Address Groups** tab.
9. Click **+Add**.
10. In the **Add Address Groups** dialog box, create a group for the X0 interface IP address of your SMA appliance and the NetExtender IP range:
    - Enter a name for the group.
    - In the left column, select the address objects you created and click the right arrow button.
    - Click **Save** to create the group when both objects are in the right column.



11. Navigate to the **POLICY | Rules and Policies > Access Rules** page, and select the **Matrix** view style.
12. Click the **SMA > LAN** icon.
13. On the page that displays for SMA to LAN, click **+Add**.
14. In the **Add Rule** window, create a rule to allow access to the LAN for the address group you just created:

Source Zone/Interface	SMA
Source Destination	LAN
Source Port	Any
Service	Any
Source	The address group you just created, such as SMA and NetExtender.
Destination	Any
Users Allowed	All
Users Excluded	None
Schedule	Always on
Select the following check box (es)	• Enable Logging • Allow Fragmented Packets

15. Click **OK** to create the rule.

This completes Scenario C.

ⓘ **NOTE:** Some gateway appliances have a default zone named SSLVPN. Do not select this zone when configuring for the SMA appliance. The SSLVPN zone is intended for use with the more limited SSLVPN features that are included in the firewall products.

Continue to *Additional Configuration* and *Testing and Troubleshooting Your Remote Connection*.

5

Additional Configuration

This section describes some additional configuration settings for your SMA 210/410 and 500v, depending on the deployment scenario you selected.

Topics:

Configuring the X0 IP Address

When deploying the SMA in any of the scenarios mentioned in Selecting a Deployment Scenario, you need to reset the IP address of the X0 interface on the SMA to an address within the range of the new or existing DMZ or the existing LAN subnet.

To configure the X0 IP address:

1. Connect your computer to X0 and log into the SMA appliance by navigating to `https://192.168.200.1` on your Web browser.

   ⓘ | **TIP:** For additional information, see the *SMA 210/410 Quick Start Guide*.
2. Using SonicOS, navigate to the **NETWORK | System > Interfaces** page.
3. In the **Interface Settings** table, click the **Configure** icon for the X0 interface.
4. In the **Edit Interface** dialog box, set the IP Address to an unused address within your DMZ or LAN subnet.
5. For the **Subnet Mask**, enter the value that matches your DMZ or LAN subnet mask, such as `255.255.255.0`.
6. Click **OK**. A warning displays that you are changing the X0 IP Address. Click **OK** to acknowledge.
7. Reset the management computer to have a static IP address in the range you just set for the X0 interface. For example, if you set X0 to `10.1.1.10`, you could set your computer to `10.1.1.20`.

8. Log into the SMA management interface again, using the IP address you just configured for the X0 interface. For example, point your browser to `https://10.1.1.10`.

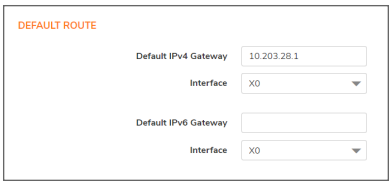
Configuring a Default Route

Refer to the following table to correctly configure your default route for the scenario you selected.

If you are using scenario:	Your upstream gateway IP address will be:
A - SMA on a New DMZ	The IP address of the DMZ interface you create
B - SMA on an Existing DMZ	The existing DMZ interface IP address
C - SMA on the LAN	The LAN interface IP address

To configure a default route:

1. Using Secure Mobile Access, navigate to the **Network > Routes** page.
2. Enter the upstream gateway device's IPv4 address in the **Default IPv4 Gateway** field or the IPv6 address in the **Default IPv6 Gateway** field.
3. Select **X0** as the interface and click **Accept**.

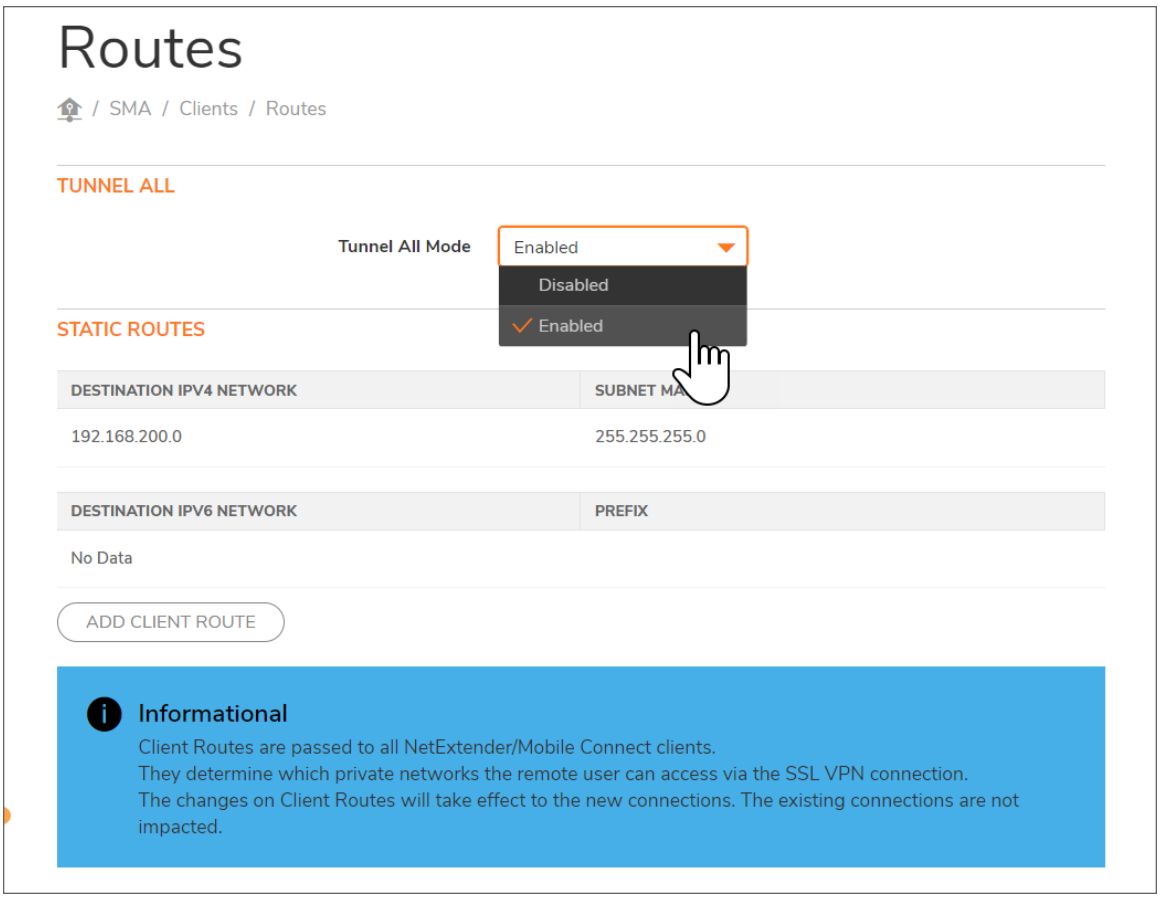


Adding a NetExtender Client Route

NetExtender allows remote clients to have seamless access to resources on your local network.

To configure a NetExtender client route:

1. Using Secure Mobile Access, navigate to the **Clients > Routes** page.



2. To force all SMA client traffic to pass through the NetExtender tunnel, select **Enabled** in the **Tunnel All Mode** drop-down menu.
3. Click **Add Client Route**.

4. Enter the network address of the trusted network to which you would like to provide access with NetExtender in the **Destination Network** field. For example, if you are connecting to an existing DMZ on

the 10.1.1.0/24 subnet and you want to provide access to your LAN network on the 192.168.168.0/24 subnet, you would enter 192.168.168.0.

5. Enter the subnet mask of the destination network in the **Subnet Mask** field. Continuing the example, enter 255.255.255.0.
6. Click **Submit** to finish adding this client route.

Setting Your NetExtender Address Range

The NetExtender address range defines the IP address pool from which addresses will be assigned to remote users during NetExtender sessions. The range needs to be large enough to accommodate the maximum number of concurrent NetExtender users you wish to support.

The range should fall within the same subnet as the interface to which the SMA appliance is connected, and it must not overlap or collide with any assigned addresses if other hosts are on the same segment as the SMA appliance.

Determine the correct subnet based on your network scenario selection:

Scenario A	192.168.200.100 to 192.168.200.200 (default range)
Scenario B	Select a range that falls within your existing DMZ subnet. For example, if your DMZ uses the 10.1.1.0/24 subnet, and you want to support up to 30 concurrent NetExtender sessions, you could use 10.1.1.220 to 10.1.1.249.
Scenario C	Select a range that falls within your existing LAN subnet. For example, if your LAN uses the 192.168.168.0/24 subnet, and you want to support up to 10 concurrent NetExtender sessions, you could use 192.168.168.240 to 192.168.168.249.

ⓘ **NOTE:** DHCP/DHCPv6 is supported and can manage the IPv4 and IPv6 addresses in the LAN and the NetExtender client address ranges.

To set your NetExtender address range:

1. Using Secure Mobile Access, navigate to the **Clients > Settings** page.
2. Enter an address range in the **Client Address Range Begin** and **Client Address Range End** fields.
3. Click **Accept** to add the **Client Address Range**.

Scenario A	192.168.200.100 to 192.168.200.200 (default range)
Scenario B	An unused range within your DMZ subnet.
Scenario C	An unused range within your LAN subnet.

If you do not have enough available addresses to support your desired number of concurrent NetExtender users, you may use a new subnet for NetExtender. This condition may occur if your existing DMZ or LAN is configured in NAT mode with a small subnet space, such as 255.255.255.224, or more commonly if your DMZ or LAN is configured in Transparent mode and you have a limited number of public addresses from your ISP. In either case,

you may assign a new, unallocated IP range to NetExtender (such as 192.168.10.100 to 192.168.10.200) and configure a route to this range on your gateway appliance.

For example, if your current Transparent range is 67.115.118.75 through 67.115.118.80, and you wish to support 50 concurrent NetExtender clients, configure your SMA X0 interface with an available IP address in the Transparent range, such as 67.115.118.80, and configure your NetExtender range as 192.168.10.100 to 192.168.10.200. Then, on your gateway device, configure a static route to 192.168.10.0, using 67.115.118.80.

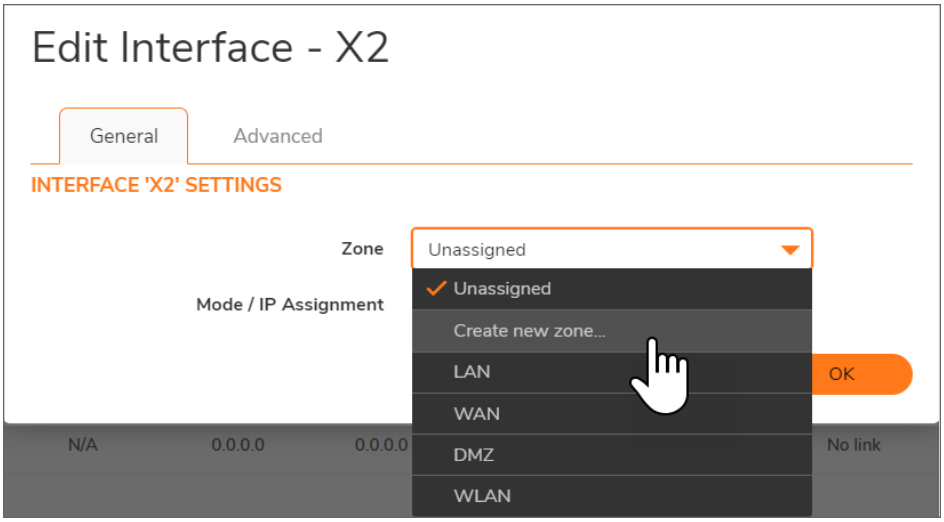
Adding a New SMA Custom Zone

Adding a new SMA custom zone on your gateway appliance is a necessary step in deploying your SMA appliance using Scenarios A and C. For more information, see the following sections:

- Connecting the SMA on a New DMZ
- Deploying SMA on the LAN

To add a new SMA custom zone on the gateway appliance:

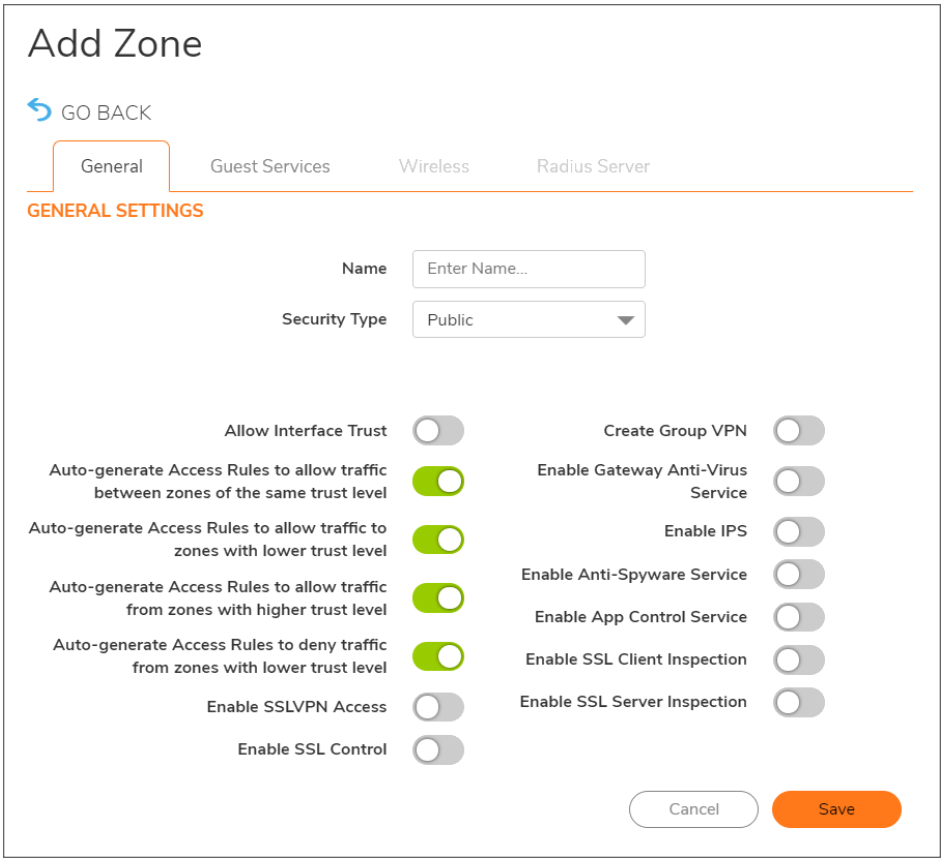
1. Using SonicOS, log into your gateway appliance as an administrator and navigate to the **NETWORK | System > Interfaces** page.
2. Click the edit icon for the interface connected to your SMA, such as X2.
3. Select **Create new zone** in the **Zone** field.



The **Add Zone** window opens.

4. Enter SMA in the **Name** field.
5. Select Public from the **Security Type** drop-down menu.
6. Clear the **Allow Interface Trust** toggle.

7. Select the following check boxes:
   - **Enable Gateway Anti-Virus Service**
   - **Enable IPS**
   - **Enable Anti-Spyware Service**



8. Click **Save**.
9. In the **Edit Interface** window again, enter the IP address for this interface in the **IP Address** field.

For example:

Scenario A	Use an IP address in the default SMA X0 subnet (default `192.168.200.x`)
Scenario C	Use an IP address in the gateway LAN subnet (default `192.168.168.x`)

10. Enter your **Subnet Mask**.
11. Optionally enter the **Default Gateway**, which is the WAN address of the gateway appliance.
12. If you want to allow management of the gateway appliance over this interface, select the desired management options.
13. If you want to allow users to log in to the gateway appliance using this interface, select the desired user login options.
14. Click **OK** to apply changes.

6

Testing and Troubleshooting Your Remote Connection

You have now configured your SonicWall gateway appliance and SMA appliance for secure remote access. This section provides information on the following topics:

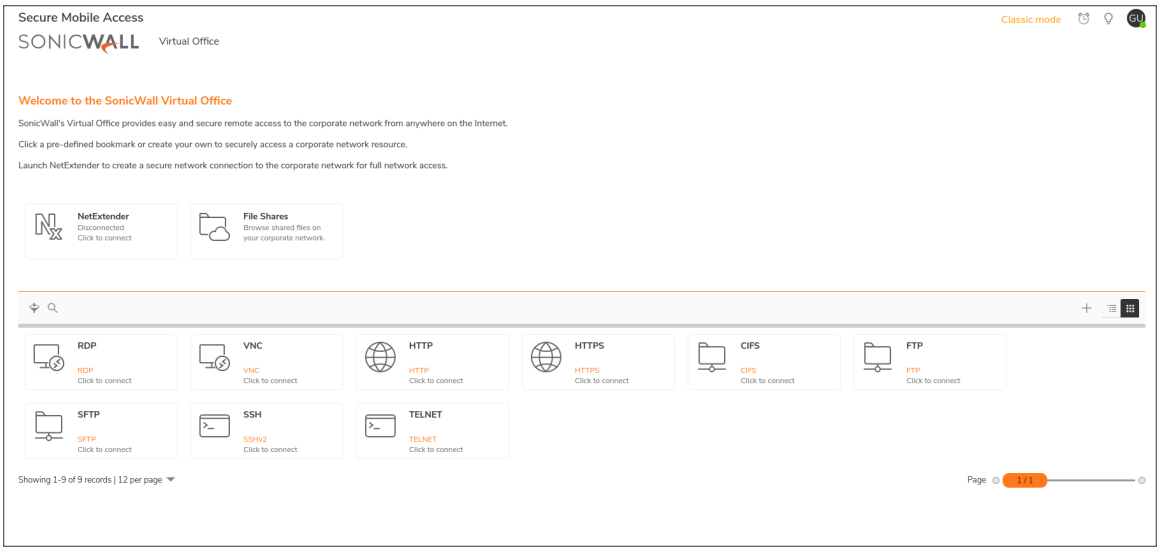
- Verifying a User Connection from the Internet
- Policy > Access Rules Matrix View

Verifying a User Connection from the Internet

You can verify your connection using a remote client on the WAN.

To verify a User Connection from the Internet:

1. From a WAN connection outside of your corporate network, launch a Web browser and enter the following:
   `https://<WAN_IP_address_of_gateway_device>`
2. When prompted, enter the **User Name** and **Password**.
3. Select **LocalDomain** from the drop-down menu and click **Login**. The **SonicWall Virtual Office** screen displays in your Web browser.



4. Click **NetExtender** to start the NetExtender client installation.
5. If prompted, click **Install** to complete the client installation.
6. Ping a host on your corporate LAN to verify your remote connection.

You have now successfully set up your SMA appliance.

ⓘ **NOTE:** It is easier for remote users to access the SMA appliance using a fully qualified domain name (FQDN) rather than an IP address. It is recommended that you create a DNS record to allow for FQDN access to your SMA appliance. If you do not manage your own public DNS servers, contact your ISP for assistance.

Policy > Access Rules Matrix View

If the SMA zone does not appear in the **POLICY | Rules and Policies > Access Rules** matrix view, verify that it is selected as the zone for the gateway interface connected to the SMA appliance.

To ensure the SMA zone displays in the matrix view:

1. Using SonicOS, navigate to the **NETWORK | System > Interfaces** page.
2. Click the **Configure** icon for X2 or the port you assigned as the SMA zone.
3. Select **SMA** as the **Zone** from the drop-down menu.
4. Click **OK**.

7

SonicWall Support

Technical support is available to customers who have purchased SonicWall products with a valid maintenance contract.

The Support Portal provides self-help tools you can use to solve problems quickly and independently, 24 hours a day, 365 days a year.

The Support Portal enables you to:

- View Knowledge Base articles and Technical Documentation
- View and participate in the Community Forum discussions
- View Video Tutorials
- Access MySonicWall
- Learn about SonicWall Professional Services
- Review SonicWall Support services and warranty information
- Register at SonicWall University for training and certification

About This Document

Secure Mobile Access Deployment Planning Guide
Updated - November 2024
Software Version - 10.2
232-005680-00 Rev C

End User Product Agreement

To view the SonicWall End User Product Agreement, go to: https://www.sonicwall.com/legal/end-user-product-agreements/.

Open Source Code

SonicWall Inc. is able to provide a machine-readable copy of open source code with restrictive licenses such as GPL, LGPL, AGPL when applicable per license requirements. To obtain a complete machine-readable copy, send your written requests, along with certified check or money order in the amount of USD 25.00 payable to "SonicWall Inc.", to:

General Public License Source Code Request
Attn: Jennifer Anderson
1033 McCarthy Blvd
Milpitas, CA 95035