

# Configuring SonicWall SSL VPN for Secure Remote Access

## CONFIGURING SONICWALL SSL VPN FOR REMOTE ACCESS



1/5

## STEPS



Configure the WAN interface



Assign the IP pool  
192.168.20.2 – 192.168.20.30



Create a user account



2/5

Install NetExtender

## BENEFITS



Secure remote access  
to internal resources



Encrypted communication  
over the Internet

## TROUBLESHOOTING



Verify WAN interface configuration



Check user account settings

### SonicWall SSL VPN Configuration Overview

Enabling secure remote access with encrypted  
VPN, dedicated IP pool, internal routing, and structure

#### troubleshooting



**Enable  
Secure Remote  
Access**

(SonicWall SSL VPN  
on WAN, Port 443)



**Grant Access  
& Validate**

SSLVPN Services Group,  
NetExtender, RDP



**Troubleshooting**

Verify VPN settings,  
IP pool, permissions



**Grant Access  
& Validate**

(192.168.6.70 - 90) -  
Route to XO

## ❖ What is SSL VPN?

- SSL VPN (Secure Sockets Layer Virtual Private Network) is a simple way to connect to your company's network securely from anywhere using the internet. It creates an encrypted "tunnel" between your device and the office network, so your data stays safe while you access files and systems as if you were physically in the office. You can use it through a web browser or a small app, and it doesn't require special hardware-just a secure login.

## ❖ Why configure it on SonicWall?

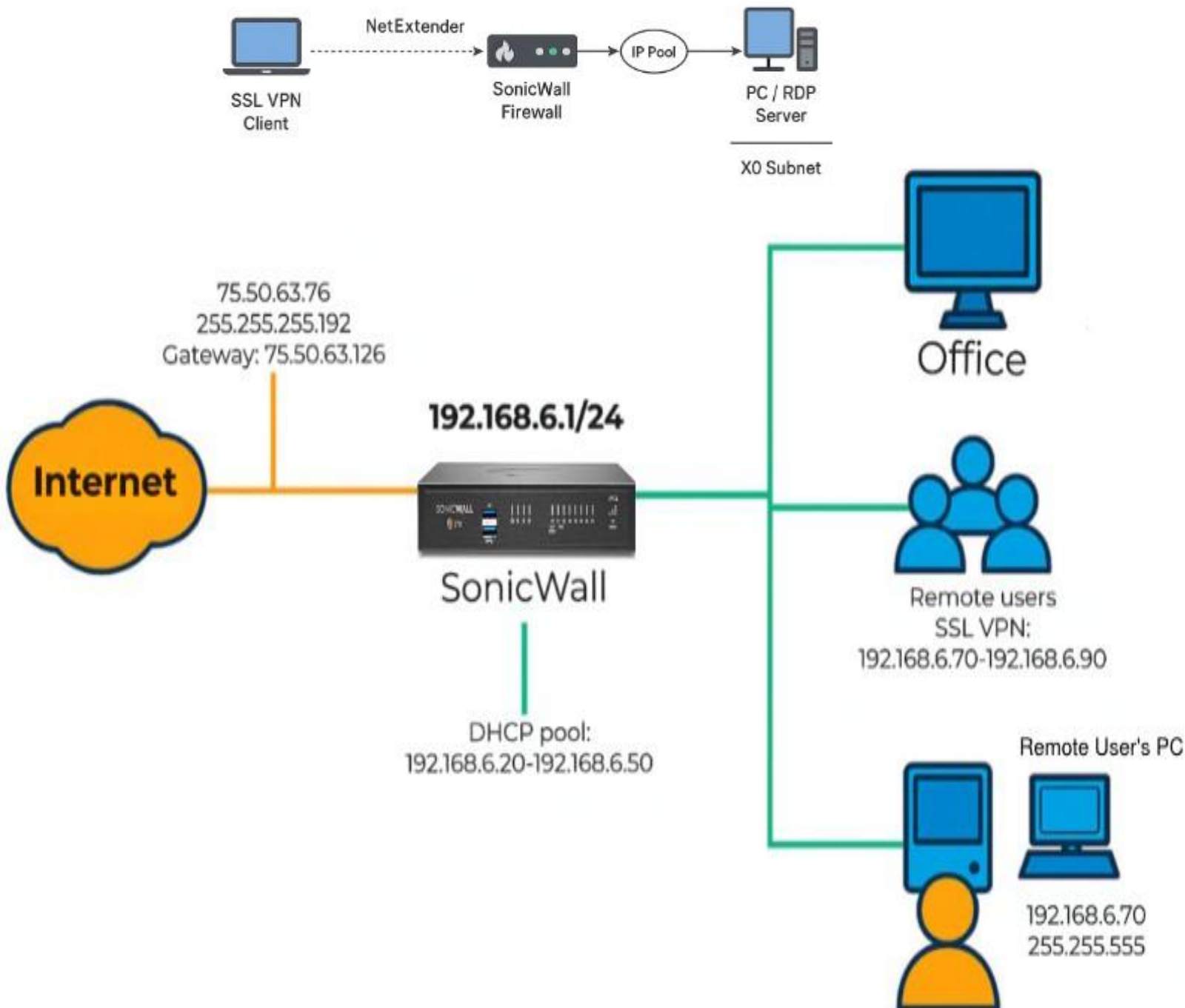
- Configuring SSL VPN on SonicWall is important because SonicWall is a trusted firewall solution that provides strong security features. By enabling SSL VPN on SonicWall, you allow secure remote access to your internal network without exposing it to threats. It uses encryption to protect data, supports user authentication, and integrates easily with existing network settings. This ensures remote employees can safely access files and systems as if they were in the office, while the firewall continues to block unauthorized access.

## ❖ key Benefits of SSL VPN for Secure Remote Access:

- **Secure Remote Access** – Employees can safely connect to the company network from anywhere using encryption.
- **Data Protection** – SSL VPN uses strong encryption to keep sensitive information safe from hackers.
- **No Special Hardware** – Works through a web browser or lightweight client, making it easy to set up.
- **User-Friendly** – Simple login process for remote workers without complex configurations.
- **Access to Internal Resources** – Lets users work as if they are in the office, accessing files and systems seamlessly.
- **Cost-Effective** – Reduces the need for expensive hardware or complex VPN setups.

## ❖ Project at a Glance

- Enables secure, encrypted remote access with SonicWall SSL VPN (port 443 on WAN)
- Assigns a dedicated SSLVPN IP pool (192.168.6.70–.90) and routes to X0 (192.168.6.0/24)
- Grants access via SSLVPN Services group and validates connectivity with NetExtender and RDP..





# CONVENIENT FOR REMOTE WORK

## Flexible Remote Access

SSL VPN enables employees to connect securely from anywhere, supporting flexibility in remote work setups.

## User-Friendly Interface

Browser-based access and lightweight clients simplify connection for all users, including non-technical employees.

## Supports Mobile Workforce

SSL VPN supports multiple device types, enabling employees to work securely on the go.

## Business Continuity

Secure remote access ensures organizations maintain productivity and resilience during work environment changes.



- ❖ Login into the SonicWall firewall and went to the Manage section to confirm the device is ready for the SSL VPN project, Where the firewall is set to assign IP addresses dynamically from the range 192.168.6.20 to 192.168.6.50 on the X0 interface. This setup ensures that any device or VPN client connecting to the network will receive an IP address, which is essential for SSL VPN to work properly and allow secure remote access.

The screenshot shows the SonicWall Administration web interface. The browser address bar indicates the URL is <https://192.168.6.1/main.html>. The interface has a top navigation bar with 'MONITOR', 'INVESTIGATE', 'MANAGE' (highlighted), and 'QUICK CONFIGURATION'. On the left, a sidebar menu shows 'Firewall Name: C0EAE4C54ECA' and various configuration sections like 'Access Points', '3G/4G/Modem', 'Policies', 'Rules', 'Objects', 'System Setup', 'Appliance', 'Users', and 'Network' (selected). The main content area is titled 'DHCPv4 Server Lease Scopes'. It includes a 'View Style' section with 'All' selected. Below is a table with columns: '#', 'Type', 'Lease Scope', and 'Interface'. A single entry is shown: #1, Dynamic, Range: 192.168.6.20 - 192.168.6.50, X0. Below the table are buttons for 'ADD DYNAMIC', 'ADD STATIC', and 'DELETE'. At the bottom, there is a section for 'Current DHCPv4 Leases'.

#	Type	Lease Scope	Interface
1	Dynamic	Range: 192.168.6.20 - 192.168.6.50	X0

- ❖ Enabled SSL VPN on the WAN zone, set the port to 4433, and chose Local Domain for user authentication.
- Manage → VPN → SSL VPN → Server Settings → Configure WAN, Port 4433, Local Domain → Accept.

SonicWall - Administration for C01 x +

Not secure https://192.168.6.1/main.html

SONICWALL™ Network Security Appliance MONITOR INVESTIGATE **MANAGE** QUICK CONFIGURATION

Firewall Name: C0EAE4C54ECA

Updates  
Licenses  
Firmware & Backups  
WXA Firmware  
Restart

Connectivity

VPN  
SSL VPN  
Server Settings  
Client Settings  
Portal Settings  
Virtual Office

Access Points  
3G/4G/Modem

Policies  
Rules  
Objects

This is the SSL VPN Access status on each Zone. Green indicates active SSL VPN status. Red indicates inactive SSL VPN status. Enable or disable SSL-VPN access by clicking the zone name.

LAN WAN DMZ WLAN

192.168.6.1 says  
The configuration on this page will reset all the active NetExtender connections, are you sure to submit?

OK Cancel

### SSL VPN Server Settings

SSL VPN Port: 4433

Certificate Selection: Use Selfsigned Certificate

User Domain: LocalDomain

Enable Web Management over SSL VPN: Disabled

Enable SSH Management over SSL VPN: Disabled

Enable Compression Control Protocol(CCP) for SSL VPN Connections: Disabled

Inactivity Timeout (minutes): 10

ACCEPT CANCEL

SonicWall - Administration for C01 x +

Not secure https://192.168.6.1/main.html

SONICWALL™ Network Security Appliance MONITOR

Firewall Name: C0EAE4C54ECA

Updates  
Licenses  
Firmware & Backups  
WXA Firmware  
Restart

Connectivity

VPN  
SSL VPN  
Server Settings  
Client Settings  
Portal Settings  
Virtual Office

Access Points  
3G/4G/Modem

Policies

### Default Device Profile

Name: Default Device Profile

### SonicPoint/SonicWave L3 Management

Name: Default Device Profile for SonicPointN

### Basic Settings

Name: Default Device Profile

Description: Default Device Profile

Zone IP V4: SSLVPN

Network Address IP V4: --Select a network--

Zone IP V6: --Select a network--

Network Address IP V6: Create new network...

Settings Client Routes Client Settings

Summarize

Register | Help | Logo

Mode: Configuration

IPv4	Address for IPv6	Zone for IPv6	Configure
?		Unknown	

Address	Zone	Configure
?	Unknown	

❖ Start configuring it by selecting SSLVPN zone and creating a new network for IPv4.

- ❖ This setup creates a range of IP addresses (192.168.6.70 to 192.168.6.90) for SSL VPN users to use when they connect remotely.

The screenshot shows the SonicWall administration interface. On the left, the 'Default Device Profile' section is visible. The main area displays the 'Basic Settings' for a device profile. A dialog box titled 'Add Address Object - Profile 1 - Microsoft Edge' is open, showing the configuration for an 'SSLVPN Pool'. The 'Name' is 'SSLVPN Pool', 'Zone Assignment' is 'SSLVPN', 'Type' is 'Range', 'Starting IP Address' is '192.168.6.70', and 'Ending IP Address' is '192.168.6.90'. A green note 'Outside of DHCP Pool' is next to the ending IP. The 'Ready' status is shown at the bottom of the dialog, with 'OK' and 'CANCEL' buttons.

- ❖ This step adds the **X0 Subnet** to the SSL VPN client routes so remote users can access the internal network.

The screenshot shows the SonicWall administration interface. On the left, the 'VPN' section is expanded, and 'SSL VPN' is selected. The 'Client Settings' tab is active. The main area displays the 'Client Routes' configuration. The 'Tunnel All Mode' is set to 'Disabled'. The 'Networks' list includes 'X2 IPv6 Primary Dynamic Address', 'X2 IPv6 Primary Dynamic Address', 'X2 IPv6 Primary Static Address', 'X2 IPv6 Primary Static Address Sub', 'X2 Subnet', and 'X0 Subnet'. The 'X0 Subnet' is highlighted with a red box. A red arrow points from the 'X0 Subnet' to the 'Client Routes' list on the right, which is currently empty. The 'REMOVE ALL' button is visible at the bottom right.

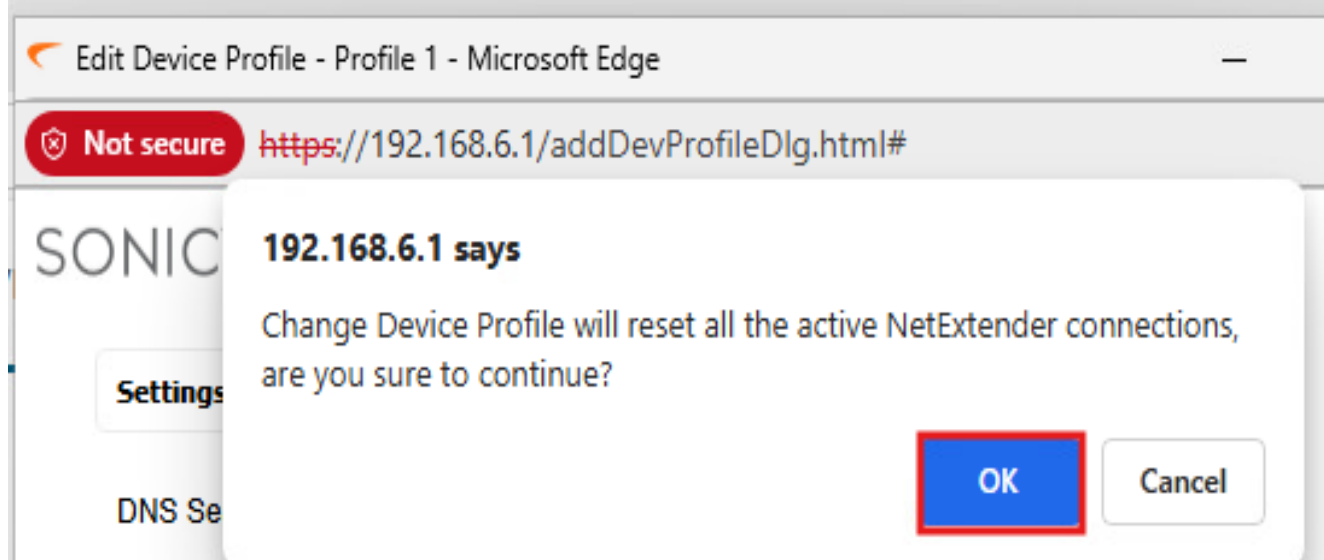


❖ X0 Subnet has been successfully added.

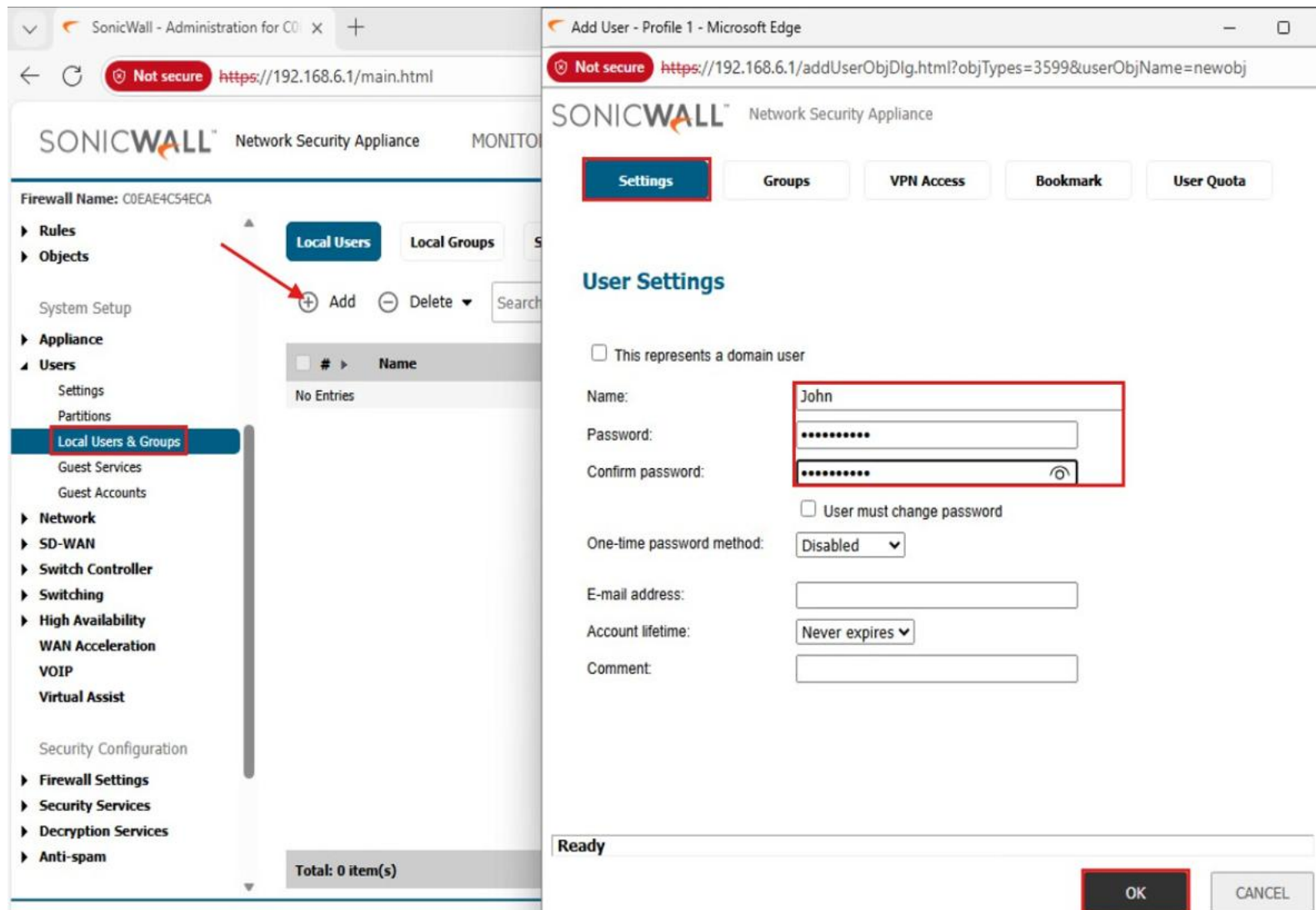
The screenshot shows the 'Client Routes' configuration page in the SonicWall management interface. The browser window title is 'Edit Device Profile - Profile 1 - Microsoft Edge' and the address bar shows 'https://192.168.6.1/addDevProfileDlg.html#'. The page has three tabs: 'Settings', 'Client Routes' (which is selected and highlighted in blue), and 'Client Settings'. Below the tabs, the 'Client Routes' section is titled. It features a 'Tunnel All Mode' dropdown set to 'Disabled'. Under the 'Networks:' section, a list of network types is shown: 'X2 IPv6 Link-Local Address', 'X2 IPv6 Primary Dynamic Address', 'X2 IPv6 Primary Dynamic Address !', 'X2 IPv6 Primary Static Address', 'X2 IPv6 Primary Static Address Sub', and 'X2 Subnet'. A blue button with a right-pointing arrow is positioned below this list. To the right, the 'Client Routes:' section contains a list box with 'X0 Subnet' selected and highlighted with a red box. Below this list box are two buttons: a grey one with a left-pointing arrow and a grey one labeled 'REMOVE ALL'.

❖ Click OK to save the SSL VPN client settings and complete the configuration.

The screenshot shows the 'Client Settings' configuration page in the SonicWall management interface. The browser window title is 'Edit Device Profile - Profile 1 - Microsoft Edge' and the address bar shows 'https://192.168.6.1/addDevProfileDlg.html#'. The page has three tabs: 'Settings', 'Client Routes', and 'Client Settings' (which is selected and highlighted with a red box). Below the tabs, the 'Client Settings' section is titled. It includes a 'DNS Search List (in order):' field with an 'ADD' button to its right. Below this is a list box for DNS search entries, with up/down arrows and a 'REMOVE' button to its right. Further down are 'WINS Server 1:' and 'WINS Server 2:' fields, both containing '0.0.0.0'. The 'NetExtender Client Settings' section follows, with several options and their corresponding dropdown menus: 'Enable Client Autoupdate:' (Disabled), 'Exit Client After Disconnect:' (Disabled), 'Allow Touch ID on IOS devices:' (Disabled), 'Allow Fingerprint Authentication on Android devices:' (Disabled), 'Enable NetBIOS over SSLVPN:' (Disabled), 'Uninstall Client After Exit:' (Disabled), 'Create Client Connection Profile:' (Disabled), and 'User Name & Password Caching:' (Allow saving of user name only). At the bottom of the page, there is a 'Ready' status bar and two buttons: 'OK' (highlighted with a red box) and 'CANCEL'.

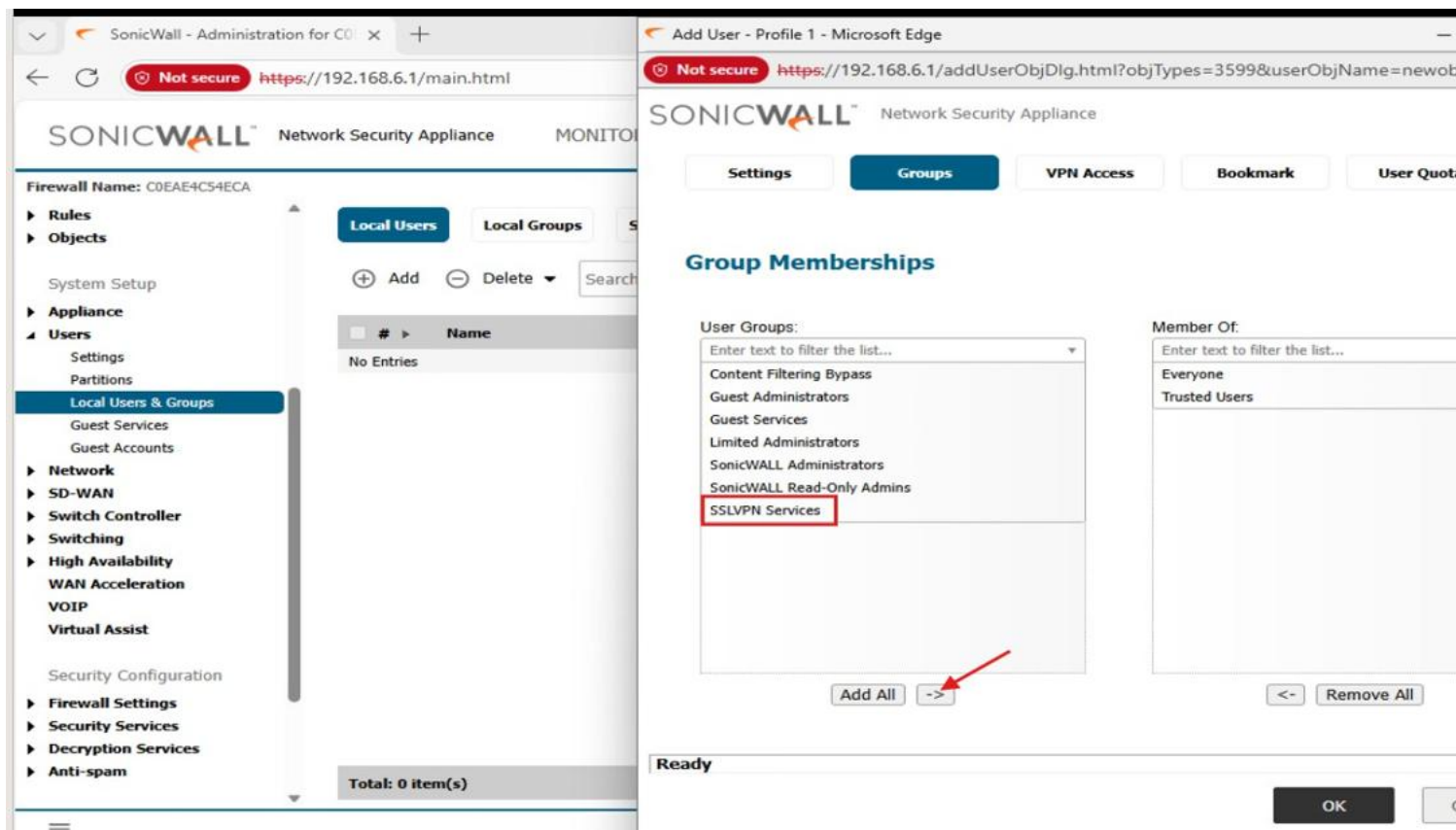


- ❖ This step creates a new local user named **John** with a password for SSL VPN access, and clicking **OK** saves the user account.

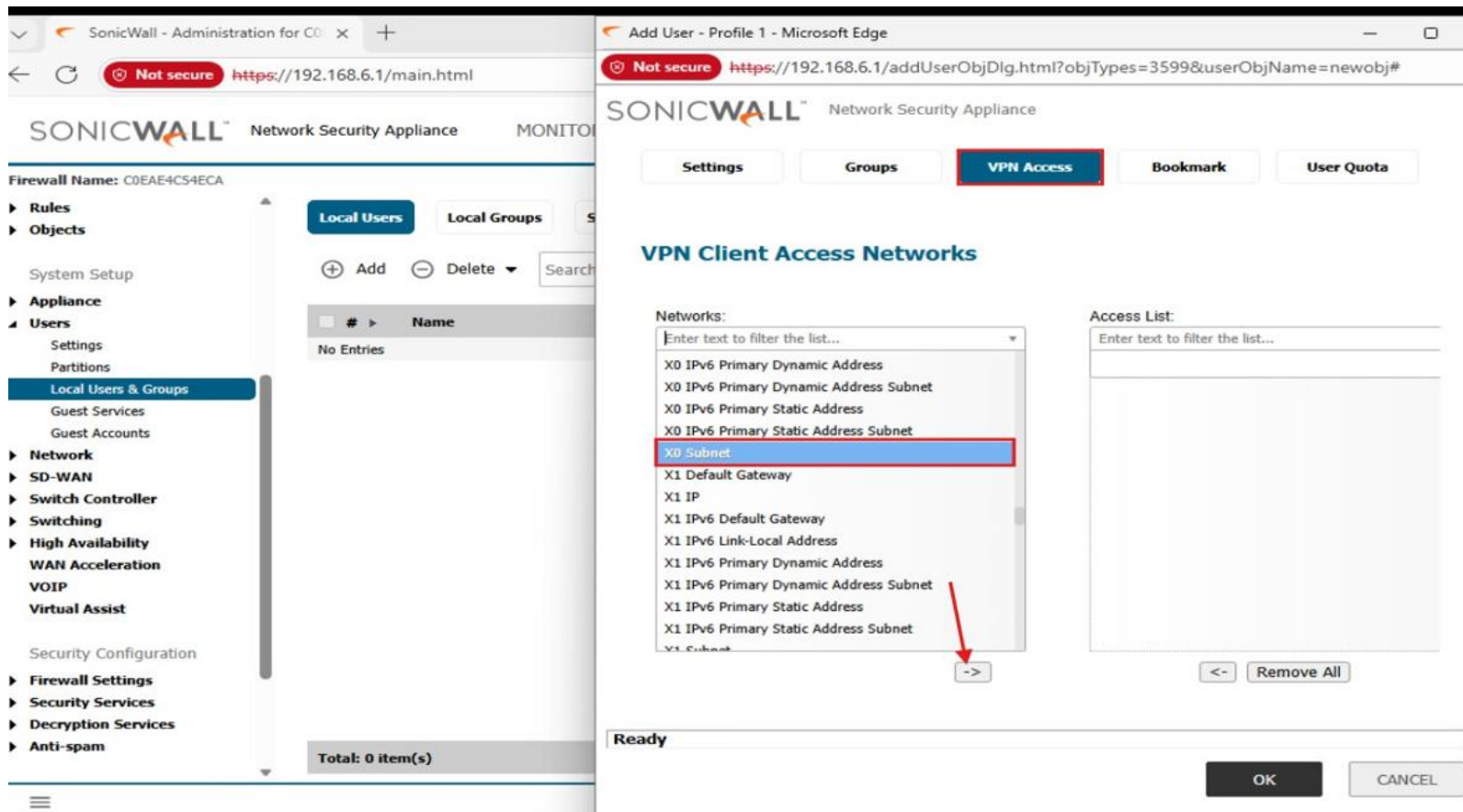




- ❖ Add the user to the **SSLVPN Services** group to allow VPN access.



- ❖ Add **X0 Subnet** to the VPN access list for internal network connectivity.



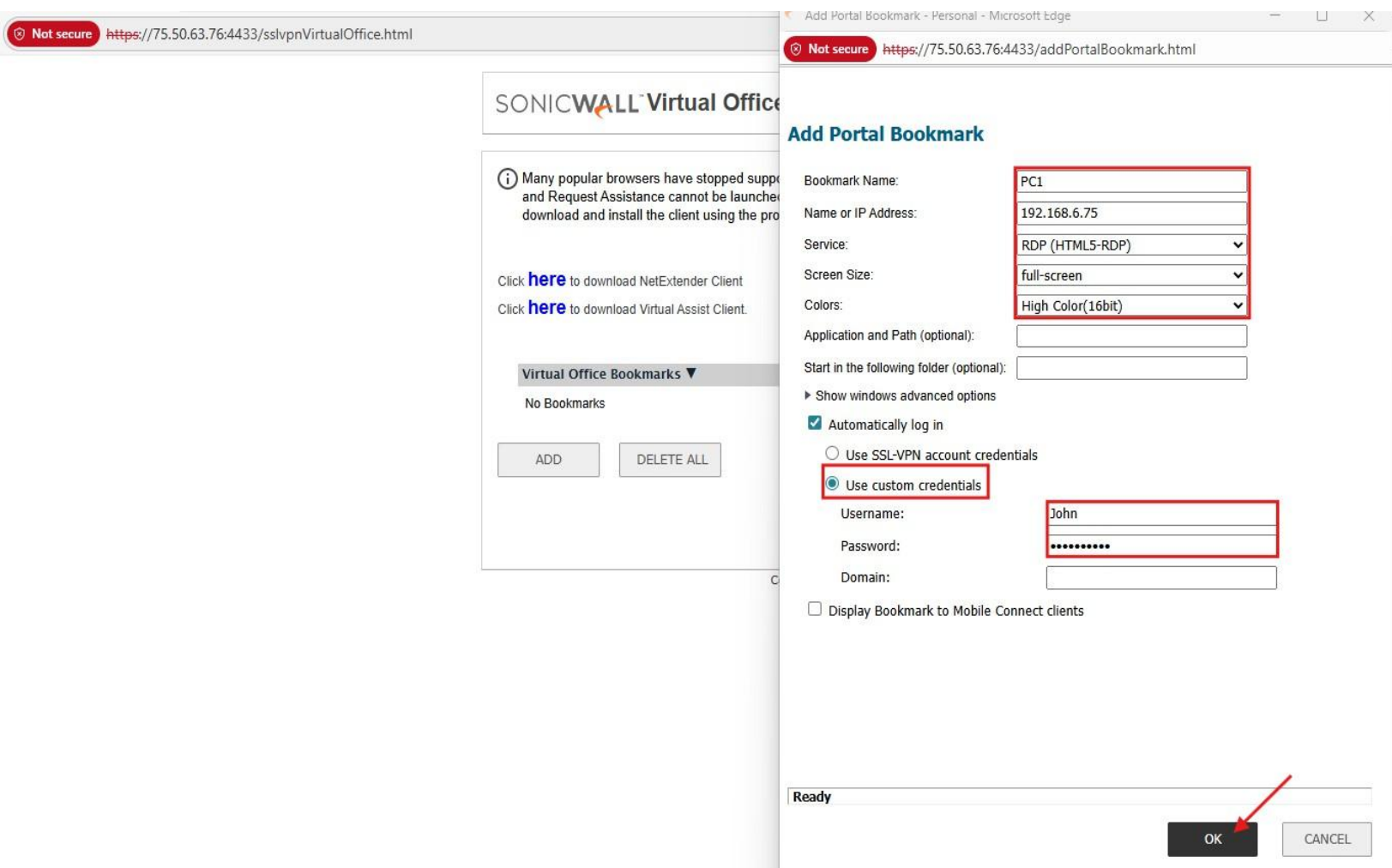
❖ Click **OK** to save VPN access settings with X0 Subnet included.

The screenshot shows the 'Add User - Profile 1 - Microsoft Edge' window with the URL <https://192.168.6.1/addUserObjDlg.html?objTypes=3599&userObjName=newobj#>. The page title is 'SONICWALL Network Security Appliance'. The 'VPN Access' tab is selected. The 'VPN Client Access Networks' section shows two lists: 'Networks' and 'Access List'. The 'Networks' list contains various IP addresses and subnets, with 'X0 Subnet' highlighted. The 'Access List' list is empty, with 'X0 Subnet' highlighted. The 'Ready' status bar is visible at the bottom. The 'OK' button is highlighted with a red box.

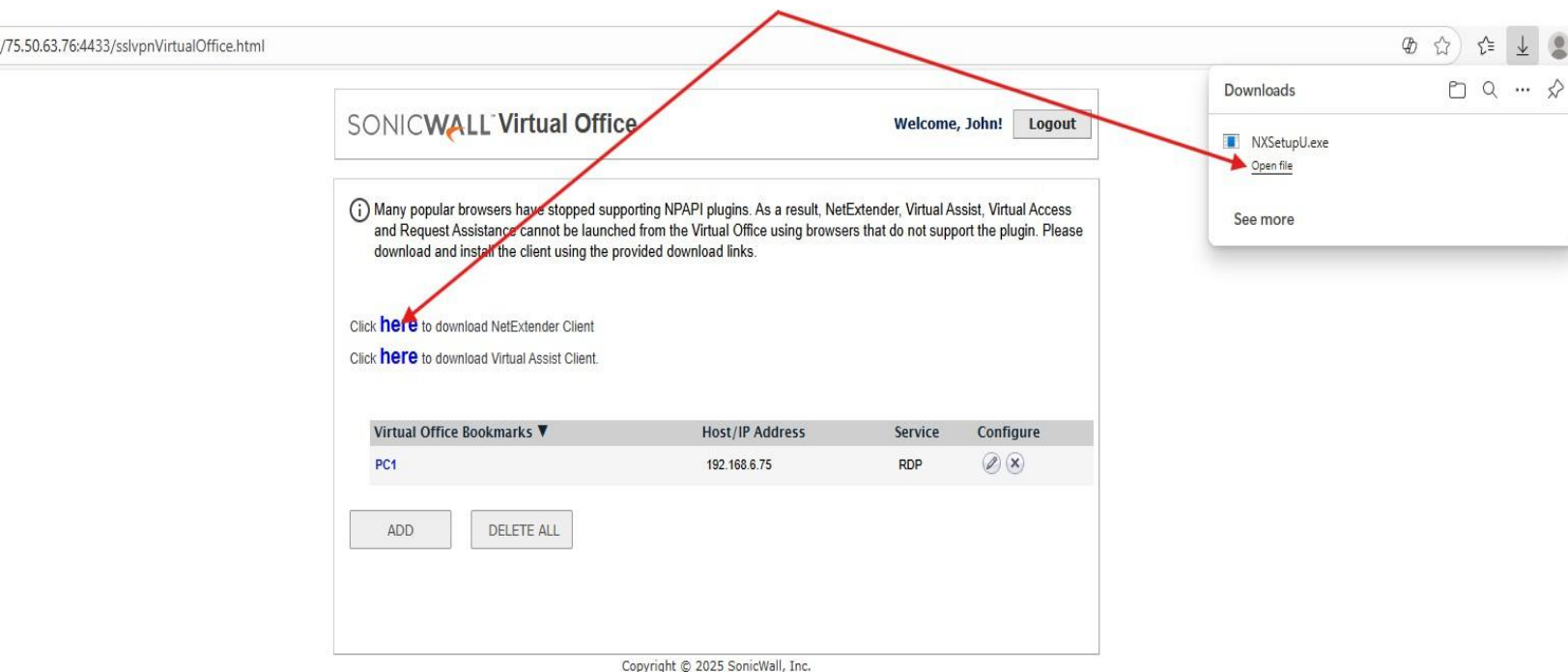
❖ Disconnect any other VPN, then log in to SonicWall Virtual Office with the new user credentials.

The screenshot shows the 'SonicWall - Virtual Office' window with the URL <https://75.50.63.76:4433>. The page title is 'SONICWALL Virtual Office'. The login form contains the following fields: 'User Name' with the value 'John', 'Password' with masked characters, and 'Domain' with the value 'LocalDomain'. The 'Login' button is highlighted with a red box and a red arrow pointing to it.

❖ Create an RDP bookmark with the PC's IP address and custom credentials, then click **OK** to save.



❖ Download and install the **NetExtender Client** to enable SSL VPN access.





❖ Click **Next** to begin installing the NetExtender client for SSL VPN access.

Not secure <https://75.50.63.76:4433/sslvpnVirtualOffice.html>

SonicWall NetExtender Setup

**Welcome to the SonicWall NetExtender Setup Wizard**

This wizard will guide you through the installation of SonicWall NetExtender.

It is recommended that you close all other applications before starting Setup. This will make it possible to update relevant system files without having to reboot your computer.

Click Next to continue.

**Next >** Cancel

**SONICWALL Virtual Office** Welcome, John! Logout

**i** Many popular browsers have stopped supporting NPAPI plugins. As a result, NetExtender, Virtual Assist, Virtual Access and Request Assistance cannot be launched from the Virtual Office using browsers that do not support the plugin. Please download and install the client using the provided download links.

Click [here](#) to download NetExtender Client

Click [here](#) to download Virtual Assist Client.

Virtual Office Bookmarks ▼	Host/IP Address	Service	Configure
PC1	192.168.6.75	RDP	<a href="#">✎</a> <a href="#">✕</a>

ADD DELETE ALL

❖ Accept the license agreement and click **Next** to continue installing NetExtender.

Not secure <https://75.50.63.76:4433/sslvpnVirtualOffice.html>

SonicWall NetExtender Setup

**License Agreement**

Please review the license terms before installing SonicWall NetExtender.

Press Page Down to see the rest of the agreement.

Software License Agreement

PLEASE READ THIS SOFTWARE LICENSE AGREEMENT ("AGREEMENT") CAREFULLY BEFORE DOWNLOADING THE SOFTWARE. BY CLICKING ON THE "NEXT" BUTTON BELOW, YOU INDICATE YOUR ACCEPTANCE OF THE TERMS OF THIS LEGAL AND BINDING AGREEMENT AND ARE CONSENTING TO BE BOUND BY AND ARE BECOMING A PARTY TO THIS AGREEMENT. IF YOU DO NOT AGREE TO ALL OF THE TERMS OF THIS AGREEMENT, CLICK THE "CANCEL" BUTTON AND THE INSTALLATION PROCESS WILL NOT CONTINUE.

If you accept the terms of the agreement, select the first option below. You must accept the agreement to install SonicWall NetExtender. Click Next to continue.

☒ I accept the terms of the License Agreement

☐ I do not accept the terms of the License Agreement

Nullsoft Install System v2.46

< Back **Next >** Cancel

**SONICWALL Virtual Office** Welcome, John! Logout

**i** Many popular browsers have stopped supporting NPAPI plugins. As a result, NetExtender, Virtual Assist, Virtual Access and Request Assistance cannot be launched from the Virtual Office using browsers that do not support the plugin. Please download and install the client using the provided download links.

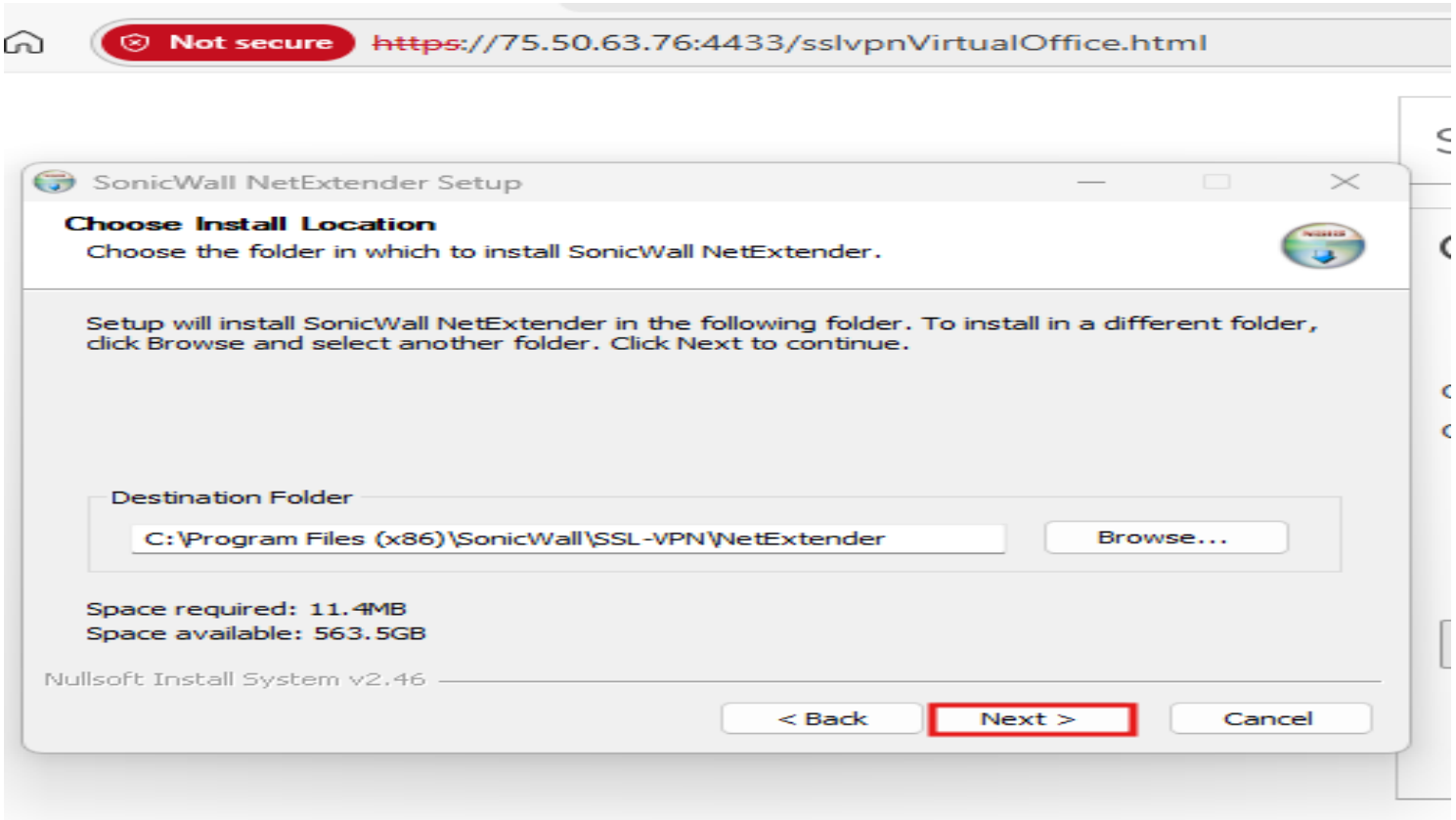
Click [here](#) to download NetExtender Client

Click [here](#) to download Virtual Assist Client.

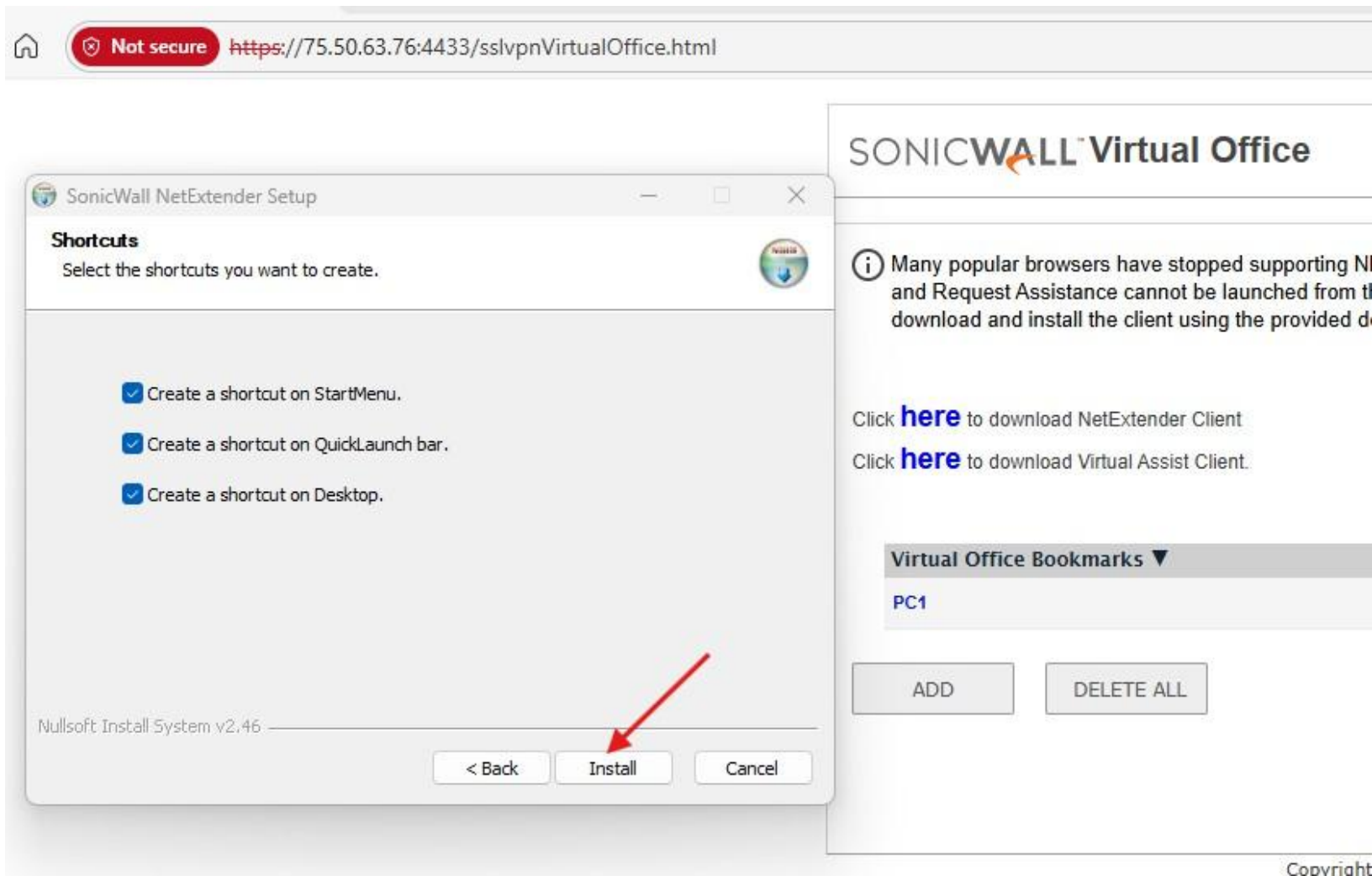
Virtual Office Bookmarks ▼	Host/IP Address	Service	Configure
PC1	192.168.6.75	RDP	<a href="#">✎</a> <a href="#">✕</a>

ADD DELETE ALL

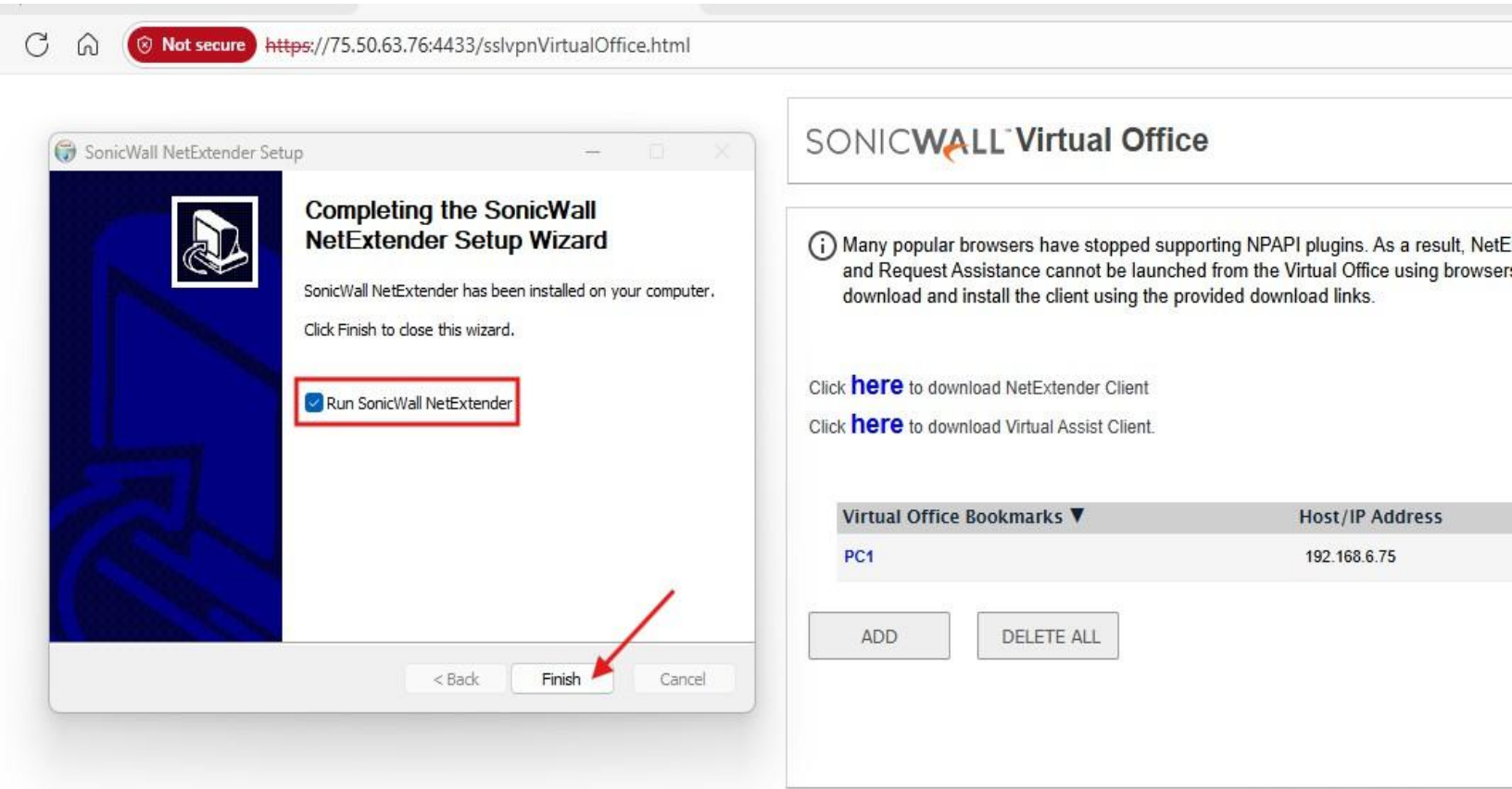
- ❖ Choose the install location and click [Next](#) to continue NetExtender installation.



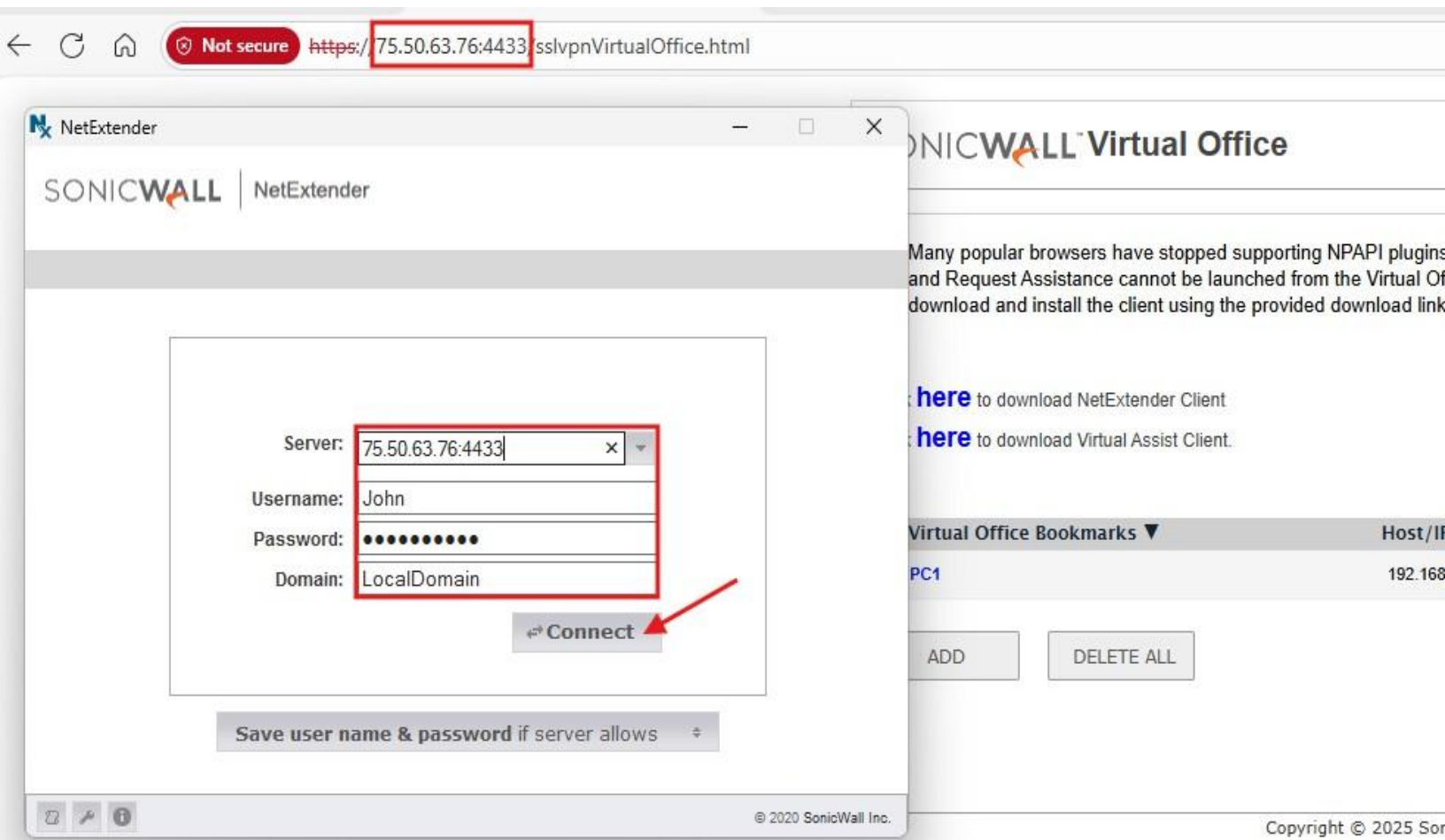
- ❖ Choose shortcut options and click [Install](#) to complete NetExtender setup.



❖ Click **Finish** to complete installation and run SonicWall NetExtender for SSL VPN access.

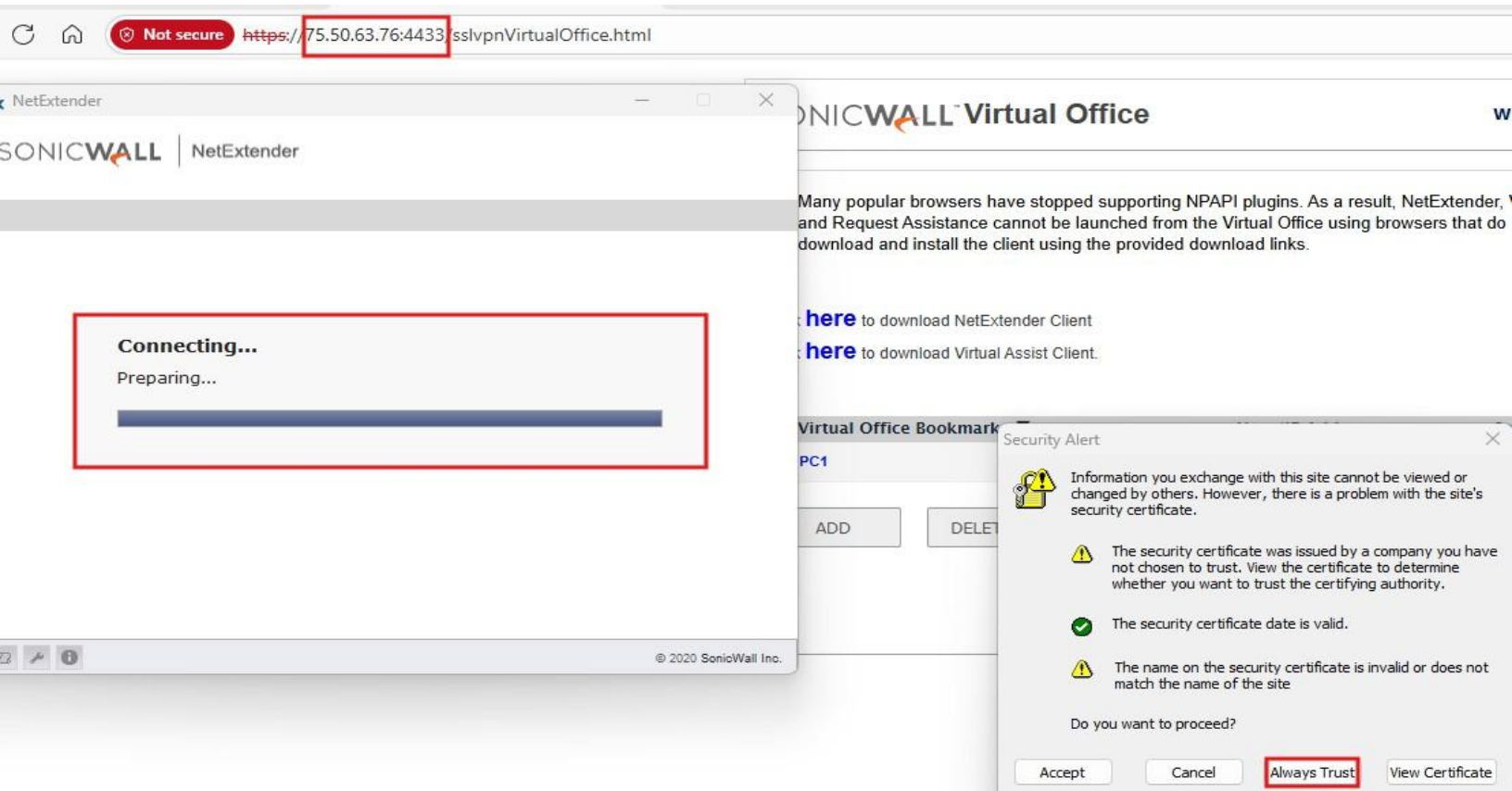


❖ Enter server details and credentials in NetExtender, then click Connect to establish the VPN connection.





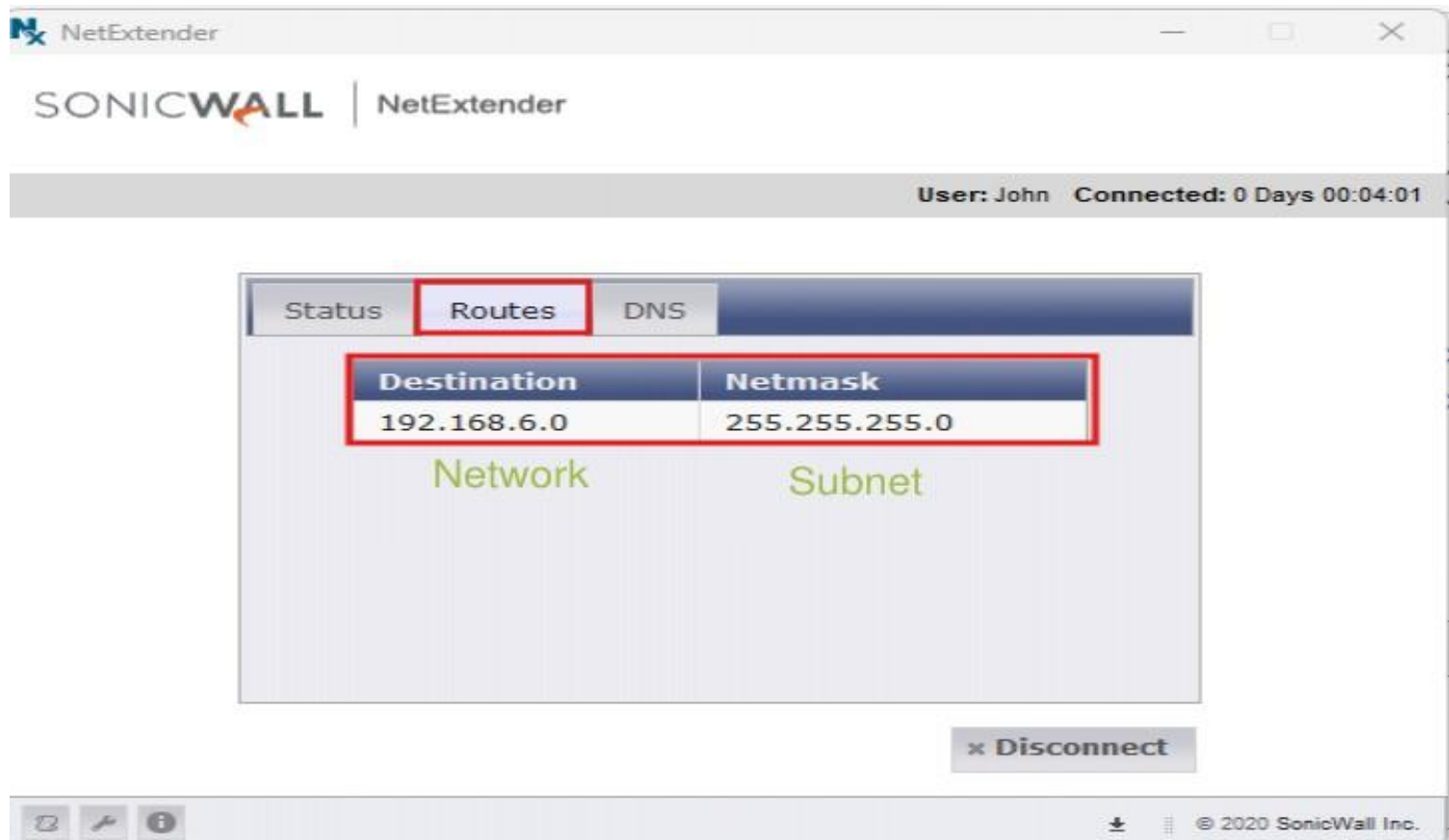
- ❖ Click **Always Trust** on the certificate prompt to complete the SSL VPN connection.



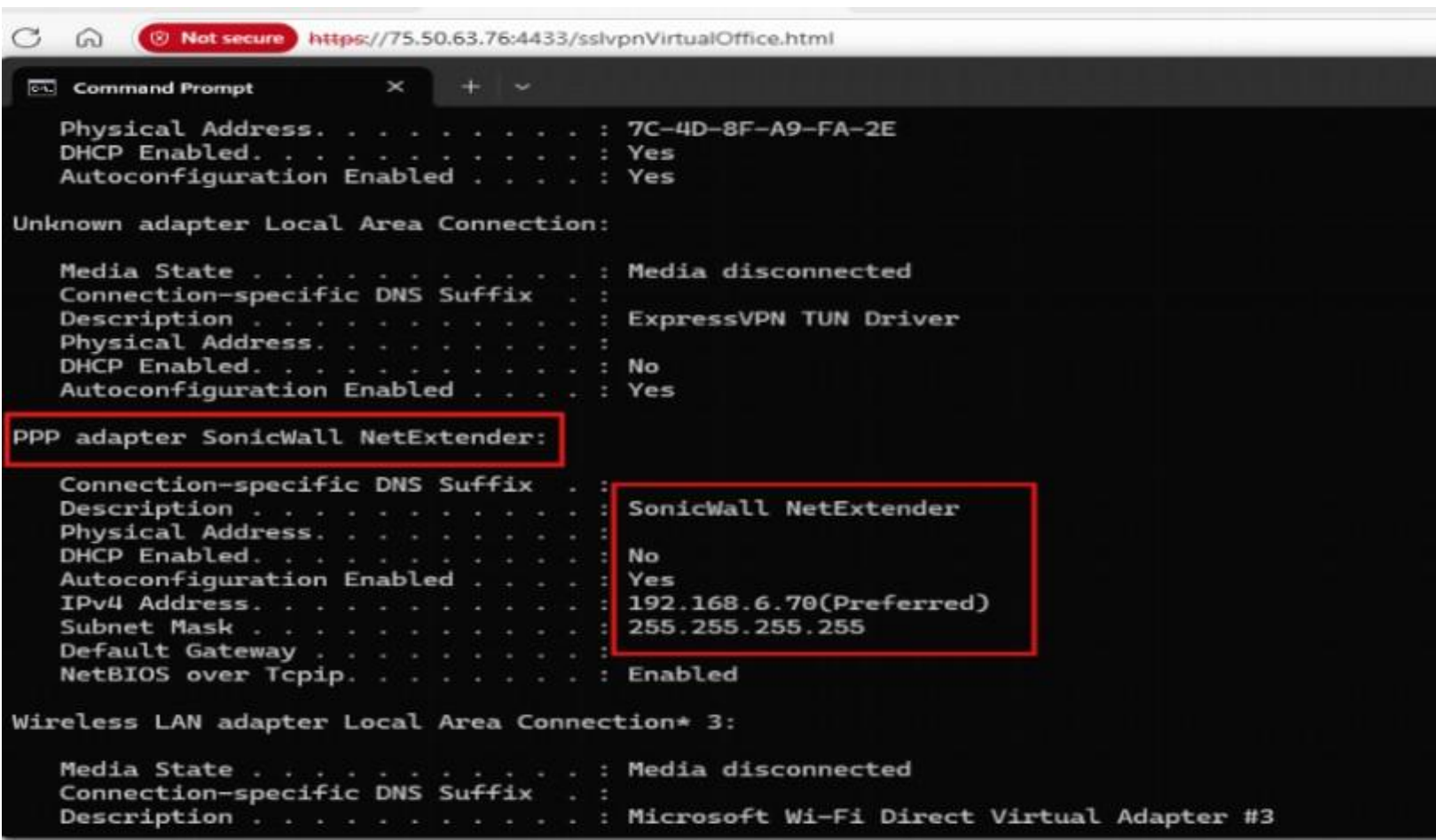
- ❖ SSL VPN is successfully connected, showing the SonicWall public IP and the private IP assigned to the PC.



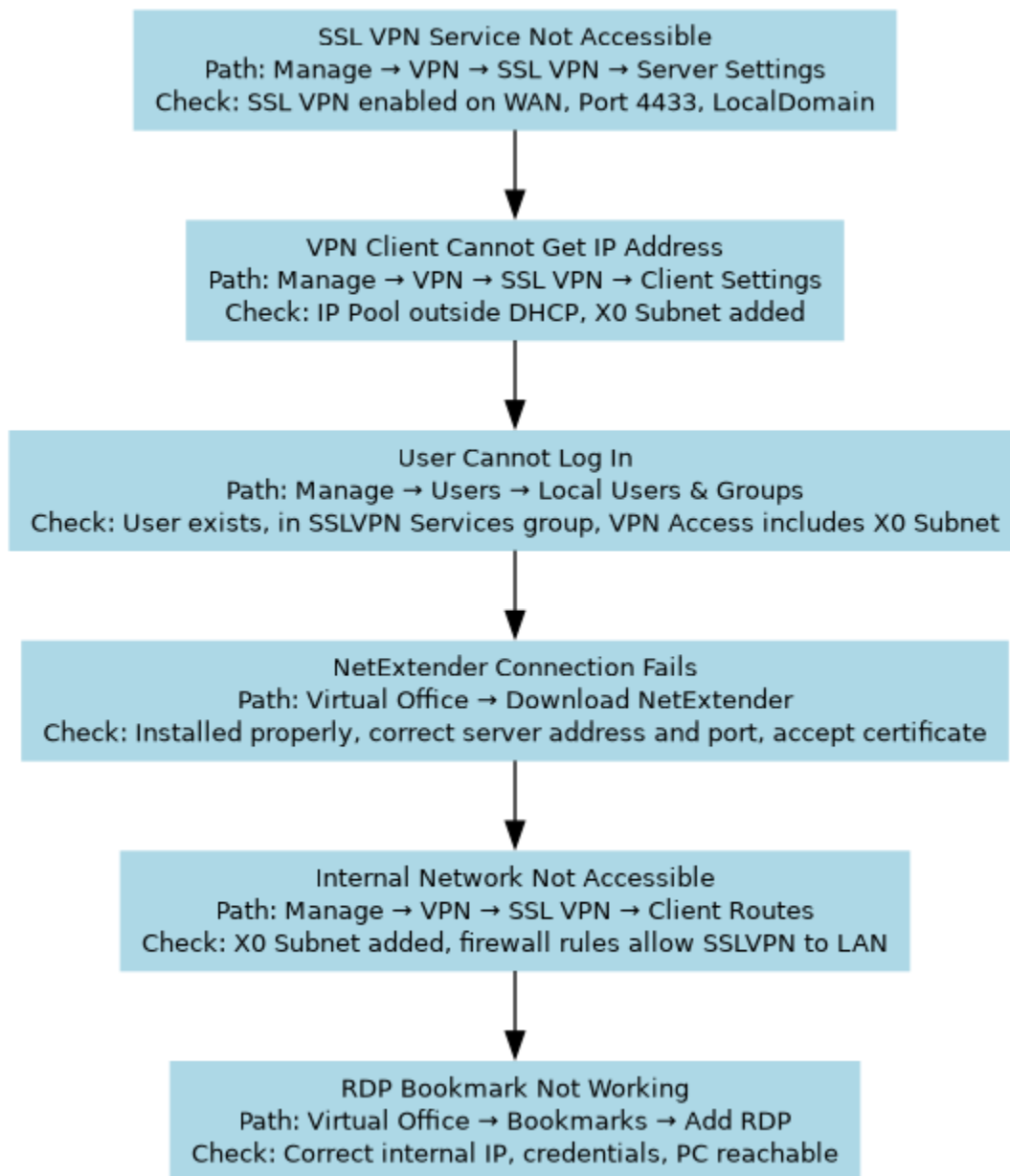
- ❖ SSL VPN route is set to allow access to the internal network 192.168.6.0/24.



- ❖ NetExtender adapter confirms VPN connection with IP 192.168.6.70 and subnet 255.255.255.255.



# SonicWall SSL VPN Troubleshooting



## Step 1: SSL VPN Service Not Accessible



### Enable SSL VPN and Configure Port

Ensure SSL VPN is enabled on the WAN zone and port 4433 is correctly set for secure connections.

### Select LocalDomain Authentication

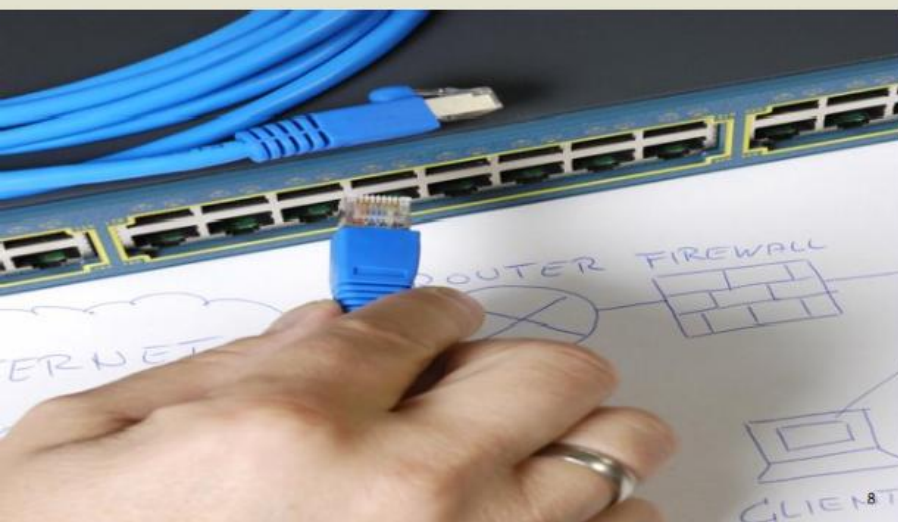
Choose LocalDomain for authentication to enable proper user verification for SSL VPN access.

### Verify Network Accessibility

Check that port 4433 is not blocked by ISP or firewall and WAN interface is properly configured.



# Step 2: VPN Client Cannot Get IP Address



## IP Pool Configuration

Ensure the VPN IP pool range is outside the DHCP scope to prevent IP address conflicts.

## Client Routes Setup

Add the X0 Subnet to client routes to enable remote user access to internal network resources.

## Common Connection Issues

Misconfigured IP pools or missing routes are frequent causes of VPN connection failures.

# Step 3: User Cannot Log In



## Verify User Account Status

Check that the user account exists and is active in the local users and groups management area.

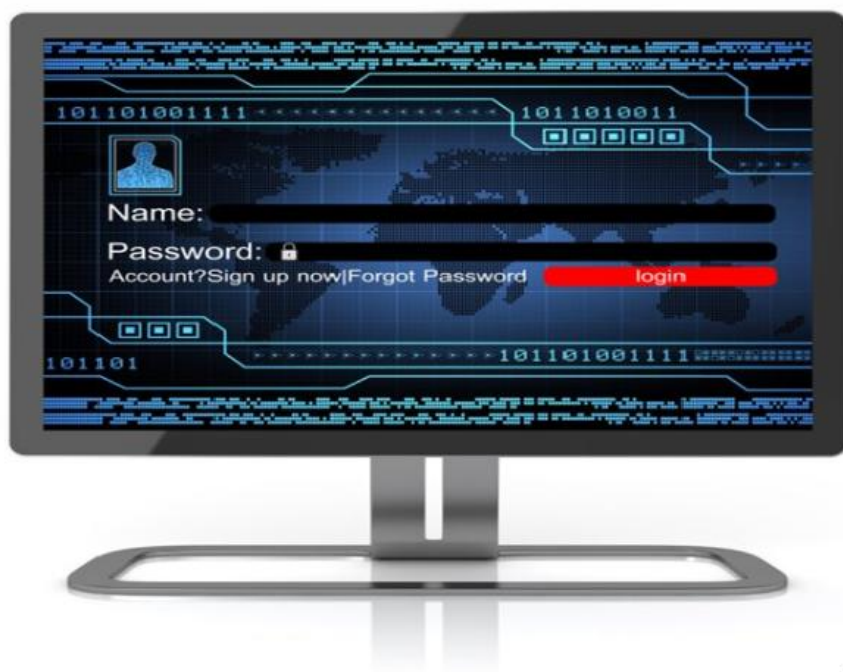
## Confirm Group Membership

Ensure the user belongs to the SSLVPN Services group for proper VPN permissions.

## Check VPN Access List

Verify the VPN Access list includes the X0 Subnet to allow network authentication and access.

# Step 4: NetExtender Connection Fails



## Downloading and Installing Client

Download and install the NetExtender client from the Virtual Office portal to begin setup.

## Verify Server Address and Port

Ensure the server address and port number (4433) are entered correctly to prevent connection issues.

## Accept Security Certificate

Accept the certificate prompt to establish a trusted connection and avoid failure.



# Step 5: Internal Network Not Accessible



## Verify VPN Client Routes

Check that the X0 Subnet 192.168.6.0/24 is included in SSL VPN client routes for proper access.



## Confirm Firewall Rules

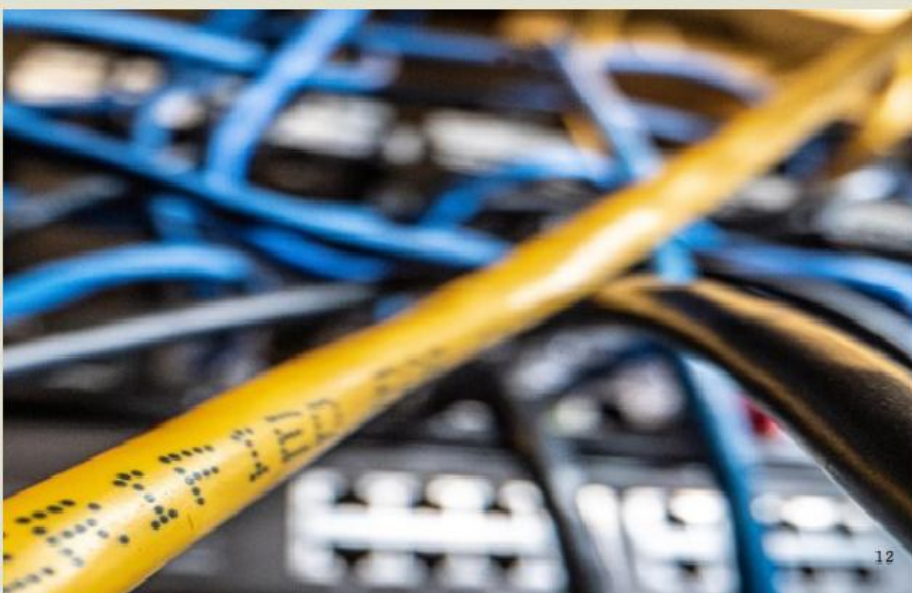
Ensure firewall policies allow traffic from SSLVPN zone to LAN to avoid connection issues.



## Prevent Access Issues

Missing routes or restrictive firewall policies can block access to internal network resources.

# Step 6: RDP Bookmark Not Working



## Creating RDP Bookmark

Set up an RDP bookmark in Virtual Office using correct internal IP and login credentials.

## Verify Target PC Status

Ensure the target PC is powered on and reachable to avoid connection failures.

## Common RDP Issues

Incorrect IP addresses or offline devices are frequent reasons for RDP connection problems.



## Summary of Key Points

### Structured Troubleshooting Steps

Following a systematic approach addresses VPN issues efficiently and ensures smooth SSL VPN experience.

### Service and Permissions Verification

Check service accessibility, IP allocation, and user permissions to maintain secure VPN connections.

### Client and Routing Checks

Verify client installation, internal routing, and bookmark functionality for proper VPN operation.

### Regular Audits for Prevention

Conduct regular audits of VPN settings and firewall rules to prevent connectivity problems.

## ❖ Conclusion

Configuring SSL VPN on SonicWall provides a secure and reliable way for remote users to access internal resources as if they were on-site. By enabling SSL VPN on the WAN interface, creating a dedicated IP pool, adding internal routes, and assigning users to the SSLVPN Services group, organizations ensure encrypted communication and proper connectivity. Implementing systematic troubleshooting steps such as verifying service settings, user permissions, client installation, and routing helps maintain smooth VPN operations. Regular audits of VPN configurations and firewall rules further strengthen security and prevent connectivity issues, making this setup ideal for supporting remote work securely and efficiently.

