

# JUNIPER NETWORKS WX CLIENT FOR MOBILE AND SMALL OFFICE USERS

---

Technical Overview, High-Level Design, and Basic Installation and Configuration  
Examples of the WX Client

## Table of Contents

<b>Introduction</b> .....	4
<b>Scope</b> .....	4
<b>WX Client Overview</b> .....	4
TCP Transport Optimization .....	4
Compression .....	4
Application-Specific Acceleration .....	4
Transparency .....	4
Licensing .....	4
WX Client Application Performance .....	5
<b>WX Client Auto Discovery</b> .....	5
Auto Discovery Overview .....	5
Auto Discovery Detailed View .....	7
Auto Discovery .....	7
Traffic Flow Interception .....	7
Auto Discovery Detailed Analysis .....	8
<b>Flow Setup and Optimization</b> .....	9
Flow Setup Overview .....	9
Flow Setup Details .....	10
Flow Setup Detailed Analysis .....	10
Optimization Services .....	11
Optimization Service Requirements .....	11
Global and Per Adjacency Services Negotiation .....	12
Optimization Service Requirements .....	13
<b>WX Client Design Considerations</b> .....	13
Hardware and Software Requirements .....	13
PC Requirements for installation of the WX Client .....	13
WXC Series Requirements for Installing JWOS 6.0 .....	13
Firewall Compatibility .....	13
Firewalls .....	13
Personal Firewall .....	13
Virus Scanning Software .....	13
VPN Compatibility .....	13
<b>WX Client Description and Deployment Scenario</b> .....	14
Basic Deployment of the WX Client .....	14
Common Examples of Non-Working Basic Inline Configurations .....	14
Firewall Considerations .....	14
VPN Overview .....	15
VPN Deployment Examples with a WXC Series Platform .....	17

WX Client Distribution and Configuration .....	19
WX Client Distributed Directly from WXC Series Platform .....	19
WX Client Distribution via SA Series Appliance .....	19
MSI Installer and Microsoft SMS .....	19
WX Client Setup Basics .....	20
Delivering WX Client Installation Package from SA Series Appliance .....	22
Basic Steps Required to Deliver the WX Client Package from an SA Series Appliance .....	23
Summary .....	24
About Juniper Networks .....	24

## Table of Figures

Figure 1: Example of application response time improvements with WX Client .....	5
Figure 2: Auto discovery overview .....	6
Figure 3: Accelerated sessions .....	6
Figure 4: Auto discovery details of WXC Series platforms and WX Client .....	7
Figure 5: TCP flow setup with established adjacency .....	9
Figure 6: TCP flow setup detail with existing adjacency .....	10
Figure 7: Global and per adjacency services negotiation .....	11
Figure 8: Per flow services .....	12
Figure 9: Per flow services mismatch .....	12
Figure 10: Basic inline deployment .....	14
Figure 11: Impact of asymmetric routing on WX Client deployment .....	14
Figure 12: TCP options stripped by firewall .....	15
Figure 13: Inline VPN deployment .....	15
Figure 14: One-armed VPN deployment .....	16
Figure 15: Proxy VPN example “does not work” with WX Client .....	16
Figure 16: Simplified VPN deployment with WXC Series behind VPN viewing all TCP sessions and performing optimization .....	17
Figure 17: WXC Series deployed with VPN in one-armed mode .....	17
Figure 18: WXC Series and VPN deployed in basic inline mode .....	18
Figure 19: Simplified WX Client and VPN non-working deployment .....	18
Figure 20: WX Client distribution from the WXC Series via https .....	19
Figure 21: SA Series SSL VPN Appliances authentication and automated WX Client download .....	19
Figure 22: Basic WX Client Setup .....	20
Figure 23: SA Series authentication and WX Client distribution .....	22
Figure 24: Remote user accessing network via Network Connect VPN and WX Client .....	22

## Introduction

Juniper Networks® WX Client is a software-based application acceleration client targeted at mobile users and very small office environments (1-3 users). The WX Client provides a completely transparent and cost-effective way to boost the productivity of mobile and small office users. By dramatically increasing the performance of applications over the WAN without requiring a dedicated hardware appliance at each location, the WX Client requires no configuration at the remote desktop and no technical knowledge from the remote user.

## Scope

This paper provides a high-level overview of the technologies used in the WX Client. Additionally, example topologies are provided to give readers a practical understanding of the WX Client solution. We will then explore some basic deployment examples. Configuration steps required for Juniper Networks WXC Series Application Acceleration Platforms and WX Client are included to provide users with a working base to use as a starting point when deploying the WX Client in their own environment.

## WX Client Overview

Juniper Networks WX Client shatters the barriers associated with providing application acceleration to mobile users. By proving a high-performance software client solution, remote and home users can now get LAN-like application performance. WX client provides the missing link in existing remote access solutions—performance. WX Client and Juniper Networks SA Series SSL VPN Appliances provide a unique remote access solution that delivers ease of management, application performance, and security.

### TCP Transport Optimization

Virtual window expansion for highly compressed traffic flows greatly increases the amount of data that can be sent each round-trip time (RTT), dramatically improving the performance of bulk traffic types like FTP, backups, and large file downloads, to name just a few. This is done in a way that is transparent to the applications and hosts involved.

### Compression

Network Sequence Caching or NSC is a scalable, disk-based compression technology that rapidly and efficiently works on both small and large data patterns, vastly reducing the amount of traffic that crosses the WAN. Because only references to data need to be sent, up to 99 percent of data can be eliminated from WAN traffic.

### Application-Specific Acceleration

Protocol-specific acceleration for Windows Common Internet File System (CIFS) file sharing dramatically reduces the amount of application chattiness on the WAN typically associated with CIFS traffic. As a result of Juniper's CIFS acceleration techniques, many transactions no longer need to traverse the WAN, reducing application response times to LAN-like levels.

### Transparency

Unlike other software client solutions, no static associations with remote acceleration devices are set up. The WX Client automatically discovers and forms adjacencies with appliances in the data center. Application transparency is also maintained on the WAN by preserving the TCP source and destination ports.

Installation is transparent when using SA Series products, as the WX Client software can be automatically installed/updated and started when the user connects to the network remotely.

Juniper's acceleration technology is fully compatible with SA Series appliances and Juniper Networks NetScreen Series Security Systems, and it has been designed to work with the most popular VPN and remote access solutions on the market today.

### Licensing

WX Client licensing is based on a number of users accessing the box concurrently. See data sheet for the specific licensing options on each WXC Series platform. Licensing is enforced on the appliance itself and does not require a separate device just for license management. When the maximum number of WX Client adjacencies is reached, no new WX Client connections will be accepted by the WXC Series platform. As users log off, those connections become available for other users.

## WX Client Application Performance

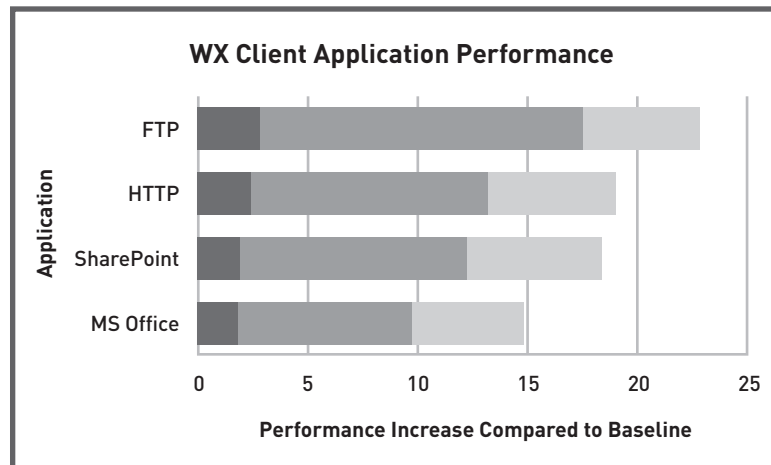


Figure 1: Example of application response time improvements with WX Client.

**Note:** Bars indicate how many times faster applications completed with WX Client compared to baseline. Sample application performance numbers for WX Client are based on second pass of data.

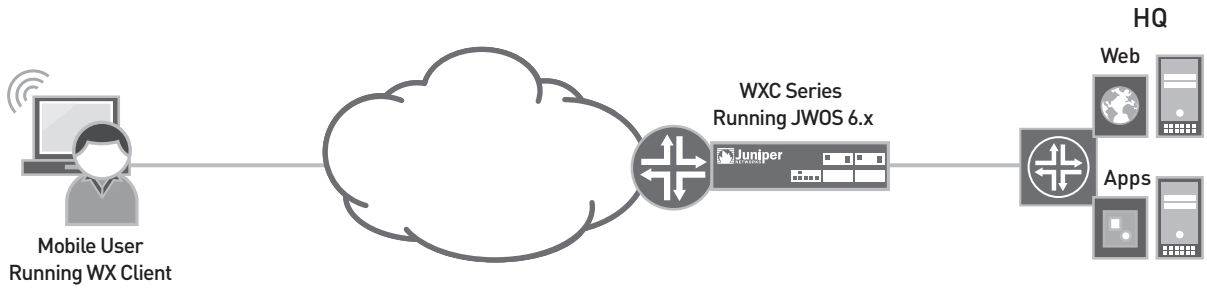
## WX Client Auto Discovery

### Auto Discovery Overview

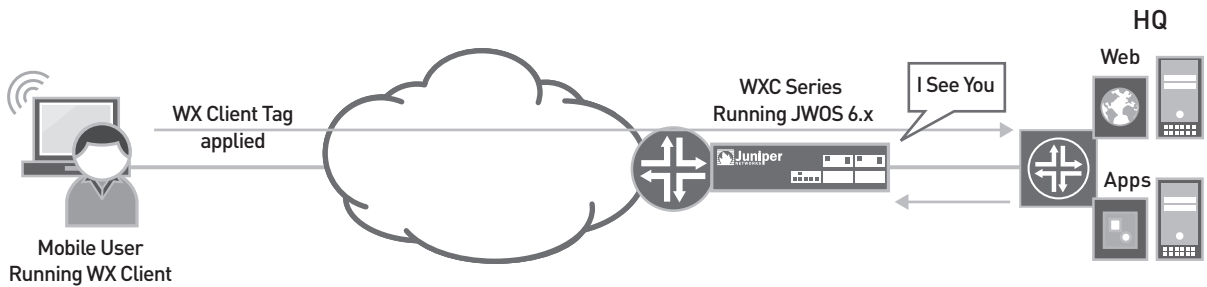
To simplify configuration and deployment of the WX Client, a secured dynamic endpoint discovery mechanism is used to form adjacencies with each other on the fly. At a high level, when TCP sessions are initiated, a tag is added to the first few packets when they go through the WX Client and the WXC Series platform. Information contained in these tags determines if the WX client and WXC Series platform should form an adjacency and if the application should be optimized. All these actions occur in a way that is transparent to both user and application. In the following sections, we will dig deeper into the details of adjacency formation and optimization of WX Client traffic.

### WX Client Auto Discovery Overview

**Stage 1: No adjacency formed between WX Client and WXC Series platform**



**Stage 2: User initiates Web session to HQ The WX Client places a Tag on the session The WXC Series platform makes a note of the Tag and waits to see if the return traffic is seen from the server**



**Stage 3: The WXC Series platform negotiates an adjacency with the WX Client**

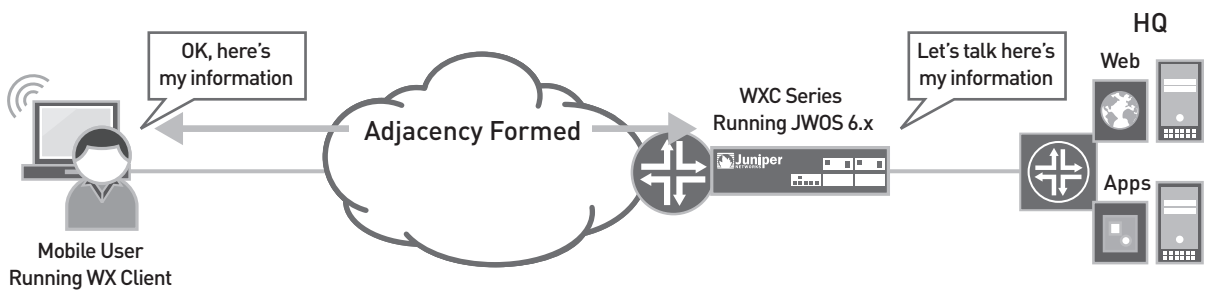


Figure 2: Auto discovery overview

\* Adjacency formation only happens on the first tagged flow from the WX Client. Once the adjacency is formed between the WX Client and the WXC Series platform, traffic is accelerated.

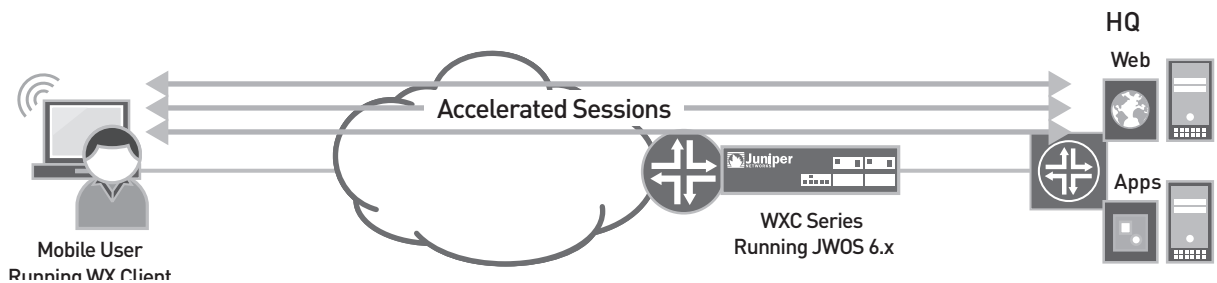


Figure 3: Accelerated sessions

## Auto Discovery Detailed View

### Auto Discovery

Auto Discovery of WX Clients and WXC Series platforms simplifies the configuration and management requirements associated with a WAN optimization client deployment. At a high level, both the WX Client and WXC Series platforms tag certain packets that pass through them. The information contained in the tags tells them if they should form an adjacency with the remote device and what traffic should be optimized. This process is described in more detail below.

### Traffic Flow Interception

The WX Client and WXC Series platforms will intercept all TCP traffic and inspect it to see if the flow matches any of the defined application policies. If a match is found, the WX Client will tag the TCP SYN packet as eligible for optimization. This happens whether or not the WX Client has an existing adjacency with any WXC Series platforms.

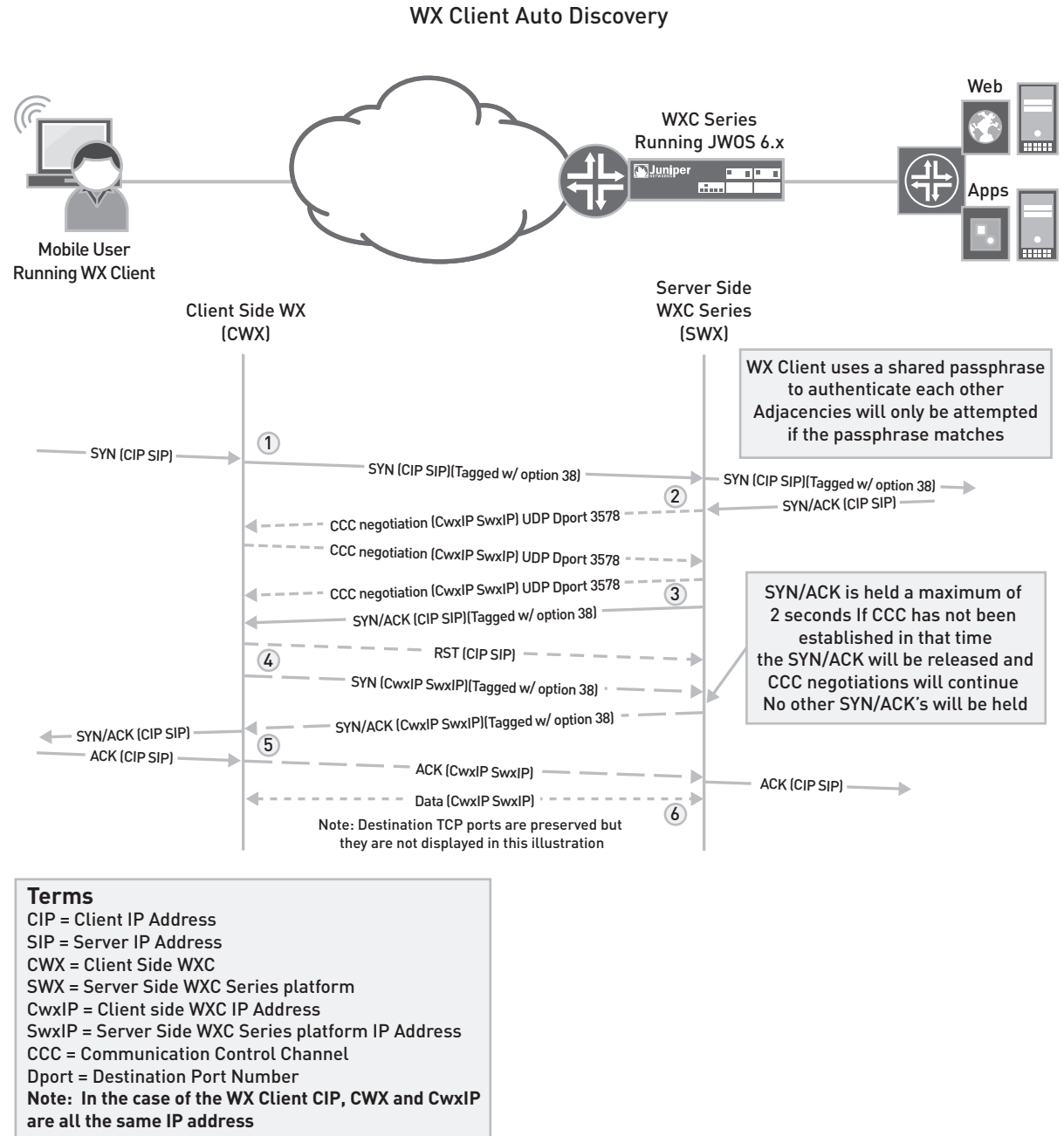


Figure 4: Auto discovery details of WXC Series platforms and WX Client

## Auto Discovery Detailed Analysis

The walk through here refers to the diagram in figure 4.

1. All TCP traffic that passes through the WX Client and matches the optimization policies will have the initial SYN packet tagged with TCP option 38. If the SYN packet with this tag is seen by a WXC Series platform running JWOS 6.0, it will do the following checks.
  - Does it have an optimization policy for this traffic type? Yes
  - Does the passphrase match? Yes
  - Is there an adjacency already established? No
  - Is it at maximum user count? No
  - Make a note of this SYN and wait to see if the return SYN/ACK is seen.
2. If the SYN/ACK is seen by the WXC Series platform, it will hold onto the SYN/ACK packet and begin communication control channel negotiations with the WX Client.
  - If communication control channel negotiations take longer than two seconds, the SYN/ACK will be released and that flow will not be optimized. However, communication control channel negotiations will continue and during this time, no other SYN/ACKs destined to the WX Client will be held until an adjacency is formed.
3. If a communication control channel was negotiated within the two second window, then the TCP SYN/ACK is tagged with option 38 and released. When the SYN/ACK is received by the WX Client, it knows that this TCP connection can be optimized.
4. In the flow setup phase, a register suppression time (RST) is sent from the WX Client to clean up the connection in the middle of the network.
  - A new SYN for the same TCP destination port number will be sent from the WX Client to the server side WXC Series.
  - When the WXC Series receives the SYN, it will respond with a SYN/ACK to the WX Client.
  - When the WX Client receives the SYN/ACK from the WXC Series, it then releases the original SYN/ACK to the PC running the WX Client.
5. When the ACK is received by the WX Client and sent to the WXC Series, the optimized TCP connection has been formed.
6. Now optimization, compression, and acceleration can be performed on this traffic flow.

You can see that the end result of the optimized TCP connection consists of three separate TCP segments: one between the WX Client and PC application itself, one between the WX Client and server side WXC Series platforms, and one between the WXC Series and server side application. Because the TCP destination port is always retained; application visibility is maintained on the WAN segment.

## Flow Setup and Optimization

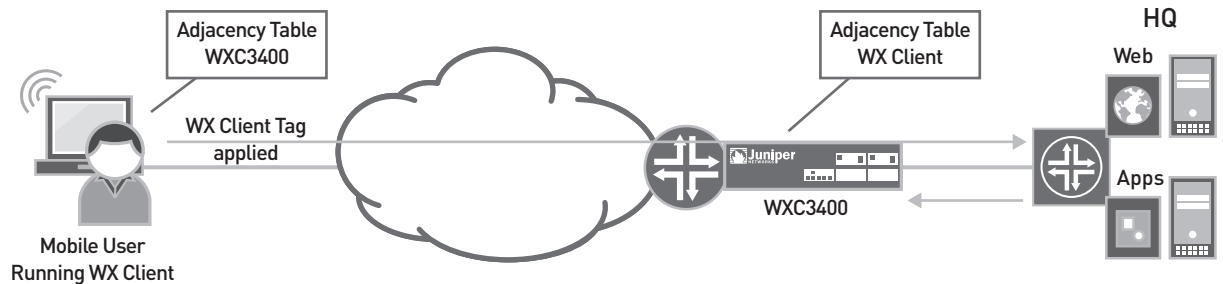
### Flow Setup Overview

To simplify configuration and deployment in highly dynamic environments like those of mobile workers, each flow is inspected and compared to the optimization policies in the WX Client and WXC Series platform configurations to determine eligibility for optimization.

If an adjacency already exists between the WX Client and WXC Series, then no communication control channel negotiation is needed. This example shows the same TCP flow setup process we looked at in the Auto Discovery section, minus the adjacency formation portion. We will also go into a little more detail on some finer points of the setup.

### TCP Flow Optimization with existing adjacency

**Stage 1: User initiates Web session to HQ The WX Client places a Tag on the session the WXC Series platform makes a note of the Tag and waits to see if the return traffic is seen from the server**



**Stage 2: The WXC Client and WXC Series platform establish TCP connection and perform optimization on the Session**

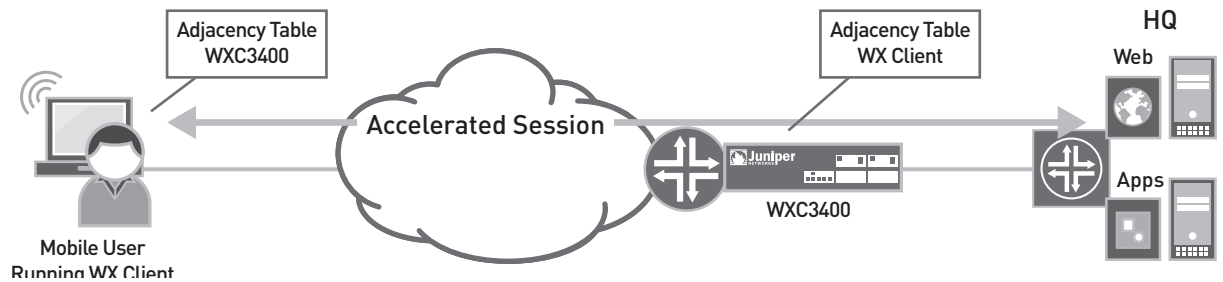


Figure 5: TCP flow setup with established adjacency

## Flow Setup Details

### TCP Flow Optimization to Adjacent WX Series Platforms

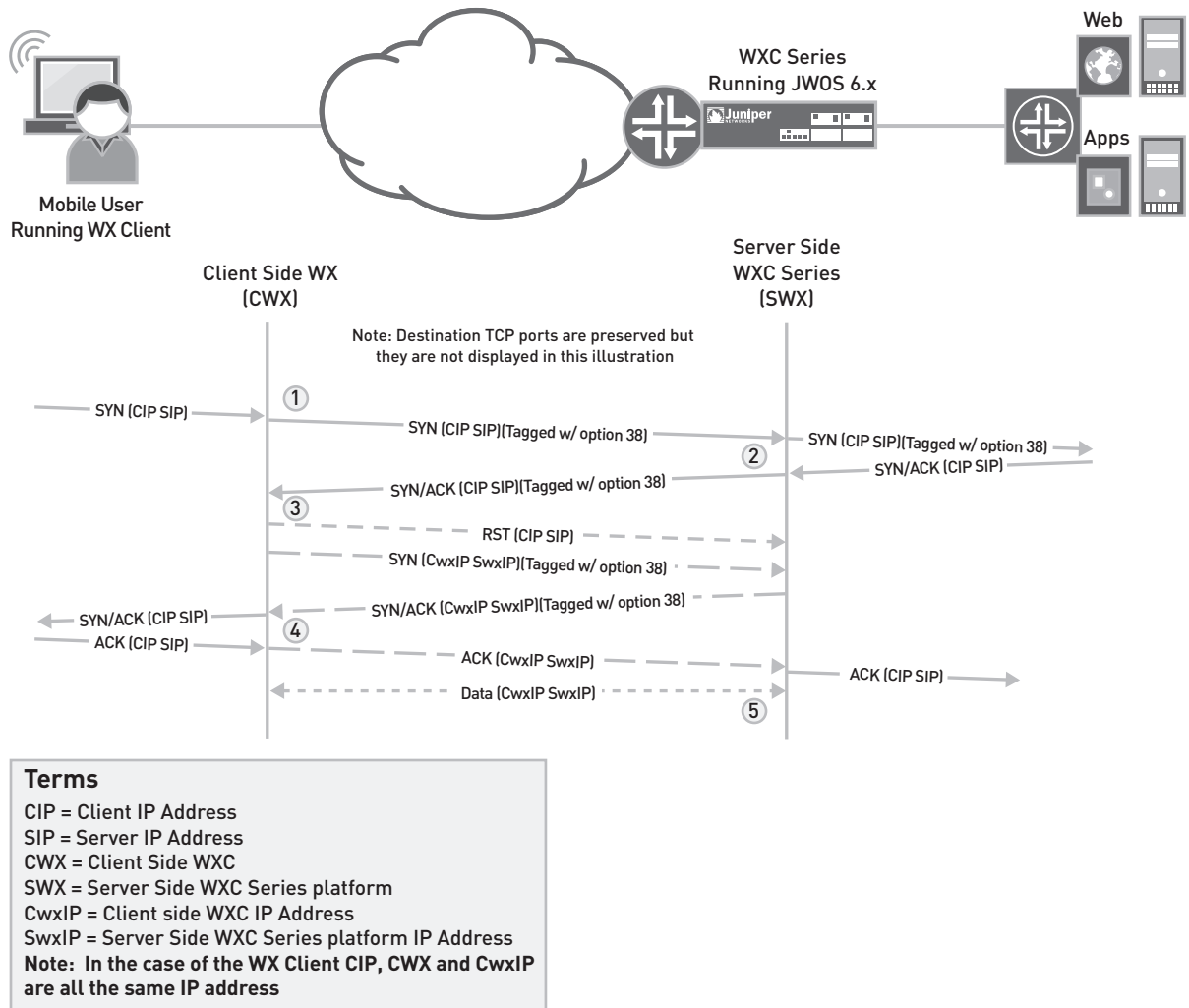


Figure 6: TCP flow setup detail with existing adjacency

### Flow Setup Detailed Analysis

When an adjacency exists between the WX Client and WXC Series, no communication control channel negotiation is needed. In this example, we look at the flow setup process between the WX Client and WXC Series platform when the adjacency has been established.

The walk through here refers to the diagram in figure 6.

1. All TCP traffic that passes through the WX Client and matches the optimization policies will have the initial SYN packet tagged with TCP option 38. If the SYN packet with this tag is seen by a WXC Series platform running JWOS 6.0, it will do the following checks.
  - Does it have an optimization policy for this traffic type? Yes.
  - Does the passphrase match? Yes.
  - Is there an adjacency already established? Yes.
  - Make a note of this SYN and wait to see if the return SYN/ACK is seen.
2. The TCP SYN/ACK from the server is tagged with option 38 and released. When the SYN/ACK is received by the WX Client, it knows that this TCP connection can be optimized.

3. In the flow setup phase, an RST is sent from the WX Client to clean up the connection in the middle of the network.
  - A new SYN for the same TCP destination port number will be sent from the WX Client to the WXC Series.
  - When the WXC Series receives the SYN, it will respond with a SYN/ACK to the WX Client.
  - When the WX Client receives the SYN/ACK from the WXC Series, it releases the original SYN/ACK to the PC running the WX Client.
4. When the ACK is received by the WX Client and sent to the WX Series, the optimized TCP connection has been formed.
5. Now optimization, compression, and acceleration can be performed on this traffic flow.

You can see that the end result of the optimized TCP connection consists of three separate TCP segments: one between the WX Client and PC application itself, one between the WX Client and WXC Series device, and one between the WXC Series and server side application. Because the TCP destination port is always retained; application visibility is maintained on the WAN segment.

## Optimization Services

In order to improve the performance and response time of traffic going through the WX Client, we apply optimization services on an application-by-application basis.

WX Client has several optimization services that can be applied to traffic.

- TCP proxy/acceleration
- Network Sequence Caching/compression
- CIFS protocol-specific acceleration and object caching

## Optimization Service Requirements

In order for some services to operate, other services are required as prerequisites. For example, all applications must have TCP acceleration enabled before any other service is applied. If TCP acceleration is not enabled for a given application, it will get no benefits. Also, in some cases services may be incompatible with one another. In the first release of the WX Client, NSC and CIFS acceleration cannot be enabled for the same application. The points below show what services are required for a given service to be enabled and what services cannot be enabled at the same time.

- NSC service requires TCP
- CIFS requires TCP
- CIFS can't be enabled at the same time as NSC (today)

## Optimization Services

**Globally Available Services:** Each device has services that are enabled globally and will use this when negotiating an adjacency

**Per Adjacency Services:** When the WX Client and WXC Series form an adjacency they negotiate what services each adjacency supports and keep track of this

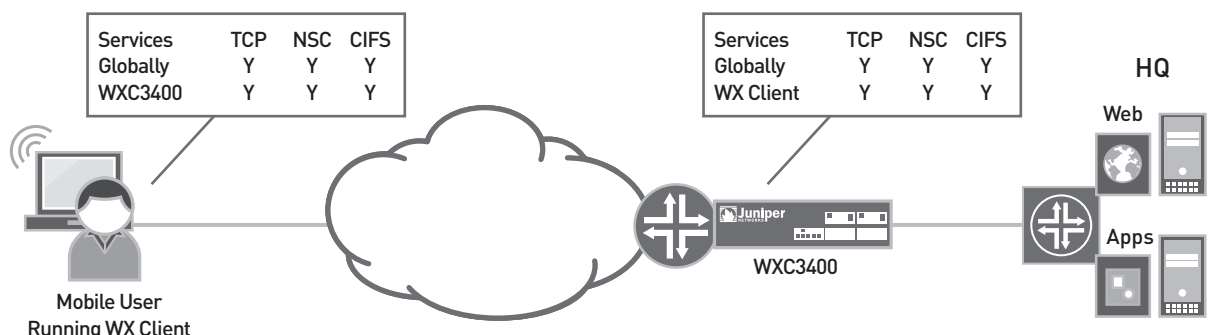


Figure 7: Global and per adjacency services negotiation

## Global and Per Adjacency Services Negotiation

Each WX Client or WXC Series platform has a set of services that are globally enabled.

Services can be enabled or disabled on a per adjacency basis. When two devices form an adjacency, they negotiate the services that are available on each side. If one side does not support a specific service, then that service will be disabled for traffic that traverses between the two devices.

Just because the services are available does not mean that these will be applied to all traffic going between the devices. This is because not all services are applicable to all types of traffic. CIFS-specific protocol optimizations would not provide any benefit to FTP traffic, as an example.

**Per Flow Services:** Based on the application policy services for that flow will be enabled or disabled

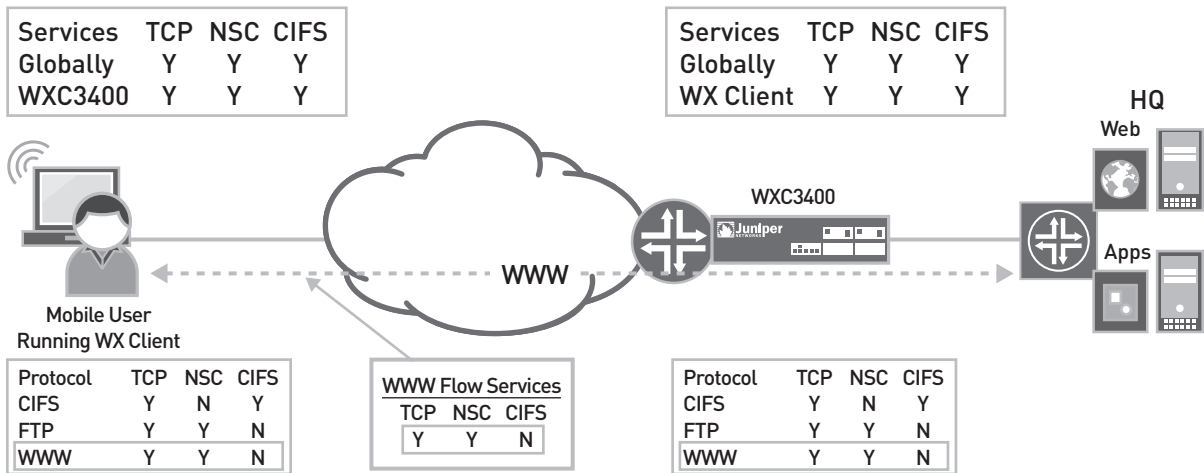


Figure 8: Per flow services

In figure 8, we show an example of a web-based traffic type “WWW.” Here the services match between the two devices and so TCP acceleration and NSC are applied to the traffic flow.

**Per Flow Services Mismatch:** Here is an example of a mismatch in services defined for the application resulting in some services not being applied

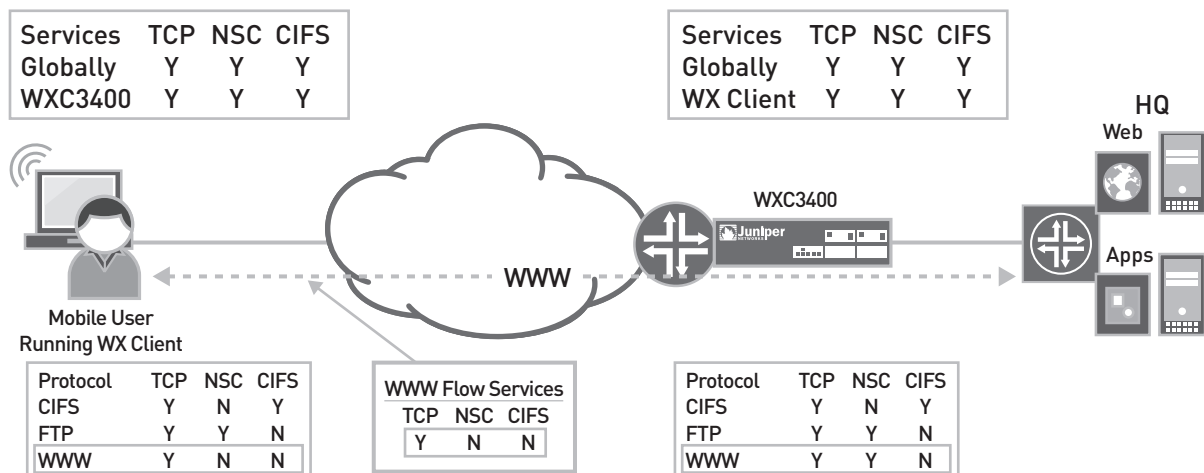


Figure 9: Per flow services mismatch

In figure 9, we show what happens to a flow when services do not match on each end. In this case, NSC was disabled for some reason on the client and resulted in this “WWW” flow only getting TCP acceleration services.

Once common services have been negotiated between two devices, the next item to consider is the application policies defined on the WX Client and WXC Series platform for each application. The WXC Series platform has specific application definitions that are used to classify traffic and the services to be applied, and this is done on a per application and per flow basis.

When a flow matches, an application definition and the services that should be applied are identified, after which a service mask is placed into the packet. This service mask is located in the TCP option 38 tag that we use for initial flow setup and auto discovery as discussed previously. Figure 8 shows an example where services match on the WX Client and WXC Series platform. Just like when an adjacency is formed and services are agreed upon, the same is true for each flow to which services are to be applied. If the services do not match on each end of the connection for a specific application, the lowest common set of services are applied to the flow. Figure 9 shows an example where policies for an application did not match on both sides.

### Optimization Service Requirements

In order for some services to function, other services are required as well. For example, for any compression or protocol level acceleration to happen, TCP acceleration must first be enabled.

## WX Client Design Considerations

### Hardware and Software Requirements

#### PC Requirements for installation of the WX Client

These requirements are based on the initial release of JWOS 6.0 software.

- First release of the WX Client supports Windows 2000 SP4 or Windows XP operating systems.
- Internet browsers need to support Java and ActiveX to download the WX Client from the WXC Series platform.

**Note:** Please see release notes for up-to-date software and hardware requirements for installation of the WX Client.

#### WXC Series Requirements for Installing JWOS 6.0

The first release of JWOS 6.0 can only be installed on the following WXC Series platforms: Juniper Networks WXC3400 Application Acceleration Platform, WXC2600 Application Acceleration Platform, and WXC590 Application Acceleration Platform. Support for other WXC Series platform will be added in future releases. There is also a minimum software version that must be running on the WXC Series prior to installing JWOS 6.0. Attempting to load JWOS 6.0 on a non supported platform could result in rendering the device inoperable.

**Note:** Please see release notes for the most recent software and hardware requirements.

### Firewall Compatibility

#### Firewalls

The following UDP and TCP ports need to be allowed between WXC Series in the data center and the WX Client's UDP and TCP port 3578 for their control communications.

Depending on your security posture, you may also need to allow application ports between the data center WXC Series and the remote WX Clients.

#### Personal Firewall

The following UDP and TCP ports need to be allowed between WXC Series in the data center and the WX Client's UDP and TCP port 3578.

### Virus Scanning Software

Some virus scanners may be incompatible with the WX Client when accessing files via CIFS share. If an issue is suspected, corrective action should be taken by disabling the virus scanner or disabling the scanning of files on shared drives. Check the release notes for up-to-date information on specific virus scanning software.

### VPN Compatibility

Juniper Networks WX Client is generally compatible with VPN solutions that provide direct access to the network by tunneling traffic directly from the PC to the network the way many IPsec and SSL VPN solutions do. See the VPN Overview section for specific examples of compatible and non-compatible VPN configurations.

**Note:** See release notes for specific VPN compatibility

## WX Client Description and Deployment Scenario

### Basic Deployment of the WX Client

The WXC Series platform must be in the path of traffic coming from and going to remote users and servers. This is critical for both Auto Discovery of WX Clients and WXC Series platform, and for optimization of traffic. The most common configuration is to place the WXC Series inline with the traffic flow. Below are some basic WXC Series placement examples illustrating both working and non-working setups.

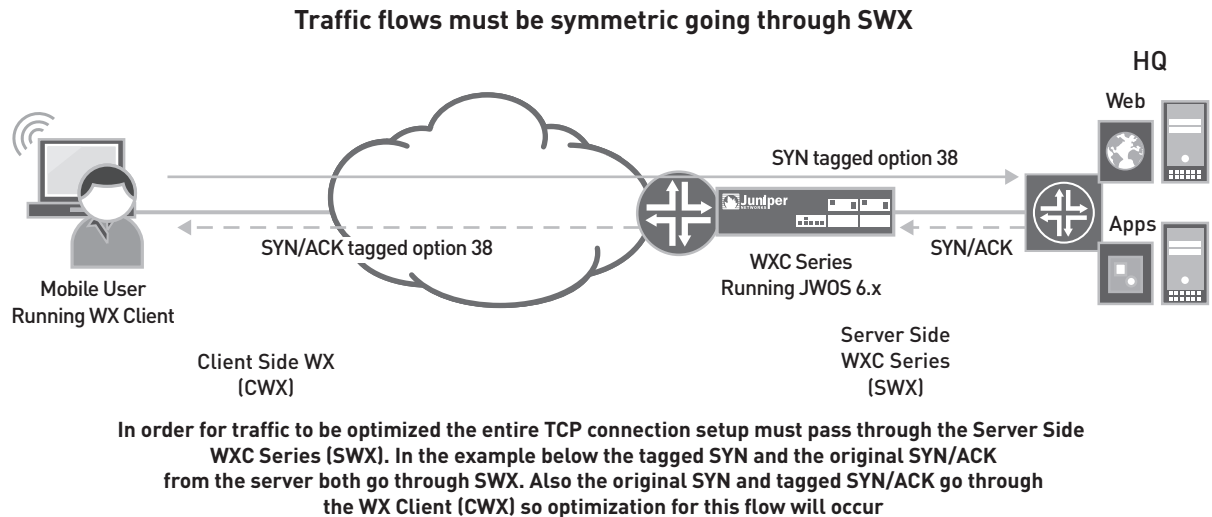


Figure 10: Basic inline deployment

### Common Examples of Non-Working Basic Inline Configurations

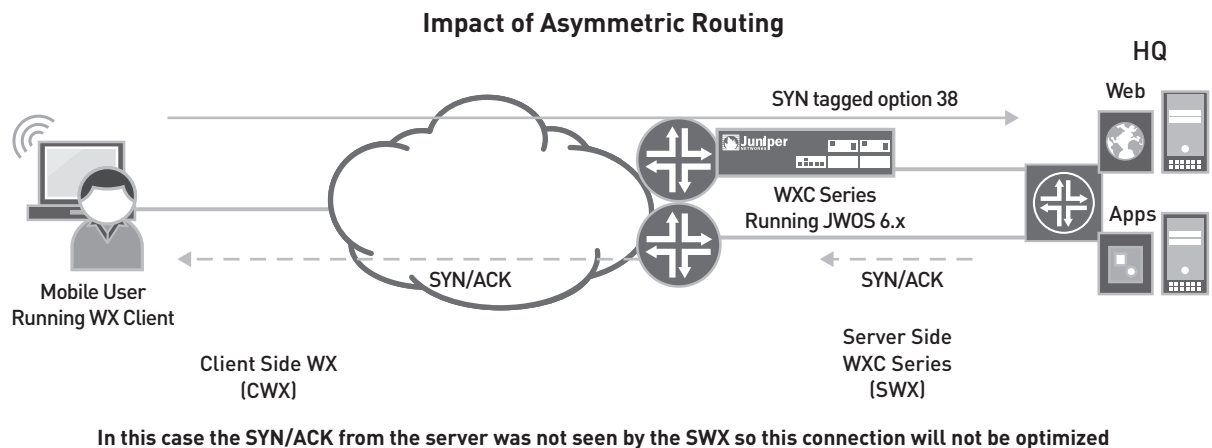


Figure 11: Impact of asymmetric routing on WX Client deployment

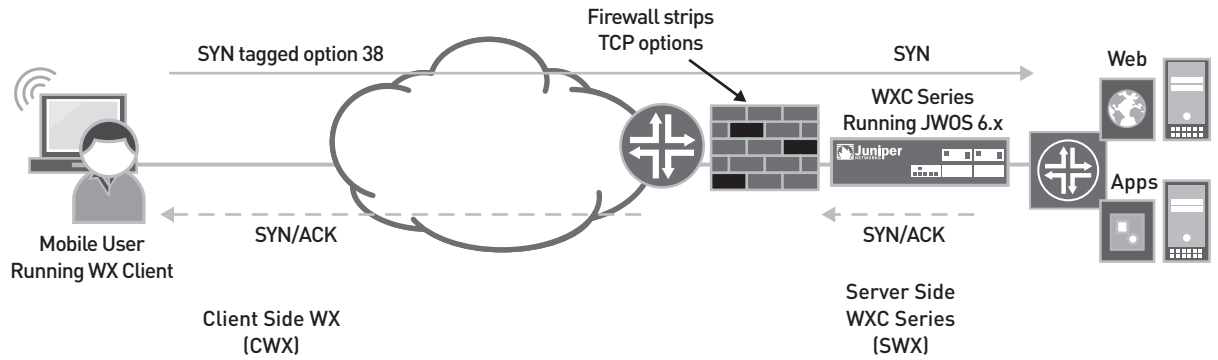
In figure 11, the traffic to and from the servers is asymmetric. This means that the WXC Series will not see the SYN-ACK from the server and will not establish an adjacency with the WX Client.

Another possibility is that only some traffic may be asymmetric, in which case you may get an adjacency and some traffic will be optimized while other traffic is not. This type of issue can be difficult to diagnose if the network traffic flow is not well understood. However, because most deployments of the WX Client will be behind some form of remote access VPN solution, this type of problem should be rare.

### Firewall Considerations

Firewalls must be configured to allow TCP and UDP ports 3578 to pass between the WX Client and the WXC Series. Firewalls cannot strip TCP options from packets. If the TCP options are stripped from the packets, then no Auto Discovery or traffic optimization can occur between the WX Clients and WXC Series platforms.

### TCP options must be preserved by firewalls



In this case the firewall is stripping TCP options off the SYN and SYN/ACK packets. So no traffic will be optimized because the CWX and SWX never see each other

Figure 12: TCP options stripped by firewall

In Figure 12, the firewall strips TCP options resulting in no auto-discover or optimization/acceleration of traffic. This is because TCP option 38 is used to auto discover devices. See Auto Discovery section for more details.

### VPN Overview

Before discussing the WX Client integration with VPN solutions, let's quickly review a couple of the most common VPN access methods at a networking level. This is important to understand because there are many types of VPN access methods, but only some of these can be accelerated. For the WX Client to be able to optimize and accelerate traffic, the VPN appliance must provide an IP address for the VPN client to communicate directly on the corporate network. Figures 13 and 14 are examples of VPNs that are compatible with the WX Client.

### Example of inline VPN deployment

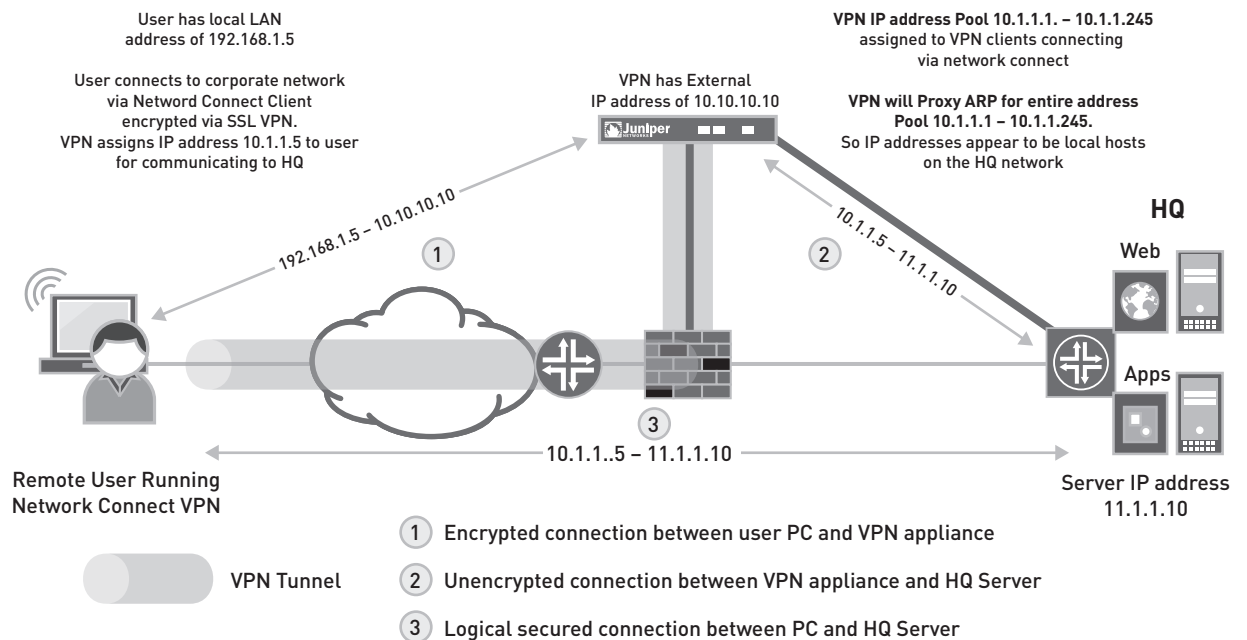


Figure 13: Inline VPN deployment

### Example of one armed VPN deployment

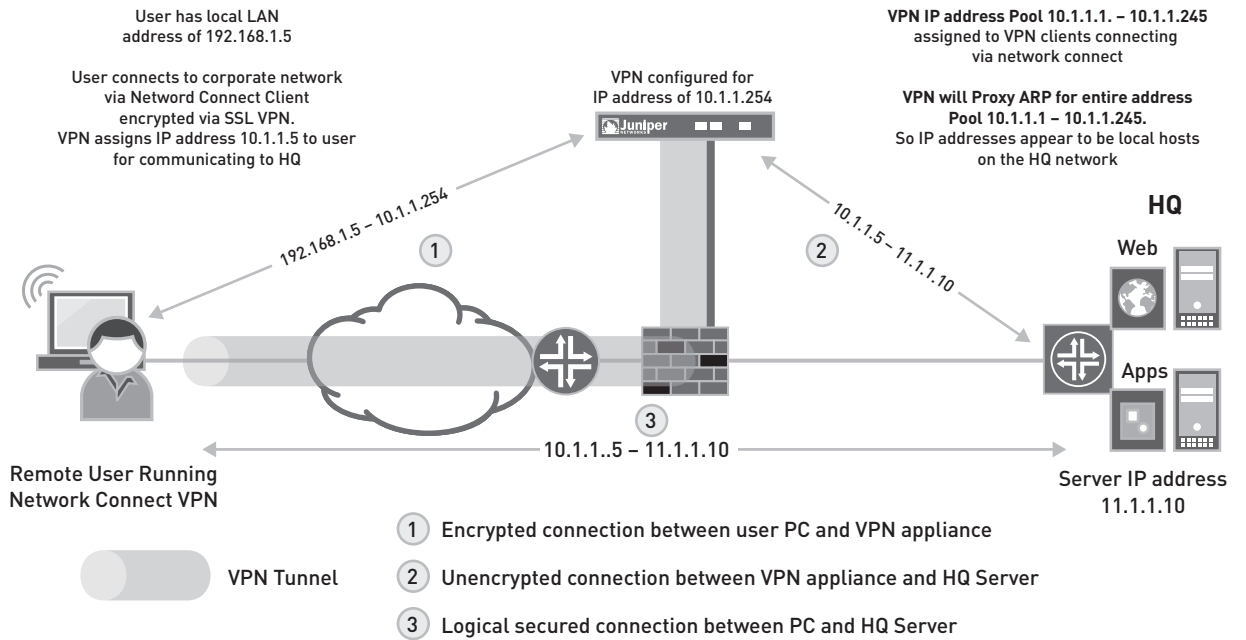


Figure 14: One-armed VPN deployment

Proxy-based VPNs are incompatible with the WX Client.

### Example Proxy VPN Incompatible with WX Client

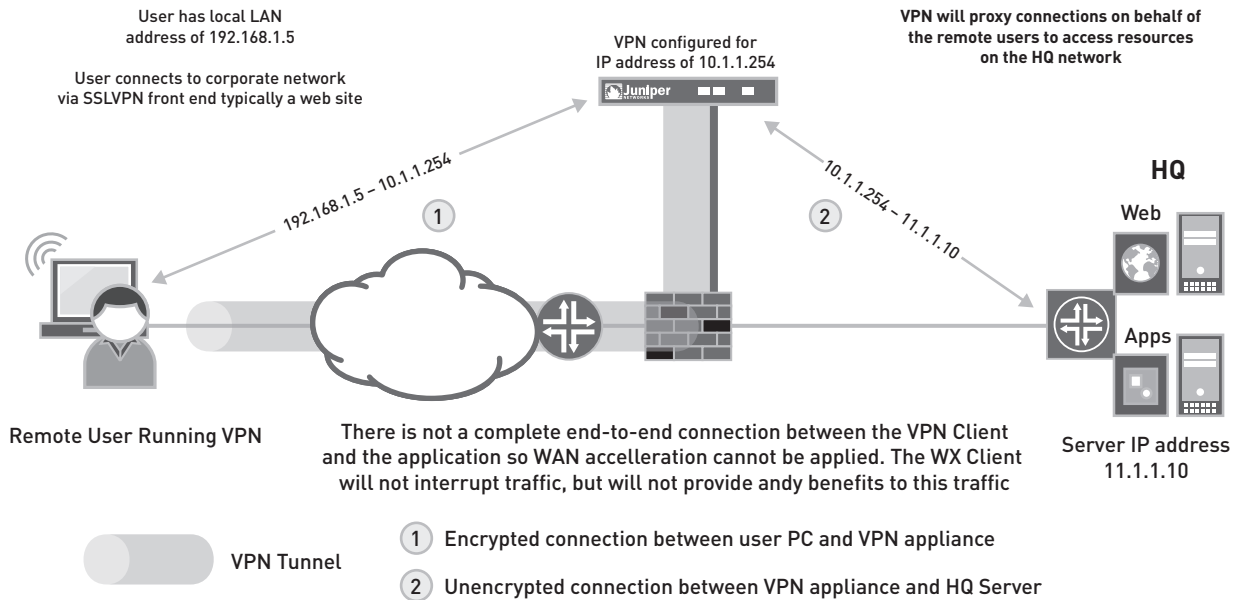


Figure 15: Proxy VPN example "does not work" with WX Client

Proxy-based VPNs will not get any benefit from the WX Client. A common example of this is the case where users establish a secure session to the VPN appliance and then the appliance proxies the connections/applications for the end user. This type of VPN typically has a Web page front end that is presented to the user, and they connect to services via bookmarks/links.

## VPN Deployment Examples with a WXC Series Platform

The WX Client will often be deployed in conjunction with VPNs of some type. When placing the WXC Series in the network, it must be located behind the VPN device to ensure that the TCP sessions can be seen and optimized. If the WXC Series is placed in front of the VPN, it will not be able to view the details of the TCP sessions and cannot perform any optimization of traffic. Below are some basic deployment examples illustrating working and non-working scenarios.

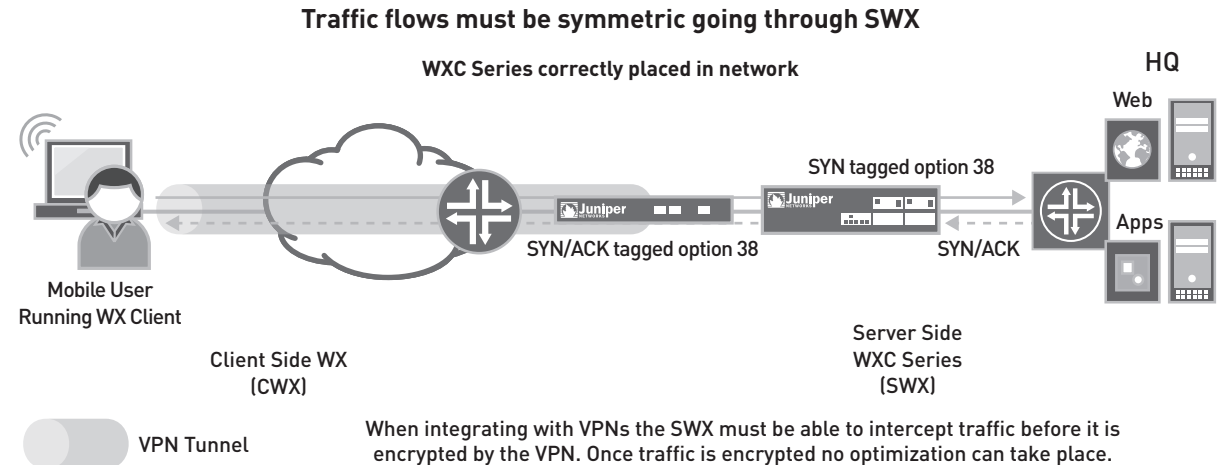


Figure 16: Simplified VPN deployment with WXC Series behind VPN viewing all TCP sessions and performing optimization

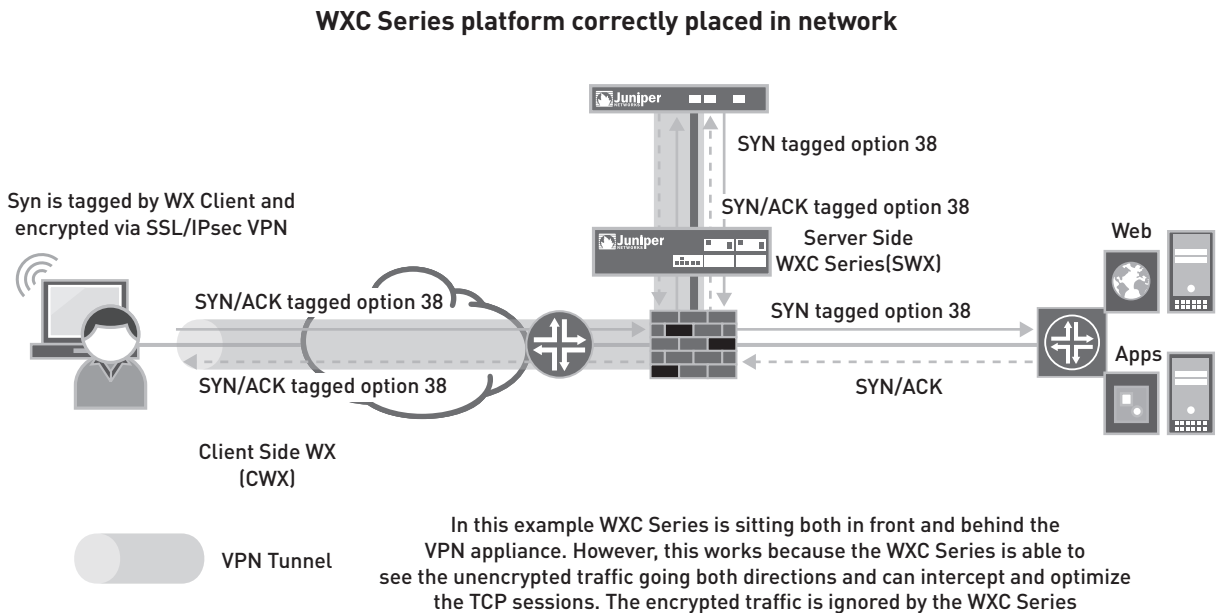


Figure 17: WXC Series deployed with VPN in one-armed mode

The example in figure 17 illustrates some of the possible configurations that might not be so straightforward. Here we have the WXC Series platform both in front and behind the VPN appliance. So while the traffic going from the VPN appliance to remote users is encrypted, the traffic is also in the clear when going from the VPN appliance to the servers. This allows the WXC Series to operate on the TCP traffic and perform optimizations on that traffic.

### Example of Inline SA Series Deployment

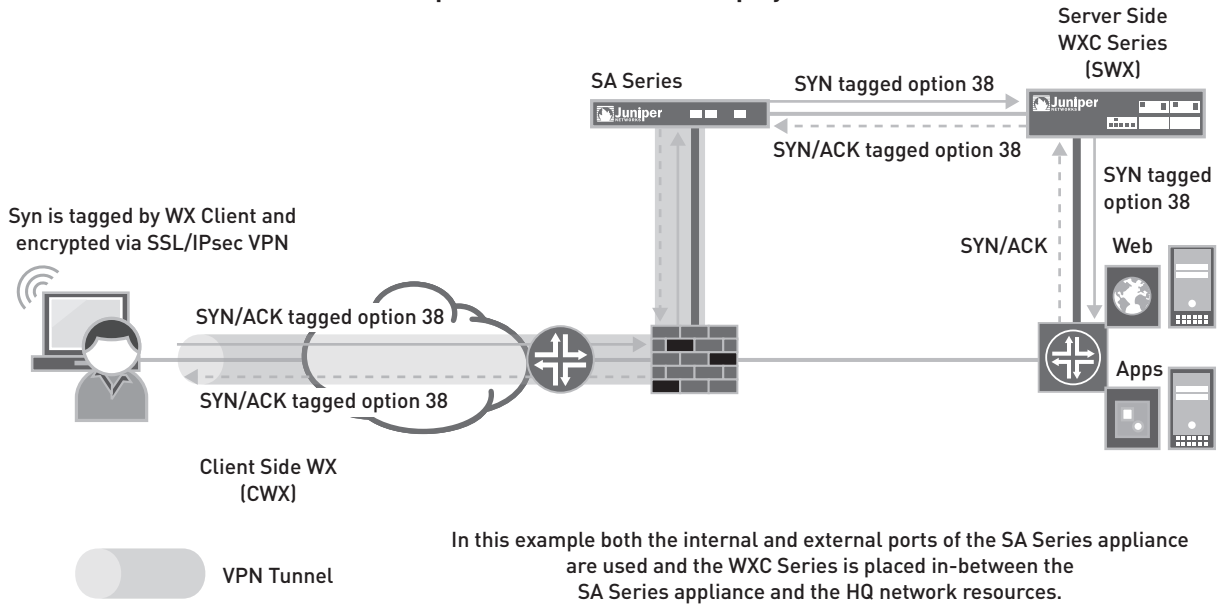


Figure 18: WXC Series and VPN deployed in basic inline mode

### WXC Series Improperly placed in network

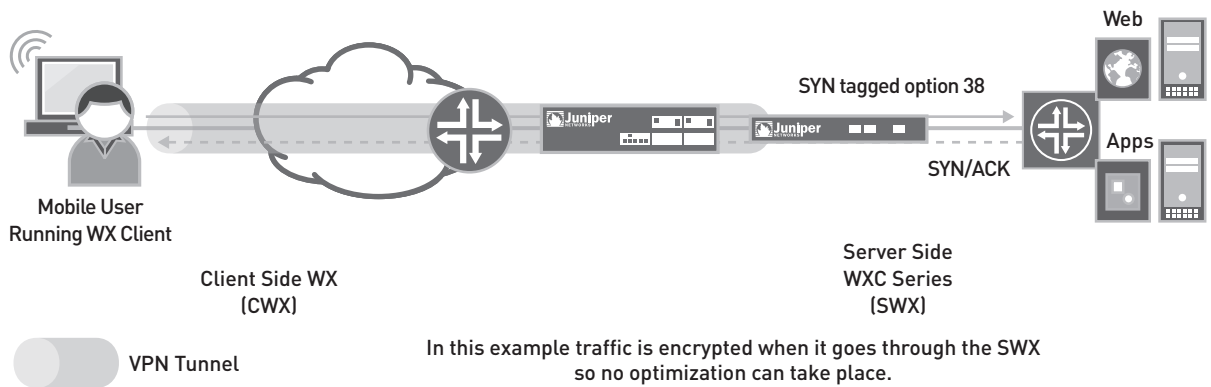


Figure 19: Simplified WX Client and VPN non-working deployment

Figure 19 is a simplified configuration example illustrating improper VPN and WXC Series placement. The WX Client must be able to see the traffic before it is encrypted. If the WXC Series is located after encryption takes place, traffic will be obscured from the WXC Series and it will never see the WX Client requests. As a result, no adjacency will form and no optimization or acceleration will take place. Here you can see that the tagged TCP packets from the WX Client are placed in the VPN, as is the return traffic.

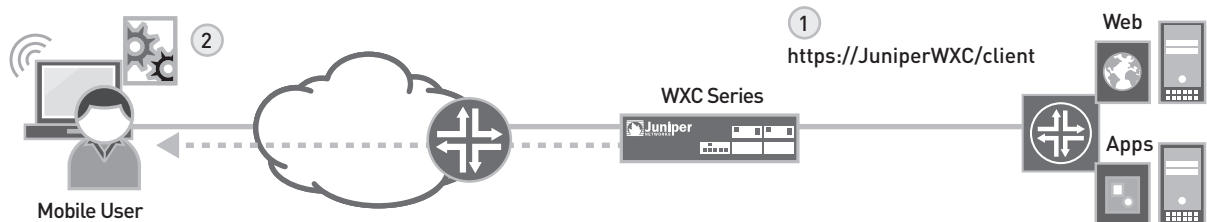
## WX Client Distribution and Configuration

All client configurations are done on the WXC Series platform and are bundled with the download of the WX Client package to the PC. There are three main ways to provide WX Client installation packages for remote PCs.

### WX Client Distributed Directly from WXC Series Platform

#### WX Client Distributed Directly from WXC Series Platform

User can access the WXC Series via https authenticate and install WXC Client software



- ① Connect to WXC Series via https client download url
- ② User installs/upgrades WX Client from web page

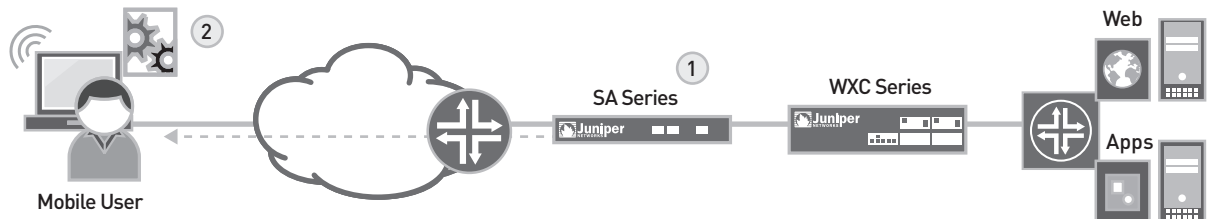
Figure 20: WX Client distribution from the WXC Series via https

The first method is to download the WX Client package directly from the WXC Series platform itself. This is done by connecting to the WXC Series via a client download URL. The URL is composed of `https://` followed by the IP address or hostname of the WXC Series with `/client` at the end. Here is a sample URL where the hostname for the WXC Series is JuniperWXC: `https://JuniperWXC/client`.

### WX Client Distribution via SA Series Appliance

#### WX Client Distribution via SA Series Policy

User authenticates to SA Series appliance and host checker installs and starts the WX Client software according to the user policy



- ① Authenticate and Connect to SA Series appliance via SSL
- ② Host Checker automatically installs upgrades WX Client and starts it

Figure 21: SA Series SSL VPN Appliances authentication and automated WX Client download

The second method is to import the WX Client installation package onto an SA Series platform. This gives IT administrators a single place to manage remote users and services. When a remote user logs into the SA Series, a policy will evaluate if the user should have the WX Client installed on his or her machine. If so, it will check to see if the package is already installed and if a newer version of the software or configuration exists on the SA Series. If the software is not already installed, the SA Series will automatically install and start the WX Client software on the remote user's PC. If the software is already installed and the configuration is up-to-date, the SA Series will start the WX Client on the PC.

### MSI Installer and Microsoft SMS

The third method is to take the MSI installer and export configurations from the WXC Series to create an MSI package for automated installation using Microsoft's SMS service.

## WX Client Setup Basics

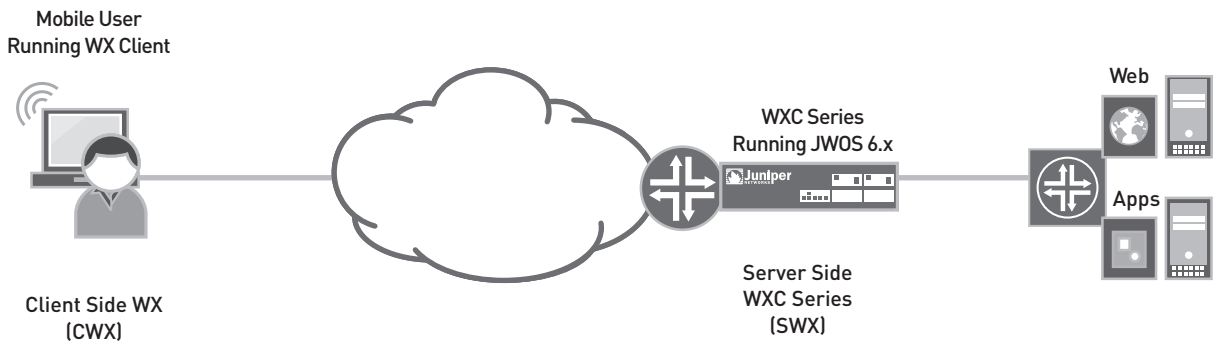


Figure 22: Basic WX Client Setup

This section goes through all of the major steps required to get a basic WX Client running.

What you will need:

- A WXC Series device capable of running JWOS 6.0 software (see software release notes for up-to-date details). In the first release, devices supported include WXC2600, WXC590, and WXC3400.
- JWOS 6.0 software
- A Windows PC running Windows 2000 SP4 or Windows XP on which to install the WX Client

Steps to install the WXC Series:

1. Install JWOS 6.0 software on compatible appliance (see release notes for details).
2. Access appliance via <https://<devicename>>.
  - Username: admin
  - Password: juniper
3. Complete JWOS Quick Start.
  - Press “Next”
4. Configure Bridge Interface br-0/0.

**Note:** Bridge interfaces are broken into two parts—local and remote. The local interface is connected toward your LAN side of the network and the remote interface is connected to the WAN router.

### Bridge Interfaces > br-0/0

Please enter the required information for the bridge on this WX device. When you click **Next**, it will automatically take you to the next bridge until all bridges detected on this device have been configured. If you do not wish to configure any other bridges, click **Finish** to complete the wizard.

<b>Bridge</b>	br-0/0
<b>IP Address</b>	<input type="text" value="10.1.1.2"/>
<b>Subnet Mask</b>	<input type="text" value="255.255.255.0"/>
<b>Default Gateway</b>	<input type="text" value="10.1.1.1"/>
<b>Local Interface</b>	ge-0/0/0
<b>Speed/Duplex</b>	<input type="text" value="Automatic"/>
<b>Remote Interface</b>	ge-0/0/1
<b>Speed/Duplex</b>	<input type="text" value="1000 full-duplex"/>

- Verify that the IP address information is correct
- Verify that the interface settings are correct
- Select “Next”

5. Select Finish.



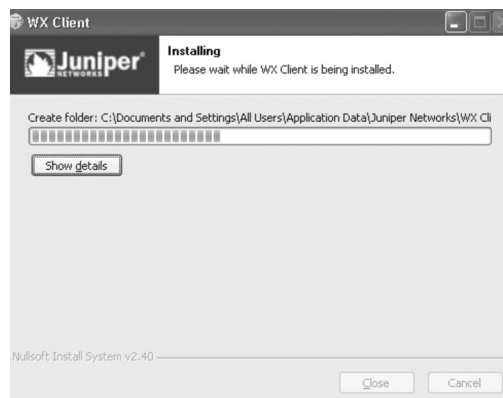
6. Insert WXC Series platform into network inline with traffic.


7. Install WX Client software on PC via Web download.

- [https://<wxc\\_appliance/client](https://<wxc_appliance/client)



- Press install now.
- WX Client will be downloaded and installed (depending on your link speed, this may take a few minutes).



- You should now see the WX Client launched and the icon on your taskbar .
- WX Client TCP traffic going through the WXC Series should now be getting optimized.

## Delivering WX Client Installation Package from SA Series Appliance

This section goes through the basic steps required to deploy the WX Client installation package via the SA Series appliance. It is assumed that the reader has a basic understanding of the SA Series SSL VPN appliance. We will only cover the steps required to install the package onto the SA Series.

### WX Client and SA Series Integration

Phase 1: User authenticates to SA Series appliance and host checker installs and starts the WX Client software

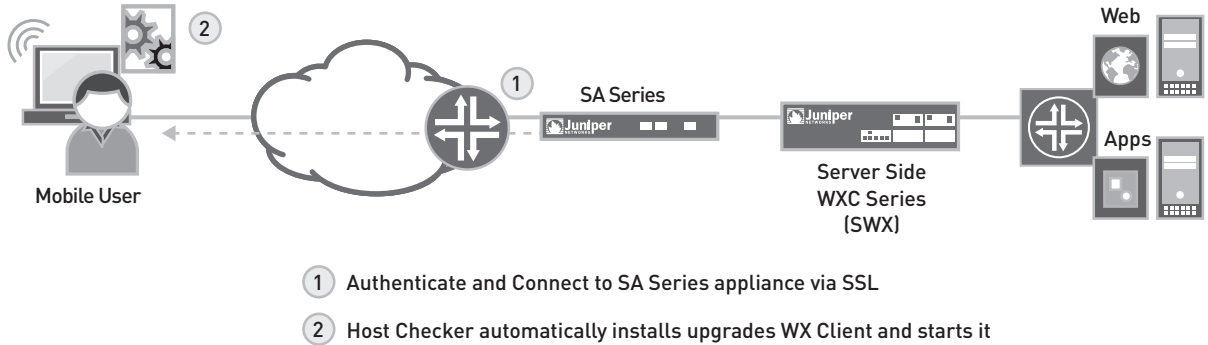


Figure 23: SA Series authentication and WX Client distribution

Once the WX Client package has been imported into the SA Series appliance, a policy can be applied to users of a specific group. When those users log in, they will have the WX Client automatically installed and started.

Phase 2: User establishes Network Connect VPN connection and WX Client optimizes and accelerates application sessions

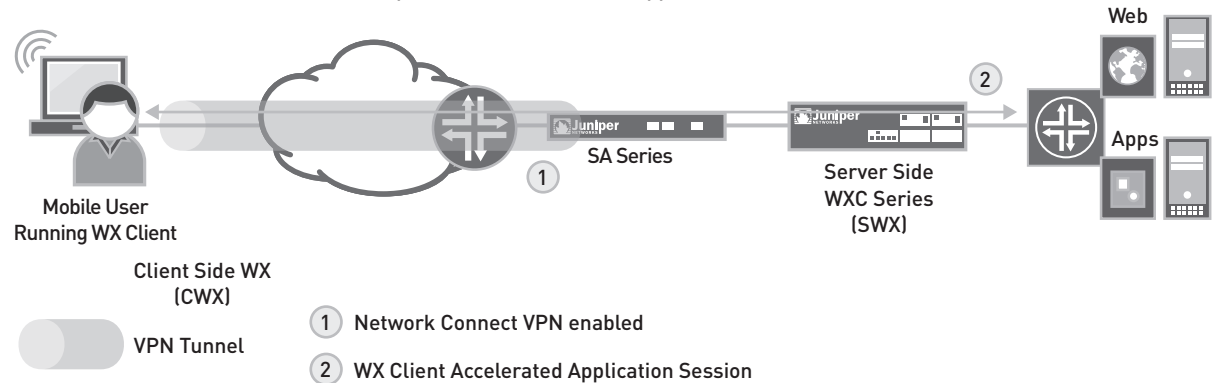


Figure 24: Remote user accessing network via Network Connect VPN and WX Client

Users now launch Network Connect and get the benefits of WAN acceleration on their remote access traffic.

## Basic Steps Required to Deliver the WX Client Package from an SA Series Appliance

On the WXC Series:

1. Navigate to the WX Client's -> Export Client Software.
2. Select Create Host Checker package for use with the SA Series.
  - Install and invoke without remediation.

**Export WX Client Software**

You can use this page to create and export a software package that can be used to deploy the WX Client to endpoint clients in your network. The software package includes the WX Client software and the default client configuration. The Host Checker package also contains deployment policy information.

Additionally you can use this page to export WX client default configuration which can be used later to create MSI package for distribution.

NOTE: In order to export a software package, this WX device must be configured to allow Client Image downloads.

**Create Host Checker package for use with SA**

If you select "Host Checker" you must also specify one of the following deployment options

Install and invoke without remediation

Install only

**Download Configuration for MSI package (for use with SMS)**

- Press Export and save the package to your local machine.

On the SA Series appliance:

1. Go to Endpoint Security-> Host Checker.
2. Select "New 3rd Party Policy."

Endpoint Security >

### New 3rd Party Policy

**Host Checker Policy Package**

Name:   
Label to reference this package.

Policies File:    
Zip file containing policy definitions.

**Remediation**

Enable Custom Instructions

Enable Custom Actions

Remediate

Kill Processes

Delete Files

Send reason strings

**Save changes?**

3. Enter a name for the policy and the name of the WX Client package you exported from the WXC Series, then press "Save Changes."
4. Go to User Realms-> Users-> Authentication Policies-> Host Checker.
5. Check "Evaluate Policies" for the policy name you created—it should look similar to the screen below.

User Authentication Realms >

## Users

General | Authentication Policy | Role Mapping

Source IP | Browser | Certificate | Password | Host Checker | Cache Cleaner | Limits

Allow users whose workstations meet the requirements specified by required host-checker policies. If no policies are selected then all users will be allowed. "Evaluate Policies" will evaluate the policy on the client. "Require and Enforce" will require and enforce the policy in order to login to this realm.

Evaluate Policies	Require and Enforce	Available Policies
<input type="checkbox"/>	<input type="checkbox"/>	All
<input type="checkbox"/>	<input type="checkbox"/>	WX Client
<input checked="" type="checkbox"/>	<input type="checkbox"/>	WX Client.WX Client should be installed and invoked

Allow access to realm if any **ONE** of the selected "Require and Enforce" policies is passed.

Save Changes

6. Press "Save Changes."

7. Now when users in this realm are authenticated, the WX Client will automatically be installed and started on their machines.

## Summary

The WX Client provides a lightweight, high-performance, and cost-effective alternative for very small offices and mobile users. Integration with Juniper Networks SA Series SSL VPN Appliances simplifies user and client management for better ROI, and enables rapid deployment of client-based WAN acceleration.

## About Juniper Networks

Juniper Networks, Inc. is the leader in high-performance networking. Juniper offers a high-performance network infrastructure that creates a responsive and trusted environment for accelerating the deployment of services and applications over a single network. This fuels high-performance businesses. Additional information can be found at [www.juniper.net](http://www.juniper.net).

### Corporate and Sales Headquarters

Juniper Networks, Inc.  
1194 North Mathilda Avenue  
Sunnyvale, CA 94089 USA  
Phone: 888.JUNIPER  
(888.586.4737)  
or 408.745.2000  
Fax: 408.745.2100

### APAC Headquarters

Juniper Networks (Hong Kong)  
26/F, Cityplaza One  
1111 King's Road  
Taikoo Shing, Hong Kong  
Phone: 852.2332.3636  
Fax: 852.2574.7803

### EMEA Headquarters

Juniper Networks Ireland  
Airside Business Park  
Swords, County Dublin,  
Ireland  
Phone: 35.31.8903.600  
Fax: 35.31.8903.601

Copyright 2009 Juniper Networks, Inc. All rights reserved. Juniper Networks, the Juniper Networks logo, JUNOS, NetScreen, and ScreenOS are registered trademarks of Juniper Networks, Inc. in the United States and other countries. JUNOSe is a trademark of Juniper Networks, Inc. All other trademarks, service marks, registered marks, or registered service marks are the property of their respective owners. Juniper Networks assumes no responsibility for any inaccuracies in this document. Juniper Networks reserves the right to change, modify, transfer, or otherwise revise this publication without notice.

To purchase Juniper Networks solutions, please contact your Juniper Networks representative at 1-866-298-6428 or authorized reseller.

