WAN OPTIMIZATION AND IPSEC FOR THE BRANCH OFFICE
# Table of Contents

Introduction ................................................................. 4
Scope ................................................................. 4
  Audience ......................................................... 4
Design Considerations .................................................... 4
  Inline vs. Off-Path Deployment .................................... 5
  WX Series Reduction Subnets ......................................... 6
  QoS and Application Policies ......................................... 6
  J Series/ISM200 limitations: ......................................... 6
Implementation ............................................................. 7
  General Topology ...................................................... 7
  Software and Hardware Versions ...................................... 7
Solution Details ............................................................ 7
Solution Description ...................................................... 7
J Series Junos OS Configuration Details ................................ 8
  Configuring J Series Routing .......................................... 8
  Configuring Security Zones ............................................. 9
  Configure IPsec Tunnel .................................................. 9
  Configure Security Policies ............................................ 10
J Series ISM200 Configuration .......................................... 12
NetScreen Series Firewall Configuration Details ...................... 13
  Detailed configuration: ................................................ 13
  Create IPsec tunnels .................................................... 13
  Enable static and OSPF routing ....................................... 13
  Configure address book entries for local and remote networks  .............................................. 14
Define policies ........................................................... 14
WX Series Configuration .................................................. 14
Verification ............................................................. 14
ScreenOS ............................................................. 14
Junos OS With Enhanced Services ....................................... 15
  WX Series .......................................................... 15
Summary ............................................................. 16
About Juniper Networks ................................................... 16
Table of Figures

Figure 1: WX Series Off-Path and Inline deployment modes .................................................. 6
Figure 2: Sample deployment topology .................................................................................. 7
Figure 3: Logical topology depicting Compression Tunnel Encapsulated within IPsec Tunnel .................... 8
Figure 4: Security zones and policies directing traffic flow within J Series router .......................... 10
Figure 5: Local static and dynamic routes displayed in the ISM200 web UI .................................. 12
Figure 6: The Endpoints screen displays tunnel status to all discovered WX Series devices .............. 12
Figure 7: Flow Diagnostics allows detailed level verification of WX Series optimization ................. 15
Figure 8: Compression performance graphs for FTP and other Applications .......................... 16
Introduction

A distributed enterprise network requires high performance optimized wide area network (WAN) connectivity and security between data centers and branch locations. Ever increasing network utilization due to web based applications, increasingly large file transfers, and centralized servers, is frequently creating network bottlenecks on WAN connections. Constrained WAN links between data centers and remote branch offices result in traffic latency and poor application performance.

Juniper Networks® delivers an application acceleration solution with Juniper Networks WX Series Application Acceleration Platforms. Deployed at the data center and branch offices, the WX Series enables network administrators to optimize existing WAN links and deliver fast application response. The WX Series integrates several technologies including advanced compression, sequence caching, TCP, and application specific acceleration along with bandwidth management to accelerate overall WAN performance.

As enterprise networks require secure communications over the WAN, an IPsec VPN encrypting WAN traffic is essential. This document presents a solution that tunnels optimized WAN traffic within a point-to-multipoint IPsec VPN. Juniper Networks addresses these requirements with the WX Series optimization and application acceleration solution and a high performance ScreenOS-based firewall that provides an IPsec-based VPN. For the branch office, the Juniper Networks J Series Services Routers with the Juniper Networks ISM200 Integrated Services Module provides both IPsec encryption and WAN optimization in a single, easy to manage, cost-efficient platform.

Scope

The solution presented in this document details the implementation of an enterprise data center to branch office IPsec VPN that further incorporates the WAN acceleration features of the WX Series.

This document details a data center to multiple branch site connectivity solution incorporating the high performance independent Juniper Networks NetScreen 5000 Series Security Systems and WX Series products at the Data Center along with the integrated J Series/ISM200 deployed at branch locations.

Branch locations typically have several requirements that are different than central corporate offices:

- Lower bandwidth requirements relative to the data center
- Ease of deployment
- Simple manageability
- Cost efficiency

The combined J Series /ISM200 platform meets these requirements by offering routing, IPsec firewall, and WAN acceleration in a single box solution.

After presenting solution features and overview, the document discusses configuration of the three different platforms, verification, and best practices.

Note: In this implementation guide, WX Series refers to both WX Series and Juniper Networks WXC Series Application Acceleration Platforms unless otherwise stated.

Audience

This document is intended for network design and operation engineers, and implementation partners supporting enterprise networks requiring optimized and secure WAN connectivity to branch offices.

Design Considerations

The following section describes the design considerations for this solution:

IPsec Encryption – In addition to acceleration, enterprise traffic to and from branch offices must be protected as it negotiates untrusted WAN networks to ensure confidential branch office communication with centrally located data centers and corporate headquarters.

While dedicated WX Series appliances can provide IPsec encryption on top of a WX Series compression tunnel, the ISM200 module does not support IPsec functionality. The underlying J Series running the Juniper Networks Junos® operating system with
enhanced series is employed to provide IPsec service at the branch office. At the data center, a dedicated ScreenOS firewall is deployed to terminate the IPsec tunnel along with a standalone WX Series which handles the compression tunnel.

**WAN Acceleration** – As enterprise traffic destined to many branch locations can be quite varied in application, latency requirements and volume, it is desirable to optimize at the WAN layer. The WX Series Framework encompasses a number of optimization and acceleration technologies to accelerate data traversing the WAN including:

- Sequence caching and compression - MSR (Molecular Sequence Reduction) – Juniper Networks WX Series platform employs compression and memory / disk based caching technologies to dramatically reduce large patterns of data.
- TCP Acceleration – Speeds up TCP setup and performance by implementing fast connection setup, active flow pipelining, and forward error correction.
- Application acceleration – WX Series employs several application specific technologies to speed up common protocols such as CIFS and MAPI.

**J Series Integration** – the Juniper Networks J Series Services Routers provide an ideal solution for branch offices as it integrates stateful flow based firewall, WX Series WAN acceleration (via the ISM200 module), and routing into a cost effective, easy to manage deployment.

**High Availability (HA)** – High availability is desirable especially at the data center end of distributed enterprise topology, but is outside the scope of this document. J Series HA can be implemented with a backup J Series. As ISM200 Integrated Services Module does not support HA, existing traffic may be interrupted upon failure, but applications can continue without WAN optimization.

**Scalability** – An effective solution for branch deployments must be able to scale in both number of locations and available bandwidth. The integrated J Series with the ISM200 module can scale up to 4 Mbps WAN link. At the data center end, the Juniper Networks WXC590 Application Acceleration Platform can scale up to 45 Mbps WAN link as a single box deployment and scaling up to 155 Mbps using a WX Series stack. The solution presented in this document was tested with a standalone Juniper Networks WXC3400 Application Acceleration Platform at the data center end.

On the data center end, a Juniper Networks ISG Series Integrated Security Gateways firewall in this example is handling both routing and firewall functionality. For a large scale deployment with several hundred branch sites, routing and firewall should be separated with appropriately sized routers and firewalls to independently manage routing and IPsec functionality.

**Branch-to-Branch Communications** – Communication to branches is handled with a point to multipoint route based VPN with the data center as the hub. As the majority of branch office traffic is to/from the data center, all traffic destined to the data center is sent over the IPsec tunnel. Branch to branch communication is tunneled through the data center as well.

**Inline vs. Off-Path Deployment**

A standalone WX Series appliance can be deployed in a network using two different topologies – inline and off-path. The simplest inline mode offers minimal disruption to an existing network as the WX Series device is completely transparent at the IP layer, appearing as a transparent bridge. Traffic from the LAN is optimized and sent through to the WAN without any IP reconfiguration required. In addition, inline mode offers the advantage that in case of failure, the WX Series device “switches-to-wire” essentially reverting to an Ethernet cable so traffic flows uninterrupted. This mode is depicted on the right side in the topology below.

The second deployment mode for WX Series appliances is off-path, also called Packet Interception mode. In this deployment the WX Series appliance is connected to a single interface of a router and traffic is routed to and from that router to the WX Series for optimization. This can be useful in cases where the router in the topology is a combined switch/router and it is not possible to deploy the WX Series inline. The Packet Interception mode requires additional consideration to determine which traffic to redirect to the WX Series appliance for acceleration. The traffic redirection can be implemented using three different ways – Route Injection via RIPv2, WCCP, and External Mode via Policy Routing.
An additional reason to select Packet Intercept mode is if implementing multiple WAN paths such as a high availability environment. In this solution where the optimized WAN traffic is being tunneled into an IPsec VPN, redundancy must be implemented at the firewall level which is outside the scope of this document.

In this document, the solution presented implements the standalone WX Series in inline mode between a LAN switch and a firewall with the firewall wrapping the optimized traffic in an IPsec tunnel. On the branch network side, using J Series Services Routers with the ISM200 for WAN optimization, the J Series is in effect using an internal off-path mode redirecting traffic via policy and routing. As the J Series Services Routers with ISM200 is an integrated router, firewall, and WX Series, it is deployed in inline fashion.

**Figure 1: WX Series Off-Path and Inline deployment modes**

**WX Series Reduction Subnets**

WX Series platforms accelerate traffic from local subnets destined to remote subnets. WX Series devices create a table of remote endpoints to which traffic can be accelerated. Correspondingly, the WX Series has to match traffic from local subnets that requires acceleration to apply the optimization policies to that traffic. Traffic that does not match passes through without optimization. With multiple local subnets, a routing protocol such as OSPF or RIP is used so the WX Series can identify local traffic for acceleration. For simpler deployments, local routes can be statically defined.

**QoS and Application Policies**

Optimized traffic can be prioritized by the WX Series based on multiple factors such as endpoints, applications, bandwidth, and latency factors. The WX Series employs a QoS setup wizard to simplify configuration of these options. QoS considerations are outside the scope of this document.

**J Series/ISM200 limitations:**

The ISM200 only supports route-based IPsec VPNs within the J Series. Policy-based VPNs are not supported. Auto-Deployment with CMS is not supported for the ISM200. For WX Series tunnels, the ISM200 only supports UDP tunnel mode (WX Series default since WX Series OS 5.5). WX Series IPComp tunnels are not supported.
Implementation

General Topology

Figure 2: Sample deployment topology

Software and Hardware Versions

The following software and hardware versions are used in this implementation:

- Juniper Networks J6350 Services Router running Junos OS with enhanced services 9.2R1.10
- NetScreen Series ScreenOS 6.1r3
- WXC3400 WX Series-OS 5.6.2
- ISM200 WX Series-OS 5.6.2

Solution Details

Solution Description

This solution employs nested dual tunnels for traffic between the data center and branch LANs. First traffic is accelerated between the LAN networks by the WX Series, which creates compression tunnels for traffic to the remote LANs. Outbound traffic not destined to remote LANs is passed through without compression. Second, compressed traffic from the WX Series is encrypted into a route based IPsec VPN tunnel.

Within this solution, the standalone firewall and WX Series at the data center handle the dual tunnels differently than the integrated J Series/ISM200. From the data center perspective, traffic destined for the branch offices is initially sent to the WX Series, where the WX Series matches for remote LANs to determine if a compression tunnel is established for the remote LAN. Both compressed and pass-through traffic is sent to the firewall. The ScreenOS based firewall further encapsulates the WX Series traffic into an IPsec VPN before sending the data out to the WAN.
In the J Series, traffic is also doubly encapsulated first within the compression tunnel and then further in the IPsec tunnel. As the J Series handles this entirely within the single device, traffic is internally routed within four security zones:

- **Trust Zone** – Traffic to/from the trusted Branch LAN
- **Untrust Zone** – WAN traffic sent to the internet
- **VPN Zone** – Encrypted IPsec traffic destined for remote LAN
- **WX Series Zone** – Traffic sent to/from ISM200 for WAN acceleration

Traffic flow is logically depicted in Figure 3.

![Logical topology depicting Compression Tunnel Encapsulated within IPsec Tunnel](image)

**Figure 3: Logical topology depicting Compression Tunnel Encapsulated within IPsec Tunnel**

**J Series Junos OS Configuration Details**

J Series Services Routers are configured in 2 steps. First the router side is configured via CLI to set up the interfaces, routing, zones, and policies. Subsequently, the ISM200 is configured via the graphical WebUI.

**Configuring J Series Routing**

Configure IP addresses for WAN, LAN, ISM200 (WX Series), and secure tunnel interfaces as follows:

```plaintext
set interfaces ge-0/0/1 unit 0 family inet address 50.1.1.1/24
set interfaces ge-0/0/2 unit 0 family inet address 10.0.0.1/24
set interfaces wx-3/0/0 unit 0 family inet address 1.1.1.1/32 destination 10.0.0.10
set interfaces lo0 unit 0 family inet address 127.0.0.1/32
set interfaces st0 unit 0 family inet address 10.11.1.1/24
```

- **WAN** interface has a public IP address and the **LAN** has a private IP address.
- **The ISM200** IP address (1.1.1.1) can be anything as it is used for internal communication within the J Series, but the destination IP address (10.0.0.10) is the actual ISM200 WX Series address used to establish the compression tunnel to the other WX Series. This destination IP address must be in the same subnet as the WX Series LAN interface.
- **As the st0 interface** establishes a point-to-point link, it is recommended both ends have IP addresses in the same logical subnet.

Configure default route to Internet next-hop, a static route to the remote LAN through the secure tunnel, and also dynamic routing protocol such as OSPF. Enable OSPF area 0.0.0.1 and assign to the LAN, WAN, and WX Series interfaces.

```plaintext
set routing-options static route 0.0.0.0/0 next-hop 50.1.1.2
set routing-options router-id 50.1.1.1
set protocols ospf area 0.0.0.1 interface ge-0/0/2.0
set protocols ospf area 0.0.0.1 interface st0.0
```
Configuring Security Zones
Since this configuration implements an IPsec tunnel between the J Series and NetScreen Series firewall, the J Series Services Routers operates in a security context and require four security zones: trust, untrust, wx-zone, and vpn.

Associate interfaces to security zones

```
set security zones security-zone trust interfaces ge-0/0/2.0
set security zones security-zone untrust interfaces ge-0/0/1.0
set security zones security-zone vpn interfaces st0.0
set security zones security-zone wx-zone interfaces wx-3/0/0.0
```

Allow relevant inbound traffic on zones. All system services are allowed on the trust zone to manage the device. On the untrust zone, ike is permitted to establish the IPsec tunnel. For the wx zone system services are allowed to manage the ISM200 and all protocols are allowed to establish the compression tunnel.

```
set security zones security-zone trust host-inbound-traffic system-services all
set security zones security-zone untrust host-inbound-traffic system-services ike
set security zones security-zone untrust host-inbound-traffic protocols ospf
set security zones security-zone wx-zone host-inbound-traffic system-services all
set security zones security-zone wx-zone host-inbound-traffic protocols all
set security zones security-zone vpn host-inbound-traffic protocols ospf
```

Define address book entries for local subnets, remote subnets

```
set security zones security-zone trust address-book address local-net 10.0.0.0/24
set security zones security-zone vpn address-book address remote-net 10.2.1.0/24
```

Configure IPsec Tunnel
Configure IKE policy and IKE gateway parameters. In this example the IKE policy for phase 1 proposal is configured with a “standard” proposal. The IKE policy and gateway parameters can be customized as needed for specific corporate requirements. The IKE gateway address corresponds to the IP address of the remote sides Untrust interface.

```
set security ike policy ike-policy mode main
set security ike policy ike-policy proposal-set standard
set security ike policy ike-policy pre-shared-key ascii-text “secretkey”
set security ike gateway ike-gate ike-policy ike-policy
set security ike gateway ike-gate address 100.1.1.2
set security ike gateway ike-gate external-interface ge-0/0/1.0
```

Configure the IPsec policy and the IPsec VPN bound to the st0 interface as this is a route-based VPN.

```
set security ipsec policy vpn-policy1 proposal-set standard
set security ipsec vpn ike-vpn bind-interface st0.0
set security ipsec vpn ike-vpn ike gateway ike-gate
set security ipsec vpn ike-vpn ike ipsec-policy vpn-policy1
```
Set Tunnel MTU to 1350 to prevent fragmentation

```
set interfaces st0.0 family inet mtu 1350
```

Configure Security Policies

When the J Series Services Router at the Branch office is operating in a security context, the following policies must be defined to direct traffic to and from the four security zones defined earlier: Trust, Untrust, VPN, and WX Series.

![Security zones and policies directing traffic flow within J Series router](image)

Create a trust-to-untrust policy to redirect all outbound WAN traffic from the trust zone to the untrust zone via the ISM200 by the application service redirect-wx. A reverse policy also directs traffic from the WAN to the ISM200 for decompression with the application service reverse redirect-wx.

**Note:** For purposes of this example, untrust traffic is permitted to reach the LAN via the trust zone. Actual deployments should create more granular security policies permitting specific, intended applications and address combinations.

```
set security policies from-zone trust to-zone untrust policy trust-to-untrust match source-address any
set security policies from-zone trust to-zone untrust policy trust-to-untrust match destination-address any
set security policies from-zone trust to-zone untrust policy trust-to-untrust match application any
set security policies from-zone trust to-zone untrust policy trust-to-untrust then permit application-services redirect-wx
set security policies from-zone untrust to-zone trust policy untrust-to-trust match source-address any
set security policies from-zone untrust to-zone trust policy untrust-to-trust match destination-address any
set security policies from-zone untrust to-zone trust policy untrust-to-trust match application any
set security policies from-zone untrust to-zone trust policy untrust-to-trust then permit application-services reverse-redirect-wx
```
Create security policies trust-to-wx and wx-to-trust to allow traffic between the trust zone and the internal wx zone.

```
set security policies from-zone trust to-zone wx-zone policy trust-to-wx match source-address any
set security policies from-zone trust to-zone wx-zone policy trust-to-wx match destination-address any
set security policies from-zone trust to-zone wx-zone policy trust-to-wx match application any
set security policies from-zone trust to-zone wx-zone policy trust-to-wx then permit
set security policies from-zone wx-zone to-zone trust policy wx-to-trust match source-address any
set security policies from-zone wx-zone to-zone trust policy wx-to-trust match destination-address any
set security policies from-zone wx-zone to-zone trust policy wx-to-trust match application any
set security policies from-zone wx-zone to-zone trust policy wx-to-trust then permit
```

Create security policies to direct traffic from the LAN destined to the corporate LAN in the VPN zone to be sent to the ISM200 for acceleration prior to encryption.

**Note:** In this example all traffic across the VPN is sent to the ISM200 by using the statement filter ‘match application any’, however known compressed traffic such as VOIP or video can be filtered at this point to bypass the ISM200.

```
set security policies from-zone vpn to-zone trust policy vpn-vpn-tr match source-address remote-net
set security policies from-zone vpn to-zone trust policy vpn-vpn-tr match destination-address local-net
set security policies from-zone vpn to-zone trust policy vpn-vpn-tr match application any
set security policies from-zone vpn to-zone trust policy vpn-vpn-tr then permit application-services reverse-redirect-wx
set security policies from-zone trust to-zone vpn policy vpn-tr-vpn match source-address local-net
set security policies from-zone trust to-zone vpn policy vpn-tr-vpn match destination-address remote-net
set security policies from-zone trust to-zone vpn policy vpn-tr-vpn match application any
set security policies from-zone trust to-zone vpn policy vpn-tr-vpn then permit application-services redirect-wx
```

Create the following two policies to permit traffic to/from the VPN zone to the internal WX Series zone for compression / decompression.

```
set security policies from-zone vpn to-zone wx-zone policy vpn-to-wx match source-address any
set security policies from-zone vpn to-zone wx-zone policy vpn-to-wx match destination-address any
set security policies from-zone vpn to-zone wx-zone policy vpn-to-wx match application any
set security policies from-zone vpn to-zone wx-zone policy vpn-to-wx then permit
set security policies from-zone wx-zone to-zone vpn policy wx-to-vpn match source-address any
set security policies from-zone wx-zone to-zone vpn policy wx-to-vpn match destination-address any
```

---

Copyright © 2009, Juniper Networks, Inc.
set security policies from-zone wx-zone to-zone vpn policy wx-to-vpn match application any
set security policies from-zone wx-zone to-zone vpn policy wx-to-vpn then permit

A default deny-all policy is also created to deny any unaccounted for traffic.
set security policies default-policy deny-all

J Series ISM200 Configuration

The WXC Series ISM200 is configured through the WXOS web interface located in Configuration > Quick Configuration > WAN Acceleration > Manage in the J-Web interface.

Within the new ISM200 J-Web interface, use Quick Setup to configure the following:

- Direct this device to an existing registration server
- Configure the Corporate WX Series IP address for registration server and set the registration server password
- Enter the License key

The ISM200 configuration is similar to the stand alone WX Series configuration. However as the ISM200 is not inline, a static route for the local subnets must be configured with the gateway pointing to the ISM200 internal IP address (1.1.1.1):

![Figure 5: Local static and dynamic routes displayed in the ISM200 web UI](image)

Under Compression, ensure options to Decompress and Enable compression to all discovered WX Series devices are selected:

![Figure 6: The Endpoints screen displays tunnel status to all discovered WX Series devices](image)
NetScreen Series Firewall Configuration Details

For the ScreenOS configuration, the following implementations must be made:

- Define interfaces, zones, and IP ranges
- Create IPsec tunnel
- Enable static and OSPF routing
- Define local and remote addresses
- Define policies to permit traffic destined to remote branches

Detailed configuration:

Define interfaces, zones and IP ranges

```bash
set zone name "VPN"
set interface "ethernet0/1" zone "Untrust"
set interface "ethernet0/3" zone "Trust"
set interface "tunnel.1" zone "VPN"
set interface ethernet0/1 ip 100.1.1.2/24
set interface ethernet0/3 ip 10.2.1.1/24
set interface ethernet0/3 nat
set interface tunnel.1 ip 10.11.1.11/24
```

Create IPsec tunnels

```bash
set ike gateway "SF-ike" address 50.1.1.1 Main outgoing-interface "ethernet0/1" preshare "secretkey" sec-level standard
set ike gateway "LA-ike" address 60.1.1.1 Main outgoing-interface "ethernet0/1" preshare "secretkey" sec-level standard
set vpn "SF-vpn" gateway "SF-ike" replay tunnel idletime 0 sec-level standard
set vpn "SF-vpn" bind interface tunnel.1
set vpn "SF-vpn" monitor optimized rekey
set vpn "LA-vpn" gateway "LA-ike" replay tunnel idletime 0 sec-level standard
set vpn "LA-vpn" id 0x3 bind interface tunnel.1
set vpn "LA-vpn" monitor optimized rekey
```

Enable static and OSPF routing

```bash
set vrouter trust-vr protocol ospf area 0.0.0.1
set enable
set route 0.0.0.0/0 interface ethernet0/1 gateway 100.1.1.1
set interface ethernet0/3 protocol ospf area 0.0.0.1
set interface ethernet0/3 protocol ospf enable
set interface tunnel.1 protocol ospf area 0.0.0.1
set interface tunnel.1 protocol ospf link-type p2mp
set interface tunnel.1 protocol ospf enable
```
Configure address book entries for local and remote networks

set address "Trust"  "local-lan" 10.2.1.0 255.255.255.0
set address "VPN"  "SF-lan" 10.0.0.0 255.255.255.0
set address "VPN"  "LA-lan" 10.20.0.0 255.255.255.0

Define policies

set policy id 1 from "Trust" to "Untrust" "Any" "Any" "ANY" nat src permit
set policy id 2 from "Trust" to "VPN" " SF-lan" " local-lan" "ANY" permit
set policy id 3 from "VPN" to "Trust" " local-lan" " SF-lan" "ANY" permit
set policy id 4 from "Trust" to "VPN" " LA-lan" " local-lan" "ANY" permit
set policy id 5 from "VPN" to "Trust" " local-lan" " LA-lan" "ANY" permit

WX Series Configuration

As the WX Series on the corporate network is deployed in in-line mode, it requires an IP address on its local port that is in the corporate LAN subnet.

1. Configure basic network connectivity via console
2. Using the WX Series Web interface, use Quick Setup to configure the following:
   a. Operational mode as active
   b. Configure the Corporate WX Series as the registration server and set the registration server password
   c. Configure Time / NTP
   d. Configure Topology as Hub as this device is at the corporate data center
   e. Enter the sum of the WAN speed for outbound connectivity.
3. Advertise the local subnet(s). By default, local subnets are not advertised for compression.
   a. After Quick setup, enable OSPF and configure Area ID to advertise multiple local subnets.
4. Enable QoS and CIFS acceleration with the QoS Setup Wizard.

Verification

ScreenOS

Within the ScreenOS cli, IPsec tunnels carrying traffic to the remote branches can be verified by listing active security associations which are created along with the VPN tunnels:

FW-> get sa active
Total active sa: 2
  total configured sa: 2
  HEX ID  Gateway     Port Algorithm   SPI   Life:sec kb Sta  PID vsys
  00000001<    50.1.1.1 500 esp:3des/sha1 d0ae8be1 3058 unlim A/U -1 0
  00000001>    50.1.1.1 500 esp:3des/sha1 6aa7966e 3058 unlim A/U -1 0
  00000002<    60.1.1.1 500 esp:3des/sha1 d0ae8be2 3063 unlim A/U -1 0
  00000002>    60.1.1.1 500 esp:3des/sha1 779334e4 3063 unlim A/U -1 0
Junos OS With Enhanced Services

For Junos OS with enhanced services on the remote J Series Services Routers, the IPsec tunnels phase 2 security association is verified as follows:

```
root@fred> show security ipsec security-associations
   total configured sa: 4
   ID   Gateway     Port Algorithm    SPI   Life:sec/kb Mon vsys
   <131073 100.1.1.2   500 ESP:3des/sha1  4e94775f 1454/ unlim  -  0
   >131073 100.1.1.2   500 ESP:3des/sha1  d0ae8bdf 1454/ unlim  -  0
```

WX Series

WX Series compression was tested using FTP and CIFS file transfer to validate caching and compression of traffic going through the IPsec tunnel.

FTP server was configured on the corporate network side and files were transferred to clients on the branch LAN networks repeatedly to validate WX Series acceleration of the traffic.

The Flow Diagnostics view available in the WX Series Web view under Admin > Tools > Flow Diagnostics allows verification of specific application flows. The view below displays an FTP traffic flow showing a substantial reduction in Bytes To WAN compared with Bytes From LAN.

![Flow Diagnostics](image)

Figure 7: Flow Diagnostics allows detailed level verification of WX Series optimization
Summary
By employing route-based multipoint IPsec VPN with application acceleration at each location, branch communications are optimized over the WAN and secure. Junos OS with enhanced services in the J Series with the ISM200 allows a simple, single device rollout for branch locations reducing expense and administrative costs while increasing manageability. WX Series acceleration to the branch allows enterprises to speed centrally managed web based applications and database access.

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.

Figure 8: Compression performance graphs for FTP and other Applications