Avaya Solution & Interoperability Test Lab

Application Notes for VoIP over a Site-to-Site IPSec VPN between Kentrox Q-Series Routers connected to an Avaya IP Office Telephony Infrastructure - Issue 1.0

Abstract

These Application Notes describe a configuration for Voice over IP (VoIP) over a site-to-site IPSec VPN between Kentrox Q-Series Routers connected to an Avaya IP Office Telephony infrastructure. The Kentrox Q-Series Q2400 and the Q2200 routers were compliance-tested with an Avaya IP Office. Emphasis was placed on verifying voice quality in a small office scenario using a site-to-site IPSec VPN in the converged network. Information in these Application Notes has been obtained through compliance testing and additional technical discussions. Testing was conducted via the Developer*Connection* Program at the Avaya Solution and Interoperability Test Lab.

1. Introduction

These Application Notes describe a configuration for supporting Voice over IP (VoIP) over a site-to-site IPSec virtual private network (VPN) on Kentrox Q-Series Routers connected to an Avaya IP Telephony infrastructure. The Kentrox Q-Series Q2400 and Q2200 routers were compliance-tested with an Avaya IP Office.

Q-Series Q2200 T1 QoS Access Router

The Q-Series Q2200 Access Router provides VPN functionality and supports Quality of Service (QoS) based on DiffServ over its WAN link. The Q2200 supports PPP and Frame Relay encapsulation.

Q-Series Q2400 QoS Access Router

The Q-Series Q2400 Access Router is a multi-port router with two T1 ports and one Ethernet WAN port. It provides the same functionality as the Q2200.

Compliance testing emphasis was placed on verifying voice quality in a small office scenario for the IPSec VPN in the converged network.

The configuration in **Figure 1** shows a corporate site connected to a branch office site via a PPP link. The corporate site consists of an Avaya IP412 Office connected to the Kentrox Q2400 router, which in turn is connected to the WAN. The branch office site consists of an Avaya IP403 Office, and it is also connected to the WAN via a Kentrox Q2200 router. A site-to-site IPSec VPN over the PPP link connects both sites. Each site contains a Layer-2 managed Ethernet switch to connect the Avaya IP Telephones and the Avaya IP Office. The corporate site also provides a DHCP server for assigning IP network parameters, VLAN information, and Option 176 settings to the Avaya IP Telephones. DHCP was used to exercise DHCP relay on the Kentrox router at the branch office. The voice and data traffic were separated onto different VLANs.

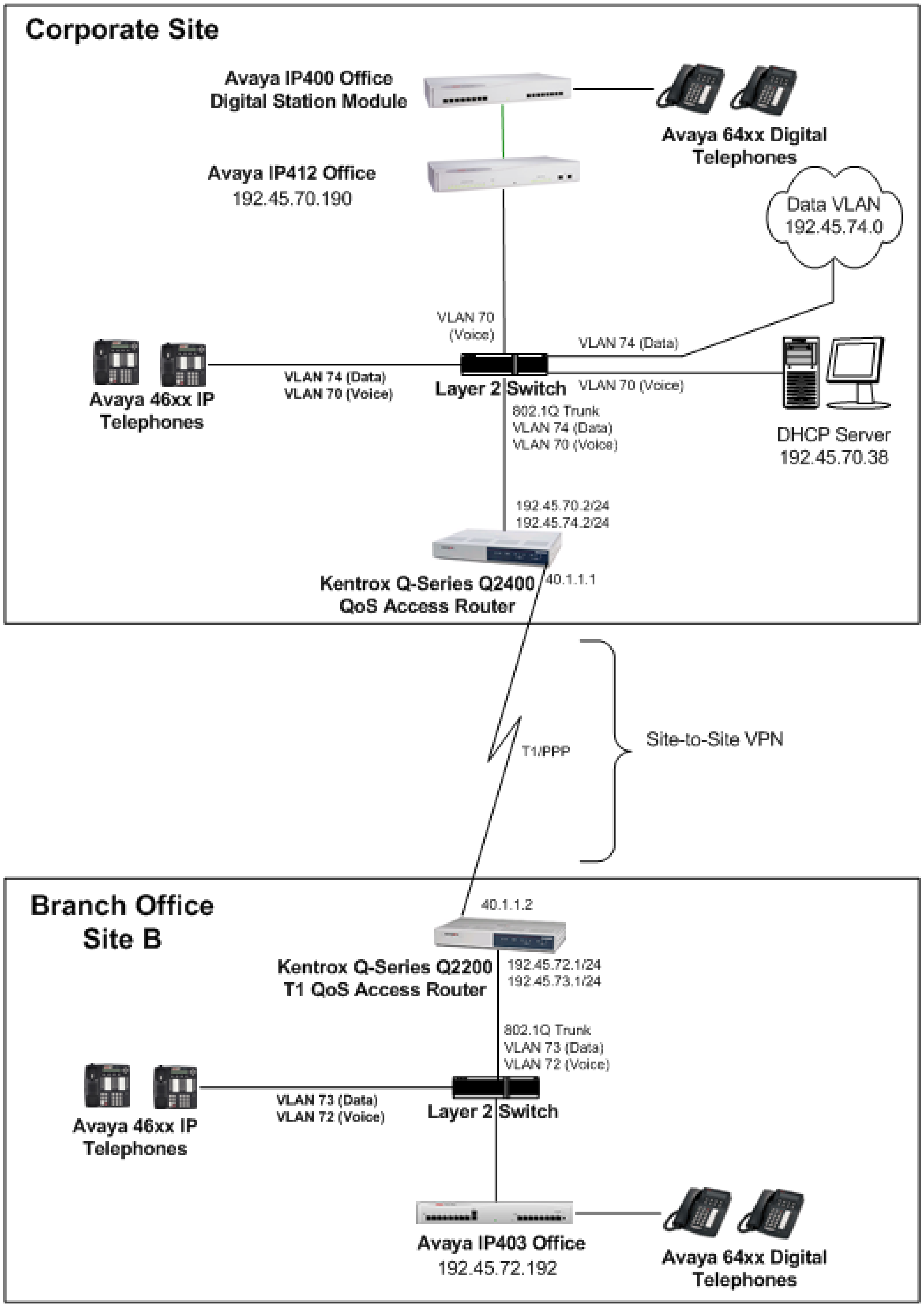


Figure 1: Network Configuration

2. Equipment and Software Validated

The following equipment and software were used for the sample configuration provided:

Equipment	Software
Avaya IP412 Office	2.1(27)
Avaya IP403 Office	2.1(27)
Avaya 4612, 4624 IP Telephones	1.81
Avaya 6400 Series Digital Telephones	--
Kentrox Q-Series Q2400 QoS Access Router	1.3
Kentrox Q-Series Q2200 T1 QoS Access Router	1.3

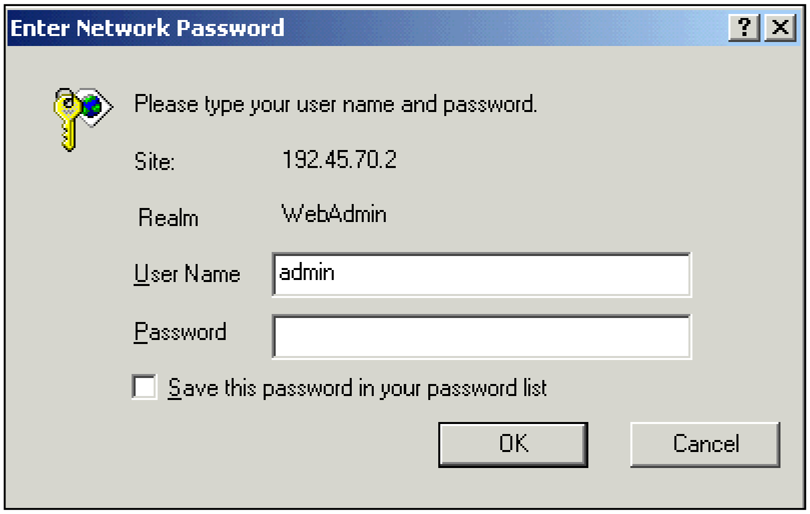
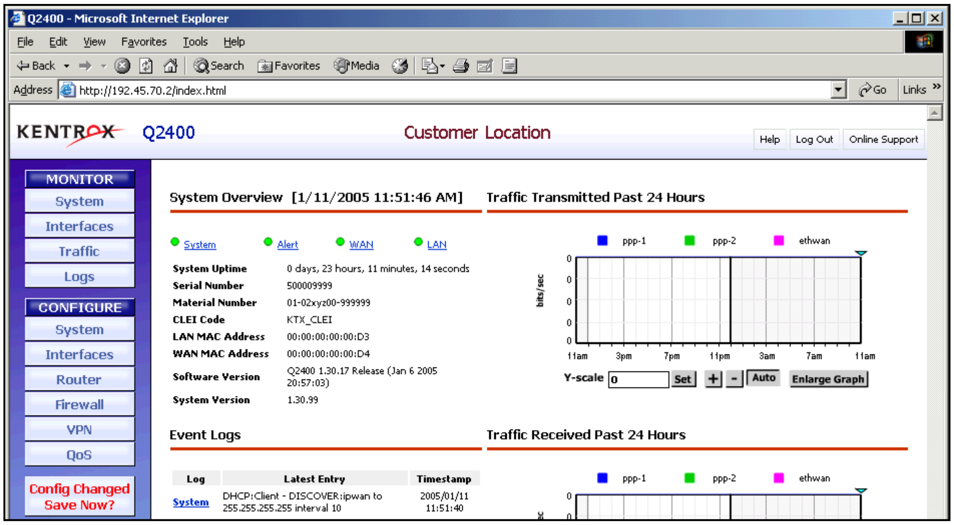
3. Configure the Kentrox Q-Series Routers for VPN

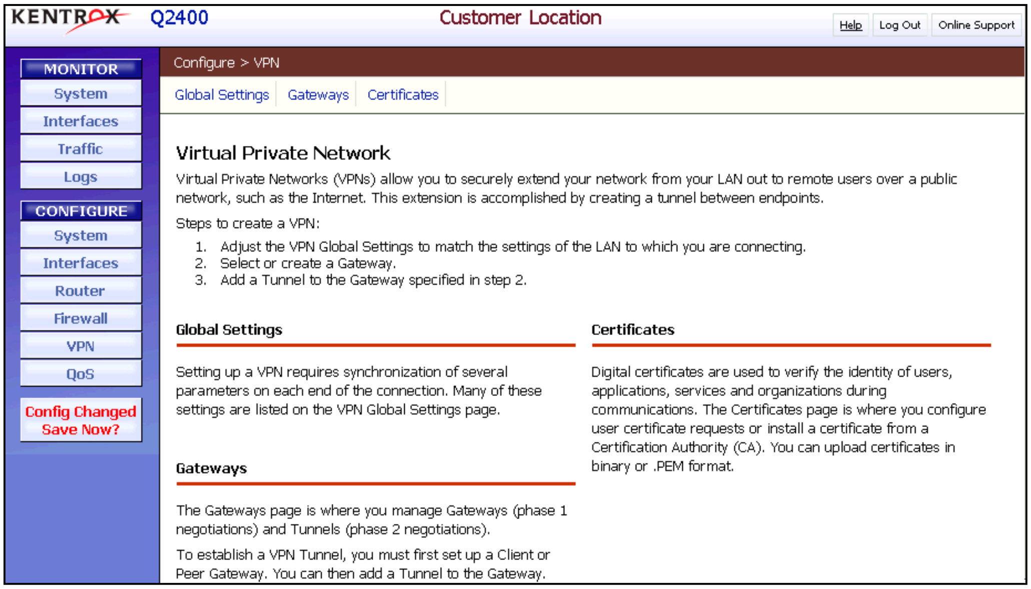
These Application Notes address setting up the site-to-site IPSec VPN between the Kentrox Q-Series routers to connect two Avaya IP Office sites. Please refer to “Application Notes for VoIP over PPP Link with Quality of Service using Kentrox Q-Series Routers with Avaya IP Office” for configuration related to the IP Office and the PPP link between the Kentrox routers.

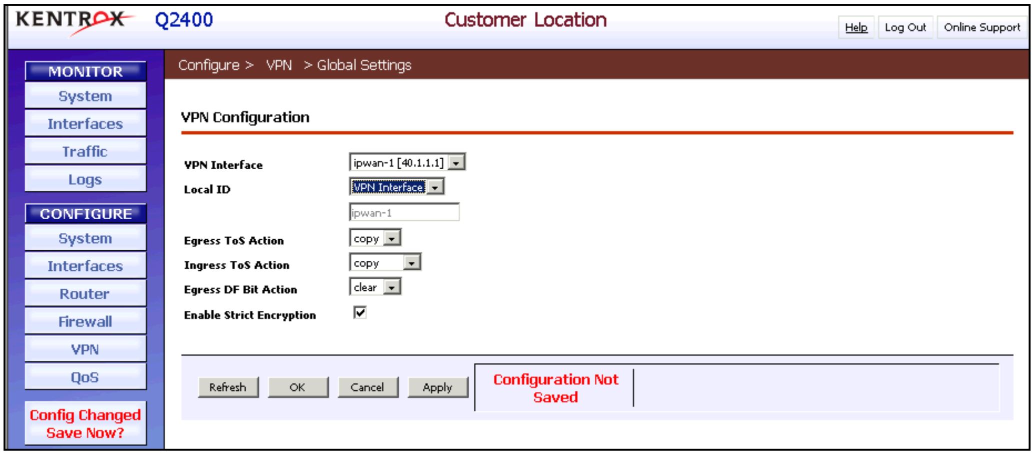
Please refer to the abovementioned Application Notes for Quality of Service configuration using the Kentrox Q-Series Routers with Avaya IP Office, as they are not provided in these Application Notes.

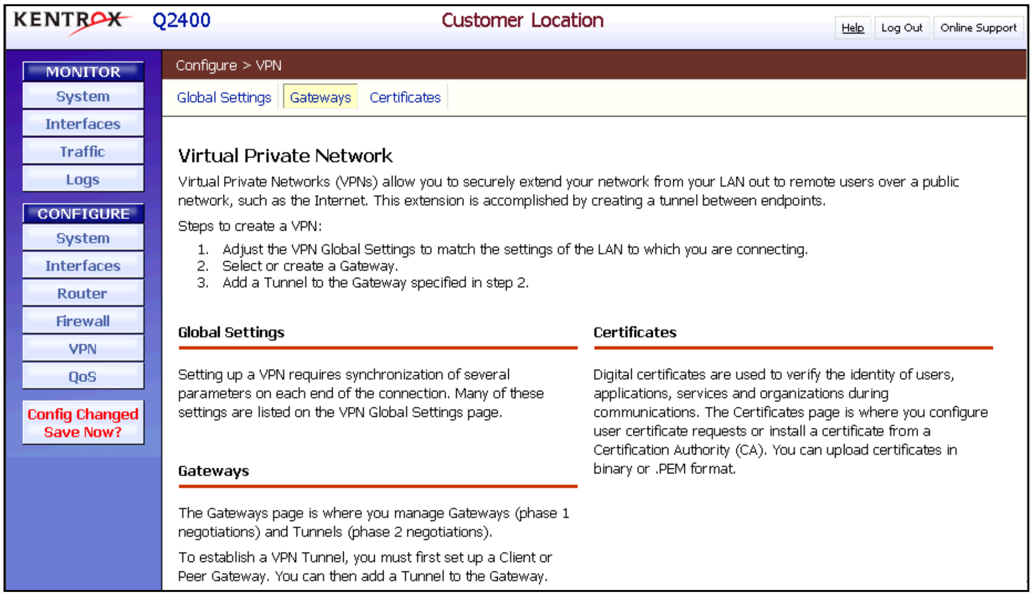
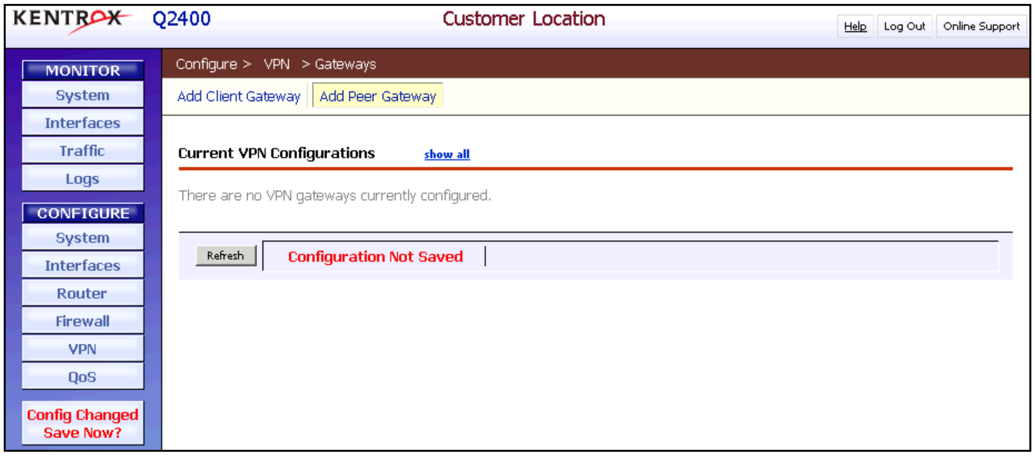
3.1. Kentrox Q2400 VPN in the Corporate Site

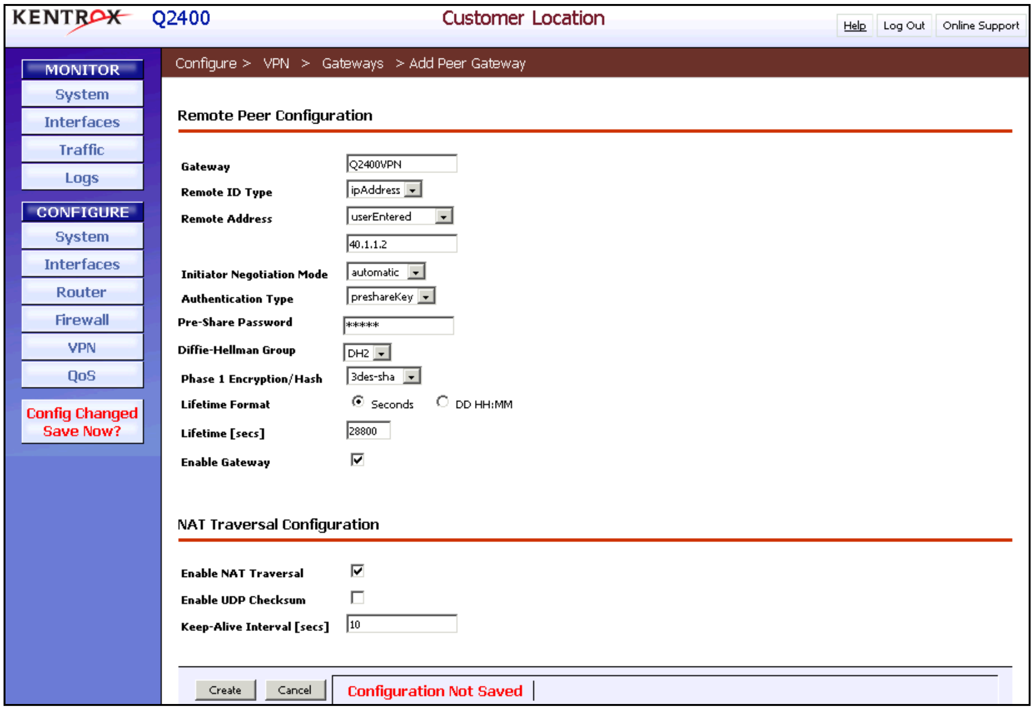
This section provides the VPN configuration of the Q2400 in the corporate site.

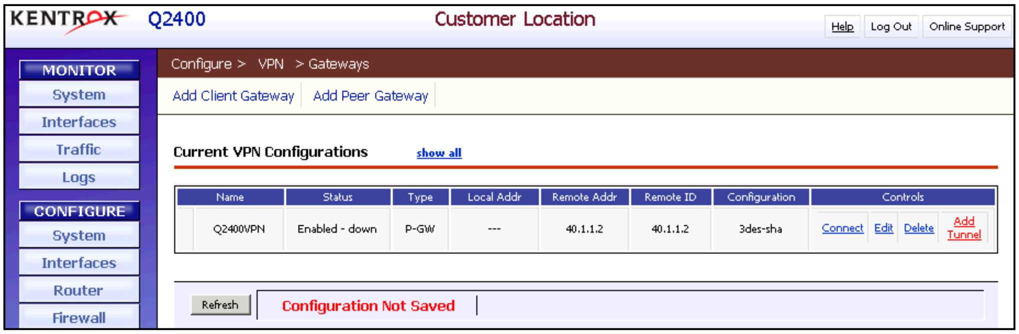
Step	Description
1.	Browse to the IP address of the Q2400 router to access the Administration web page. Log into the Q2400 using the appropriate credentials when the Q2400 authentication window appears.  Enter Network Password Please type your user name and password. Site: 192.45.70.2 Realm WebAdmin User Name admin Password □ Save this password in your password list
2.	Once successfully logged in, the Q2400 main window is displayed. All of the configuration options are selected from the tree view on the left side of the Q2400 main window.  Q2400 - Microsoft Internet Explorer Address http://192.45.70.2/index.html KENTROX Q2400 Customer Location File Edit View Favorites Tools Help Back Search Favorites Media Go Links Help Log Out Online Support MONITOR System Interfaces Traffic Logs CONFIGURE System Interfaces Router Firewall VPN QoS Config Changed Save Now? Traffic Transmitted Past 24 Hours ppp-1 ppp-2 ethwan bits/sec 0 0 0 0 0 11am 3pm 7pm 11pm 3am 7am 11am Y-scale 0 Set + - Auto Enlarge Graph Traffic Received Past 24 Hours ppp-1 ppp-2 ethwan System Overview [1/11/2005 11:51:46 AM] ● System ● Alert ● WAN ● LAN System Uptime 0 days, 23 hours, 11 minutes, 14 seconds Serial Number 500009999 Material Number 01-02xyz00-999999 CLEI Code KTX_CLEI LAN MAC Address 00:00:00:00:00:D3 WAN MAC Address 00:00:00:00:00:D4 Software Version Q2400 1.30.17 Release (Jan 6 2005 20:57:03) System Version 1.30.99 Event Logs Log / Latest Entry / Timestamp System / DHCP:Client - DISCOVER:ipwan to 255.255.255.255 interval 10 / 2005/01/11 11:51:40

Step	Description
3.	Select **VPN** under CONFIGURE in the tree view. In the Configure > VPN page that appears, click **Global Settings**.  KENTROX Q2400 Customer Location Help Log Out Online Support MONITOR System Interfaces Traffic Logs CONFIGURE System Interfaces Router Firewall VPN QoS Config Changed Save Now? Configure > VPN Global Settings Gateways Certificates **Virtual Private Network** Virtual Private Networks (VPNs) allow you to securely extend your network from your LAN out to remote users over a public network, such as the Internet. This extension is accomplished by creating a tunnel between endpoints. Steps to create a VPN: 1. Adjust the VPN Global Settings to match the settings of the LAN to which you are connecting. 2. Select or create a Gateway. 3. Add a Tunnel to the Gateway specified in step 2. **Global Settings** Setting up a VPN requires synchronization of several parameters on each end of the connection. Many of these settings are listed on the VPN Global Settings page. **Gateways** The Gateways page is where you manage Gateways (phase 1 negotiations) and Tunnels (phase 2 negotiations). To establish a VPN Tunnel, you must first set up a Client or Peer Gateway. You can then add a Tunnel to the Gateway. **Certificates** Digital certificates are used to verify the identity of users, applications, services and organizations during communications. The Certificates page is where you configure user certificate requests or install a certificate from a Certification Authority (CA). You can upload certificates in binary or .PEM format.

Step	Description
4.	In the Configure > VPN > Global Settings page that appears, set *VPN Interface* to **ipwan-1 [40.1.1.1]**, *Egress ToS Action* to **copy**, *Ingress ToS Action* to **copy** and click **OK**.  KENTROX Q2400 Customer Location Help Log Out Online Support Configure > VPN > Global Settings MONITOR System Interfaces Traffic Logs CONFIGURE System Interfaces Router Firewall VPN QoS Config Changed Save Now? Refresh OK Cancel Apply Configuration Not Saved VPN Configuration VPN Interface: ipwan-1 [40.1.1.1] Local ID: VPN Interface ipwan-1 Egress ToS Action: copy Ingress ToS Action: copy Egress DF Bit Action: clear Enable Strict Encryption ☑ **NOTE**: The Q-Series routers keep traffic marked with DSCP 46 (EF) in its own priority queue. However, DSCP 34 (AF4) marked traffic is kept in a Weighted Fair Queue (WFQ) with all other DSCP values. To ensure highest priority for both signaling and audio, a policy was created to map DSCP 34 to 46 at both the corporate and branch site Q-Series routers. This ensures that signaling and audio packets are transmitted using the priority queue, instead of WFQ. Setting the Egress ToS Action field to copy ensures this QoS policy is applied for the VPN. For further information about the QoS configuration required for Kentrox Q-Series routers with Avaya IP Office, please refer to [1] in Additional References.

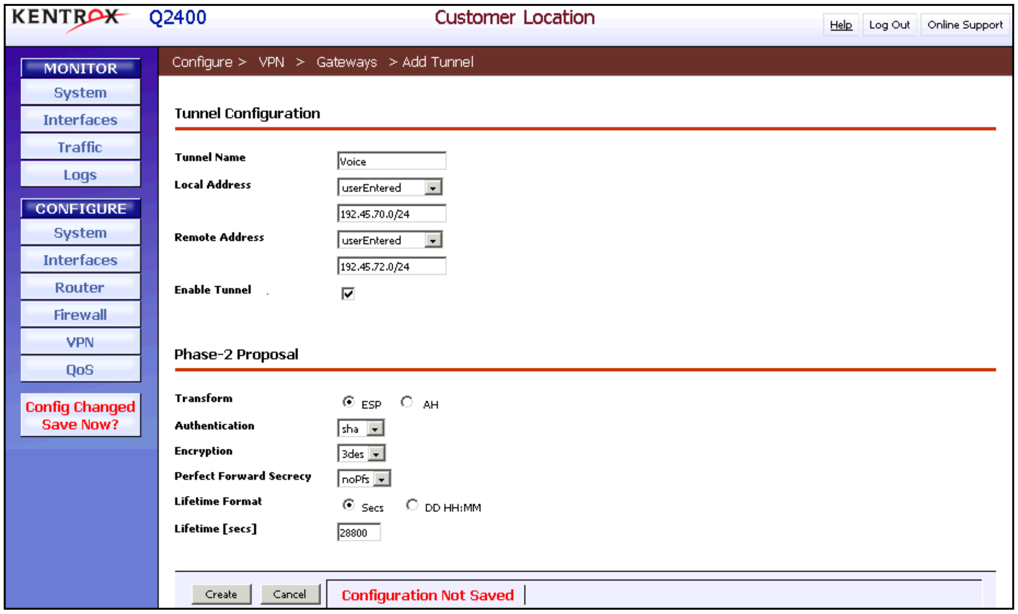
Step	Description
5.	Select **VPN** under CONFIGURE in the tree view. In the Configure > VPN page that appears, click **Gateways**.  KENTROX Q2400 Customer Location Help Log Out Online Support MONITOR System Interfaces Traffic Logs CONFIGURE System Interfaces Router Firewall VPN QoS Config Changed Save Now? Configure > VPN Global Settings Gateways Certificates Virtual Private Network Virtual Private Networks (VPNs) allow you to securely extend your network from your LAN out to remote users over a public network, such as the Internet. This extension is accomplished by creating a tunnel between endpoints. Steps to create a VPN: 1. Adjust the VPN Global Settings to match the settings of the LAN to which you are connecting. 2. Select or create a Gateway. 3. Add a Tunnel to the Gateway specified in step 2. Global Settings Setting up a VPN requires synchronization of several parameters on each end of the connection. Many of these settings are listed on the VPN Global Settings page. Gateways The Gateways page is where you manage Gateways (phase 1 negotiations) and Tunnels (phase 2 negotiations). To establish a VPN Tunnel, you must first set up a Client or Peer Gateway. You can then add a Tunnel to the Gateway. Certificates Digital certificates are used to verify the identity of users, applications, services and organizations during communications. The Certificates page is where you configure user certificate requests or install a certificate from a Certification Authority (CA). You can upload certificates in binary or .PEM format.
6.	In the Configure > VPN > Gateways page that appears, click **Add Peer Gateway**.  KENTROX Q2400 Customer Location Help Log Out Online Support MONITOR System Interfaces Traffic Logs CONFIGURE System Interfaces Router Firewall VPN QoS Config Changed Save Now? Configure > VPN > Gateways Add Client Gateway Add Peer Gateway show all Refresh Current VPN Configurations There are no VPN gateways currently configured. Configuration Not Saved

<table>
<tr><th>Step</th><th>Description</th></tr>
<tr><td>7.</td><td>In the Configure > VPN > Gateways > Add Peer Gateway page that appears, set <i>Gateway</i> to <b>Q2400VPN</b>, <i>Remote Address</i> to <b>userEntered 40.1.1.2</b>, <i>Initiator Negotiation Mode</i> to <b>automatic</b>, <i>Authentication Type</i> to <b>preshareKey</b>, <i>Pre-Share Password</i> to the desired password for the site-to-site IPSec VPN, <i>Diffie-Hellman Group</i> to <b>DH2</b>, <i>Phase 1 Encryption/Hash</i> to <b>3des-sha</b>, <i>Lifetime Format</i> to <b>Seconds</b>, <i>Lifetime [secs]</i> to <b>28800</b>, check <b>Enable Gateway</b>, check <b>Enable NAT Traversal</b> and click <b>Create</b>.


Configure > VPN > Gateways > Add Peer Gateway
Remote Peer Configuration
Gateway: Q2400VPN
Remote ID Type: ipAddress
Remote Address: userEntered
40.1.1.2
Initiator Negotiation Mode: automatic
Authentication Type: preshareKey
Pre-Share Password: *****
Diffie-Hellman Group: DH2
Phase 1 Encryption/Hash: 3des-sha
Lifetime Format: ● Seconds ○ DD HH:MM
Lifetime [secs]: 28800
Enable Gateway: ☑
NAT Traversal Configuration
Enable NAT Traversal: ☑
Enable UDP Checksum: □
Keep-Alive Interval [secs]: 10
Create Cancel Configuration Not Saved</td></tr>
<tr><td>8.</td><td>In the Configure > VPN > Gateways page, click <b>Add Tunnel</b>.


Configure > VPN > Gateways
Add Client Gateway Add Peer Gateway
Current VPN Configurations show all
<table>
<tr><th>Name</th><th>Status</th><th>Type</th><th>Local Addr</th><th>Remote Addr</th><th>Remote ID</th><th>Configuration</th><th>Controls</th></tr>
<tr><td>Q2400VPN</td><td>Enabled - down</td><td>P-GW</td><td>---</td><td>40.1.1.2</td><td>40.1.1.2</td><td>3des-sha</td><td>Connect Edit Delete Add Tunnel</td></tr>
</table>
Refresh Configuration Not Saved</td></tr>
</table>

<table>
<tr><th>Step</th><th>Description</th></tr>
<tr><td>9.</td><td>In the Configure > VPN > Gateways > Add Tunnel page that appears, set <i>Tunnel Name</i> to <b>Voice</b>, <i>Local Address</i> to <b>userEntered 192.45.70.0/24</b>, <i>Remote Address</i> to <b>userEntered 192.45.72.0/24</b>, check <b>Enable Tunnel</b>, <i>Transform</i> to <b>ESP</b>, <i>Authentication</i> to <b>sha</b>, <i>Encryption</i> to <b>3des</b>, <i>Lifetime Format</i> to <b>Secs</b>, <i>Lifetime [secs]</i> to <b>28800</b> and click <b>Create</b>.



Configure > VPN > Gateways > Add Tunnel

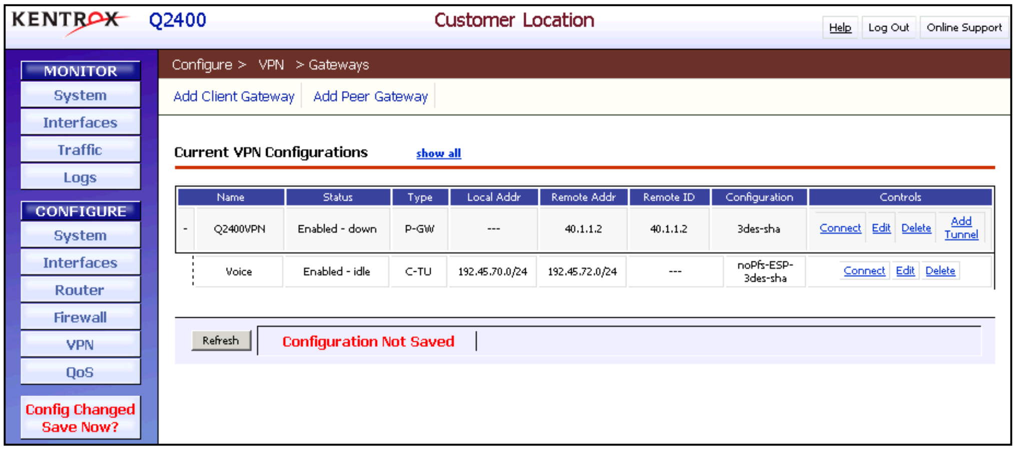
Tunnel Configuration

<table>
<tr><td>Tunnel Name</td><td>Voice</td></tr>
<tr><td>Local Address</td><td>userEntered
192.45.70.0/24</td></tr>
<tr><td>Remote Address</td><td>userEntered
192.45.72.0/24</td></tr>
<tr><td>Enable Tunnel</td><td>☑</td></tr>
</table>

Phase-2 Proposal

<table>
<tr><td>Transform</td><td>● ESP ○ AH</td></tr>
<tr><td>Authentication</td><td>sha</td></tr>
<tr><td>Encryption</td><td>3des</td></tr>
<tr><td>Perfect Forward Secrecy</td><td>noPfs</td></tr>
<tr><td>Lifetime Format</td><td>● Secs ○ DD HH:MM</td></tr>
<tr><td>Lifetime [secs]</td><td>28800</td></tr>
</table>

Create | Cancel | Configuration Not Saved
</td></tr>
<tr><td>10.</td><td>In the Configure > VPN > Gateways page, click <b>Add Tunnel</b> again.



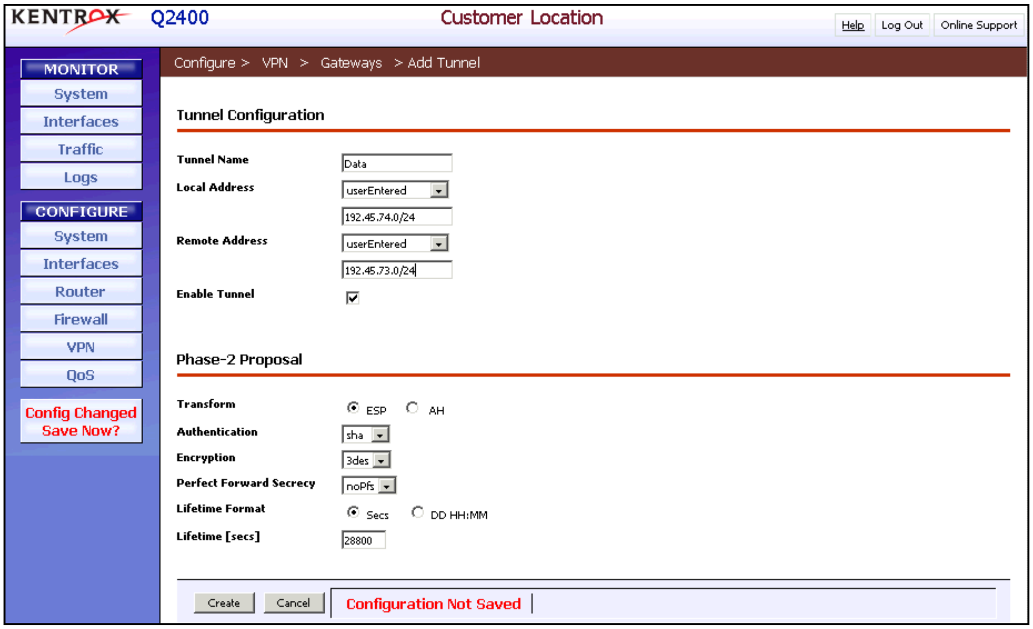
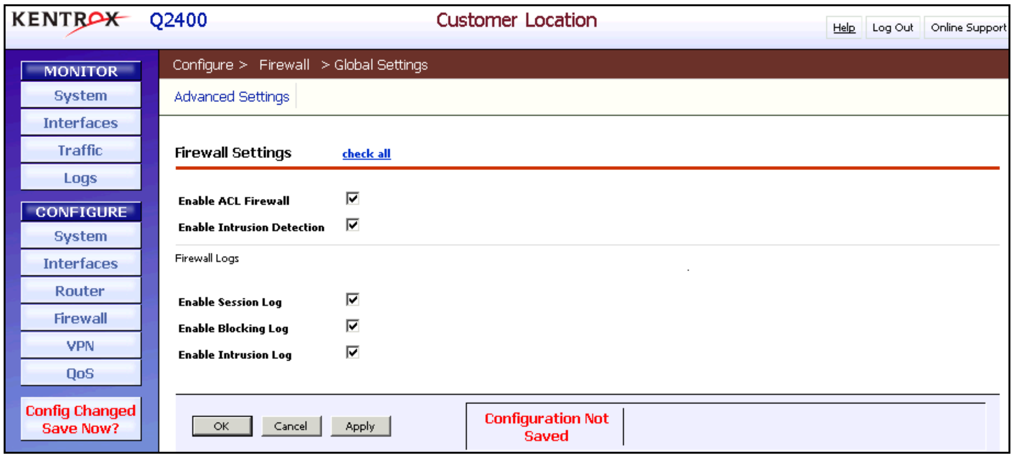
Configure > VPN > Gateways

Add Client Gateway | Add Peer Gateway

Current VPN Configurations show all

<table>
<tr><th></th><th>Name</th><th>Status</th><th>Type</th><th>Local Addr</th><th>Remote Addr</th><th>Remote ID</th><th>Configuration</th><th>Controls</th></tr>
<tr><td>-</td><td>Q2400VPN</td><td>Enabled - down</td><td>P-GW</td><td>---</td><td>40.1.1.2</td><td>40.1.1.2</td><td>3des-sha</td><td>Connect Edit Delete Add Tunnel</td></tr>
<tr><td></td><td>Voice</td><td>Enabled - idle</td><td>C-TU</td><td>192.45.70.0/24</td><td>192.45.72.0/24</td><td>---</td><td>noPfs-ESP-3des-sha</td><td>Connect Edit Delete</td></tr>
</table>

Refresh | Configuration Not Saved
</td></tr>
</table>

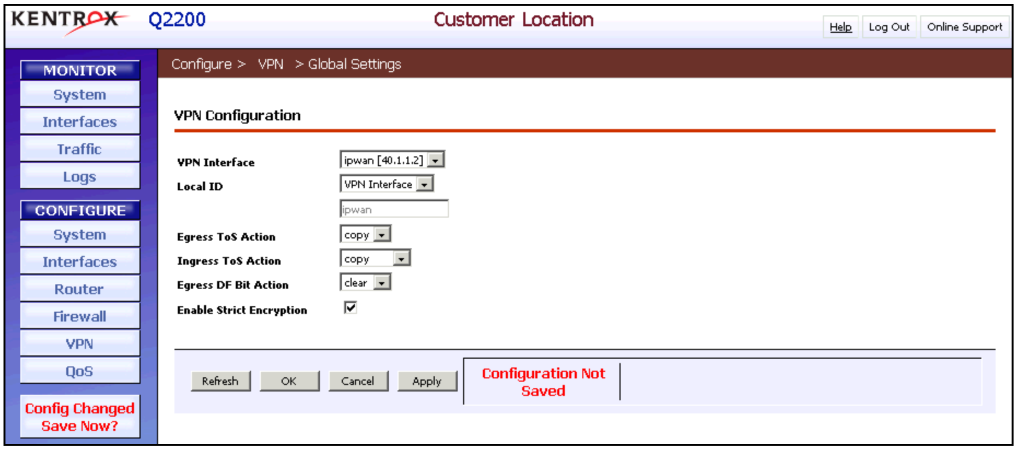
Step	Description
11.	In the Configure > VPN > Gateways > Add Tunnel page that appears, set *Tunnel Name* to **Data**, *Local Address* to **userEntered 192.45.74.0/24**, *Remote Address* to **userEntered 192.45.73.0/24**, check **Enable Tunnel**, *Transform* to **ESP**, *Authentication* to **sha**, *Encryption* to **3des**, *Lifetime Format* to **Secs**, *Lifetime [secs]* to **28800** and click **Create**.  KENTROX Q2400 Customer Location Help Log Out Online Support MONITOR System Interfaces Traffic Logs CONFIGURE System Interfaces Router Firewall VPN QoS Config Changed Save Now? Configure > VPN > Gateways > Add Tunnel Tunnel Configuration Tunnel Name: Data Local Address: userEntered 192.45.74.0/24 Remote Address: userEntered 192.45.73.0/24 Enable Tunnel ☑ Phase-2 Proposal Transform ● ESP ○ AH Authentication: sha Encryption: 3des Perfect Forward Secrecy: noPfs Lifetime Format ● Secs ○ DD HH:MM Lifetime [secs]: 28800 Create Cancel Configuration Not Saved
12.	Select **Firewall** under CONFIGURE in the tree view (not shown). In the Configure > Firewall page that appears (not shown), click **Global Settings**. In the Configure > Firewall > Global Settings page that appears, check **Enable ACL Firewall**, **Enable Intrusion Detection**, **Enable Session Log**, **Enable Blocking Log**, **Enable Intrusion Log** and click **OK**.  KENTROX Q2400 Customer Location Help Log Out Online Support MONITOR System Interfaces Traffic Logs CONFIGURE System Interfaces Router Firewall VPN QoS Config Changed Save Now? Configure > Firewall > Global Settings Advanced Settings Firewall Settings check all Enable ACL Firewall ☑ Enable Intrusion Detection ☑ Firewall Logs Enable Session Log ☑ Enable Blocking Log ☑ Enable Intrusion Log ☑ OK Cancel Apply Configuration Not Saved

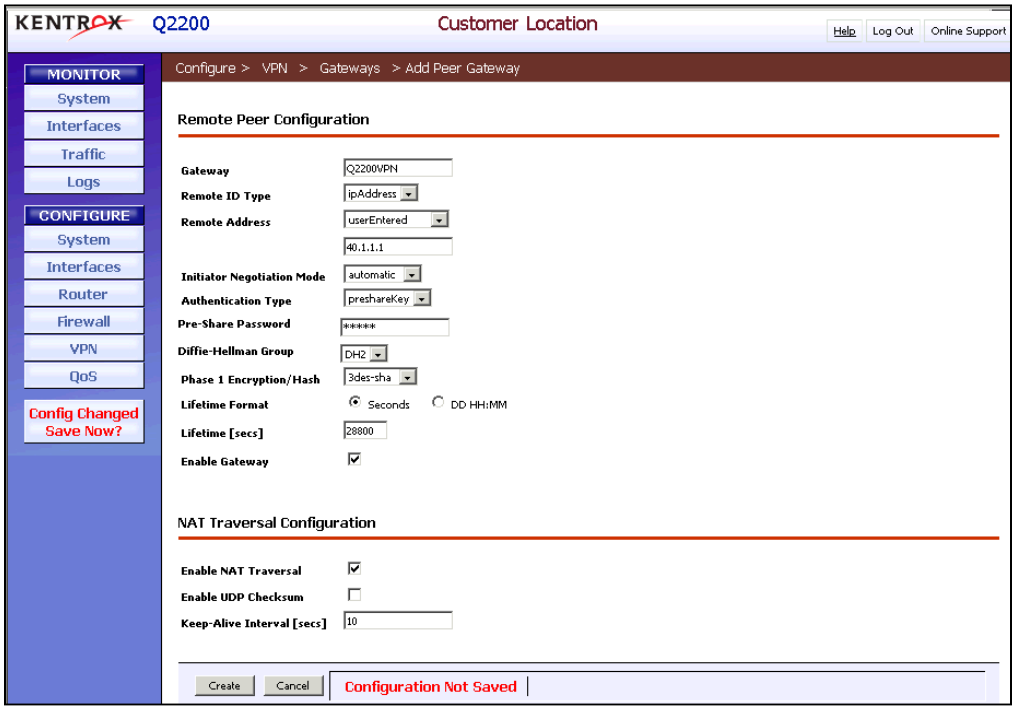
Step	Description
13.	Select **Router** → **NAT** under CONFIGURE in the tree view. In the Configure > Router > NAT page that appears, check **NAT** and click **OK**.
14.	Select **System** → **Save Config** under CONFIGURE in the tree view to save the configuration.

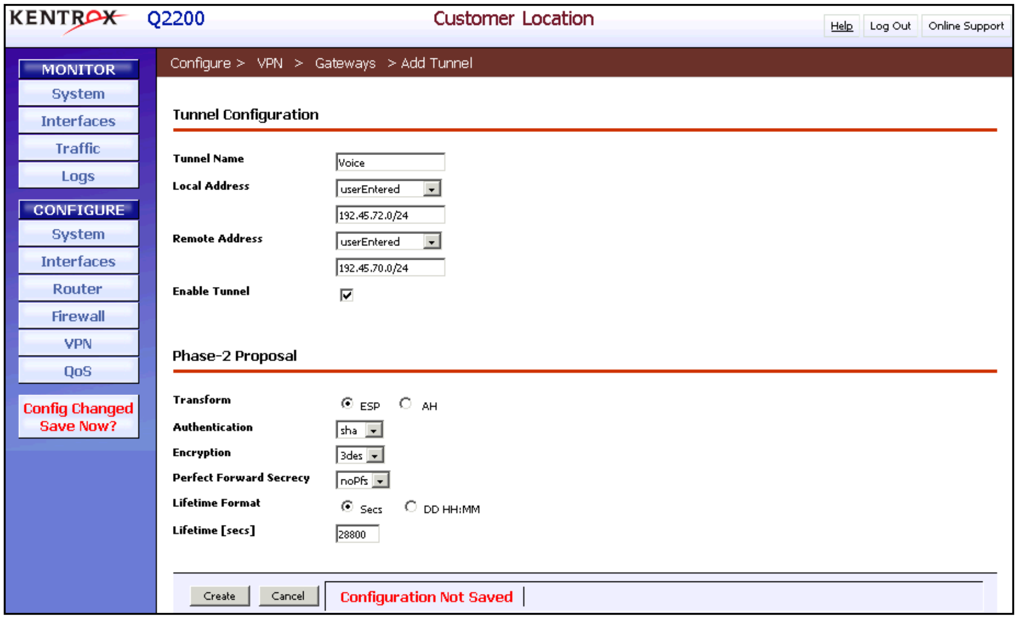
3.2. Kentrox Q2200 VPN in Branch Office Site

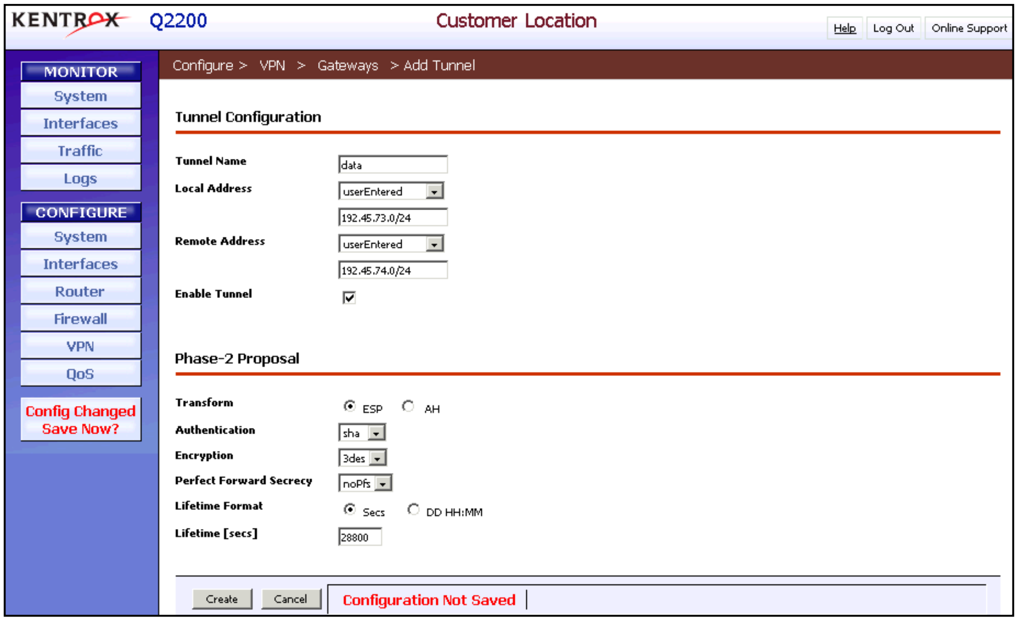
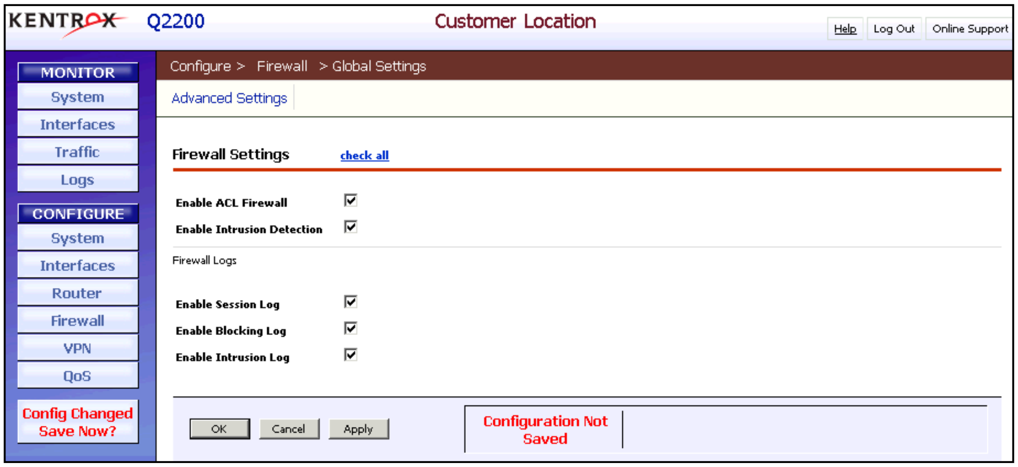
This section provides the VPN configuration of the Q2200 in the Branch Office Site. The Q2400 browser based administrative interface is the same for the Q2200. Therefore, some screens have been omitted in this section.

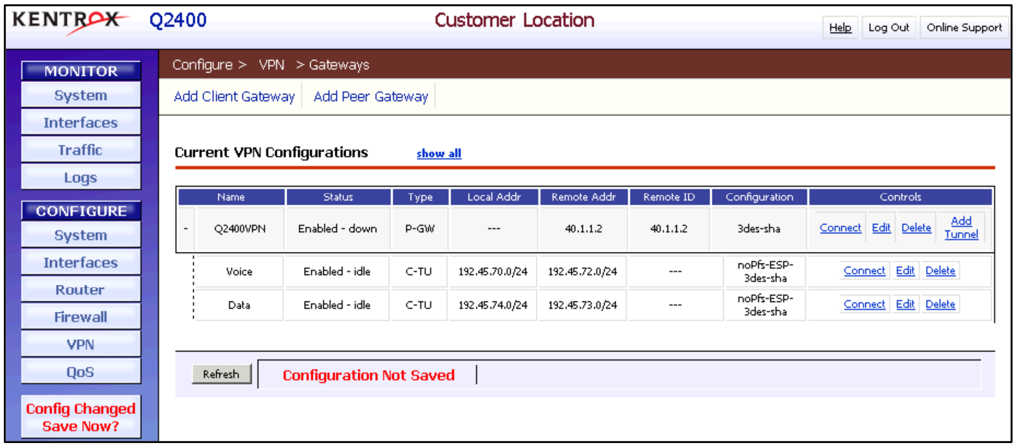
Step	Description
1.	Browse to the IP address of the Q2200 router to access the Administration web page. Log into the Q2200 using the appropriate credentials when the Q2200 authentication window appears.
2.	Once successfully logged in, the Q2200 main window is displayed. All of the configuration options are selected from the tree view on the left side of the Q2200 main window.
3.	Select **VPN** under CONFIGURE in the tree view. In the Configure > VPN page that appears, click **Global Settings**.

Step	Description
4.	In the Configure > VPN > Global Settings page that appears, set *VPN Interface* to **ipwan-1 [40.1.1.2]**, *Egress ToS Action* to **copy**, *Ingress ToS Action* to **copy** and click **OK**.  KENTROX Q2200 Customer Location Help Log Out Online Support MONITOR System Interfaces Traffic Logs CONFIGURE System Interfaces Router Firewall VPN QoS Config Changed Save Now? Configure > VPN > Global Settings Refresh OK Cancel Apply VPN Configuration VPN Interface: ipwan [40.1.1.2] Local ID: VPN Interface ipwan Egress ToS Action: copy Ingress ToS Action: copy Egress DF Bit Action: clear Enable Strict Encryption ☑ Configuration Not Saved **NOTE**: The Q-Series routers keep traffic marked with DSCP 46 (EF) in its own priority queue. However, DSCP 34 (AF4) marked traffic is kept in a Weighted Fair Queue (WFQ) with all other DSCP values. To ensure highest priority for both signaling and audio, a policy was created to map DSCP 34 to 46 at both the corporate and branch site Q-Series routers (not shown in these Application Notes). This ensures that signaling and audio packets are transmitted using the priority queue, instead of WFQ. Setting the *Egress ToS Action* field to **copy** ensures this QoS policy is applied for the VPN. For further information about the QoS configuration necessary for Kentrox Q-Series routers with Avaya IP Office, please refer to [1] in Additional References.
5.	Select **VPN** under CONFIGURE in the tree view. In the Configure > VPN page that appears, click **Gateways**.
6.	In the Configure > VPN > Gateways page that appears, click **Add Peer Gateway**.

Step	Description
7.	In the Configure > VPN > Gateways > Add Peer Gateway page that appears, set *Gateway* to **Q2200VPN**, *Remote Address* to **userEntered 40.1.1.1**, *Initiator Negotiation Mode* to **automatic**, *Authentication Type* to **presharekey**, *Pre-Share Password* to the same password used on the Q2400, *Diffie-Hellman Group* to **DH2**, *Phase 1 Encryption/Hash* to **3des-sha**, *Lifetime Format* to **Seconds**, *Lifetime [secs]* to **28800**, check **Enable Gateway**, check **Enable NAT Traversal** and click **Create**.  KENTROX Q2200 Customer Location Help Log Out Online Support MONITOR System Interfaces Traffic Logs CONFIGURE System Interfaces Router Firewall VPN QoS Config Changed Save Now? Create Cancel Configure > VPN > Gateways > Add Peer Gateway Remote Peer Configuration Gateway: Q2200VPN Remote ID Type: ipAddress Remote Address: userEntered 40.1.1.1 Initiator Negotiation Mode: automatic Authentication Type: preshareKey Pre-Share Password: ***** Diffie-Hellman Group: DH2 Phase 1 Encryption/Hash: 3des-sha Lifetime Format: ● Seconds ○ DD HH:MM Lifetime [secs]: 28800 Enable Gateway: ☑ NAT Traversal Configuration Enable NAT Traversal: ☑ Enable UDP Checksum: □ Keep-Alive Interval [secs]: 10 Configuration Not Saved
8.	In the Configure > VPN > Gateways page, click **Add Tunnel**.

Step	Description
9.	In the Configure > VPN > Gateways > Add Tunnel page that appears, set *Tunnel Name* to **Voice**, *Local Address* to **userEntered 192.45.72.0/24**, *Remote Address* to **userEntered 192.45.70.0/24**, check **Enable Tunnel**, *Transform* to **ESP**, *Authentication* to **sha**, *Encryption* to **3des**, *Lifetime Format* to **Secs**, *Lifetime [secs]* to **28800** and click **Create**.  KENTROX Q2200 Customer Location Help Log Out Online Support MONITOR System Interfaces Traffic Logs CONFIGURE System Interfaces Router Firewall VPN QoS Config Changed Save Now? Create Cancel Configure > VPN > Gateways > Add Tunnel Tunnel Configuration Tunnel Name: Voice Local Address: userEntered 192.45.72.0/24 Remote Address: userEntered 192.45.70.0/24 Enable Tunnel: ☑ Phase-2 Proposal Transform: ● ESP ○ AH Authentication: sha Encryption: 3des Perfect Forward Secrecy: noPfs Lifetime Format: ● Secs ○ DD HH:MM Lifetime [secs]: 28800 Configuration Not Saved
10.	In the Configure > VPN > Gateways page, click **Add Tunnel** again.

Step	Description
11.	In the Configure > VPN > Gateways > Add Tunnel page that appears, set *Tunnel Name* to **data**, *Local Address* to **userEntered 192.45.73.0/24**, *Remote Address* to **userEntered 192.45.74.0/24**, check **Enable Tunnel**, *Transform* to **ESP**, *Authentication* to **sha**, *Encryption* to **3des**, *Lifetime Format* to **Secs**, *Lifetime [secs]* to **28800** and click **Create**.  KENTROX Q2200 Customer Location Help Log Out Online Support MONITOR System Interfaces Traffic Logs CONFIGURE System Interfaces Router Firewall VPN QoS Config Changed Save Now? Configure > VPN > Gateways > Add Tunnel Tunnel Configuration Tunnel Name: data Local Address: userEntered 192.45.73.0/24 Remote Address: userEntered 192.45.74.0/24 Enable Tunnel ☑ Phase-2 Proposal Transform ● ESP ○ AH Authentication: sha Encryption: 3des Perfect Forward Secrecy: noPfs Lifetime Format ● Secs ○ DD HH:MM Lifetime [secs]: 28800 Create Cancel Configuration Not Saved
12.	Select **Firewall** under CONFIGURE in the tree view. In the Configure > Firewall page that appears, click **Global Settings**. In the Configure > Firewall > Global Settings page that appears, check **Enable ACL Firewall**, **Enable Intrusion Detection**, **Enable Session Log**, **Enable Blocking Log**, **Enable Intrusion Log** and click **OK**.  KENTROX Q2200 Customer Location Help Log Out Online Support MONITOR System Interfaces Traffic Logs CONFIGURE System Interfaces Router Firewall VPN QoS Config Changed Save Now? Advanced Settings check all Configure > Firewall > Global Settings Firewall Settings Enable ACL Firewall ☑ Enable Intrusion Detection ☑ Firewall Logs Enable Session Log ☑ Enable Blocking Log ☑ Enable Intrusion Log ☑ OK Cancel Apply Configuration Not Saved
13.	Select **Router** → **NAT** under CONFIGURE in the tree view. In the Configure > Router > NAT page that appears, check **NAT** and click **OK**.

Step	Description
14.	Select **System → Save Config** under CONFIGURE in the tree view to save the configuration.
	Bring up VPN on both Q-Series routers
15.	In the Configure > VPN > Gateways page, click **Connect** in the Q2200VPN row to bring up the VPN on the Q2200 router. Repeat the same step for the Q2400VPN on the Q2400 router (not shown). 

Current VPN Configurations

	Name	Status	Type	Local Addr	Remote Addr	Remote ID	Configuration	Controls
-	Q2400VPN	Enabled - down	P-GW	---	40.1.1.2	40.1.1.2	3des-sha	Connect Edit Delete Add Tunnel
	Voice	Enabled - idle	C-TU	192.45.70.0/24	192.45.72.0/24	---	noPfs-ESP-3des-sha	Connect Edit Delete
	Data	Enabled - idle	C-TU	192.45.74.0/24	192.45.73.0/24	---	noPfs-ESP-3des-sha	Connect Edit Delete

Configuration Not Saved

4. Interoperability Compliance Testing

Interoperability compliance testing covered testing of the site-to-site IPSec VPN in the Avaya/Kentrox configuration. Prioritization of voice traffic was achieved by implementing DiffServ-based QoS on the PPP link (see [1] in Additional References). Voice and data traffic were segmented in the enterprise network using VLANs.

4.1. General Test Approach

Testing was performed manually. Specifically, compliance testing verified that VoIP media and signaling traffic could be carried together with low priority data traffic over the site-to-site IPSec VPN while still achieving acceptable voice quality.

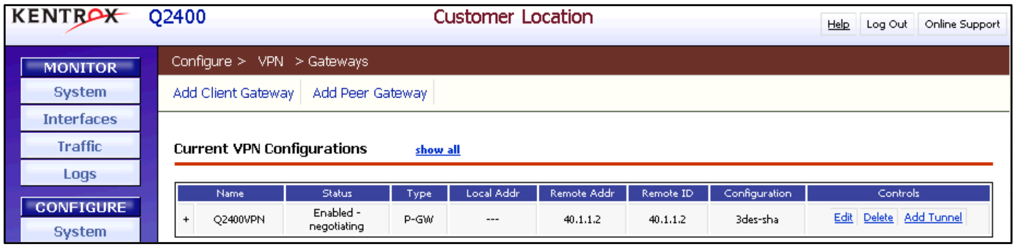
4.2. Test Results

Feature testing passed. The Q-Series QoS implementation (including the signaling packet DSCP remarking) over the site-to-site IPSec VPN yielded acceptable voice quality.

5. Verification Steps

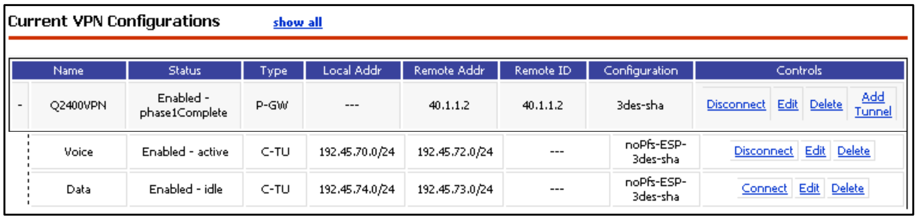
This section provides the steps for verifying the VPN is up on the Q-Series routers. In general, the verification steps include:

1. In the Configure > VPN > Gateways page, review the VPN status field to verify that the VPN comes up on the Q2400 router. The VPN is up when the status field reports *Enabled – phase1Complete* for Q2400VPN. Verify the same is reported for Q2200VPN on the Q2200.



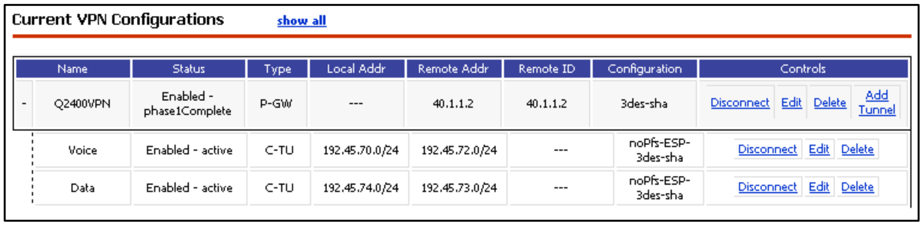
Current VPN Configurations

	Name	Status	Type	Local Addr	Remote Addr	Remote ID	Configuration	Controls
+	Q2400VPN	Enabled - negotiating	P-GW	---	40.1.1.2	40.1.1.2	3des-sha	Edit Delete Add Tunnel



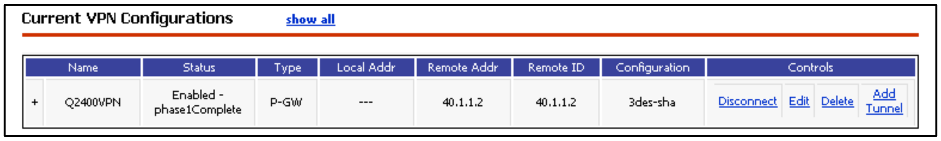
Current VPN Configurations

	Name	Status	Type	Local Addr	Remote Addr	Remote ID	Configuration	Controls
-	Q2400VPN	Enabled - phase1Complete	P-GW	---	40.1.1.2	40.1.1.2	3des-sha	Disconnect Edit Delete Add Tunnel
	Voice	Enabled - active	C-TU	192.45.70.0/24	192.45.72.0/24	---	noPfs-ESP-3des-sha	Disconnect Edit Delete
	Data	Enabled - idle	C-TU	192.45.74.0/24	192.45.73.0/24	---	noPfs-ESP-3des-sha	Connect Edit Delete



Current VPN Configurations

	Name	Status	Type	Local Addr	Remote Addr	Remote ID	Configuration	Controls
-	Q2400VPN	Enabled - phase1Complete	P-GW	---	40.1.1.2	40.1.1.2	3des-sha	Disconnect Edit Delete Add Tunnel
	Voice	Enabled - active	C-TU	192.45.70.0/24	192.45.72.0/24	---	noPfs-ESP-3des-sha	Disconnect Edit Delete
	Data	Enabled - active	C-TU	192.45.74.0/24	192.45.73.0/24	---	noPfs-ESP-3des-sha	Disconnect Edit Delete



Current VPN Configurations

	Name	Status	Type	Local Addr	Remote Addr	Remote ID	Configuration	Controls
+	Q2400VPN	Enabled - phase1Complete	P-GW	---	40.1.1.2	40.1.1.2	3des-sha	Disconnect Edit Delete Add Tunnel

2. Once the VPN is up, verify IP communication from the WAN router to the following network devices and interfaces by using the **ping** command.

   - Ping the Avaya IP Office.
   - Ping the Avaya IP telephones registered to the Avaya IP Office.
   - Ping the DHCP server.

3. Verify DHCP relay on the Q-Series is functioning by confirming that the IP Telephones on the Q2200 side of the network receive their IP addresses from the DHCP server on the Q2400 side of the network.

4. Check that the Avaya IP Telephones have successfully registered using the IP Office **System Monitor**.

5. Place inter-site calls between the Digital and IP telephones. If the call cannot be established, check the status of the IP trunks on the IP Offices using the IP Office **System Monitor**.

6. Support

For technical support on the Kentrox Q-Series routers, contact Kentrox Technical Support using any of the following options:

- Toll-free: (800) 733-5511
- Direct: (503) 643-1681
- Email: care@kentrox.com

7. Conclusion

These Application Notes describe the configuration steps required for configuring a site-to-site IPSec VPN between the Q-Series Q2400 and Q2200 routers into a small office and/or low traffic Avaya IP Office infrastructure. The Avaya IP Office delivered the voice traffic to the routers for transmission over the VPN together with data traffic.

8. Additional References

This section references the Avaya and Kentrox product documentation that are relevant to these Application Notes. The Avaya product documentation can be found at http://support.avaya.com and the Kentrox product documentation can be found at http://www.kentrox.com.

[1] Application Notes for VoIP over PPP Link with Quality of Service using Kentrox Q-Series Routers with Avaya IP Office
[2] Avaya IP Office 2.1 Manager, Issue 15c, May 2004.
[3] Kentrox QoS Access Router User's Guide, Software Release 1.3, Document #650-00319-03.

Please e-mail any questions or comments pertaining to these Application Notes along with the full title name and filename, located in the lower right corner, directly to the Avaya Developer*Connection* Program at devconnect@avaya.com.