Extreme Retail Select: BOX#5

Abstract:

To overcome the challenges associated with designing, purchasing, deploying, and operating network services at retail locations to deliver differentiated experiences, Extreme Networks has announced its Extreme Retail Select solution. It provides everything retailers need in simple, pre-packaged solutions that can be ordered by a single SKU. Retailers can select the appropriate package based on their requirement for either 'essential' connectivity or for high-performance, 'evolved' environments, and based on store size. The Essential package includes the performance required to connect customers, employees, and point-of-sale devices safely and securely. It will also provide out-of-the-box analytics. The Evolved package is designed to enable greater levels of performance for advanced retail applications, such as augmented reality smart shelves, dynamic pricing, and in-store IoT.

This document is a step-by-step quick deployment guide to implement SD-WAN, wired and wireless networks in multiple store locations.
Contents

Box#5: Network Architecture .................................................................3
  Things you need to have to bring your stores up ..................................3
  Wiring a store .........................................................................................4

Box#5: Network Policy and Licensing .......................................................5
  ExtremeCloud IQ Getting Started .........................................................5
  ExtremeCloud IQ Network Policy .........................................................5
  ExtremeCloud IQ Licensing .................................................................6
  Adding XR600P as Layer 3 VPN Gateway into account .........................6

Box#5: Router, VPN, SD-WAN configuration ............................................10
  Network Allocation ................................................................................10
  Router Template ...................................................................................13
  VPN Service ..........................................................................................14
  SD-WAN ..................................................................................................15
  Routing Policy .......................................................................................16

Box#5: Access Point template ..................................................................19

Box#5: Switch template ............................................................................20

Box#5: Wireless Networks .........................................................................22

Box#5: Device Onboarding .......................................................................23

Revision History .......................................................................................26
Box#5: Network Architecture

Box #5 consists of dual SD-WAN/VPN routers XR600P, dual switches SR2324P, six Access Points AP305C and ten subscription licenses. That provides redundancy for the store connectivity.

Routers (XR600P) can be connected to Internet via single or multiple Internet Service Providers (ISP) utilizing WAN0/WAN1 Ethernet ports and/or USB ports for 3G/LTE modems.

Routers (XR600P) will establish L3 VPN connection to HQ (or Data Center) XR600P working as Layer 3 VPN Gateway. Only traffic destined to HQ will be encapsulated into VPN, the remaining traffic will go directly to Internet. If one router will fail, the second router will still provide connectivity to the HQ and to Internet due to Virtual Router Redundancy Protocol (VRRP) will be enabled on store routers during the configuration.

Routers (XR600P) are also responsible for providing DHCP service to any in-store devices such as switches, Access Points and any wired or wireless clients.

Note: Offered design in this document can be used for deployment size up to 256 stores (depends to the traffic requirements between stores and HQ). If you have more stores in your organization, the IP subnets need to be designed accordingly.

Things you need to have to bring your stores up

- Hardware for stores (Routers, Switches, Access Points)
- HQ/Data Center VPN Concentrator (if you planning to send some data back to your HQ/Data Center and between the stores)
- List of hardware Serial Numbers (csv file)
Wiring a store

Connect **WAN0(ETH0)** and (if applicable) **WAN1(ETH1)** of both XR600P routers to your ISP providers.

Connect port **G1** of switch **SW-1** with port **ETH2** of branch router **Router-1**.

Connect port **G1** of switch **SW-2** with port **ETH2** of branch router **Router-2**.

Connect AP’s to ports **G2-G4** of the switches **SW-1** and **SW-2**.

Connect ports **G24** between **SW-1** and **SW-2** to establish inter-switch connection.

![Figure 2: Wiring a store](image-url)
Box#5: Network Policy and Licensing

**ExtremeCloud IQ Getting Started**

Please contact your Sales Representative for the account creation. You will be getting Welcome email from Extreme Networks with the link to set up a password.

**ExtremeCloud IQ Network Policy**

Create a new Network Policy by clicking on *ADD NETWORK POLICY* button (or by navigating to *Configure*→*Network Policy*→*Add Network Policy* if other policy already exists)

Make sure all types are checked: *Wireless, Switches, Routing*. Enter a name for this Policy, set *enable Presence Analytics* to on, then click on the *SAVE* button. After the policy is saved, click on *Exit* button. The remaining parts of Network Policy configuration will be done at later steps.
ExtremeCloud IQ Licensing

Subscription licenses are included in the package. If you don’t have licenses installed yet, please add them now. Navigate to Global Settings, select Administration→License Management, enter your Entitlement Keys.

Adding XR600P as Layer 3 VPN Gateway into account

The XR600P for the VPN gateway role is not included into the package. Please purchase separately!

**Note:** Dedicated VMware-appliance (VGVA) can be used instead of HQ/Data Center XR600P to terminate route-based Layer 3 IPsec VPN tunnels from stores SD-WAN routers

The XR600P need to be installed in your HQ/Data Center as Layer 3 VPN Gateway to terminate VPN tunnels from remote stores.

This device can be installed in One-Armed or Two-Armed configuration – method of connection to the HQ/Data Center network.

*One-Armed Layer 3 VPN Gateway:* Connect WAN0 port of XR600P to your HQ network directly. Make sure the router XR600P can receive incoming traffic UDP ports 500 and 4500

*Two-Armed Layer 3 VPN Gateway:* Connect WAN0 port of XR600P to the DMZ part of your HQ network and WAN1 port of XR600P to your HQ network directly.

For this deployment we will be using One-Armed VPN gateway only
Navigate to **ONBOARD**, the wizard for adding devices will start. Add the serial number of XR600P which will be installed at HQ/Data Center.

Click **NEXT** a few times (up to the step *Create Network Policy*), select **Use existing network policy**, then **NEXT** and **FINISH**.

Navigate to **MANAGE**, select the device, click **Edit** button.

Then go to **Configure, Configuration**→**Device Configuration**, configure following details:
**Host Name:** Enter the name for HQ XR600P VPN gateway

**Device Function:** Layer 3 VPN Gateway

Deploy Mode: One-armed

**Network Policy:** select the Network Policy you created earlier

**IPv4 Address:** this is IP address of management interface. Enter any address which **will not conflict** with any network address range in your deployment – neither from HQ/Data Center network, nor from remote branches.

Click on **SAVE DEVICE CONFIGURATION.** Then Click on **UPDATE** button, select Complete Configuration Update, **PERFORME UPDATE**, then close the window

On the **MANAGE** screen Scroll to the right to find Public IP address of the device.

**Note:** If Public IP Address is not displayed, use Column Picker 🏛️ to select what field is shown on the screen.
If your XR600P is located behind a NAT, the IP address of ETH0 will be different from the Public IP address. You can find this address by selecting the device, navigating to Actions → Advanced → CLI Access

then type the command “show interface eth0”

You need to know this address so you can guide your HQ/Data Center network router on how to reach the remote branches (e.g. add static routes: to reach “remote branches networks” go to eth0 of XR600P)

You can fill out this form for your reference re: HQ/Data Center network

Table 1. HQ/Data Center network details

<table>
<thead>
<tr>
<th>Name</th>
<th>IP /subnet</th>
</tr>
</thead>
<tbody>
<tr>
<td>HQ XR600P ETH0 Interface</td>
<td></td>
</tr>
<tr>
<td>HQ XR600P MGT0 Interface</td>
<td></td>
</tr>
<tr>
<td>HQ Public IP address</td>
<td></td>
</tr>
<tr>
<td>Corporate network(s)</td>
<td></td>
</tr>
<tr>
<td>Corporate DNS servers</td>
<td></td>
</tr>
</tbody>
</table>
Box#5: Router, VPN, SD-WAN configuration

Go to Configure section and click on Edit icon of Network policy

Network Allocation

Network Allocation is a configuration page where you will create subnets for the stores. The system will automatically split the defined super-nets into the smaller (/24) subnets for the individual stores.

The Guest subnet will be the same for all locations since there are no expectations of communicating between guests and corporate, as well as guests in different locations.

The NAT service is automatically provided by the XR600P store router.

Navigate to Router Settings → Network Allocation. The default Management network (192.168.0.0) is offered; please modify the default subnet value according to the Table 2 (below) with edit button.

Then use ADD button to add additional VLANs/subnets into the store configuration according to this table:

<table>
<thead>
<tr>
<th>VLAN name</th>
<th>VLAN ID</th>
<th>Subnet</th>
<th>Network Type</th>
<th>At each site</th>
</tr>
</thead>
<tbody>
<tr>
<td>Store-MGMT</td>
<td>1</td>
<td>10.240.0.0/16</td>
<td>Management</td>
<td>Unique</td>
</tr>
<tr>
<td>Staff</td>
<td>241</td>
<td>10.241.0.0/16</td>
<td>Internal Use</td>
<td>Unique</td>
</tr>
<tr>
<td>PoS</td>
<td>242</td>
<td>10.242.0.0/16</td>
<td>Internal Use</td>
<td>Unique</td>
</tr>
<tr>
<td>IoT</td>
<td>243</td>
<td>10.243.0.0/16</td>
<td>Internal Use</td>
<td>Unique</td>
</tr>
<tr>
<td>Guest</td>
<td>255</td>
<td>10.255.0.0/23</td>
<td>Guest Use</td>
<td>The same</td>
</tr>
</tbody>
</table>
Note: If your HQ/Data Center already has any network listed in Table 2, please allocate other Subnets for your remote branches

The above configuration is good for up to 256 branches with /24 networks (253 clients per branch per subnet). If more branches need to be configured, please consider adding new Network Policy with additional network allocations as well as additional XR600P router in HQ.

To create a new VLAN, click on ADD, then select ☑, then New in Network Allocation VLAN section, then type the name of VLAN and VLAN ID

To create subnet, click on New in Subnetwork Space section

Configure subnet: enter the name, select the Network type (Management for VLAN1, Guest Use for VLAN 255, and Internal Use for the rest VLAN's – see Table 2); select Create a unique subnetworks at each site for any non-Guest VLAN, and Replicate the same subnetwork at each site for the Guest subnetwork; slide Partition the local IP address space into subnetworks slider to 256 (making each subnetwork with /24 mask) for non-guest VLANs. The Guest network will be the same at each branch, so selecting mask /23 will make enough addresses for the purpose of guest onboarding.
Scroll further down to Advanced Settings, enable *Use Arp to check for IP address conflicts*

Further down click + to add a new DNS service

Enter the Name, select *Supply external DNS server IP addresses*, add DNS servers. Click SAVE, then SAVE the Network Allocation

**Note:** For the Guest Network you can create different DNS Service with the list of public DNS Servers

Repeat the same procedure for all VLANs as per Table 2. Finally, you will have this list of VLANs and Subnetwork spaces:
Network Allocation

<table>
<thead>
<tr>
<th>VLAN</th>
<th>Subnetwork Space</th>
<th>Network Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td></td>
<td>MGMT</td>
<td>For network devices only (APs and Switches)</td>
</tr>
<tr>
<td>241-Staff</td>
<td></td>
<td>INTERNAL</td>
<td>Store staff access</td>
</tr>
<tr>
<td>242-PoS</td>
<td></td>
<td>INTERNAL</td>
<td>Point of Sales only</td>
</tr>
<tr>
<td>243-IoT</td>
<td></td>
<td>INTERNAL</td>
<td>All IoT devices</td>
</tr>
<tr>
<td>255-Guest</td>
<td></td>
<td>GUEST</td>
<td>Guest wireless users</td>
</tr>
</tbody>
</table>

Router Template

Navigate to **Device Template**, click **Add**, choose **XR600P**

Enter the **Template Name**, on interface ETH2 click on + button to create a new Port Type

Enter the name (e.g. XR-Trunk-Stores) of **New Port Type**, change the **Port Usage to Trunk Port** (802.1Q VLAN Tagging), keep **Native VLAN to 1**, in the list of **Allowed VLANs** add following VLANs: **241,242,243,255**, click on **SAVE PORT TYPE**
also change the Port Type of ETH3 to trunk port created in previous step.

Click on Advanced Settings and select Upgrade to the latest version. Click on Save button.

VPN Service

**Note:** It is recommended to use custom generated certificates for VPN connectivity instead of default ones. Details can be found in the Help section on Extreme Cloud IQ

Navigate to VPN Service. Enable VPN Service, click in ADD to add a new service.
Enter the name of the VPN service. Set the *Number of branches to be created* to 256; In the drop-down VPN Gateway select the XR600P from HQ added previously. Enter the **public** IP address of XR600P into External IP address (see Table 1). Click on **Save** button.

**Note:** If XR600P(HQ) is located behind firewall, please make sure that ports **UDP 500** and **UDP 4500** are opened for incoming connections. If XR600P(HQ) is located behind NAT, you also need to add port forwarding to your HQ router.

### SD-WAN

Navigate to SD-WAN, **Enable SD-WAN**, then click **ADD** to add **SD-WAN Route Group**

Enter the name of the group, under **WAN Priority** select the WAN links in desired order of highest to lowest routing priority. If you have USB with 3G/LTE modem you can select it as priority 3 and 4. Click on **Save**.
Routing Policy

Routing Policy will enable stores to forward network traffic to its destination depends on different criteria – e.g. some packets will go into VPN back to HQ/Data Center, some will go directly to Internet; guest packets will never be able to reach Corporate or store networks.

Navigate to Routing Policy. *Enable Routing Policy*, then click on *ADD* to add Routing Policy

Enter the *Name* for the Policy, then build following five Rules:

*Rule #1/Rule#2: Deny guest traffic to access corporate/store network*

**Source:** Type = User Profile, Value = Any Guest, Application Service Set = Any

**Destination:** Type = Network Address, Value = <your HQ network>/<Store network>

**Forwarding Action:** Drop

*Rule #3: Tunnel traffic to HQ network into VPN/SD-WAN*

**Source:** Type = Any

**Destination:** Type = Network Address, Value = <your HQ network>
Forwarding Action: Group1  (the SD-WAN route group created in previous step)

**Rule #4: Tunnel traffic to Remote Branches into VPN/SD-WAN**

**Source:** Type = Any

**Destination:** Type = Network Address, Value = 10.240.0.0/14  (the super-net of all store networks)

Forwarding Action: Group1  (the SD-WAN route group created in previous step)

**Rule #5: Send all remaining traffic directly to Internet**

**Source:** Type = Any

**Destination:** Type = Any

Forwarding Action: Primary WAN

Backup Forwarding Action: Backup-WAN1

To create `<your HQ network>` or `<your Store network>` click on select icon in Value field, then select New from the Network section

Then create an entry with your HQ/Data Center network.
Repeat this step for the Branch super-net (one entry will cover 10.240.0.0/16-10.243.0.0/16 networks)

<table>
<thead>
<tr>
<th>Name *</th>
<th>Stores</th>
</tr>
</thead>
<tbody>
<tr>
<td>Subnet</td>
<td>10.240.0.0</td>
</tr>
<tr>
<td></td>
<td>255.255.0.0</td>
</tr>
</tbody>
</table>

**Note:** If HQ/Data Center has more than one network to which you want to allow VPN access from remote stores, you need to either create a super-net entry for HQ/Data Center (if it’s possible), or enter additional rules into the routing policy for each network.
Box#5: Access Point template

Navigate to Device Templates section, AP Templates, click on ADD, choose AP305C

Enter the template name. Navigate to Advanced Settings

Select Country Code according to your country, verify that Update firmware to the latest version and Reboot after uploading options are selected (default settings). Then Save Template.
Box#5: Switch template

Navigate to Device Templates section, select the Switch Templates tab, click on ADD, choose SR2348P

Enter the template name, enable STP, select RSTP(Rapid STP), enable IGMP Snooping, Enable immediate leave and Suppress redundant IGMP membership reports

Navigate to Port Configuration, select Ports 1-4,24 click on Assign→Create New

Enter a Name for new Port Type (e.g. Trunk-Stores), select Trunk Port (802.1Q VLAN Tagging) as Port Usage, keep Native VLAN set to 1, enter following VLAN’s in the list of Allowed VLANs: 1,241,242,243,255. Click on SAVE PORT TYPE
Scroll down, enable *Edge Port* on *STP Settings*

If you need to connect PoS or IoT device directly to the switch, create another port type and assign it to the port. Here is an example of preparing a port to be ready for PoS device connected directly: select a port, then **Assign**→**Create New**, type the name, select **Access Port**, choose **PoS VLAN** from the list.
Box#5: Wireless Networks

Below is an example of how to configure a simple PSK-based network (SSID). All other Wireless Network types (Open/Guest onboarding/802.1X/PPSK) can be made based on the business needs of your organization. Extreme Networks does not recommend to assign more than three SSID to the same Radio of Access Point to avoid unnecessary media utilization by sending/receiving additional wireless management frames.

Navigate to Wireless Networks, click on ADD and choose All other Networks (standard)

Select the Personal tab, enter a Name for the wireless network (SSID), then Key Value a password for wireless access. Under User Access Settings click on + sign.

In Create User Profile dialog enter a name of this User Profile (e.g. Staff), select Staff VLAN to be associated with this profile, then SAVE USER PROFILE

Click on SAVE button.
Box#5: Device Onboarding

Before onboarding store devices, push the configuration changes to XR600P(HQ)

Go to MANAGE, select the device, then click on UPDATE DEVICE. You can select Delta Configuration Update.

Navigate to ONBOARD in the main menu.

Import file with serial numbers of devices then click NEXT

At the step 4 select Use existing network policy

**Note:** Due to know bug#APC34048 the XR600P branch routers need to be connected to the network before assigning Branch ID and configuring VRRP is possible*

*Connect XR600P (Router-1 and Router-2) to the network.

*Wait till routers got provisioned and available in CloudIQ.
Select both branch routers, click on Actions→Assign BranchID

Create a New Branch ID by clicking on New link (or + sign), enter the name/ID of the branch, then click SAVE twice to return to the screen

Click on any of those branch routers, then Configure→Device Configuration→Additional→VRRP.

Enable VRRP, check all VLANs/Subnets for both routers to participate, select one of the router with “H” and other with “M” or “L” priority. In Additional VRRP settings check Preempt Mode and TrackWan option for all available VLANs. Click on SAVE, then UPDATE

*Make sure the routers got updated and available in CloudIQ, then you can connect all remaining devices in the store according to Figure 2.

**Note:** If switches were already connected before enabling VRRP on routers you might need to reboot/power cycle it due to change in the network

Finally, you should see all devices are up as well as VPN tunnel
You can also validate that the tunnel is up and running by issuing a CLI command on your branch router XR600P. For that select your branch router XR600P, go to Actions→Advanced→CLI Access

Issue the command “show vpn ipsec-tunnel”
## Revision History

<table>
<thead>
<tr>
<th>Date</th>
<th>Revision</th>
<th>Changes Made</th>
<th>Author</th>
</tr>
</thead>
<tbody>
<tr>
<td>Dec 2019</td>
<td>0.1</td>
<td>Initial Draft</td>
<td>Yury Ostrovsky</td>
</tr>
<tr>
<td>Dec 2019</td>
<td>0.2</td>
<td>Review</td>
<td>Aren Gates</td>
</tr>
<tr>
<td>Feb 2020</td>
<td>0.3</td>
<td>Review</td>
<td>Envision team</td>
</tr>
<tr>
<td>Feb 2020</td>
<td>1.0</td>
<td>Release</td>
<td></td>
</tr>
</tbody>
</table>