Remote Access Solution Guide
Hardware, Software and Security

More now than ever, modern-day problems require modern-day solutions; remote work is now top of mind for every organization. At Extreme, we are proud to connect our customers, their customers, and communities regardless of location. We know that it’s not easy to get connected and stay connected, which is why we are helping thousands of organizations, schools, and people access the essential tools that they need to continue working, learning, and living. Combining the very best of our technologies, we are offering a variety of special remote network kits that helps to easily extend the network beyond your office, school, or shop walls.

Remote Access solutions encompass the use of equipment at the main headquarters (the head-end), equipment at the remote sites (edge devices) and software to create a Virtual Private Network (VPN) providing a secure connection, or tunnel across the WAN and GRE tunnels. VPNS are a key component of Extreme’s enterprise wide solution and as a result we offer solutions for multiple use cases, the following chart defines your options based on existing hardware and use cases:

<table>
<thead>
<tr>
<th>Use Case</th>
<th>Greenfield</th>
<th>Brownfield</th>
<th>Extender</th>
</tr>
</thead>
<tbody>
<tr>
<td>Remote Branch</td>
<td>Portable Branch Kit (SD-WAN, AP, XIQ)</td>
<td>Fabric Connect installed base XA1400 series with FC VPN</td>
<td>To extend connectivity to remote locations. Can be deployed over broadband, cellular and private WANs</td>
</tr>
<tr>
<td>Teleworking</td>
<td>Power users and Executives: L2 VPN with XR routers Employees: L2 VPN with Access Point</td>
<td>XCA with L2/L3 VPN</td>
<td>To allow employees and executives to perform work from and alternate worksite (e.g. home)</td>
</tr>
<tr>
<td>Distance Learning</td>
<td>L2 VPN with Access Point</td>
<td>XCA with L2/L3 VPN</td>
<td>Distance or online learning for users</td>
</tr>
<tr>
<td>Remote Patient Care</td>
<td>Defender for IoT (XCA with AP3912/SA201)</td>
<td>Defender for IoT (XCA with AP3912/SA201)</td>
<td>Facilitates home-based patient care through the secure connectivity of patient telemetry systems and other medical devices</td>
</tr>
<tr>
<td>Rapid outdoor Wi-Fi connectivity</td>
<td>Cloud-managed wired and wireless mesh (Remote office reluctant to use cloud)</td>
<td>WiNG-based wireless mesh (for customer reluctant to use cloud)</td>
<td>Helps hospitals and other organizations to extend secure wireless connectivity to pop-up sites</td>
</tr>
</tbody>
</table>

To support these use cases Extreme offers multiple hardware and software-based solutions providing scalable enterprise-class VPN services for up to thousands of VPN tunnels to secure communication to remote locations. These solutions offer simplified provisioning, increased network resilience, end-to-end visibility and control, reduction in costs vs MPLS links and most importantly, security. Not believing in a one size fits all, Extreme offers multiple options based on number of remote sites, existing onsite products and deployment complexity.
The following chart defines your options:

<table>
<thead>
<tr>
<th>VPN Service Manager</th>
<th>Use Cases</th>
<th>VPN Type</th>
<th>Customer Type</th>
<th># of Tunnels Supported</th>
<th>VPN Performance</th>
<th>Head-end Equipment</th>
<th>Remote Site Hardware (Extreme)</th>
<th>Deploy Complexity</th>
<th>High Availability</th>
<th>Management Choice</th>
</tr>
</thead>
<tbody>
<tr>
<td>ExtremeCloud IQ</td>
<td>Small Branch SOHO</td>
<td>L2 and L3 IPSEC</td>
<td>Greenfield Brownfield</td>
<td>Up to 1,000</td>
<td>100 Mbps to 250 Mbps</td>
<td>Hardware or Software</td>
<td>Branch Router or AP</td>
<td>ZTP</td>
<td>YES</td>
<td>Cloud or On-Prem</td>
</tr>
<tr>
<td>Extreme Cloud Appliance</td>
<td>Small/Large Branch SOHO</td>
<td>L3 IPSEC</td>
<td>Brownfield</td>
<td>Up to 10,000 APs</td>
<td>Up to 25 Gbps (Aggregate)</td>
<td>XCA</td>
<td>AP</td>
<td>ZTP</td>
<td>YES</td>
<td>On-Prem</td>
</tr>
<tr>
<td>WING Controller</td>
<td>Small/Large Branch SOHO</td>
<td>L2 and L3 IPSEC</td>
<td>Brownfield</td>
<td>Up to 4,000</td>
<td>Up to 8 Gbps (Aggregate)</td>
<td>WING Controller</td>
<td>AP</td>
<td>Basic to Advanced</td>
<td>YES</td>
<td>On-Prem</td>
</tr>
<tr>
<td>XA1440 Fabric Connect</td>
<td>Small Branch</td>
<td>L2/L3 VSN IPSEC</td>
<td>Brownfield</td>
<td>Up to 124 VSNs</td>
<td>Up to 500Mbps</td>
<td>Fabric Enabled Switch</td>
<td>XA1440 (Switch)</td>
<td>Advanced</td>
<td>YES</td>
<td>On-Prem</td>
</tr>
</tbody>
</table>

**ExtremeCloud IQ L2/L3 VPN Services**

ExtremeCloud IQ (XIQ) has multiple options to provide secure VPN services to remote sites: VPN services between XR Branch Routers, the use of VPN Gateway Virtual Appliance (VGVA) or a mixture of both. Offering flexibility to simply deploy VPN and GRE termination services, providing scalable enterprise-class L2 or L3 VPN services for thousands of VPN tunnels from remote access locations.

**Solution Basics**
- ExtremeCloud IQ provides all network connections, configuration and L2/L3 VPN services
- Deployment Options:
  - Leverage multiple XR Branch Routers (both ends) to provide L2/L3 VPN services
    - XR600P can act as either a VPN server/concentrator or remote endpoint, while the XR200P operates only as a VPN endpoint.
  - Leverage Extreme’s VGVA services to provide the L2 or L3 VPN termination at the headquarters (Head-end).
    - For L2 - ExtremeCloud IQ enabled access points (APs) terminate the L2 VPN tunnel at each remote location
    - For L3 - Either an XR200P or XR600P branch router terminate the L3 VPN tunnel at each remote location
- All configuration accomplished via cloud services, I.e. Plug-and-Play
- **Configuration specifics** available

**Solution Components** (not all may be required)
- ExtremeCloud IQ
- VGVA Service (optional)
- ExtremeCloud IQ enabled APs
- XR200P or XR600P

**Functional Parameters**
- Number of tunnels supported: Up to 10,000
- Performance: 100-250Mbps VPN
- Tunnel Types: L2VPN and L3 IPSEC
- Complexity to Configure: Plug and Play (ZTP)
ExtremeCloud Appliance (XCA) (Includes Defender)

ExtremeCloud Appliance VPN services securely connects HQ to remote sites (@Home), providing connectivity for up to 10,000 Managed APs. Allows IT administrators to extend corporate defined management, policies and authentication to branches and end-user locations.

The Basics
- Leverage ExtremeCloud Appliance (XCA) to provide all network connections, configuration and VPN services
- Leverage ExtremeCloud Appliance to provide L3 VPN termination at the headquarters (Head-end). The remote site connectivity is provided with any ExtremeWireless (10.51+) or WiNG7 APs for L3 IPSEC VPN services
- All configuration accomplished via XCA
  - Configuration specifics available

Functional Parameters
- Number of tunnels supported: Up to 10,000
- Tunnel Types: L3 IPSEC
- Performance: Up to 150Mbps
- Complexity to Configure: Standard XCA Campus configuration

Extreme WiNG Controller With Software VPN Capabilities

Extreme’s WiNG wireless solution provides for the creation of secure tunnels between networked devices. Tunnels are sets of SA (security associations) between two peers. Multiple types of secure connections can be defined based on the protocols used.

The Basics
- Leverage Extreme’s WiNG controllers to provide all network connections, configuration and VPN services
- Leverage authentications services on the WiNG controller to provide the L2 or L3 VPN termination at the headquarters (Head-end). The remote site connectivity will have VPN connection to any of the defined WiNG APs. Configuration options allow for the creation of either L2VPN services or L3 IPSEC services
- All configuration accomplished via the WiNG controller
  - Configuration specifics available

Functional Parameters
- Number of tunnels supported: Up to 1000
- Performance: Up to 8Gbps Encrypted (aggregated) traffic
- Tunnel Types: L2VPN and L3 IPSEC
- Complexity to Configure: Basic to Advanced (dependent on solution GRE/IPSEC)
ExtremeAcesss Platform 1400
With Fabric Connect VPN

Fabric Connect Solution Diagram

Solution Components
• Fabric-enabled switch at head-end
  • XA1400 series or VSP can be used at HQ
• FCVPN software license
• XA1440 at remote sites
• XMC Management (Optional)

Remote Access Solution Components

Product Details

XCA
ExtremeCloud Appliance targets the on-premises campus solution. ExtremeCloud Appliance delivers cloud-like simplicity, management with tightly integrated services and features on-premises deployments require, complemented with simplified licensing. ExtremeCloud Appliance is also available as a virtual machine (VM) for customers that have their own private cloud services.

XR600P
SD-WAN Router, 6x GE Ethernet Ports, 4x PoE PSE Ports, 2x USB, Console Port, with included power supply. Identify Carrier approved wireless broadband cards.

ExtremeCloud IQ
3rd Generation Cloud Based Enterprise Network Management Offering Intuitive Configuration Workflows, Real-Time and Historical Monitoring, and Simplified Troubleshooting.

VGVA
The VPN Gateway Virtual Appliance (VGVA) is designed to simplify VPN and GRE termination, and is a key component of Extreme’s SD-WAN solution. As a software-based VMware-compliant solution, the VGVA provides scalable enterprise-class VPN termination for thousands of layer 2/3 VPN tunnels from remote access locations.

AP305C Cloud AP
ExtremeCloud IQ: Indoor Wi-Fi 6 AP, 2x2 radios with Dual 5 GHz capabilities and 1x1GbE port. Integrated light/power sensors and BLE. AI/ML green mode. Internal antennas.
AP150W
Enterprise-grade, Indoor Wallplate, 802.11ac MU-MIMO, Wave 2 Dual-Radio 3x3:3 Access Point and Switch. Compact enterprise-class wallplate access point and switch with embedded IoT technology designed for wall or desktop mount. Ideal for use-cases such as hotel rooms, cruise ships, residential halls, or other multi-dwelling unit deployments.

AP30
Industry’s first pluggable enterprise access point designed for instant, continuous, and adaptable client and IoT connectivity. Can be quickly and conveniently plugged into any power socket, and network connected via mesh or existing Ethernet data points enabling faster deployments, reduced cabling and installation costs, and flexible network access in any location.

IoT Defender S/W
Extreme Defender for IoT is a unique, award-winning solution, that delivers security for endpoints which have limited or even no embedded security capabilities. It is especially targeted to aging wired devices that need to roam around a room, a building or even a campus. It complements a customer’s existing security infrastructure by adding in-line defense directly at the IoT device itself. And it can be deployed over any network infrastructure to enable secure IoT management without significant network changes.

SA201 Adapter
The Defender for IoT Adapter delivers enterprise-grade performance and personalized protection for vulnerable wired devices. Placed between the network and the device, the Defender Adapter works in conjunction with the Defender Application (a value-add application on the ExtremeCloud Appliance) to secure, isolate, track and monitor IoT devices.

WiNG APs
Extreme Networks offers Wi-Fi Infrastructure solutions that is built on a foundation of products with unlimited scalability, reliability and security services providing the industry’s most extensive suite of Wi-Fi 6 (11ax) and Wi-Fi 5 (11ac) access points and management solutions.

XA1400 Access Switches
Designed to extend the reach of Extreme Fabric Connect technology to remote sites, the ExtremeAccess Platform 1400 Series with Fabric Connect VPN software delivers fully featured network virtualization capabilities in a cost-effective hardware appliance. Optimized for remote locations, the ExtremeAccess Platform extends secure multi-service capabilities across either Service Provider WAN or Public Internet links in a compact form factor ideal for small sites. It offers a simplified, yet secure way to extend campus fabric services to branch locations.