Knowledge Base Document

BranchSDO SD-WAN Best Practices

Author: BranchSDO Product Management

[v1.0] | [4/22/2019]

[Applies to Netsurion BranchSDO CXD 2500 and CXD 2800 edge devices]
## Contents

Contents ........................................................................................................................................................... 2  
Overview .......................................................................................................................................................... 3  
Bandwidth and your ISP ................................................................................................................................... 3  
What types of businesses is BranchSDO most appropriate for: asking the right questions ......................... 4  
  What is the size of my business? ..................................................................................................................... 4  
  What are my connectivity needs? ..................................................................................................................... 4  
  What type of connectivity do I need? DSL, Cable or LTE only? ..................................................................... 4  
  How easy is remote troubleshooting on my current solution? ...................................................................... 4  
  Does the current solution secure the edge today? ......................................................................................... 4  
  Does the current solution offer VPN? ........................................................................................................... 5  
  Does the current solution offer and/or enable PCI DSS Compliance? ....................................................... 5  
  How does the current solution handle the changing demand for bandwidth? ........................................... 5  
Other FAQs: ...................................................................................................................................................... 5  
  The site’s internet is slow. How do I resolve? ................................................................................................. 5  
  How fast are solutions being deployed today? ............................................................................................... 5  
  How agile are current deployments? ............................................................................................................... 6  
  Do I centrally manage hundreds or thousands of deployments? ................................................................. 6  
  How do I upgrade a CXD when needed? ....................................................................................................... 6  
  When best effort internet may fail you ....................................................................................................... 6  
BranchSDO CXD ................................................................................................................................................ 7  
  How to approach and define segmenting the CXD? ....................................................................................... 7  
  How to decide which CXD model do I need? ................................................................................................. 8  
  Which features should I turn on? ..................................................................................................................... 9  
Appliance Benchmarks ............................................................................................................................................... 11  
  How many Wi-Fi clients can I have on a CXD and Extended Access Point? .............................................. 11  
  What about the Integrated Wi-Fi within the CXD? ....................................................................................... 12  
Integrated LTE .................................................................................................................................................... 12  
  Sample deployment options and use cases ................................................................................................. 13  
About Netsurion .................................................................................................................................................... 15  
Contact Us ....................................................................................................................................................... 15
Overview

This technical document provides guidelines to choose the right Netsurion BranchSDO SD-WAN solutions based on real-world deployments, Netsurion standard benchmarks, and in-depth feature descriptions. Netsurion BranchSDO SD-WAN solutions offer multiple networking and security features in a simple-to-deploy, consolidated form factor. Given the number of networking and security features that can be deployed with any given CXD, device performance will vary depending on the use-case. Choosing the right CXD depends on the use-case and deployment characteristics. This “Best Practices” guide is designed to help answer the following questions:

- How do I decide which CXD model I need?
- How will the CXD perform?
- Which features should be turned on?

Bandwidth and your ISP

BranchSDO requires one (or can support up to 4) incoming RJ45 internet connections to feed the network. If you are not using an existing office LAN, this will usually be DSL, cable (broadband), or LAN connection.

When choosing an internet service provider (ISP), you will need to consider what bandwidth will be needed—both download and upload. The needs will vary depending on the type of network, how many simultaneous users there are, and the type of network activity from those users.

The highest demand for bandwidth comes from streaming video services such as Netflix, Hulu and YouTube, video chat services such as Skype and FaceTime, and automatic backup and file syncing systems such as Dropbox. Just a few users sharing files or streaming video can quickly use up all available bandwidth. BranchSDO helps manage this with port-based QoS segmentation bandwidth limits and the ability to block individual users based on network-level steering.

Even with the management capability of BranchSDO, the more bandwidth you have available on the network, the better the experience will be for the network users. But more bandwidth does not always equal more throughput. Some plans are “best-effort” which means that the advertised speed is the upper limit and not what you may actually get most of the time. For example, if you are on a 20 Mbps best-effort plan, only speeds of up to 20 Mbps may occasionally be reached and most of the time the speeds will be far less. Second, the more devices or clients that are connected to the network, which may also include people connected via Wi-Fi, also reduce the speed as they all consume some bandwidth depending on what they are doing at any given time.
What types of businesses is BranchSDO most appropriate for: asking the right questions

BranchSDO is a good fit for any multi-location business that is looking for connectivity, security and or compliance solutions that will allow to adapt to changing demands and to integrate the cloud, big data, and the Internet of Things (IoT) into network operations. Retail and Hospitality are obvious great fits, but there are many others. To know if BranchSDO is the right fit, there are a few important questions to ask and answer when considering BranchSDO:

What is the size of my business?
- BranchSDO is a great fit for the multi-location business with less than 150 seats per location. Not suitable for locations with more than 150 seats in one location.
- BranchSDO is a great fit for Small to Medium format retailers/services/restaurants/branches with overly simple networks (Kiosks, POS, CC machines, limited back office, limited other tech)
- BranchSDO is a great fit for 1-8 POS Terminals (depending on the CXD) connected directly to the LAN Ethernet Ports (or via single connection from switch)

What are my connectivity needs?
- Employee traffic through Wi-Fi on a dedicated SSID
- Guest traffic through Wi-Fi on a separate dedicated SSID
- Need connectivity continuity through cellular failover

What type of connectivity do I need? DSL, Cable or LTE only?
- BranchSDO is designed as an option for customers to bring their own bandwidth
- However, keep in mind some telcos still deliver static or PPPoE connections. If so, the customer needs to ask for a dynamic connection to avoid connection issues
- The BranchSDO cellular capability is NOT to be used as the primary circuit when broadband is available

How easy is remote troubleshooting on my current solution?
- Easy-to-use analytics allow users to manage and view WAN traffic, LAN network performance and the quality of experience at the edge. Easy at a glance dashboard allow you to monitor device statuses in real time and set proactive usage alerts for optimized 4G LTE data usage, data pooling** (**offered for Managed customers ONLY) among locations, and network uptime.

Does the current solution secure the edge today?
- BranchSDO enables port-based segmentation, which keeps credit card and other sensitive data completely separate from other applications and third-party networks. Taking an approach of “Zero-Trust”, we focus on securing the network from the “inside out vs outside in”.

---

**

**offered for Managed customers ONLY
• Segmenting a single network, creating multiple parallel networks is a relatively simple solution. Separate applications such as guest Wi-Fi, POS, third-party applications, and other store applications are assigned completely separate networks or “air-gapped” networks. This physical separation of the network prohibits attackers from using a compromised device to pivot to other servers and networks, including those that hold sensitive data.

**Does the current solution offer VPN?**

• BranchSDO offers basic site-to-site VPN based SSL\TLS service.
  
  o *Hub-n-Spoke filtering of sites is SOW-based service*

• We do not support IPSec or GRE tunnel termination—however we do support IPSec pass-through allowing tunnels to terminate on a device behind the CXD

**Does the current solution offer and/or enable PCI DSS Compliance?**

• Netsurion offers its direct customers BranchSDO PCI DSS Readiness Package, which provides necessary regulatory functions and reporting related to the network and the device for PCI DSS readiness

• For Managed services, Netsurion can help with QSA and enrollment on Data Breach Financial Protection (DBFP)

• For Self Service and our MSP partners, we can recommend a partner with our eco-system for your PCI DSS needs.

**How does the current solution handle the changing demand for bandwidth?**

• BranchSDO embedded 4G LTE modem with dynamic traffic shaping and QoS allows you to leverage 4G LTE for failover and QoS for port-based bandwidth management

**Other FAQs:**

**The site’s internet is slow. How do I resolve?**

• A slow internet connection can be very frustrating. [Here’s a test](#) that you can run to check internet speeds and [some tips to help improve the experience.](#)

  o **NOTE:** The speed test will not work using a wireless data connection such as 3G, 4G, or LTE. Tests run over a Virtual Private Network (VPN) may also experience errors or slower-than-expected results. Try disconnecting from the VPN and running the test again.

**How fast are solutions being deployed today?**

• Agility is core to the BranchSDO offering. Combining the orchestrator and the CXD, we are able to deploy a solution within minutes instead of days

• The CXD works with the orchestrator to pull down an “initial configuration” that allows you to quickly enable the site
How agile are current deployments?

- BranchSDO orchestration is cloud-based remote management of network and security policies that can be easily assigned at a global or local level; traffic and network analytics providing real-time and historical views

Do I centrally manage hundreds or thousands of deployments?

- Netsurion pairs a compact, yet powerful edge device (BranchSDO CXD) with an intuitive, web-based configuration and management console (BranchSDO Orchestrator). Network administrators can manage thousands of deployments from one central pane of glass, without the need for ground support

How do I upgrade a CXD when needed?

- First, before the upgrade, it is always recommended to re-boot the CXD
- As always, you should refer to the user guide that is located in the orchestrator lower left-hand corner of the dashboard
- Also, to ensure the upgrade takes place, you should always try and leverage a WAN (broadband) circuit - most firmware upgrades require a consent bandwidth
- The steps are: Login to the BranchSDO Orchestrator and access the specific CXD. In the “Configuration” tab select the drop down for “Upgrade” or refer to the user guide

When best effort internet may fail you

- Every hour for internet downtime costs retailers ~$8,000\(^1\) vs spending less than a dollar a day for wireless failover

\(^1\)Source: [https://cloudscale365.com/blog/high-cost-of-internet-downtime/](https://cloudscale365.com/blog/high-cost-of-internet-downtime/)
BranchSDO CXD

Purpose built for multi-location business endpoints, equipped with built-in cellular and Wi-Fi modems, the CXD 2500 and CXD 2800 are designed to simplify any deployment that requires a redundant, integrated, secure, compliant and segmented solution. This is ideal for small remote locations that want the highest level of redundancy and availability. The CXDs are simple to deploy and minimal pre-configuration is necessary.

How to approach and define segmenting the CXD?

Inserted in this document are example templates that can be used as a way to quickly create a segmentation that enables “inside out vs outside in” segmentation. These templates can help you to quickly determine how to configure the CXD.

BranchSDO Site Segmentation Example
How to decide which CXD model do I need?

<table>
<thead>
<tr>
<th>Features/Options</th>
<th>CXD 2500 AT&amp;T</th>
<th>CXD 2500 VZW</th>
<th>CXD 2800 VZW/AT&amp;T</th>
</tr>
</thead>
<tbody>
<tr>
<td>Customer Type</td>
<td>Small</td>
<td>Small</td>
<td>Med</td>
</tr>
<tr>
<td>Processor</td>
<td>580 MHz MIPS 24k CPU Core, 128MB or DDR2 RAM</td>
<td>580 MHz MIPS 24k CPU Core, 128MB or DDR2 RAM</td>
<td>717MHz, quad core arm A7 CPU 1GB RAM, 256MB DDR3</td>
</tr>
<tr>
<td>Form Factor</td>
<td>Desktop, Wall Mount</td>
<td>Desktop, Wall Mount</td>
<td>Desktop, Wall Mount</td>
</tr>
<tr>
<td>Cloud Management</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>Total LAN Network Interfaces</td>
<td>4 10/100Mbps</td>
<td>4 10/100Mbps</td>
<td>9 10/100/1000Mbps</td>
</tr>
<tr>
<td>Total WAN Network interfaces (LAN ports Switchable)</td>
<td>4</td>
<td>4</td>
<td>4</td>
</tr>
<tr>
<td>MPLS</td>
<td>No</td>
<td>No</td>
<td>No</td>
</tr>
<tr>
<td>IPsec Tunneling</td>
<td>No</td>
<td>No</td>
<td>No</td>
</tr>
<tr>
<td>USB 2.0 Port</td>
<td>N/A</td>
<td>N/A</td>
<td>Yes</td>
</tr>
<tr>
<td>Flash</td>
<td>N/A</td>
<td>N/A</td>
<td>Up to 128MB</td>
</tr>
<tr>
<td>Routing</td>
<td>IPV4</td>
<td>IPV4</td>
<td>IPV4</td>
</tr>
<tr>
<td>VPN Tunneling to Netsurion Gateway</td>
<td>SSL/TLS</td>
<td>SSL/TLS</td>
<td>SSL/TLS</td>
</tr>
<tr>
<td>Dual WAN</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>VLANs</td>
<td>15</td>
<td>15</td>
<td>15</td>
</tr>
<tr>
<td>Stateful FW</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
</tbody>
</table>
Which features should I turn on?
SD-WAN products come with a variety of security and networking features. Understanding the benefits and tradeoffs of these features is crucial to getting the maximum-benefit without unnecessary performance degradation.

<table>
<thead>
<tr>
<th>Feature</th>
<th>Benefits</th>
<th>Performance Impact</th>
<th>Recommendations</th>
</tr>
</thead>
<tbody>
<tr>
<td>Deep Packet Inspection (DPI)</td>
<td>From packet inspection-can act as an intrusion detection combining BranchSDO Global profiles</td>
<td>High</td>
<td>Deep packet inspection can <strong>slow down your network</strong> due to the resources required to handle the increased processing load. Disabling DPI can improve the network’s speed.</td>
</tr>
<tr>
<td>Auto VPN</td>
<td>Secure, encrypted traffic between locations</td>
<td>Medium</td>
<td>You should consider offloading traffic to the broadband circuit vs backhauling across the VPN, and deploy the on-board security services at the edge for internet traffic. Max VPN throughput for 2500 is</td>
</tr>
<tr>
<td>BranchSDO SD-WAN Best Practices</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>----------------------------------</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Family Friendly Content Filtering</th>
<th>Using DNSSec. (208.67.222.123 or 208.67.220.123) Blocks known adult and potentially controversial or sensitive internet content, web proxies and anonymizers, and known phishing sites.</th>
<th>Low</th>
<th>Disabling this feature could have an impact on your content and allowing for inappropriate information to be visible</th>
</tr>
</thead>
<tbody>
<tr>
<td>URL/White/Black Listing</td>
<td>IP addresses, Hashes, Email addresses, and URLs that can be classified as known good (white list) or known bad (black list). Other security policies will be bypassed for white/black-listed traffic, with all white list traffic being allowed and all black list traffic being blocked.</td>
<td>Medium</td>
<td>Keep the number of white/black list below ~150 entries. Leverage FQDN as an option.</td>
</tr>
<tr>
<td>Port-Based QoS</td>
<td>QoS is designed to ensure that high-priority services maintain sufficient internet access.</td>
<td>Medium</td>
<td>Define based on a specific port and traffic profile for the best use</td>
</tr>
<tr>
<td>Segmentation</td>
<td>Assign completely separate networks, or “air-gapped” at port level</td>
<td>Low</td>
<td>Max 15 VLANs (includes 4 SSIDs).</td>
</tr>
<tr>
<td>Logging</td>
<td>Audit Log and Audit trail</td>
<td>Low</td>
<td>**CXD Audit logs are not traditional sysLogs—however, they do meet PCI DSS in combination with the Audit Trail within the Orchestrator</td>
</tr>
</tbody>
</table>

**Note:**

Audit Logs: For PCI DSS compliance. Endpoints connecting/disconnecting (Wi-Fi + DHCP), endpoints accessing the internet (flow information) (to get endpoint flow information, DPI MUST be enabled)

Audit Trial: Any "Edit"->"Save" operations done on Orchestrator. What was edited? Who edited? And when?
Appliance Benchmarks

Benchmarks are designed to help compare BranchSDO CXD appliances to other vendors. These tests assume perfect network conditions with ideal traffic patterns. When measuring maximum throughput for a certain feature, all other features are disabled. Actual results in production networks will vary.

<table>
<thead>
<tr>
<th></th>
<th>CXD 2500</th>
<th>CXD 2800</th>
</tr>
</thead>
<tbody>
<tr>
<td>Connected Wired Clients</td>
<td>30</td>
<td>75</td>
</tr>
<tr>
<td>Max throughput with all security features enabled (w/DPI)</td>
<td>45Mbps</td>
<td>550Mbps</td>
</tr>
<tr>
<td>Max Stateful firewall throughput in passthrough mode</td>
<td>80Mbps</td>
<td>750Mbps</td>
</tr>
<tr>
<td>Max VPN throughput</td>
<td>10Mbps</td>
<td>25Mbps</td>
</tr>
<tr>
<td>Max concurrent VPN Tunnels</td>
<td>200</td>
<td>300</td>
</tr>
<tr>
<td>Max Network Objects</td>
<td>180</td>
<td>300</td>
</tr>
<tr>
<td>WAN to LAN Port Forwarding Objects</td>
<td>100</td>
<td>200</td>
</tr>
<tr>
<td>Static routes</td>
<td>100</td>
<td>300</td>
</tr>
<tr>
<td>LAN to LAN Objects</td>
<td>20</td>
<td>30</td>
</tr>
<tr>
<td>WAN to LAN NAT’ing</td>
<td>150</td>
<td>250</td>
</tr>
<tr>
<td>Traffic Steering (LAN to WAN)</td>
<td>14 Entries</td>
<td>30 Entries</td>
</tr>
</tbody>
</table>

How many Wi-Fi clients can I have on a CXD and Extended Access Point?

Although there is no hard limit on the number of client devices that can be deployed, for purposes of this “best practices” document all tests were performed with the client counts shown in the table below. Exceeding these client counts may result in performance that varies based on DPI on and DPI off.

<table>
<thead>
<tr>
<th></th>
<th>CXD 2500</th>
<th>CXD 2800</th>
<th>A62 Extended Wi-Fi</th>
</tr>
</thead>
<tbody>
<tr>
<td>No DPI Recommended direct Wi-Fi client devices</td>
<td>50</td>
<td>115</td>
<td>145</td>
</tr>
</tbody>
</table>
What about the Integrated Wi-Fi within the CXD?
The on-board Wi-Fi modem in the CXD 2500 supports 802.11 b/g/n protocols in a 2.4 GHz single band mode. 4 unique SSID’s are supported with VLAN segmentation if desired. The 2.4GHz band supports 3 non-overlapping channels 1, 6, 11. Interference from microwave ovens, Bluetooth devices, and cordless phones is expected in that range. The range for 2.4GHz is 60-90 feet or more or about 1500 square feet from the Wi-Fi modem. The number of connected users will vary as the 2.4 GHz can support up to 130 Mbps per connection. However, the number of available non-overlapping channels is limited. Expect decent throughput with 5-10 users, degrading thereafter (your customer’s internet connection must support this number of users as well).

The on-board Wi-Fi modem in the CXD 2800 supports 802.11 b/g/n/ac protocols in a dual-band 2.4 GHz/5 GHz mode with MIMO technology to deliver faster connections with wider channels. Expect decent throughput with xxx users, degrading thereafter (your customer’s internet connection must support this number of users as well).

<table>
<thead>
<tr>
<th>CXD 2500</th>
<th>CXD 2800</th>
</tr>
</thead>
<tbody>
<tr>
<td>802.11 b/g/n Access Point</td>
<td>802.11 ac/a/b/g/n Access Point</td>
</tr>
<tr>
<td>2.4 GHz ISM band</td>
<td>2.4 and 5GHz ISM band 2x2 MIMO</td>
</tr>
<tr>
<td>15-25 users</td>
<td>150 users</td>
</tr>
<tr>
<td>maximum client speeds 80 Mbps</td>
<td>maximum client speeds 290 Mbps</td>
</tr>
<tr>
<td>4 SSID’s</td>
<td>4 SSID’s</td>
</tr>
</tbody>
</table>

Integrated LTE
The CXD 2500 is a single SIM with Verizon as a default connection. AT&T SIM’s have a longer provisioning time. The CXD 2500 is perfect for IoT applications where small bytes of data are sent over the 4G network or for POS environments. VPN is available on both models and cellular failover with a “failsafe” VPN experience is also available on both models. *T-Mobile has been tested but this is a BYOS (bring your own SIM) process and only available for specifically approved customers. The CXD 2800 is a dual SIM unit with both Verizon and AT&T cards. The CXD 2800 has “carrier detection” and the SIM with the strongest signal will be the default primary LTE WAN upon turnup.

<table>
<thead>
<tr>
<th>CXD 2500</th>
<th>CXD 2800</th>
</tr>
</thead>
<tbody>
<tr>
<td>Integrated 4G LTE CAT1</td>
<td>Integrated 4G LTE CAT4</td>
</tr>
<tr>
<td>LTE Bands 2,4,13</td>
<td>LTE Bands 2,4,12,13,14</td>
</tr>
<tr>
<td>CAT1 Speed 10 Mbps</td>
<td>Cat4 Speed 150 Mbps</td>
</tr>
<tr>
<td>Single SIM (Verizon-AT&amp;T)</td>
<td>Dual SIM (AT&amp;T, Verizon, *T-Mobile)</td>
</tr>
<tr>
<td>Single SIM</td>
<td>Carrier detection at turn up</td>
</tr>
</tbody>
</table>

*Note: T-Mobile is supported but as part of a bring your own cellular option.*
Sample deployment options and use cases

No Existing Security

Existing Integrated Router Firewall

BranchSDO Deployment Option #1
- Only trust traffic runs through SD WAN / Non-trust traffic runs directly to router
- Strong PCI configuration

BranchSDO Deployment Option #2
- All traffic runs through SD WAN
- Increased standardization speeds deployment
- Limited control over bandwidth impacts QoS

BranchSDO Deployment Option #3 (NetSuron FWs only)
- All traffic runs through existing firewall then SD WAN
- Segmentation by ports routes trust traffic through UTM / non-trust goes directly out to web
- Strong QoS control

BranchSDO Deployment Option #3 (NetSuron FWs only)
- All traffic runs through existing firewall then SD WAN
- Segmentation by ports routes trust traffic through UTM / non-trust goes directly out to web
- Strong QoS control
Common Deployment Options

**Broadband + LTE**
- Ideal for branches and/or remote locations
- Suitable for small branch sites
- Broadband access with optional split tunnel
- Carrier-agnostic LTE/4G backup for high availability

**Dual Broadband + LTE**
- Ideal for branches locations and/or remote carrier redundancy
- Carrier-agnostic LTE/4G backup for high availability

**Dual Broadband**
- Ideal for branch locations and/or networks without MPLS
- For high availability locations carrier dependency
About Netsurion
Netsurion powers secure and agile networks for highly distributed and small-to-medium enterprises and the IT providers that serve them. In such environments, the convergence of threat protection and network management are driving the need for greater interoperability between the NOC (network operations center) and the SOC (security operations center) as well as solutions that fuse technology and service to achieve optimal results. To this end, Netsurion has converged purpose-built network hardware, innovative security software, and flexible managed services.

Netsurion’s SD-Branch solution, BranchSDO, is a comprehensive network management and security solution consisting of SD-WAN, next-gen security, cellular, Wi-Fi, and PCI DSS compliance tools and support. At the heart of the solution is the CXD, Netsurion’s SD-WAN edge appliance.

Netsurion’s Security Operations solution, EventTracker, delivers advanced threat protection and compliance benefits in a variety of deployment options: a SIEM platform, a co-managed SIEM service with 24/7 SOC, and a managed SIEM for MSPs.

Contact Us
Corporate Headquarters
Netsurion
Trade Centre South
100 W. Cypress Creek Rd
Suite 530
Fort Lauderdale, FL 33309

Sales
Toll Free: (877) 333-1433 x 1
Tel: (410) 953-6776 x 1