netcloud™ by cradlepoint

NetCloud Exchange

Secure Connect, SD-WAN, ZTNA, and the Service Gateway

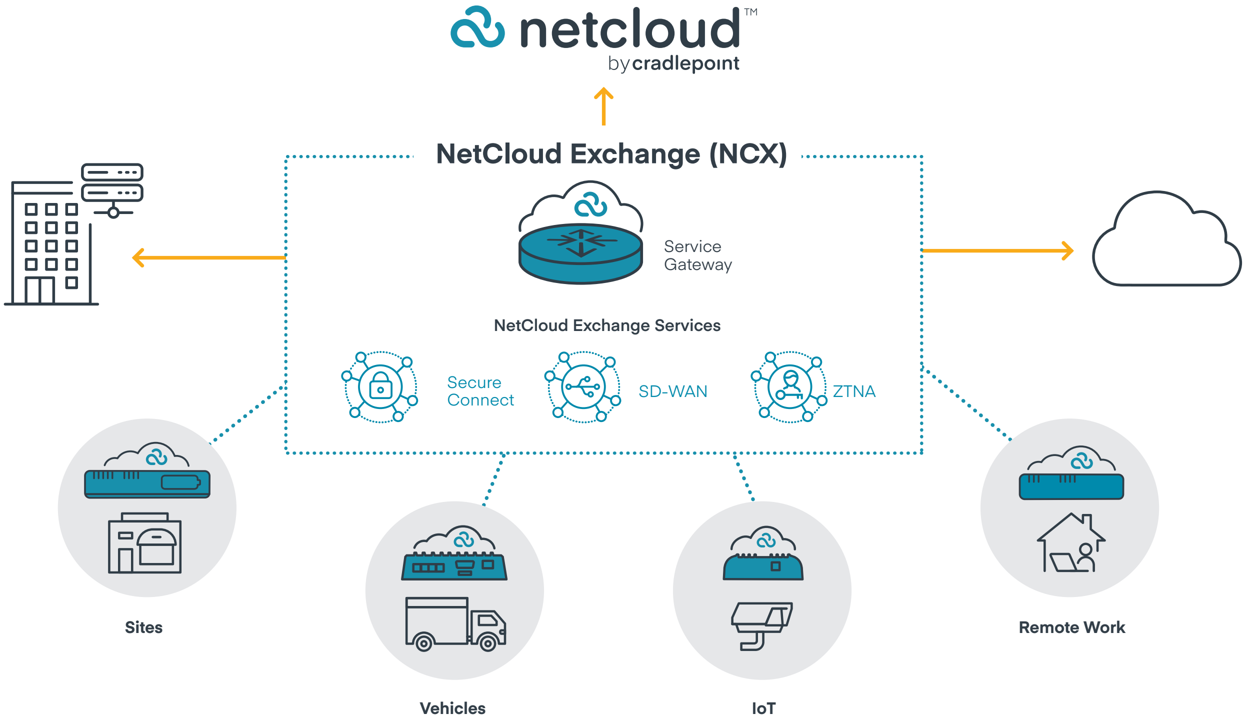
As an extension to Cradlepoint NetCloud Service, NetCloud Exchange (NCX) is a cloud-native WAN architecture that integrates advanced SD-WAN, security, and 5G — sharing common components, policies, and processes — all managed through a single pane of glass. NCX offers the following services.

NCX Service Gateway is the service delivery foundation for NCX and provides the secure data-plane and policy enforcement capabilities for Cradlepoint routers in sites, vehicles, IoT, and remote workers to digital resources in the cloud, data center, and external sites. The gateway houses the common engines that power SD-WAN, ZTNA and subsequent security services at the network level. Delivered for a virtual infrastructure, cloud environment, or downloaded onto a physical server, the Service Gateway can be delivered on-premises or in a hosted environment. The Service Gateway is easily provisioned via NetCloud and managed like other Cradlepoint solutions and is compatible with both existing and future Cradlepoint routers.

NCX Secure Connect is a network security solution that offers a simple-to-manage alternative to complex VPN infrastructures for securely connecting sites, vehicles, IoT, and remote workers. NCX Secure Connect provides any-to-any connectivity and drastically reduces the attack surface by building undiscoverable network resources. Secure Connect unlocks operational agility through built-in tunnel orchestration and simplifies configuration with name-based routing and overlapping IP addressing.

NCX SD-WAN service delivers SD-WAN with a specific focus of optimizing traffic over Wireless WANs. Cellular-centric enterprises can amplify their LTE/5G experience while realizing the benefits of enhanced SD-WAN built for wireless scale and simplicity. Organizations can easily enhance application quality of experience and optimize traffic across redundant cellular providers and across hybrid WANs. Secure Connect service is a pre-requisite for the NCX SD-WAN service.

NCX ZTNA service leverages fine-grained policies, identity and context information to grant users zero trust access to corporate resources. Instead of providing shared access to network segments, connections are defined to corporate resources and are only built upon authentication. NCX ZTNA proactively maintains the security posture with continuous verification. Organizations can protect commonly unprotected devices by placing them into trust segments using Cradlepoint routers and access is provided using a selection of clientless and client-based options.



| cradlepoint.com

cradlepoint PART OF ERICSSON

Key solution capabilities

Simplified configuration

NetCloud Exchange simplifies the cumbersome process of IP addressing in deploying new sites for simplified setup and faster network rollout. By allowing reuse of IP addresses, and an easier to understand name-based addressing scheme, Secure Connect is significantly easier to deploy across thousands of locations and eliminates complex network configurations for higher operational efficiency and agility. Once the secure connectivity is established, traffic and user-based policies can be set up and applied across the distributed edge, giving administrators granular control and deep visibility into the users and their authorized applications.

Secure foundation

NetCloud Exchange establishes a zero-trust foundation as soon as it is deployed by eliminating default network level access and only allowing access to defined resources. When Secure Connect links Cradlepoint routers through the NCX Service Gateway, the networking, application, and data details become obscured to outside elements, which makes the IP addresses undiscoverable. This private networking scheme locks out external access and significantly reduces the attack surface to explicit resources defined by the ZTNA service.

ZTNA restricts resource users from moving to unauthorized parts of network using existing SAML 2.0 identity sources and context, through micro segmentation and explicit access. Using the fine-grained policies from the central policy engine and identity store, users with different levels of risk can access the same resources appropriately without sharing the same network. This single policy engine and native environment improves performance by eliminating the latency that exists between multiple policy engines and their potential for conflicting instructions.

Scalable and cloud native

NetCloud centralized, cloud management provides end-to-end visibility for users, devices, and applications with dashboards, analytics, and insights. The edge nodes, the Service Gateway, and the Secure Connect and SD-WAN, and ZTNA services are deployed, orchestrated, and managed through NetCloud to automate processes and unlock services as needed to scale. Additional resiliency can be added to the Service Gateway deployment by choosing the optional high availability bundle.

Streamlined traffic management

For organizations seeking the best possible user experience and a reduction in network costs, NCX SD-WAN is designed to take the complication out of SD-WAN and optimize cellular usage. Built on zero-trust principles and the Secure Connect foundation, NCX SD-WAN capabilities reside at the network level leveraging shared functions like profiling over 3,500 applications and providing visibility into end-to-end traffic flows.

Learn more at **cradlepoint.com/netcloud-exchange**

Key benefits:

- Orchestrates Secure Connect tunnels between the Cradlepoint routers and the Service Gateway to deliver SD-WAN and ZTNA services at scale
- Simplifies IP address management by allowing overlapping IP addresses with Private NAT techniques
- Reduces network attack surfaces by using invisible network resources, and explicit access
- ZTNA functionality focused on privileged remote access and extended workforce remote access and BYOD
- Application and security -based policies that can be implemented network-wide in a few simple steps
- Captures network traffic flows and delivers this data for visibility in NetCloud Manager dashboards
- Ability to optimize traffic across multiple WAN connections (cellular, wired, and Wi-Fi as WAN)
- Application engine recognizes over 3,500 applications
- Cellular optimization including carrier-centric traffic steering, inline traffic measurement, and cellular-centric policy criteria (such as signal strength and data usage)
- Direct Internet Access from sites
- Visibility into the performance of applications down to the individual SaaS data center
- Service Gateway operates in virtual infrastructure, cloud environments, or as software on customer-hosted servers
- Service Gateway deploys as standalone gateway or as a resilient, high-availability active/standby cluster

cradlepoint PART OF ERICSSON