NetCloud PERIMETER

Next-Generation WAN: Software-Defined Perimeter

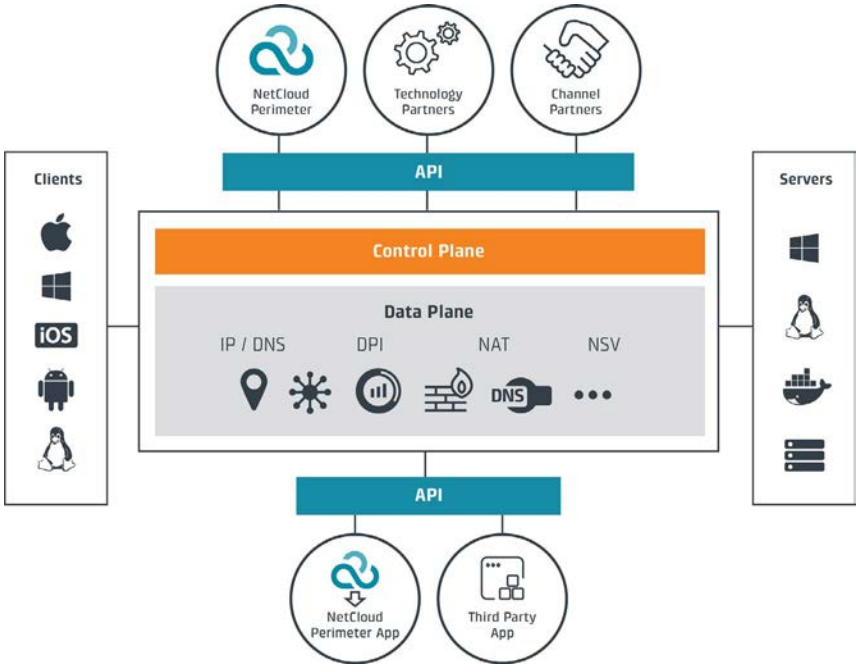
NetCloud Perimeter provides a simple, cloud-based alternative to VPN. It allows companies to build and deploy virtual overlay networks in minutes, connecting all their IoT devices and remote and mobile workers to business-critical resources. Offering cloud-based security, the NetCloud Perimeter service eliminates the hardware, complexity, and operational costs of traditional WANs. It enables easy deployment of changes at the network edge while maintaining security, visibility, and control as business requirements evolve.

Now IT teams can build and deploy secure virtual overlay networks in minutes to connect:

- Remote or mobile workforces using Windows, iOS, Android, or Linux devices
- IoT devices such as: kiosks, digital signs, cameras, sensors, meters, etc.

And create a software-defined perimeter—across the Internet or any private or public cloud.

NetCloud Perimeter works with existing network and security infrastructures. It requires no hardware or configuration, scales instantly, and is subscription-based. Build multiple secure overlay networks, tailored for purpose and per account, to scale and perform independently based on business needs.



Key Features:

Simplicity

- Deploys in minutes
- No configuration
- No changes to existing network infrastructure

Security

- Encrypted data-in-transit (256-bit AES)
- No data stored in cloud
- Cloaked IP address space
- Enables micro-segmentation for zero-trust WANs
- Certificate-based Auto-PKI (X.509 CA)

Reliable

- Runs on top-tier cloud providers around the world
- Fully redundant architecture
- Self-healing, self-optimizing
- Seamless failover

OS Support

- Windows 7/8, Mac 10.7+
- Windows, Android, & iOS phones & tablets
- Windows 2008R2 / 2012 & Linux servers
- Docker containers

Multi-Layer Security: Protects End-to-End, Everywhere

As enterprises continue to embrace workforce mobility, BYOD, and public cloud, protecting network borders and endpoints is no longer sufficient. NetCloud Perimeter's security foundation is a multi-layer, network-based approach to security that protects users, devices, and workloads wherever they're deployed. Key elements include:

- **Secure Overlay:** Abstraction of logical network & address space from the Internet
- **Encryption:** Protects data in-transit end-to-end with the strength of 256-bit encryption
- **Network Virtualization:** Enables zero-trust WANs through micro-segmentation
- **Multi-layer Authentication:** Device, virtual network, domain & certificate level
- **Secure Internet Access** sends all traffic from target IoT devices through the dark virtual cloud network

These security building blocks help protect against a myriad of network-based attacks:

- IP address-related attacks (port scans, spoofing, DNS poisoning, & DDoS)
- Packet sniffing exploits (Firesheep & other nefarious sniffing programs)
- Authentication hacks (unchanged passwords, brute force & single factor)

Zero-Trust WANs: Contain Threats When & Where They Happen

As more subnets connect over the WAN, the "attack surface" of a breach or malware infection grows both inside or outside the firewall. To significantly limit the impact of such events, NetCloud Perimeter's virtual networks can be microsegmented on a site, departmental, or even user- and device-level. The result is a zero-trust WAN that automatically isolates threats and quarantines them when and where they happen.

Rapid Deployment: Define in Minutes, Deploy With Your Tools

Define and deploy virtual networks, connect local and remote users, small offices, IoT devices and sensors, kiosks, digital signage, and even VMs, containers, and servers in minutes rather than days. NetCloud Perimeter works with popular automation, orchestration, and client software distribution tools, including Puppet, Chef, and Microsoft SCCM.

Business Benefits

- Reduce WAN-related OPEX
- Eliminate hardware costs & complexity
- Pay as you grow
- Rapidly connect your mobile workforce & IoT devices securely no matter their location
- Enhance security & compliance
- Enable BYOD

Use Cases:

IoT Devices, Sensors

- Connect IP-enabled devices to secure network
- Enable remote control & management
- Leverage LTE & WiFi connections to eliminate costly cabling
- Reduce time to deploy from days or hours to minutes

Enable Access to Resources Anywhere

- Micro-segment networks with policy engine to enable appropriate access
- Connects any private & public cloud
- Provide application access across providers
- Extend existing networks without additional infrastructure
- Scales up/down instantly

Remote/Mobile Access

- Global availability
- Windows, Android & iOS mobile device support
- Persistent, always-on
- LAN experience
- Zero-trust—isolate access to select servers

Extend Active Directory Domains

- Maintain domain security
- Keep remote users always connected to AD domain from anywhere
- No user action required
- Eliminate cached passwords
- Instantly push policy & security patches
- Enforce AD DNS use

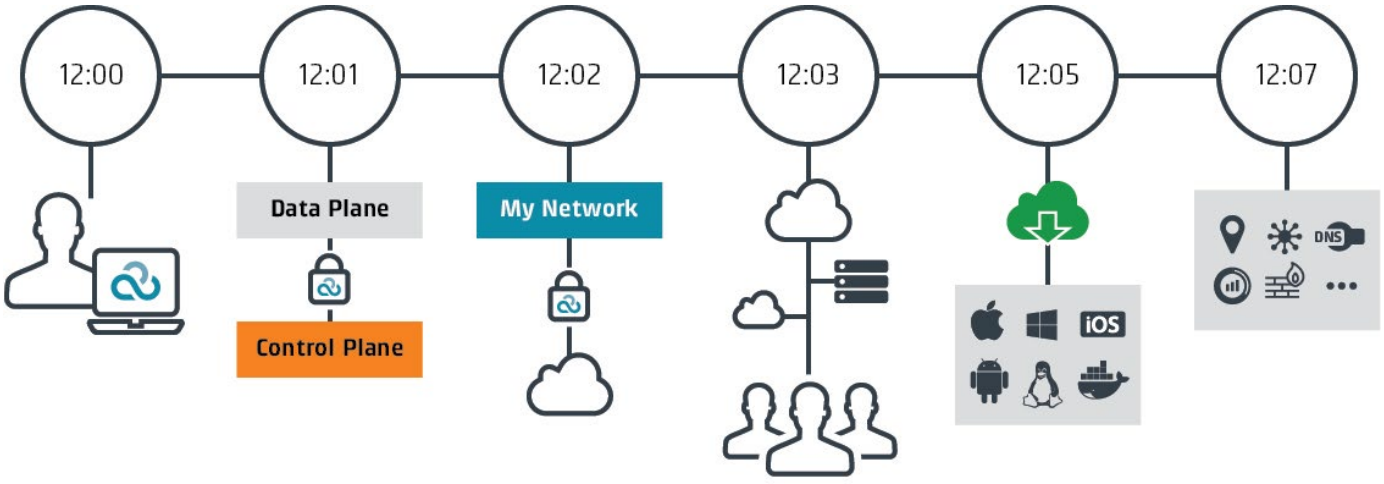
Virtualized Services within NetCloud Perimeter

Extend the visibility, security, and control of perimeter networks within NetCloud Perimeter. In a few clicks, you can add services such as Active Directory integration, security policy deployment and micro-segmentation, and network bandwidth monitoring.

Power of the Cloud: Global Reach, Enterprise Scale, Full Resiliency

The NetCloud Perimeter platform overlays top-tier cloud data centers around the world, including Amazon AWS, Rackspace and Digital Ocean. This enables massive scale to accommodate large networks and traffic loads, and local points of presence to 80 percent of the world's computing population. When a disruption occurs, the platform's SDN and multi-cloud architecture enables affected networks to be automatically migrated to another data center—often within the TCP protocol connection timeout—so users' sessions are maintained and users themselves are often unaware of any issue.

LEARN MORE: **CRADLEPOINT.COM/NETCLOUD-PERIMETER**



12:00: Administrator names network. NetCloud Perimeter spins up L3 switch in cloud.
12:01: NetCloud Perimeter's Data Plane securely calls Control Plane to allocate network.
12:02: NetCloud Perimeter secures network with PKI & 256-bit AES encryption. Network is allocated.
12:03: Administrator adds devices to network, invites users, adds devices, servers, VMs, and even containers.
12:05: Users download on preferred OS enabling them to communicate securely, be located anywhere and be more productive!
12:07: Administrator layers on services—ADConnect, GeoView, Application Monitor, Firewall, IDS, etc.