cherry

cherry-solutions.com

Cherry SDP

Improve your network security with Cherry's Software Designed Perimeter that trusts nobody and verifies everything.

Introducing Cherry SPD

Cherry SDP is the world's first Software Designed Perimeter (SDP) that integrates Network Access Control (NAC) to realize the Black Cloud of perfect SDP security.

Cherry SDP is an open, user ID-centric network security solution designed to improve the limitations of existing network-centric security.

VPNs: a thing of the past?

Network security is growing increasingly important, especially in the age of COVID-19, when more people are working from home outside of company networks.

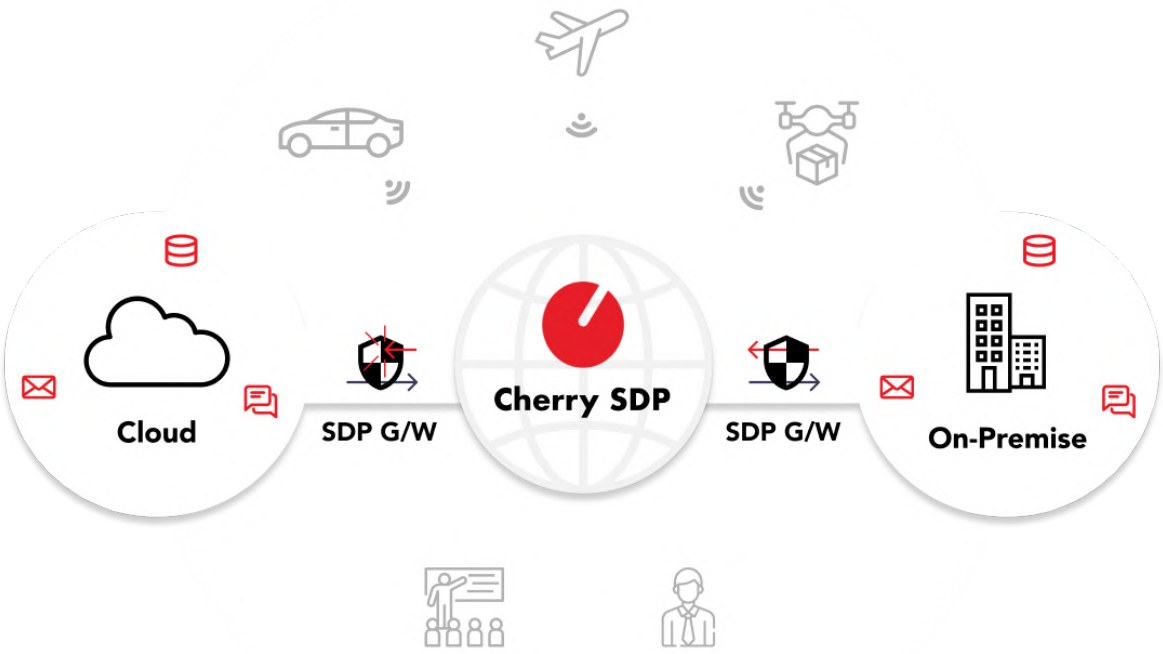
However, legacy network access control such as VPNs are coming under fire for a number of serious shortcomings:

- Increased cybersecurity threats
- Lack of control or visibility
- They are expensive and complex

Software Defined Perimeter (SDP) solutions offer a remedy.

The motto of an SDP is “trust nobody, verify everything” - all users are authenticated and authorized, and all devices are verified.

Unlike VPNs, SDPs provide centralized network access control, are highly scalable, offer identity-centric user authentication and guarantee enhanced security with no lateral movement.



Cherry SDP - Trust nobody, verify everything

Cherry SDP

Cherry SDP connects communications securely outside the company, controlling applications associated with “privileges granted to users”. This allows individuals and businesses to operate free of security concerns.

Control over network access devices

Prevent unauthorized or unregistered devices (laptop, desktop, mobile) from starting connections, using SDP authorization.

Risk-based policy support

SDP’s system makes access decisions based on a variety of risk criteria, including threat information, malware proliferation and new software.

Promiscuous network access restrictions

Because of policies that restrict access to certain services and hosts, access to the network segmanet or subnet is not granted. This minimizes the network attack area and prevents malicious users or software from scanning ports and vulnerabilities.

Control application and device access

SDP can specify programs and devices that can access services, preventing malicious users or malware from connecting to the resource.

Connect anything

With SDP technology, you can connect to the IT services your employees need without having to pay for additional administrative management or hardware.

With Cherry SDP, you can secure your network, do business anywhere in the world with unlimited space, control IoT devices and save money through reduced infrastructure costs - no dedicated line needed.

Functions

The solution is infinitely scalable, and service targets and permissions can be flexibly fine-tuned.

Server stealth:

Hides network information to make it difficult for attackers to identify targets.

DDOS attack prevention:

Blocks transmission of non-authorized packets through use of Single Packet Authorization (SPA).

Dynamic Firewall:

Whitelist-based firewall with ability to permit or block access in real time. If there is no access within a few seconds, it changes to blocking status.

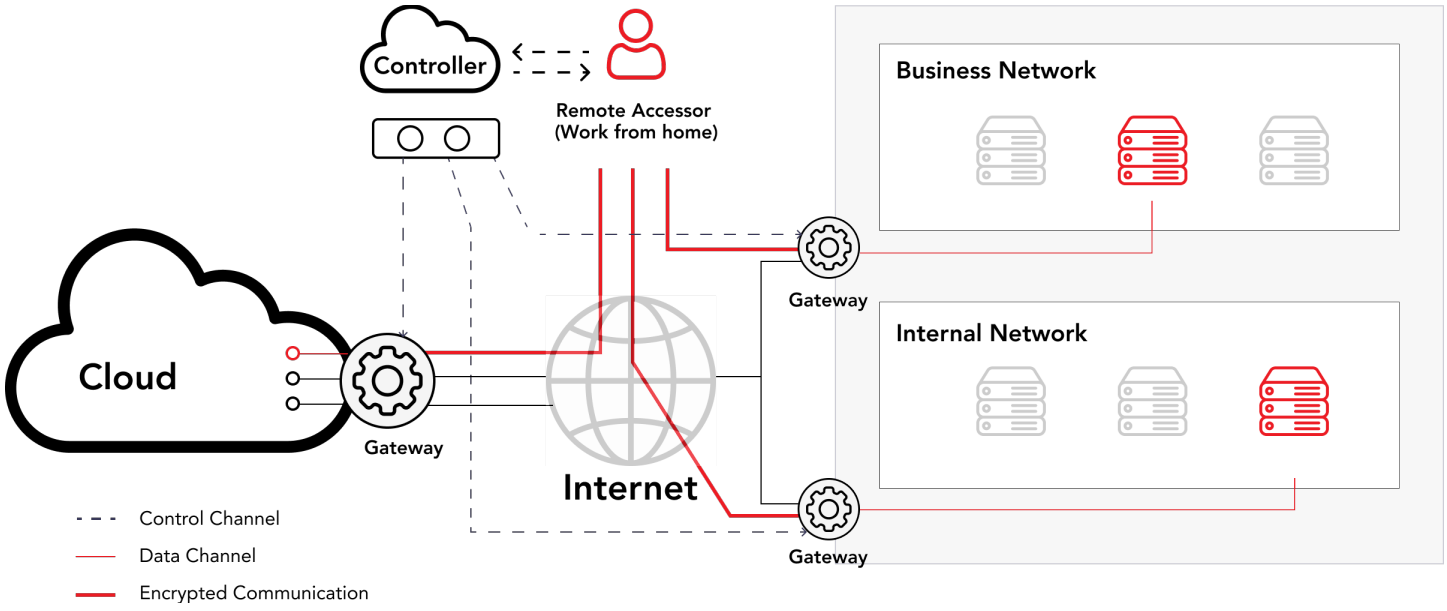
App Binding:

SDP communication is possible only for applications registered by the administrator.

Safe Networking:

Provides a secure network by IPSEC secure tunnel communication.

Cherry SDP architecture



Get in touch with our team

info@cherry-solutions.com

www.cherry-solutions.com

Cosmo Tower, 326, Wangsimni-ro,
Seongdong-gu, Seoul, Republic of Korea