Secure Remote Access

SOLUTION BRIEF

Enable secure remote access with granular controls for mobile users or third parties

Users work anytime and anywhere

Users work anytime and anywhere these days. Hence, they need to have the possibility to seamlessly and securely access all internal resources independent of where they are.

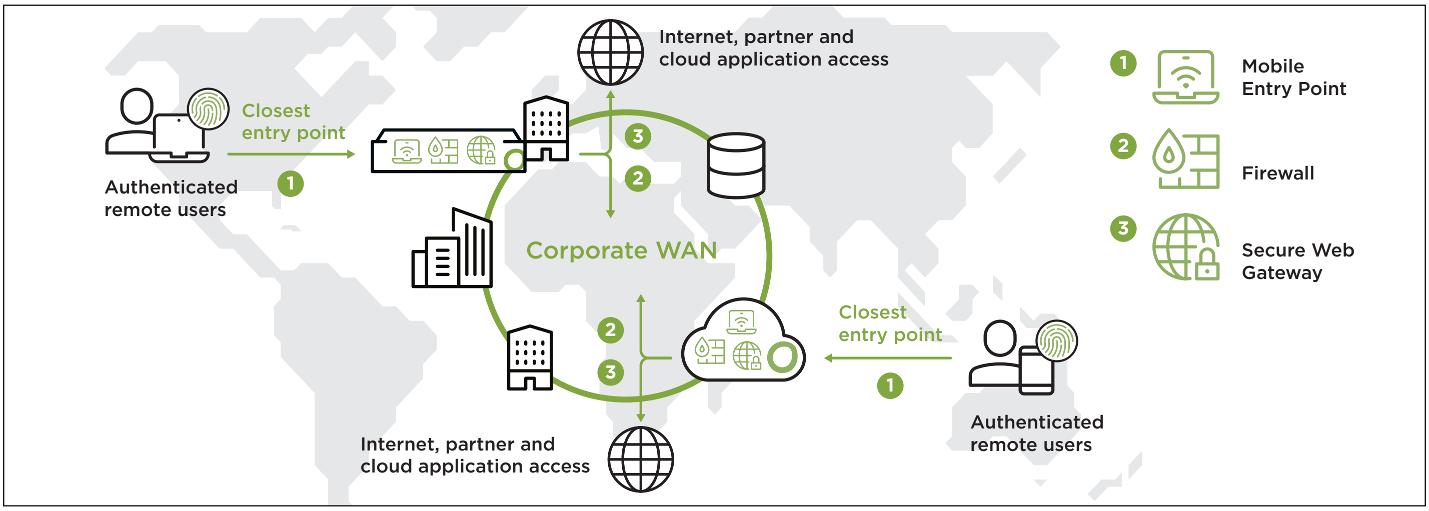
Enforcing security policies is especially important for mobile users. In addition, users should be protected from internet threats when browsing on their corporate devices, even if they are traveling and are not in the office. Nevertheless, the user experience should not differ when connected remotely.

Different security policies might be necessary due to third parties requiring access to specific resources in the corporate network such as data and machines.

A secure access solution

Open Systems provides secure remote access for mobile users. Connected users can surf the internet while being protected by the Secure Web Gateway service, or access corporate resources in the company network.

Secure Remote Access by Open Systems


Internet, partner and cloud application access
Closest entry point
Authenticated remote users
1
3
2
Corporate WAN
2
3
Closest entry point
1
Authenticated remote users
Internet, partner and cloud application access
1 Mobile Entry Point
2 Firewall
3 Secure Web Gateway

Global coverage

By deploying Mobile Entry Points (access points) to existing or additional SD-WAN edge devices, global coverage can be provided to your mobile users.

Due to the deployment on SD-WAN edge devices, a reliable and secure connection to the corporate WAN is provided.

Secure access

The built-in firewall functionality allows granular control from connected mobile users to internal and external resources based on the user’s authorization level.

In combination with the Secure Web Gateway, the Mobile Entry Points provide secure internet access for mobile users.

Expert-level operations

Enjoy the peace of mind that 24x7 monitoring, incident handling, and change management brings – provided by our L3 engineers.

Central policy setup and control allows you to enforce global security policies and configuration.

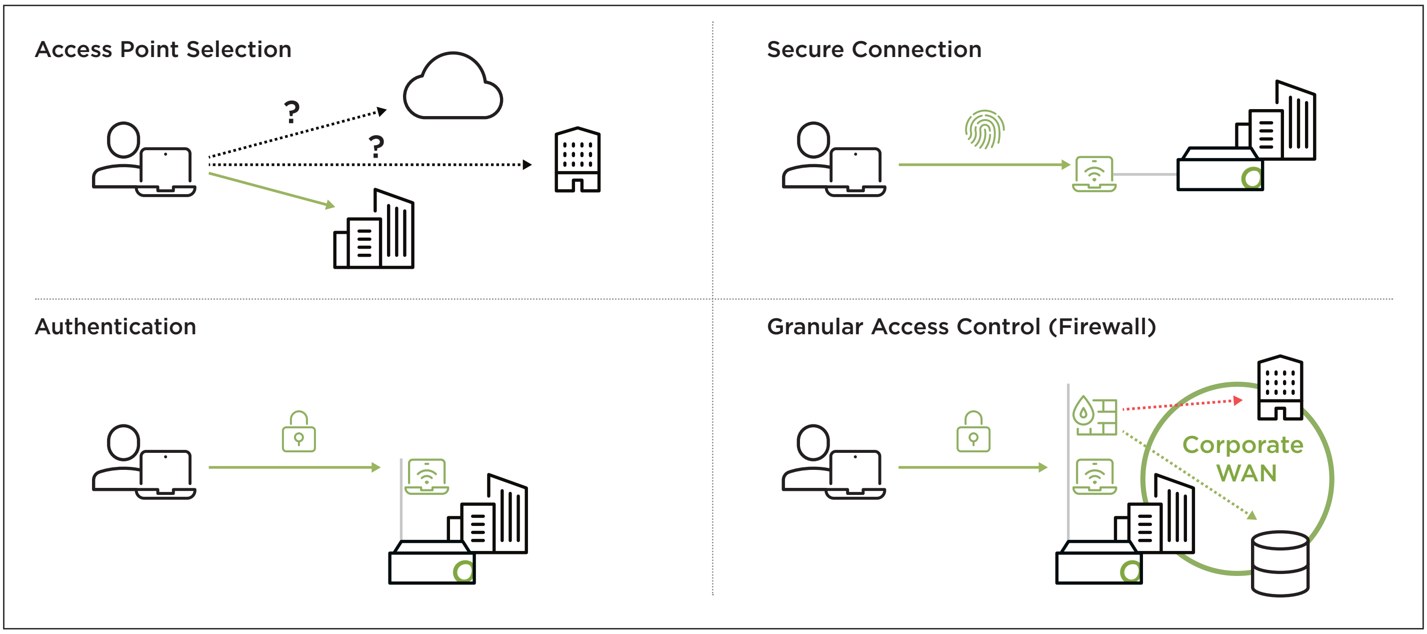
How does the Secure Remote Access solution work?

Access Point Selection: Either fixed, manually selectable, or using a GeoDNS provider of choice, the right Mobile Entry Point is selected (on-premises or in the cloud).

Authentication: Depending on a customer's requirements, authentication can either be done using username/password or a combination of user credentials and software/hardware token. Using certificates further improves the security or even allows seamless user authentication by using the certificate only.

Secure Connection: A secure and encrypted (DTLS) connection is established between the client and a Mobile Entry Point so that the exchanged traffic is encrypted and remains private.

Granular Access Control (Firewall): By assigning users to different corporate access groups, the access to corporate resources can be differentiated either globally or on specific Mobile Entry Points.



Corporate Access

Corporate Access supports an organization's mobile workforce and partner collaboration by providing secure access to corporate network resources. It establishes a network-level connection, allowing clients such as personal computers, laptops, and mobile phones to access network resources from home or from anywhere in the world as if they were on site. Clients are authenticated according to the organization's policy, and access to corporate resources is restricted based on user groups.

Mobile Web Security

In combination with the Secure Web Gateway, the Mobile Entry Point provides secure internet access for mobile users. With Mobile Web Security, remote users can surf the internet while being protected by the Secure Web Gateway service.

Multi-factor authentication

Multiple authentication flows can be configured for different connections. In combination with the Identity Server, the users can be synced from the Windows Active Directory. Two-factor authentication can be used and managed in the Open Systems Customer Portal. In combination with Azure AD/MFA or other Identity Providers, different authentication methods and levels meet customers' requirements.

Open systems

Open Systems is a secure access service edge (SASE) pioneer supporting enterprises in their digital transformation journey. Our cloud-delivered Secure SD-WAN and Managed Detection and Response (MDR) services unify security and comprehensive networking capabilities, enabling organizations to connect their clouds, branches, applications and users anywhere in the world, in a secure and agile way. Open Systems' service delivery platform combines AIOps and automation with 24x7 experts to deliver immediate peace of mind and future-proof business-critical infrastructure.

Learn more at **open-systems.com** | Approved for public use. (CC, MS, 26 Aug 2020, v1.1)