![Barracuda logo — Your journey, secured.]

Advanced secure access for remote and mobile workers

with Barracuda CloudGen Firewall

Introduction

With today's mobile and remote workforce, the focus is on employee productivity rather than location. Work is being done anytime and anywhere—at home, in the coffee shop, on a train. Giving workers the freedom to do their work outside the office and without fixed hours is a growing trend.

Bring Your Own Device (BYOD) is another trend that's becoming the workplace norm. Your employees probably aren't just using equipment chosen by the IT department. Instead, they're using the laptops, tablets, and smartphones of their choice. And there are a lot of choices, including Windows systems, MacBook laptops, iPhones, Androids, and more.

Remote working and BYOD benefit both your business and your employees: They get work-life balance and you get increased productivity and reduced expenses.

Using corporate resources on the go

Mobile working brings advantages to your business, but it also brings challenges. Security is a primary concern. Controlling access to corporate resources for your mobile workforce is essential, especially when they're using free Wi-Fi hotspots at the airport and other locations. Protect your business by giving mobile employees a quick, flexible, reliable and completely secure way to connect to internal enterprise applications, information and network resources. But make it easy.

Your employees shouldn't have to be IT experts to establish a secure connection. Use a simple and user-friendly interface to have them enter their credentials and quickly connect.

BYOD also provides challenges for the IT department. Supporting a wide variety of devices and operating systems is at the top of the list. Plus, work use of private devices limits the involvement of IT; your employees control software and app installation, as well as who's actually using the device. If your business has or adopts a BYOD policy, it must ensure that devices connecting to the network to access sensitive information are protected from malware. With the right networking infrastructure in place, security concerns about BYOD can be mitigated the same way they are for company-issued devices.

Working from home

Working from home means your employees need reliable always-on access to applications and resources that sit inside the enterprise network. Barracuda CloudGen Firewall in combination with the Barracuda Network Access Client provide the most stable and transparent VPN connectivity for Windows, macOS, and Linux with richer performance and functionality compared to standard IPsec client software.

Secure remote access with CloudGen Firewall

There's no one-size-fits-all solution for providing secure remote access to corporate information. But your business can (and must) provide mobile and remote employees with secure connectivity that is optimized for your specific work environment.

With Barracuda CloudGen Firewall, you have multiple options for providing that secure network access for your employees, without time-consuming client configuration and management.

Browser remote access

Browser-based remote access designed for employees that occasionally but quickly need access to protected company resources with only a limited set of functionality required. The Barracuda SSL VPN Portal provides simple, browser-based remote access for desktop and mobile devices. Employees browse apps, network folders, and files the same way they do when connected to the office network.

For security, all network communication is sent through the encrypted and authenticated SSL tunnel to the SSL VPN gateway on the Barracuda CloudGen Firewall.

The portal supports most commonly used devices, including Apple iOS and Android.

CudaLaunch

Provide fast, Java-independent access to commonly used applications on the company network, whether hosted on premises or in the cloud. CudaLaunch, an easy-to-use connectivity app for BYOD and mobile devices, looks the same on every platform and requires no enrolment or control of private devices.

Consistent interfaces across client types simplify IT helpdesk support for rapidly changing mobile and BYOD devices.

Available for Windows, macOS, Apple iOS, and Android, CudaLaunch can be downloaded and installed free of charge from every app store. CudaLaunch is self-configuring after logon with the users id and password.
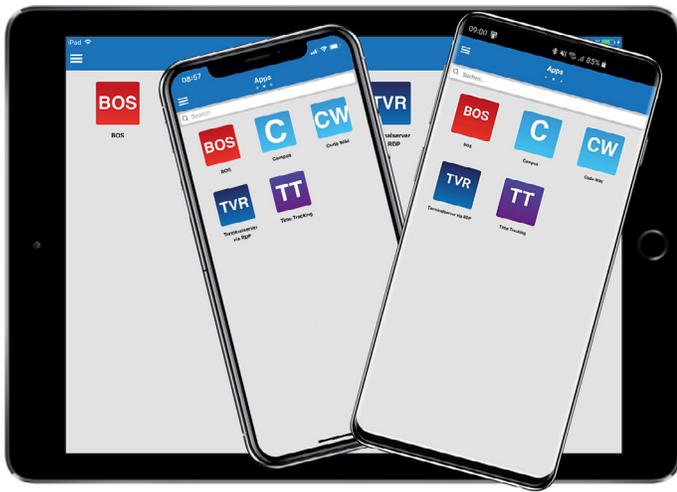

Consistent user experience across different operating systems

Network Access Client

Protect your network when desktop computers connect from outside the office. Providing richer performance and functionality than standard IPsec client software, the Barracuda Network Access Client includes quick restoration of VPN tunnels, "always-on" VPN connections for PCs, redundant VPN gateway support, selective routing of network traffic through the VPN tunnel, requiring less bandwidth with built-in traffic compression, and optimal VPN-gateway detection based on location.

The Barracuda Network Access Client provides centrally managed Network Access Control (NAC) and an advanced personal firewall, enforcing client health and security policies for remote employees connecting to the corporate network from a desktop computer in their home office.

The Network Access Client, designed for a wide variety of business devices, supports Windows, macOS, and Linux.
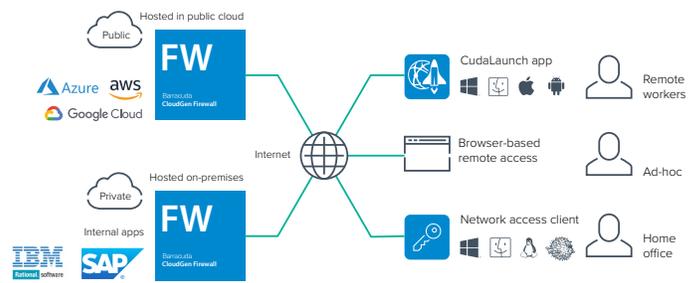
Remote access architecture

Authentication support

Protect your organization's critical information with secure authentication. Barracuda CloudGen Firewall supports a wide variety of external authentication services, including Microsoft® Active Directory, LDAP, Radius, MSNT, RSAACE, SMS Passcode, and RSA tokens.

For additional security, different authentication types can be combined to implement robust multi-factor authentication.
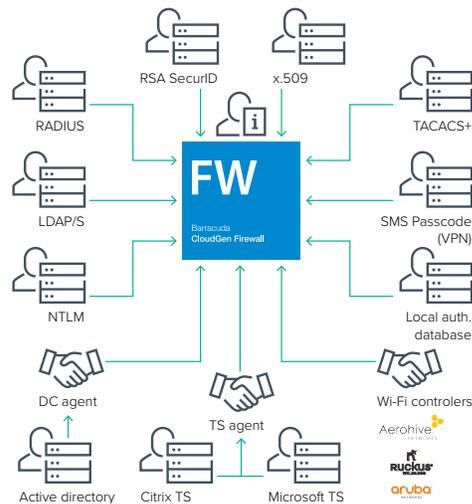
Supported authentication methods

Manageability

Manage security policies in a single place. Access-control policies are inherited from the Barracuda CloudGen Firewall, providing unified security across all types of remote access, including CudaLaunch, SSL VPN, Barracuda Network Access Client, and standard IPsec VPN connections.

CudaLaunch is designed with zero-touch provisioning and easy central management for large deployments.

Summary of Advanced Remote Access features

Barracuda provides all the connectivity features you need to ensure that remote workers of all kinds can securely access corporate resources:

- High performance custom VPN protocol
- Reduced bandwidth need with built-in traffic compression
- Multi-factor and risk-based authentication
- Mobile portal
- Network Access Control (NAC)
- Easy to use mobile apps for all platforms
- Central management
- Zero-touch provisioning
- Self-configuration

CloudGen Firewall for mobile and remote workers

Securely leverage the benefits of working remotely and BYOD with Barracuda's remote access solutions.

Mitigate the risks of unauthorized access and data loss with the comprehensive security features of Barracuda CloudGen Firewall for mobile and remote access.

Manage security policies in one place for all types of remote access, including CudaLaunch, SSL VPN, Network Access Client, and standard IPsec.

Barracuda's remote access solutions are easy to manage, easy to use, and help reduce IT costs.

Conclusion

Employees need mobile and remote access to your network, whether hosted in the cloud or on-premises; you need a secure way to provide it, to increase productivity, flexibility, and convenience.

BYOD provides similar business benefits, but adds new security challenges and risks, including enabling access, controlling access, and preventing data loss.

Control network access, protect sensitive data, and block unwanted applications. Reduce the risks associated with BYOD. Our Barracuda CloudGen Firewall incorporates advanced client-to-site VPN capabilities, using SSL, IPsec, and Barracuda's proprietary high performance TINA protocol to ensure remote employees easily and securely access network resources without time-consuming client configuration and management.

Barracuda.
Your journey, secured.