

Duo Network Gateway

Extend Zero-Trust Access to On-Premises and Public Cloud Applications

Although the global pandemic of 2020 has changed the ways many people work and from where they work, how we connect to our applications looks the same as it always did. In the not-so-distant past, organizations approached access management in a binary way: either the person was inside an office or not, and often the only way someone outside the office could access internal apps was by using a Virtual Private Network (VPN) on a corporate-managed device. However, VPN is not without its challenges – it can be clunky and difficult to manage, it can impact the user experience, and it lacks contextual changes such as the user or device for enforcing policies.

Fortunately, there is an alternative – a different way to protect access to internal applications that doesn't impact user experience and is more scalable than a VPN. It is the Duo Network Gateway (DNG), a remote access proxy security solution that helps employees, remote workers, and contractors access the applications they need to do their job by increasing productivity and reducing friction. It gives you granular access control per web application, set of Secure Shell (SSH) servers, Remote Desktop Protocol (RDP) servers¹, and user groups. You can specify different policies to make sure only trusted users and endpoints can access your internal services.



Duo Benefits

- Provides frictionless access to users as if they are on the network – no changes, no retraining needed.
- Establishes device trust before granting access to apps
- Verifies user identities with multi-factor authentication (MFA)
- Secures access to hybrid and multi-cloud environments

¹ RDP in public preview as of November 2021

Why Duo Network Gateway?

Security

- Reduces exposure to critical apps by providing application-level access from anywhere
- Controls access to specific internal applications to avoid the risk of lateral movement and privilege abuse
- Guards sensitive information with visibility into all corporate managed and Bring Your Own (BYO) devices
- Allows granular policy enforcement such as requiring users authenticate with high assurance levels for Multi Factor Authentication (MFA) using FIDO2 security keys (WebAuthn) or Duo Push, and from a corporate managed device for more sensitive apps

Ease of Use

- Solution has been designed to be deployed easily, is less complex to set up and has fewer hardware and bandwidth requirements compared to traditional VPN access solutions
- Provides users a consistent login experience across apps and secure access to hybrid and multi-cloud environments (on-premises, Azure, AWS, Google Cloud Platform)
- Enables VPN-less secure remote access for browser-based applications
- Assists with transitioning the workforce to cloud-based applications (Salesforce, Dropbox, etc.) as it can provide a cloud-like end user experience for your organization's on premises applications
- Allows IT administrators to easily implement per-application policies and least privilege models

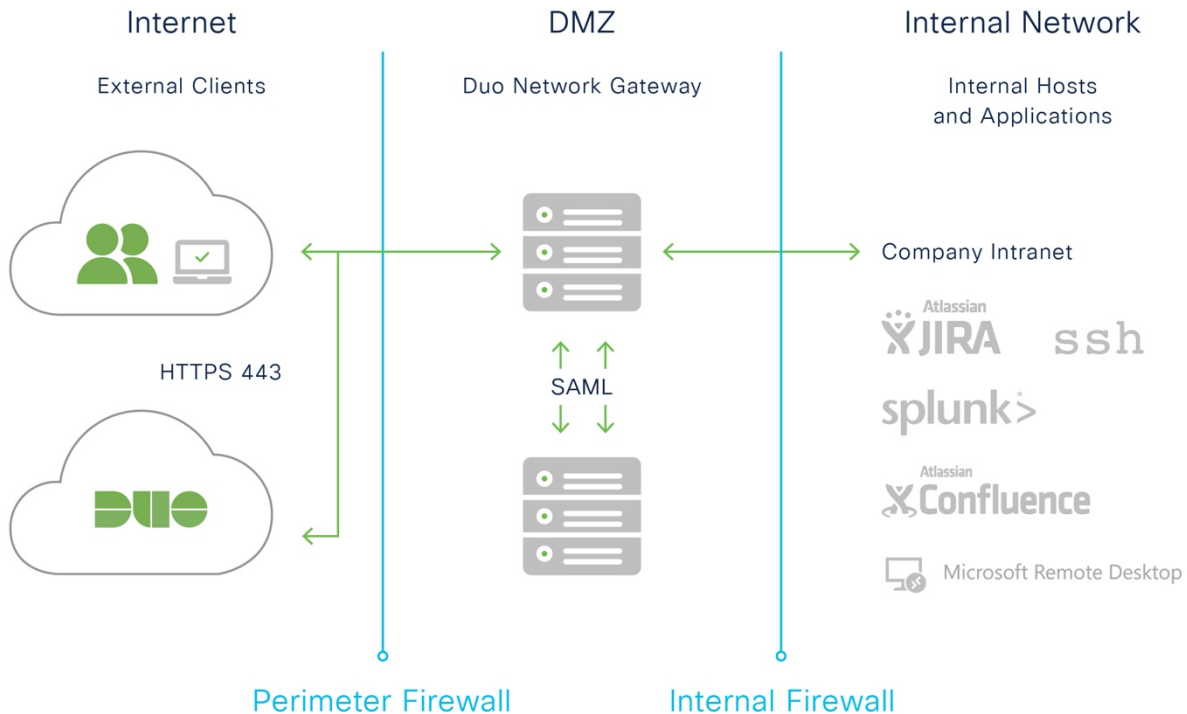
Lower TCO

- Offers a simple per user subscription model with no limit on the number of internal resources that can be protected
- Integrates the work of many security tools in one platform: adaptive authentication, endpoint visibility and control, remote access, and single sign-on (SSO)

“We chose to implement Duo Beyond because it aligns with our own vision of zero-trust security. When integrated with Sophos Mobile control, it helps us securely and confidently provide mobile access to our employees, and provides additional visibility into all assets that are accessing corporate resources.”

Ross McKerchar

Chief Information Security Officer, Sophos



How Duo Network Gateway Works

DNG is a reverse proxy that allows users to access your on-premises websites, web applications, and certain Transmission Control Protocol or TCP services (RDP, SSH)² without having to worry about managing VPN credentials, while also adding login security with the [Duo Prompt](#). Users can securely access your internal web applications from any device, using any browser, from anywhere in the world, without having to install or configure remote access software on their device. They can also remotely SSH to configured hosts through Duo Network Gateway after installing Duo's connectivity tool. Once users authenticate to DNG, they must approve a two-factor authentication request before they can access different protected services.

Session awareness minimizes the need to repeat MFA prompts as users access additional services and hosts via your gateway. Furthermore, you can specify different policies to make sure only trusted users and endpoints are able to access internal services.

There are two prerequisites for DNG:

- Use a SAML 2.0 Identity Provider (IdP) as the primary authentication source for DNG. You can use [Duo Single Sign-On \(SSO\)](#) or a third-party provider such as Microsoft [AD FS](#), [OneLogin](#), or [Okta](#).
- Deploy a physical or virtual modern 64-bit Linux server in your perimeter network (or [DMZ](#)).

² RDP in public preview as of November 2021

Pricing

	Duo Free	Duo MFA	Duo Access	Duo Beyond
Multi-Factor Authentication	✓	✓	✓	✓
Single Sign-On	✓	✓	✓	✓
Passwordless authentication to SSO apps (Duo or 3 rd party)	✓	✓	✓	✓
Policy Enforcement		✓	✓	✓
Adaptive Authentication			✓	✓
Device Visibility			✓	✓
Device Remediation			✓	✓
Device Health App			✓	✓
Trusted Endpoints				✓
Duo Network Gateway				✓
Monthly Price	Free up to 10 users	\$3/User	\$6/User	\$9/User

To learn how to implement Duo Network Gateway, visit duo.com/docs/dng.

Summary

For your business to keep employees productive no matter where they are accessing work applications and services from, you need a remote access solution that will provide a seamless user experience backed with strong zero-trust based security. Duo Network Gateway has helped hundreds of companies around the globe achieve this already. Let Duo help you, too.

For more information about Duo product capabilities, please visit duo.com/product.