Teleport

A Modern and Secure Alternative to VPNs and Bastions

Secure, scalable, zero-trust infrastructure access for modern, distributed organizations

VPN Challenges

- Multiple security vulnerabilities
- Expensive and complex to maintain
- Source of performance bottlenecks
- Create compliance problems

Teleport Benefits

- Easily implement zero trust
- Reduced operational complexity
- Better performance and user experience
- Provides evidence for compliance audits

As organizations shift to distributed work models and cloud-based architectures, the need for secure, scalable, and manageable infrastructure access has become crucial. Traditional solutions like VPNs and bastions, while initially effective, are increasingly viewed as complex, costly, and vulnerable to security risks. Teleport offers a more robust alternative, designed to improve access control while maintaining high security standards and reducing overhead.

Challenges

VPNs and bastions were originally implemented to provide secure remote access and shield internal systems from unauthorized access. However, these solutions present several challenges:

- **Security Vulnerabilities:** VPNs often create broad network access, which can expose an organization to attacks if a single credential is compromised. VPNs are also challenging to configure for least-privileged access, leading to over-permissioning.
- **Complexity and Maintenance Overhead:** VPNs and bastions require constant management, including handling certificates, rotating keys, and ensuring software patches. These factors increase IT workload and expose networks to potential misconfigurations.
- **Performance Bottlenecks:** VPNs can become performance bottlenecks, especially with increased remote access demands. Routing all traffic through a central VPN server often results in slow response times, frustrating end users and reducing productivity.
- **Compliance Challenges:** VPNs and bastions often lack the auditing and monitoring capabilities necessary to meet modern compliance requirements. This lack of visibility can hinder the ability to conduct proper security assessments and demonstrate regulatory adherence.

What is Teleport?

Teleport Infrastructure Identity Platform modernizes identity, access, and policy for infrastructure, for both human and non-human identities. This includes servers, Windows desktops, CI/CD bots, public/private clouds, Kubernetes clusters, databases and web applications. It delivers on-demand, least privileged access to infrastructure on a foundation of cryptographic identity and zero trust.

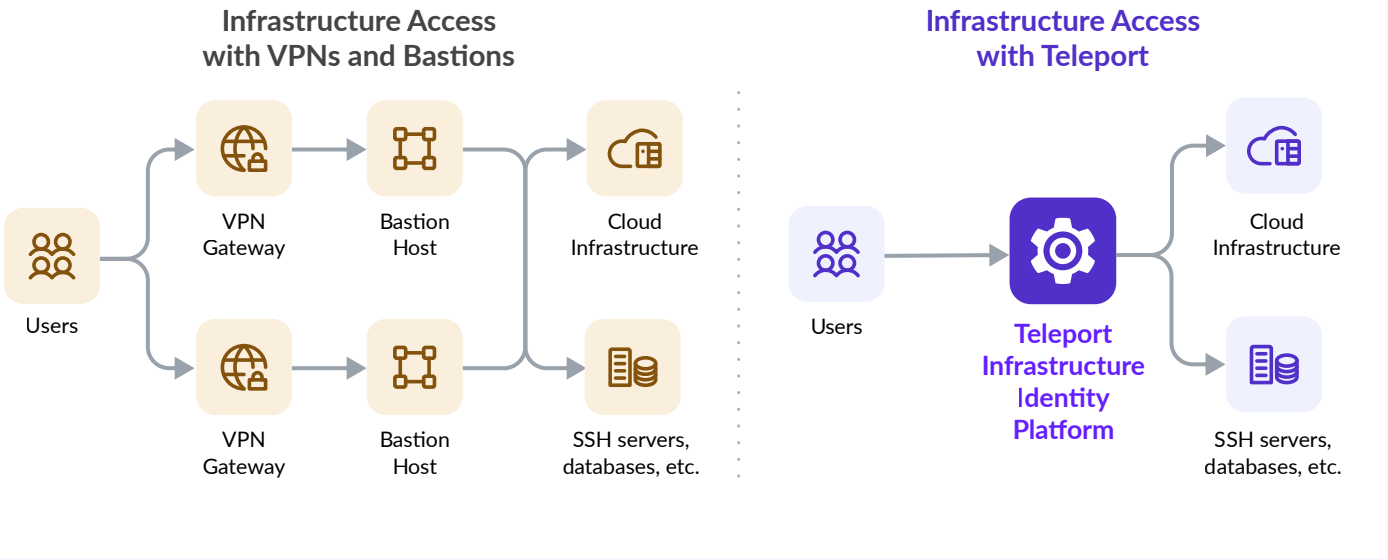
It eliminates the need for VPNs and bastion hosts by using identity-based, role-specific access and short-lived certificates, which restrict access to only necessary resources. This approach follows zero-trust principles, enhancing security, compliance, and reducing complexity in infrastructure access control. Teleport Access also includes session logging and audit capabilities, ensuring traceability and compliance for all access events.

How It Works

Teleport replaces VPNs and bastions by providing a unified platform for secure, seamless infrastructure access control across SSH, Kubernetes, databases and web apps.

Unlike traditional VPNs, which often grant broad network-level access, Teleport connects users only to the specific resources they need. This approach:

- **Enables Zero-Trust Architecture:** By relying on identity-based access controls, Teleport implements a zero-trust model, limiting access to verified users and devices while continuously validating their identity.
- **Uses Identity-Based Access:** Instead of using IP-based restrictions or static credentials, Teleport generates short-lived certificates tied to user identity, which ensures that access is strictly governed by policies.
- **Provides Audit and Session Recording:** Teleport logs all access attempts and provides session recordings, making it easier for organizations to monitor access, enforce compliance, and conduct forensic analysis.



Teleport replaces VPNs and bastions with a more scalable solution that provides least privilege access, granular RBAC, secure and direct access to infrastructure resources, and auditing and observability capabilities.

Benefits of Teleport Over VPNs and Bastions

Teleport offers several advantages over traditional VPNs and bastions, making it a more effective solution for modern infrastructure access:

- **Enhanced Security with Zero Trust:** Teleport follows a zero-trust approach, where users are authenticated based on their identity rather than their network location. This approach significantly reduces the risk of unauthorized access, as each access request is verified before connection, removing broad network access risks associated with VPNs.
- **Reduced Operational Complexity:** By eliminating the need for VPN configurations, certificate management, and static credentials, Teleport reduces the complexity involved in managing infrastructure access. This simplification allows IT teams to focus on more strategic initiatives rather than ongoing maintenance of VPN configurations and access permissions.
- **Improved Performance and User Experience:** Teleport connects users directly to resources without routing traffic through a central VPN server, reducing latency and improving performance. This streamlined connection method enhances the user experience, especially for remote and distributed teams accessing cloud or on-premises resources.
- **Streamlined Compliance and Auditing:** With built-in logging, session recording, and identity-based auditing, Teleport makes it easier to comply with security and data protection regulations. These capabilities allow for transparent and comprehensive audits, helping organizations meet compliance standards more efficiently than traditional VPNs or bastions.
- **Cost-Effectiveness:** By replacing VPNs and bastions with a single access platform, Teleport reduces the need for multiple access solutions and the associated infrastructure costs. Organizations can consolidate infrastructrure access control, resulting in lower overhead costs and simplified access policies.

Conclusion

Teleport provides a modern, unified approach to secure infrastructure access that addresses the complexity and expense of using VPNs and bastions. By eliminating credentials and standing privileges, and implementing zero trust principles, Teleport hardens security, mitigates risk, and eliminates friction for engineers.

As security demands evolve, solutions like Teleport offer organizations a scalable, effective, and user-friendly approach to managing infrastructure access by eliminating legacy tools like VPNs and bastions.