netbird

WHITE **PAPER**

Why Should You Migrate From Fortinet to NetBird, Now.

In search of simplicity, security, reliability and ROI

Organizations using Fortinet SSL VPN are at a critical inflection point. Fortinet has decided to deprecate its widely used SSL VPN. This is no product update; in fact, this signals that traditional, appliance-centric remote access that organizations have been relying on thus far, is unreliable, insecure and unsustainable. Fortinet's deprecation strategy is to make organizations migrate to another of Fortinet's complex solutions. Alternatively, organizations could utilize this opportunity to strategically shift in the direction of security, reliability and operational efficiency.

This forced migration is not the problem that organizations would want to manage, when already dealing with endless patch cycles, performance issues and escalating costs stuck inside Foretinet's ecosystem, not to mention the dropped connections, cryptic error messages, performance bottlenecks and recurring security vulnerabilities. Escaping this cycle of continuous high-touch maintenance is a must.

In this white paper, we will discuss how migrating to NetBird, a modern Zero Trust networking platform built on the proven, high-performance WireGuard® protocol, directly solves the foundational security and reliability challenges associated with the Fortinet ecosystem. By moving from a centralized, appliance-based model to a decentralized, peer-to-peer overlay network, organizations can eliminate single points of failure, drastically reduce attack surface, and empower teams with simple, yet fast, reliable, and secure access to anything, anywhere.

Contents

Breaking Down the Fortinet Migration

If you're using Fortinet SSL VPN in your organization, the message is clear - the secure remote access strategy that you've built with SSL VPN tunnels is disrupted, affecting business productivity. Operationally, Fortinet's strategy of making you move to FortiClient is a challenging change. Fortinet is completely removing SSL VPN tunnel mode from both the GUI and CLI across all FortiGate models with the release of FortiOS 7.6.3 and beyond. This means that your existing configurations will not be carried over during the firmware upgrade - your remote access configurations will cease to function, disconnecting your entire remote workforce.

High-Stakes Migration

This forced migration sets you on a path of a complex and high-stakes migration project with a high probability of failure, especially if yours is a diverse IT environment with non-Windows endpoints. There are several user-reported instances that neither IPsec or ZTNA solutions work reliably on macOS, suggesting that you have to spend a considerable amount of time and effort to adequately test these critical migration paths for your modern, heterogeneous enterprise. Fortinet's own migration guides and documentation reveal a complex process involving multiple, manual conversion steps for both your FortiGate and FortiClient configurations.

Moving Laterally, From One Problem to Another

Fortinet's migration path is a lateral move requiring a different set of technical considerations, evaluation and testing. If you migrate to IPsec, you remain chained to an appliance-centric model that is known for performance bottlenecks. If you decide to move to Fortinet's ZTNA (FortiClient) offering, you will quickly discover that it is a scaled-up feature bolted onto their existing firewall (FortiGate) architecture, with its own set of limitations.

The deprecation of SSL VPN was a reactive measure to contain a spiraling crisis of security vulnerabilities and technical debt within their product. The deprecated SSL VPN required an exposed web page, making it a constant and attractive target for adversaries probing for vulnerabilities.

For the Network & Security Engineer: A Battle for Stability and Visibility

As network and security engineers, you're fighting a daily battle to ensure that your workforce is connected and can securely access any application or resource from anywhere. However, with Fortinet, you spend most of your time troubleshooting connectivity and performance issues.

- **Instability and unpredictability:** Help desks are overwhelmed with tickets about frequent connection drops and your users complain about their client often getting stuck at 98% when connecting, or it shows as connected but doesn't pass any traffic - eventually leading to constant reboots and escalating support requests.
- **Cryptic error codes:** It's frustrating to see connection failures, and even more so to see generic error codes. Codes like, Unable to establish VPN connection. `The VPN server may be unreachable (-6005),` provide no actionable information, leaving you to blindly troubleshoot a wide range of potential causes, from an incorrect gateway configuration to an obscure SAML authentication timeout setting.
- **Operational complexity:** With FortiGate and FortiManager, simple tasks can become multi-step processes working across GUIs, CLI syntax and the sheer number of commands; creating friction, slowing teams, and leaving room for costly human error.
- **Performance bottlenecks:** If you enforce a full-tunnel VPN policy for security, all user traffic, including internet-bound requests, must be backhauled through the central FortiGate appliance. This doubles latency and places an enormous resource load on the firewall, impacting user bandwidth and creating a bottleneck for your entire remote workforce.
- **Problematic DNS resolution:** One of the persistent bugs with FortiClient is a tendency to affect DNS resolution. FortiClient frequently fails to correctly set DNS settings on the endpoint's network interface, and fails to resolve internal hostnames that disrupt secure connectivity and business productivity.
- **Endless patching:** Endless patches and firmware updates are what you deal with when inside Fortinet's ecosystem. Though each new patch/firmware is deployed to remove bugs, each of them carry the potential to introduce new and equally disruptive issues.

A Barrier to Agility For DevOps and SecOps

The Fortinet ecosystem could be challenging for DevOps and SecOps that are focused on agility and innovation.

- **Automation is an afterthought:** Though Fortinet provides APIs and connectors, the automation experience is less streamlined than what you want it to be. For instance, the FortiClient EMS API might allow you to programmatically create a configuration profile but lack the corresponding function to list existing ones, forcing you to build fragile workarounds that come in the way of agility and innovation.
- **Rigid appliance-centric ZTNA:** FortiClient is less suited for dynamic, hybrid and cloud-native environments. FortiClient is fundamentally tied to the FortiGate appliance, requiring you to manually configure static access proxies, virtual IPs and firewall rules on a piece of hardware. It can be slow, rigid, and too manual for CI/CD pipeline agility, or any kind of automated infrastructure.
- **Overly permissive security:** Attempting to integrate Fortinet tools into your CI/CD toolchain often requires granting several broad, high-privilege permissions. Fortinet connectors require extensive rights across code repositories, pull requests, and pipelines, directly conflicting with the principle of least privilege, creating security blindspots in your most critical development infrastructure.

Fortinet's True Cost of Ownership (TCO) and Return on Investment (ROI)

The true cost of ownership hides in the complexity with mandatory add-ons, friction, and ongoing operational and security overhead. To choose the right remote access strategy, you need to look at the full TCO, not just the quote.

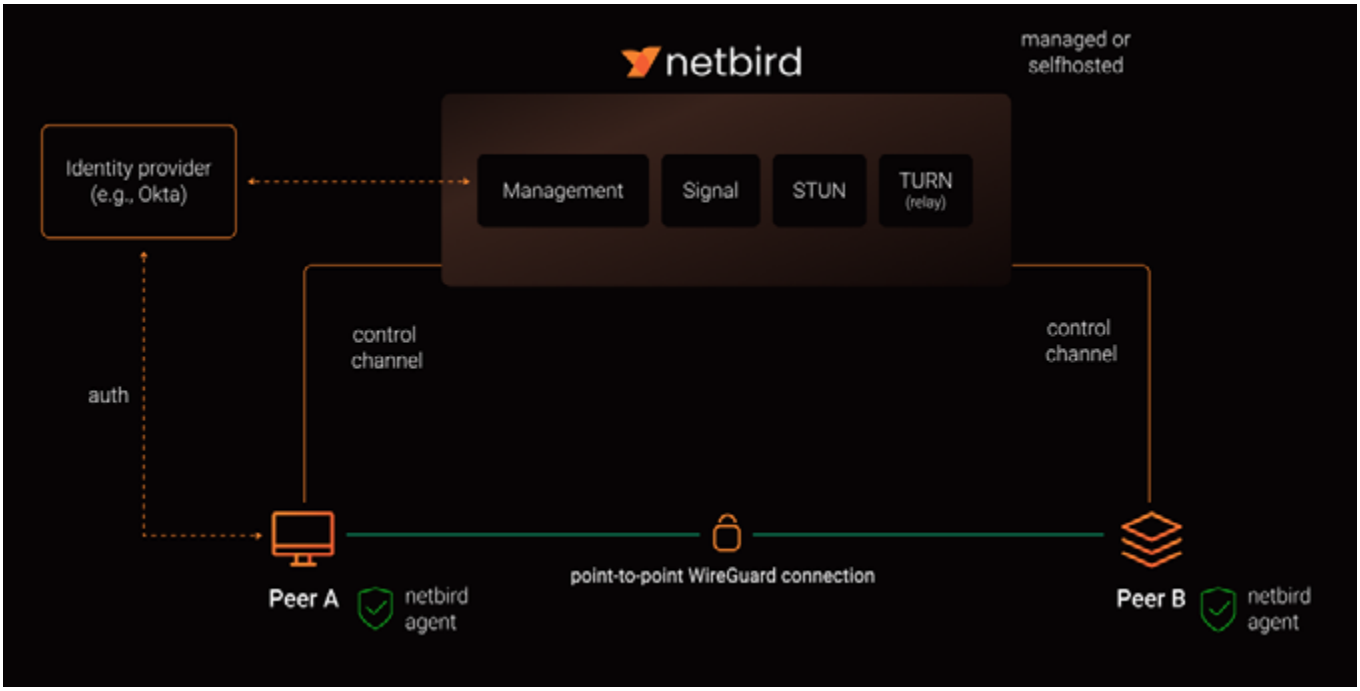
- **A mandatory, multi-product stack:** To make the most out of FortiClient, the solution requires a stack of separately licensed products. You must purchase licenses for FortiClient EMS for central management. To get meaningful visibility and log analysis, you need a FortiAnalyzer appliance or VM. Your TCO is never for a single product but for an expensive, mandatory bundle of interdependent components.
- **Operational overhead:** Licensing is only one part of the total cost equation. Operational overhead costs time and money due to repetitive work just to maintain the solution, spending hundreds of hours on endless troubleshooting of bugs and performance issues. This means that you are caught in a constant cycle of patching and upgrading the Fortinet fabric, a risky process that often creates new problems. This is compounded by the complex configuration interfaces of FortiGate and FortiManager, turning simple tasks into laborious processes and diverting valuable engineering resources from more critical initiatives.
- **Downtime costs:** Every time your VPN connection drops, a user cannot access a critical application, or a DevOps engineer has to stop a strategic project to troubleshoot a FortiClient issue, your business loses money. These micro-outages and productivity drains accumulate into a significant impact on your organization's bottom line.
- **Breach costs:** In just one year, over 200 vulnerabilities were published for Fortinet products, with critical flaws in their VPNs appearing almost monthly. A few of them: **(i) CVE-2024-54019** - 'vulnerability in FortiClient Windows may allow an unauthorized attacker to redirect VPN connections via DNS spoofing or another form of redirection'. **(ii) CVE-2024-47574** - 'An authentication bypass using an alternate path or channel in Fortinet FortiClient Windows allows low privilege attackers to execute arbitrary code with high privilege via spoofed named pipe messages.' **(iii) CVE-2024-50564** - 'A use of hard-coded cryptographic key (CWE-321) vulnerability in FortiClient Windows may allow a low-privileged user to decrypt interprocess communication via monitoring named pipe.' **(iv) CVE-2025-25251** - 'An Incorrect Authorization vulnerability [CWE-863] in FortiClient Mac may allow a local attacker to escalate privileges via crafted XPC messages.'.. Just to highlight a few. There are numerous others for the deprecated Fortinet SSL VPN. Vulnerabilities are the primary targets for adversaries and ransomware gangs, and organizations affected by these face both financial and reputational costs.

Why Switch to NetBird?

Investing in a modern ZTNA solution like NetBird is not just about adopting a better security tool. It is an investment in business continuity, operational efficiency, and a future-proof secure IT architecture. The ROI is measured not only in reduced licensing and hardware costs but, more importantly, in reclaimed engineering hours, increased workforce productivity, and the confident avoidance of a catastrophic security incident.

Built on WireGuard®: The Foundation of Speed, Security and Reliability

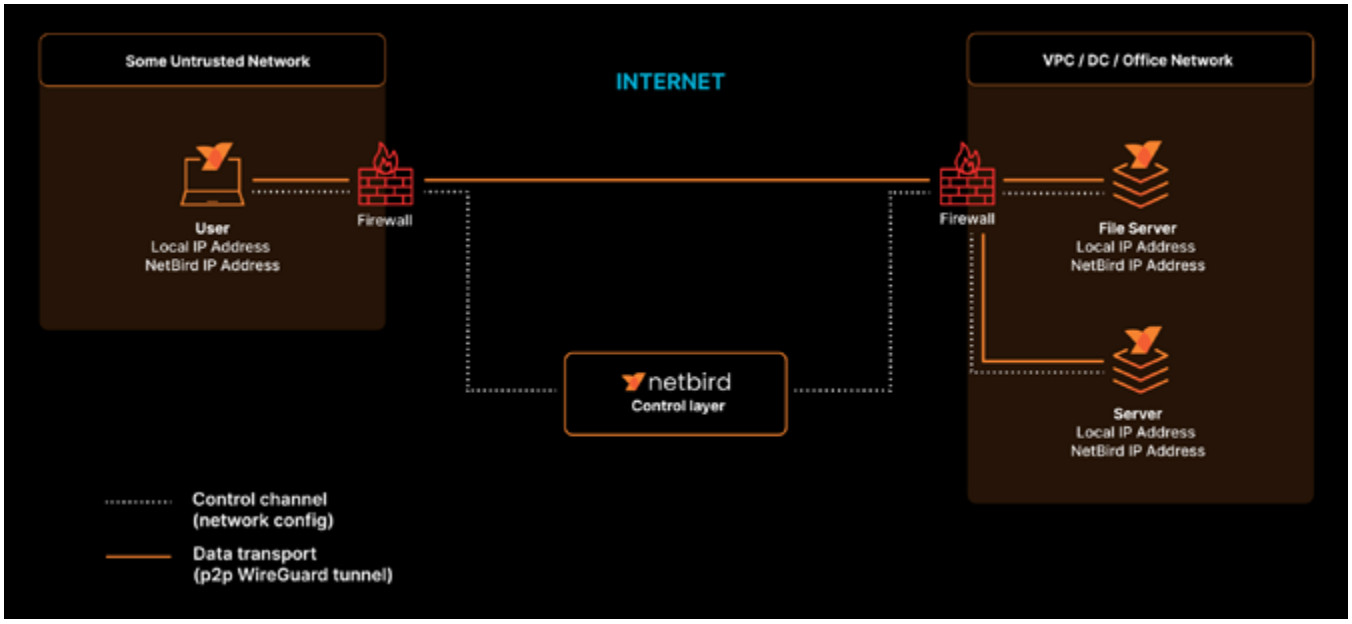
NetBird, built on the trusted WireGuard® protocol, is a modern, open-source networking platform that simplifies secure connectivity between devices, teams, and cloud environments - your computers, devices, machines, and servers connect to each other directly over a fast encrypted tunnel.



Why WireGuard®? Because it is lean, fast, and secure by design. Unlike the proprietary complex IPsec protocol suite used by Fortinet, WireGuard has a remarkably small codebase. This minimalism dramatically reduces the potential attack surface and makes the code simple enough for security experts to audit thoroughly, giving you confidence in its integrity.

True Peer-to-Peer (P2P) Secure Overlays: Eliminating Bottlenecks and Single Points of Failure

The fundamental difference between NetBird and Fortinet lies in the network topology. Fortinet operates on a classic hub-and-spoke model, forcing all remote access traffic through a central FortiGate appliance. This creates a single point of failure and a massive performance bottleneck.



In contrast, NetBird creates a decentralized, P2P overlay network. With native and built-in integration with your identity provider of choice, your devices, servers, and cloud resources form direct, encrypted tunnels to each other. This decentralized P2P architecture has several benefits:

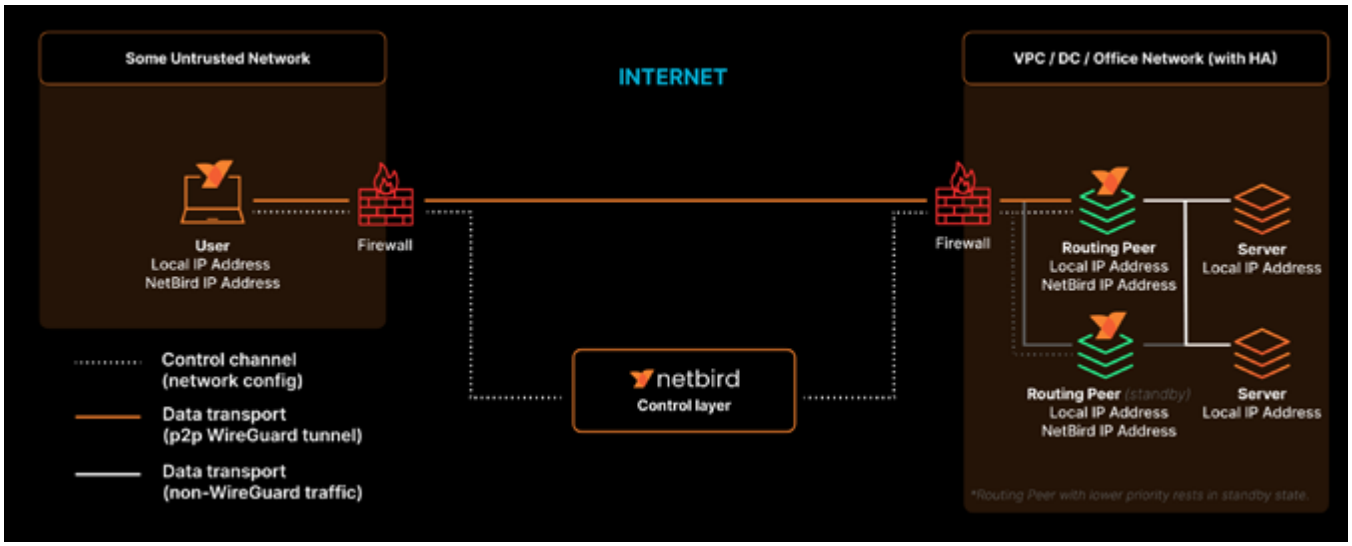
Zero bottlenecks: Traffic flows on the most direct path possible between peers, eliminating the latency and bandwidth constraints of backhauling all traffic through a central gateway.

Enhanced resilience: The network has no single point of failure. If your on-premise data center loses connectivity, your users can still access resources in your cloud environments, and your cloud-to-cloud connections remain fully operational.

Scalability and privacy: Your data is yours. NetBird's architecture consists of a lightweight client on each peer and a cloud-based management plane that handles authentication, key exchange, and policy distribution. Crucially, your data traffic never flows through the management service, ensuring maximum performance, scalability, and privacy.

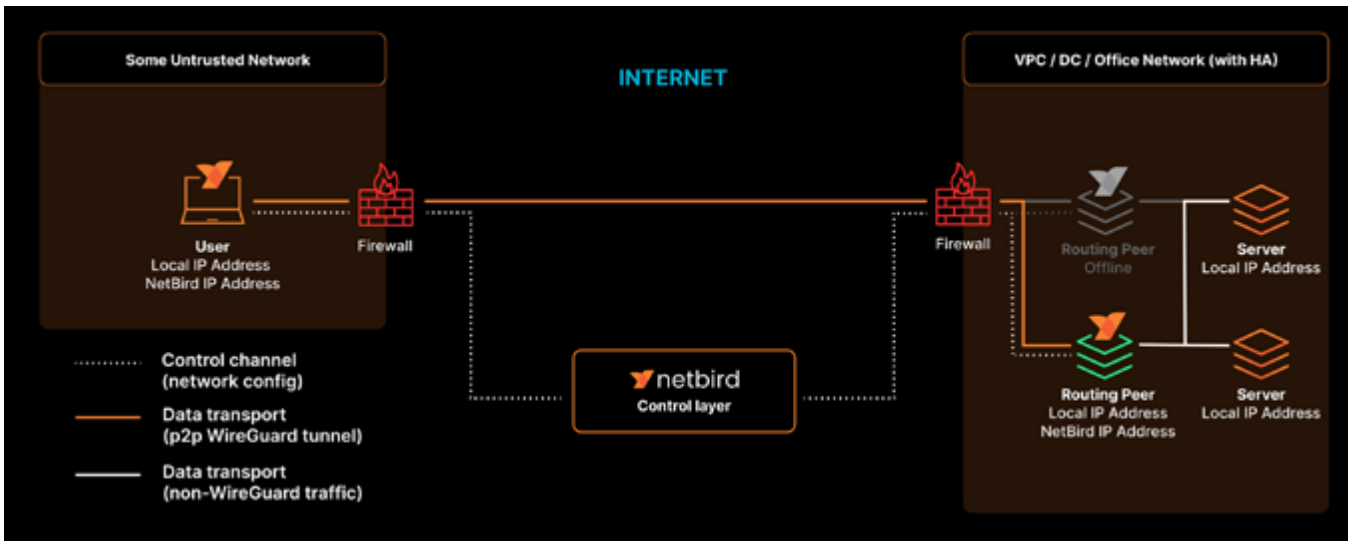
Agentless Remote Access for Internal Resources: Simplifying Complex Networks

For environments where you cannot or do not wish to install an agent—such as managed database services (e.g., AWS RDS), printers, legacy servers, or sensitive IoT devices, NetBird Networks feature provides a powerful and super-simple solution. This feature allows you to deploy one or more NetBird agents as "routing peers" inside your private network segments (like an AWS VPC or an on-premise LAN).



These routing peers act as a bridge between the NetBird overlay and your internal network. From the central NetBird dashboard, you can then define granular, identity-based access policies that permit specific user groups to access specific internal resources (defined by IP address, hostname, or even wildcard domains) through that routing peer. The end resource is accessed securely without ever having the NetBird agent installed on it. This gives you the full security benefit of Zero Trust—least-privilege, identity-based access—without the operational overhead of universal agent deployment.

NetBird ensures robust connectivity with built in high availability. You get the flexibility to install multiple routing peers to avoid a single point of failure. There's no limit on the number of routing peers that you can create; NetBird automatically determines the optimal path, prioritizing routing peers based on metrics (high/low priority) and connection attributes such as direct or relayed connections.



> Our testing with NetBird showed that a router peer that was actively handling traffic for a given peer could suddenly halt operation, and the client would experience a sub 2 second connectivity interruption while their traffic was rerouted to another host. This addressed the final pillar in our user experience aspirations as we could respond to incidents, security, operational, or otherwise with ease and confidence that Yelpers can continue working without disruption.
>
> yelp

Further, you can extend NetBird's SASE (Secure Access Service Edge) capabilities to effectively gate SaaS applications. You can define a public domain, for example ***office365.microsoft.com*** as a resource and whitelist the public IP of the routing peer in your Microsoft 365 settings. When NetBird is installed on the users' machines, access to this cloud resource/SaaS application will be routed through the routing peer, while blocking access to anyone else trying to access the application.

This means that NetBird is a true ZTNA solution that is designed to solve the root causes of traditional VPN problems. In contrast, FortiClient ZTNA, is merely a new feature layered on top of a fundamentally flawed, appliance-centric architecture. While Fortinet's ZTNA changes the policy model, it still relies on the FortiGate as a centralized proxy, tethering you to the same underlying bottlenecks, security vulnerabilities, reliability issues, and operational complexity.

Feature	Fortinet (FortiClient ZTNA)	NetBird
Core Architecture	Appliance-centric, hub-and-spoke model within a proprietary hardware and software ecosystem. All ZTNA traffic is proxied through a central FortiGate appliance, creating a bottleneck.	Software-defined, peer-to-peer secure overlay network built on an open-source foundation. Traffic flows directly between peers over encrypted tunnels, eliminating bottlenecks.
Security Model	A ZTNA policy layer bolted onto a traditional perimeter-based trust model. Access is granted to a central proxy, not directly to the resource. Rules are complex and configured on the appliance.	Identity-first Zero Trust from the ground up. The principle of "never trust, always verify" is enforced with granular, identity-based access controls applied directly at the source and destination peers.
Performance & Protocol	Relies on IPsec, a complex and heavy protocol. Prone to severe performance degradation with full-tunnel policies, higher latency due to traffic backhauling, and being blocked on public networks.	Built on WireGuard®, a modern, lightweight, and high-performance protocol. Delivers high-throughput, low-latency direct connections. Establishes and maintains stable connections even when networks change.
Management & Usability	Requires a complex and costly stack of multiple components (FortiGate, FortiClient EMS, FortiAnalyzer) that is difficult to deploy and operationalize. Users report complex user interfaces that increase management overhead and require specialized expertise.	A single, unified, and intuitive web-based management plane provides centralized control. Designed for simplicity, making it easy to deploy and operationalize without extensive specialized training.
DevOps & Automation	Automation is an afterthought. Integration is hampered by limited APIs and rigid, overly-permissive security models. The architecture is challenging for modern Infrastructure-as-Code (IaC) practices.	Built for automation from day one. Offers seamless integration through a comprehensive Public API, a command-line interface (CLI), and a first-class Terraform provider for true IaC workflows.
Scalability & TCO	High TCO driven by expensive hardware appliances, complex multi-product licensing, and significant hidden operational costs from managing instability and complexity. Pricing is often not straightforward.	Transparent, flexible, and predictable user-based pricing with no hardware costs. A powerful, self-hosted version is available for free. Low operational overhead is a core design principle.

A more granular comparison can be found here.

The Migration Playbook: Your Seamless Transition to NetBird

Moving to NetBird is a low-risk, phased process that you can execute on your own terms, without disrupting business operations. This playbook outlines a seamless, phased transition that allows you to realize the value of NetBird at every step.

Phase 1: Deploy (With a Fully-Featured Free Trial) and Co-Exist with Fortinet

You can begin your migration without touching your existing Fortinet setup. Simply sign up and install the lightweight NetBird agent on the endpoints of a pilot group, such as your DevOps or IT team. Integrate with your SSO (e.g. Entra ID, Okta, etc) for seamless access permissions for your users and groups. The NetBird client can run alongside FortiClient without conflict. Use this initial deployment to provide secure access to a new cloud application or to a specific development environment. With zero risk to your production environment, empower your most technical users to experience the performance and reliability benefits firsthand, while proving the value of the platform.

Phase 2: Use Routing Peers for Seamless Remote Access

Extend NetBird's reach without deploying agents everywhere. Deploy NetBird agents as routing peers into your key network segments, such as your AWS VPC. Easily create granular access policies that mirror the access permissions currently defined in your FortiGate firewall rules. Enable your pilot users to access all the same resources they could through the Fortinet VPN, but now via NetBird's high-throughput, low latency network. You can now conduct a direct, side-by-side comparison of performance, stability, and user experience.

Phase 3: Expand and Decommission

After proving the value and validated configurations, you can begin the gradual rollout to your wider user base. Leverage NetBird setup keys to easily automate deployment and add machines to your network at scale. As you migrate user groups over to NetBird for their primary remote access, you can gradually decommission the corresponding SSL VPN or IPsec configurations on your Fortinet. This phased approach minimizes change management overhead and ensures a smooth transition for all users.

Phase 4: Decommission Fortinet

Once all remote access use cases are confidently handled by NetBird, you can confidently decommission Fortinet SSL VPN. You will have successfully migrated from a complex system to a simple, resilient, and secure network.

Next Steps: Reclaim Your Network, Securely

Sticking with the Fortinet ecosystem means accepting a future of escalating complexity, unpredictable costs, and constant security fire drills. NetBird is your most frictionless path to reclaiming control of your network. It is a strategic upgrade that delivers immediate and measurable results:

- **Radical Simplicity:** Eliminate the complex, multi-product stack and the endless hours your team spends on troubleshooting and patching.
- **Frictionless Security:** Drastically reduce your attack surface with a true Zero Trust, peer-to-peer architecture.
- **Tangible ROI:** Slash your TCO by removing expensive hardware, opaque licenses, security vulnerabilities and the hidden costs of lost productivity.

Don't just take our word for it. Take action now and see for yourself why engineering teams are making the switch.

> NetBird Eliminated our networking and access control complexity overnight, as if by magic. It's like having an enterprise-grade network that configures itself.
>
> Chinmay Pai, DevOps Engineer, ZERODHA

> NetBird has fundamentally transformed our network management operations, eliminating outages, simplifying operations, and enabling secure, scalable connectivity through code. What used to be a fragile, error-prone setup is now a robust, policy-driven system that fits the way we structure and secure our infrastructure.
>
> Sport Alliance

1. **Get started in minutes:** Our how-to videos walk you through everything from initial setup to configuring advanced access controls.
2. **Experience the difference today:** The best way to understand the power of NetBird is to use it. You can create a secure network in under 5 minutes. Sign up for our free plan and connect your first few devices.
3. **Secure Your Future:** Get started with NetBird for free or request a demo to begin your migration to a faster, simpler, and more secure network.

netbird
open source zero trust networking

NetBird is an open source Zero Trust Networking platform designed by engineers, for engineers. NetBird makes it radically simple to deploy secure private networks for modern organizations. Built on the trusted, high-performance WireGuard® protocol, NetBird eliminates the limitations of traditional VPNs by establishing high-throughput, low-latency decentralized private networks. NetBird's architecture provides a single, intuitive management console to enforce granular, identity-based access policies, integrating with your existing Identity Provider (IdP) for SSO and MFA.