

Securing Business Continuity

Netskope One Private Access is a Universal ZTNA solution, underpinned by the NewEdge Network to ensure unparalleled business continuity. Unlike legacy VPNs or first-generation ZTNA, it eliminates operational burdens by delivering reliable, identity-centric access to critical applications without compromising performance or security.

Quick glance

- **Fewer manual interventions:** Automate failover to decrease admin intervention.
- **Decentralized zero trust engine:** Decentralized authentication in each data center, preventing bottlenecks and ensuring access independent of management planes.
- **Optimized traffic routing:** Bypass ISP congestion using multi-path selection and telemetry to steer users to the fastest path.
- **Hosted business continuity plan (BCP) options:** Deploy on-premises ZTNA brokers or SASE gateways as standby to ensure business continuity.
- **Alternative access paths:** Deploy a second tenant for resilient backup.

“In just four months, we deployed Netskope technologies across 200 sites and 14,000 users without any business disruption. We provided security without compromising the performance of our business.”

Andrea Bergamini, Vice President, Global Infrastructure and CISO at Orbia

The challenge

Users on first-generation ZTNA solutions are inherently vulnerable to access loss during service degradation. This stems from monolithic architectures that tightly couple management and data planes, leaving them susceptible to regional public cloud failures and internet service provider (ISP) outages. Recovery often forces network teams into fire drills involving manual DNS overrides, emergency firewall changes, and the resurrection of decade-old VPN services. The end result is a poor user experience, lost productivity for both users and admins, and an undesired fall back to broad network access.

The solution

Netskope One Private Access is underpinned by NewEdge, the world's largest and most peer-connected security cloud. Its distributed architecture enforces access and security policies locally at the edge. This occurs independent of the management plane where applications and policy configurations are stored, to provide 99.999% availability and graceful failover. To ensure total coverage, on-premises ZTNA brokers extend these capabilities directly into customer environments or regions lacking a local NewEdge data center.

Decentralized zero trust engine

First-generation ZTNA solutions rely on a centralized management plane (MP) for authentication and policy enforcement, creating bottlenecks during peak logins and complete outages if the MP degrades. Their monolithic architecture tightly couples the data plane to the MP, so any MP disruption halts service entirely.

Netskope One Private Access takes a distributed approach. Each NewEdge data center independently authenticates and authorizes users and devices, regardless of MP availability. The result is instantaneous authentication, immediate tunnel setup, and fast access to private applications, even under high concurrency or MP degradation.

Key capabilities:

- **Inline authentication:** Authentication services are hosted in every NewEdge data center. The NewEdge traffic management service ensures users always connect and authenticate at the closest location.
- **Localized policy cache:** Each NewEdge data center maintains a real-time local policy cache per connected user, updated instantly when administrators modify policy. This enables zero trust enforcement independent of the MP.

“Eliminate single points of failure with intelligent, multi-path steering for continuous, secure access across all devices.”

Traffic steering: Ensuring continuous connectivity

First-generation ZTNA makes traffic steering a single point of failure. Netskope One Private Access eliminates this with multiple steering options, if the primary degrades, users reconnect via a secure alternative.

The Netskope One Client and publishers learn brokers from NewEdge—ranked by shortest round-trip-time (RTT)—and connect to the closest. NewEdge’s globally resilient architecture ensures reliable application access.

Key capabilities:

- **Client stability:** Netskope maintains a validated golden release on a three-month cadence, with automatic updates and software rollback to ensure endpoint stability.
- **Intelligent broker selection and dynamic failover:** Administrators define primary and fallback broker preferences. NewEdge traffic management evaluates RTT across candidates and selects the optimal primary broker. If the primary degrades, the Netskope Client automatically fails over to the designated fallback.
- **Publisher auto-reconnect:** Publishers continuously monitor latency across nearby brokers. If the active connection degrades beyond a set threshold, the publisher automatically reconnects to the next closest broker, always using the best available path.
- **Local DNS fallback:** If the NewEdge traffic management service is unreachable, both the Netskope Client and publishers fall back to local DNS resolution to maintain uninterrupted broker selection.
- **Browser-based fallback:** When the Netskope Client cannot initiate a tunnel, users access web and non-web-based applications (such as RDP and SSH) via the Netskope One Enterprise Browser or clientless Private Access browser, with seamless fallback between the two.

“Extend zero trust resilience with on-premises options that provide local failover and reliable application access during network disruptions.”

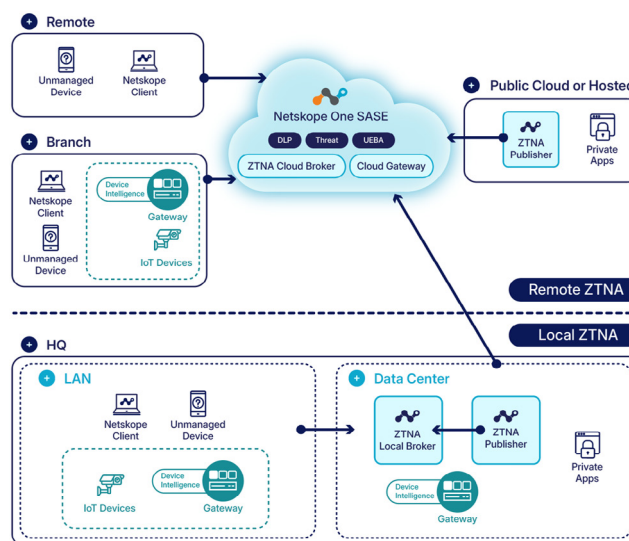


Figure 1: Netskope Universal ZTNA architecture: Unified cloud and local brokers providing seamless, secure access and consistent policy for all remote and on-premises users.

Cloud-scale resilience and redundancy

Netskope One Private Access is built on NewEdge, a dedicated infrastructure designed for resilience. Unlike solutions relying on third-party public cloud routing, NewEdge dynamically routes around disruptions to maintain continuous access.

Key capabilities:

- **Full compute everywhere:** NewEdge runs full compute and security services in every data center, eliminating backhaul latency. Over-provisioned infrastructure and proactive capacity planning support a 99.999% uptime SLA.
- **Route control:** Traffic is automatically rerouted in real time to bypass congestion or micro outages, ensuring low latency during ISP issues or unexpected network events.
- **Broker health monitoring:** Degraded or maintenance-bound data centers are removed from rotation automatically. Affected clients and publishers fail over to healthy alternatives without user intervention.
- **Hot standby BCP tenant:** Customers can configure a secondary Netskope tenant on a separate management plane, pre-provisioned with users, applications, and policies for rapid failover. Organizations using a third-party ZTNA provider can also deploy Netskope as a high-availability secondary without additional client installs.
- **Agentless and self-service BCP:** Users can switch to clientless browser access for web and non-web applications without IT intervention, or self-install the Netskope One Enterprise Browser without local admin rights.

Hosted business continuity options

Netskope also offers on-premises ZTNA broker instances, to complement cloud brokers in NewEdge, extending Private Access where a NewEdge data center isn't feasible.

Option 1: Local broker

The local broker is a virtualized, single-tenant Private Access broker deployed on customer infrastructure, enforcing the same ZTNA policies as cloud brokers. The NewEdge traffic management service continuously monitors it for availability and latency.

Before tunnel setup, the Netskope Client queries the traffic management service to identify the closest broker, cloud or local, and connects to the lowest-latency option. Automatic or manual failover resets the tunnel and recalculates the optimal broker.

Administrators can deploy local brokers in hot standby, prioritize them via traffic steering policies, or incorporate them into a business continuity plan.

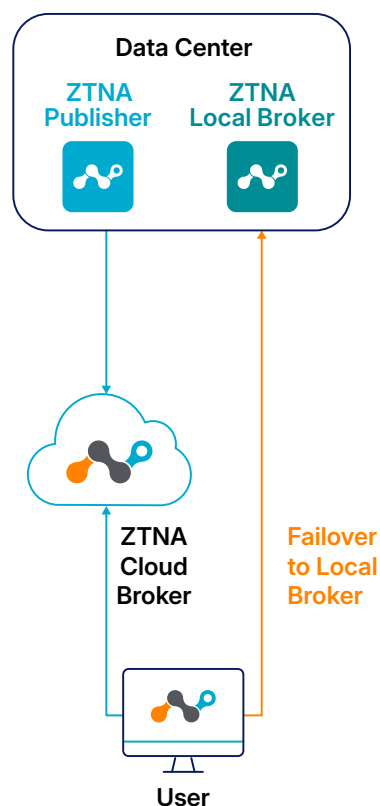


Figure 2: Business continuity with failover to the Private Access local broker.

Option 2: Netskope One SASE Gateway

The Netskope One SASE Gateway is a converged networking and security function deployable as a virtual or physical instance within the customer's data center. It operates independently of the Private Access management plane, ensuring resilience during service degradation.

The Netskope Client prioritizes standard brokers but automatically pivots to the SASE Gateway via an encrypted Layer 3 tunnel when primary brokers are unavailable. The gateway handles authentication and enforces zero trust policies before granting access.

Administrators can deploy gateways in hot standby, define Layer 3 failover policies, and maintain identity-based enforcement during management plane disruptions.

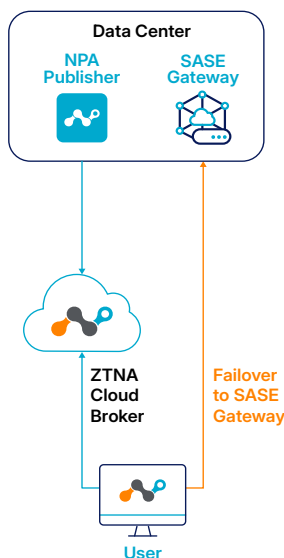


Figure 3: Business continuity with failover to the SASE Gateway.

BENEFITS	DESCRIPTION
Architectural resiliency	Eliminates single points of failure by decoupling the management plane from the data plane, delivering an industry-leading 99.999% SLA.
Decentralized security	Prevents login bottlenecks by hosting authentication and localized policy caches in every NewEdge data center, allowing for independent enforcement.
Intelligent traffic steering	Automatically fails over to the best available path based on real-time telemetry, health, and policy, ensuring users stay connected even if a primary tunnel degrades.
Reduced operational burden	Minimizes fire drills and manual interventions such as emergency DNS or firewall changes through automated failover and intelligent broker selection.
Seamless user experience	Provides instantaneous authentication and immediate tunnel setup, with automatic reconnect capabilities that switch users to the fastest path without intervention.
Flexible hosted continuity	Offers on-premises local brokers and SASE gateways as hot standbys to extend zero trust access to local environments or regions without a cloud data center.
Global performance	Leverages dedicated NewEdge infrastructure to bypass ISP congestion and "black swan" events via intelligent route control and overprovisioned capacity.
Multi-path fallback	Ensures continuity through diverse steering methods, including local DNS fallback, the Netskope One Enterprise Browser, and Private Access browser access (clientless).
Secondary vendor redundancy	Acts as a high-availability backup for third-party ZTNA solutions, allowing users to transition to a pre-provisioned Netskope environment without installing new agents.
Endpoint stability	Ensures client-level reliability through a strictly validated golden release cadence with built-in auto-update and software rollback capabilities.



Interested in learning more?

[Request a demo](#)

Netskope (NASDAQ: NTSK), a leader in modern security and networking for the cloud and AI era, addresses the needs of both security and networking teams by providing optimized access and real-time, context-based security for the AI ecosystem inclusive of agents, applications, tools, LLMs, people, devices, and data. Thousands of customers, including more than 30 of the Fortune 100, trust the Netskope One platform, its Zero Trust Engine, and its powerful NewEdge network to reduce risk and gain full visibility and control over cloud, AI, SaaS, web, and private applications – providing security and accelerating performance without trade-offs. Learn more at netskope.com, Netskope.ai, on [LinkedIn](#), and [Instagram](#).

©2026 Netskope, Inc. All rights reserved. Netskope, NewEdge, SkopeAI, and the stylized "N" logo are registered trademarks of Netskope, Inc. Netskope Active, Netskope Cloud XD, Netskope Discovery, Cloud Confidence Index, and SkopeSights are trademarks of Netskope, Inc. All other trademarks included are trademarks of their respective owners.