SONICWALL®

Why You Need ZTNA

A Buyer's Guide

Remote access (user accessing applications while outside the office) is no longer an exception. Users want the flexibility to work from office, home or anywhere in-between with consistent user experience. VPN worked well when majority of the users were accessing the applications only from branch office and applications were deployed on-prem. Now with growing 'work from anywhere' culture and applications being anywhere (on-prem or on-cloud(s)), IT teams are dealing with multitudes of 'micro' branches where traditional VPN solutions just can't keep up and the threat actors are aware of it.

Limitations with traditional VPN solutions serving anywhere workforce include:

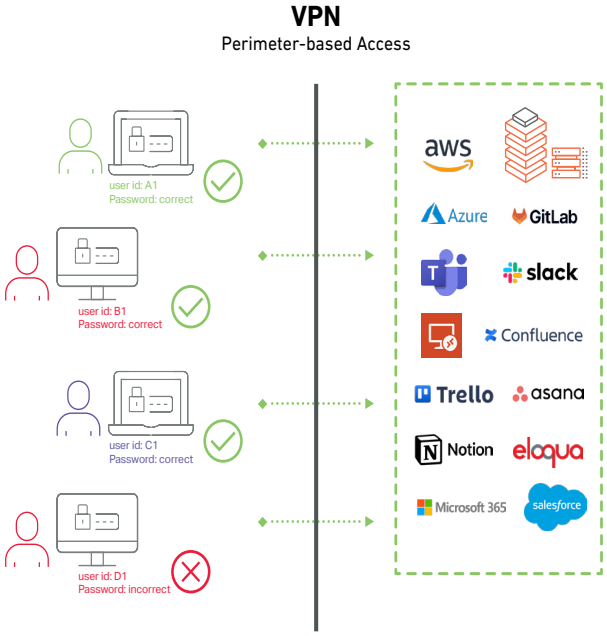
- Reliance on user credentials only for access
- Perimeter-based, as in, once in, user gets broad network access
- Lack of proper support for third party/temporary users
- Backhauling traffic to the data center for security scanning

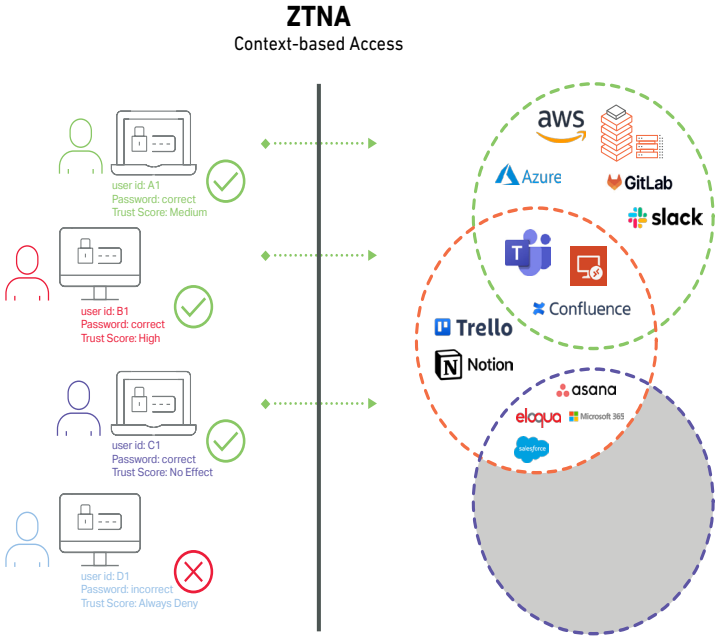
On top of that, MFA fatigue is real! MFA can be helpful but to a certain extend. The average US smartphone user receives 46+ notifications daily, interrupting their focus nearly every half hour. Cybercriminals exploit this distraction, tricking users into to agree to something they shouldn't triggering a breach.

With all these challenges taken into account, Zero Trust Network Access (or ZTNA) is considered more secure and fool-proof than the traditional VPN solutions out there today. ZTNA is a modern security model based on "never trust, always verify" approach. It creates a logical access boundary around applications based on identity and context. It verifies users and grants access to specific applications based on policies. ZTNA operates on an adaptive trust model, where trust is never implicit.

Feature	Traditional VPN	ZTNA
Access model	Broad, network-based	Granular, application-based
Security posture	Perimeter-based	Context-based
User Experience	Slow, can be complex	Faster, simpler
Visibility and Control	Limited visibility into user activity	Better visibility and granular control
Scalability	Less scalable, esp. for large-scale	Adaptable to changing needs

In ZTNA, a trust level (aka Trust score) is calculated based on the user ID, device ID, and device security posture then evaluated against policy, and if approved, short-lived certs are issued to permit access, which is then a direct path to the approved application or resource. ZTNAs employs continuous authorization, should the user's trust score drop to an unacceptable level, existing access sessions are suspended.





If your organization supports work from anywhere and leverages on-cloud and on-premises applications, ZTNA can bolster your security strategy. Here is quick guide on evaluating a ZTNA solution:

Feature / Capability		SonicWall	Vendor 1	Vendor 2
Easy to deploy	Immediate value – simple deployment	✓		
	100% software platform, no hardware or virtual appliance required	✓		
	Supports public and private cloud or on-premises installation	✓		
	Purpose built cloud-native ZTNA	✓		
	Requires minimal or no changes to corporate network infrastructure	✓		
Integration	Integrates easily with existing security tools	✓		
	Identity Provider for authentication	✓		
	MDM / EMM / UEM tools for device trust	✓		
	Export events/audit Logs to SIEMs (Splunk Phantom, Demisto, etc.)	✓		
	EDR for real-time device health signals	✓		
Access Controls	Easy-to-use, human-readable policy engine	✓		
	Trust scoring framework	✓		
	Continuous device trust validation (incl. EDR running/OS version/firewall/encryption)	✓		
	Supports for both managed devices and BYOD	✓		
	Real-time event monitoring and alerting	✓		
	Continuous authorization via short-lived certificates and tokens	✓		
	Granular, API-level controls	✓		
	User-to-application segmentation without providing access to the network	✓		
	Least privilege access restricts lateral movement	✓		
	APIs for policy and config automation	✓		
Architecture	Cloaks applications from public internet	✓		
	An identity-aware proxy architecture designed for multi-cloud environments	✓		
	A lightweight app installed on devices to continuously verify posture and establish trust	✓		
	Option for both hosted and self-hosted network of PoPs	✓		
	Integrates easily with existing IAMs through leading IAM marketplaces	✓		
	Incorporates native PKI for certs and integrates with existing PKI	✓		
Use Cases	Supports on-premises, hybrid- and multi-cloud, and SaaS use cases	✓		
	Hosted Web Applications – HTTP	✓		
	Servers – SSH/RDP, and Kubernetes	✓		
	Services – Database and other TCP	✓		
	Custom JSON	✓		
User Experience	A unified services catalog for all of their services and web-apps	✓		
	One-click access and autorun capabilities to infrastructure services	✓		
	Replaces user/password authentication to SSH with short-lived certificates	✓		
	Supports passwordless zero trust access	✓		
	Option to expose trust score metrics to end users thereby decreasing support calls	✓		
	Trust score shown to end users to help improve their device security posture	✓		
	Supports Windows/macOS/Linux/Android/iOS/iPadOS	✓		
Network	Requires minimal or no changes to existing networking infrastructure	✓		
	Roll out incrementally one service or application at a time	✓		
	No overlapping IP addresses and subnets to manage	✓		
	Uses cryptographic identity instead of IP address for network access	✓		
	Integration with SonicWall Gen 7 Firewall	✓		

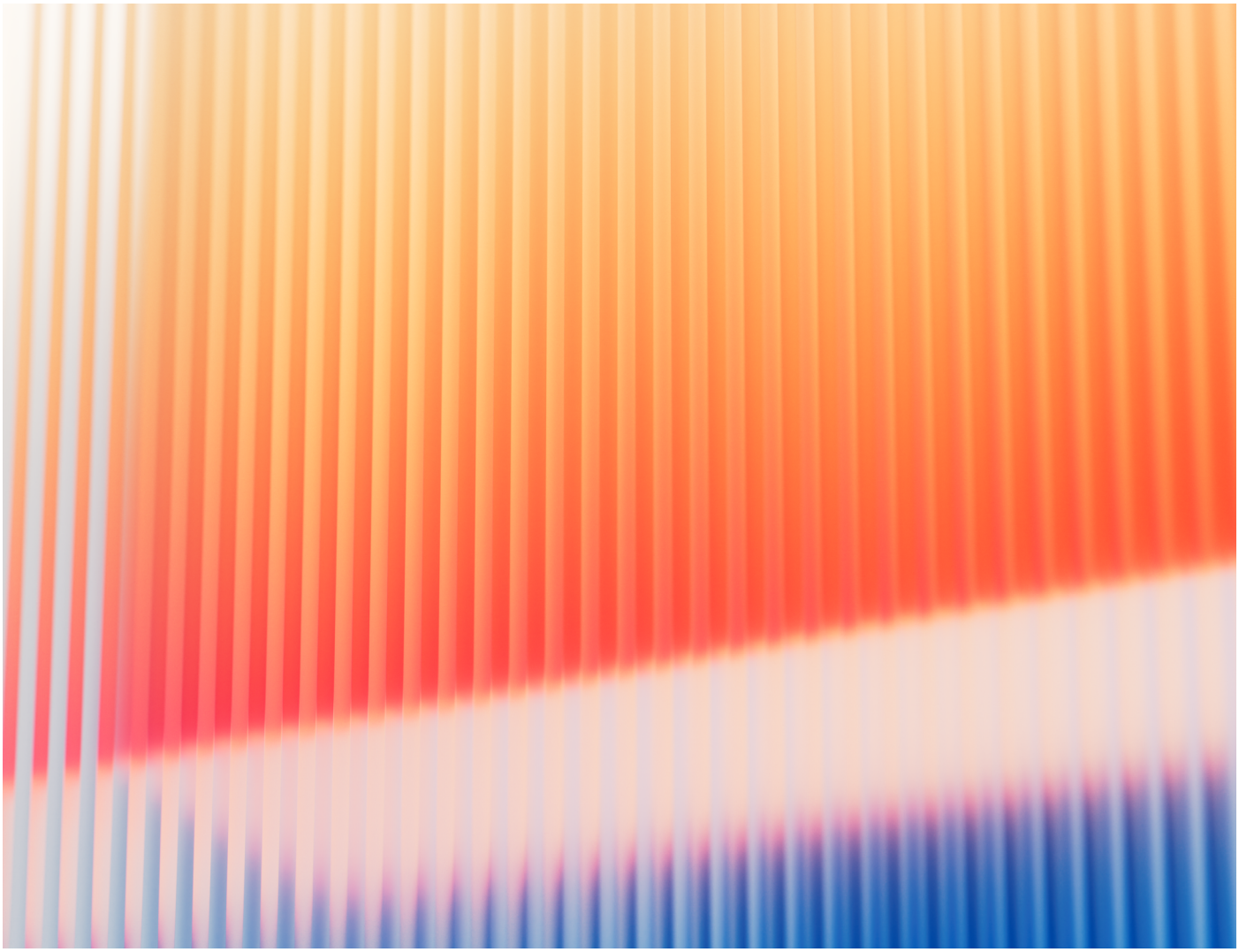
SONICWALL

About SonicWall's ZTNA solution, Cloud Secure Edge:

Cloud Secure Edge is known for its easy, fast, and secure approach to 'zero-trust' access to any application from any device and any location protecting both user and the business.

Try it by yourself by booking for a demo here.

Learn more about Cloud Secure Edge here.



About SonicWall

SonicWall is a cybersecurity forerunner with more than 30 years of expertise and a relentless focus on its partners. With the ability to build, scale and manage security across the cloud, hybrid and traditional environments in real time, SonicWall can quickly and economically provide purpose-built security solutions to any organization around the world. Based on data from its own threat research center, SonicWall delivers seamless protection against the most evasive cyberattacks and supplies actionable threat intelligence to partners, customers and the cybersecurity community.

SonicWall, Inc.
1033 McCarthy Boulevard | Milpitas, CA 95035
Refer to our website for additional information.
www.sonicwall.com