

Request for Proposal: Zero Trust Network Access (ZTNA)

Template from RFPhub.com. Replace everything in square brackets, adjust the Must-have/Nice-to-have priorities, and delete this note and the instructions section before you issue the RFP.

Instructions for the buyer (delete before issuing)

A ZTNA evaluation involves security, network, identity, endpoint and help-desk teams, and the hardest early task is finding out what your VPN actually carries today. The example schedule in this template runs about 11 weeks from kickoff to contract award; allow more if your proof of concept covers several data centers or cloud regions.

1. **Inventory what your VPN carries today (weeks 1-2).** Pull VPN logs and list the private applications users reach, where each one is hosted, the protocols it uses and who uses it. Flag the awkward cases early: server-initiated connections, voice and video, applications reached by IP address rather than host name, and site-to-site traffic. Record the numbers vendors will price against: employees, contractors, devices, applications and hosting locations.
2. **Assemble the buying team.** Include security, network, identity and endpoint owners, the owners of your main private applications, and the help desk, which will field the first access problems. Add procurement and legal, plus whoever manages contractor and partner relationships if third-party access is in scope.
3. **Settle the scope, and decide whether you need an RFI (weeks 2-3).** Decide whether you're buying ZTNA on its own or a wider SSE or SASE platform (see the next section). If that's still open, or your long list has more than five vendors, issue a short RFI asking how each vendor handles your awkward application types, contractor access and service locations, and use the answers to build a shortlist.
4. **Tailor and issue the RFP (weeks 3-6).** Delete requirements that don't apply, adjust priorities, and add your environment details and application

inventory to Section 1. Give vendors three weeks to respond, with a written question-and-answer window in the first week.

5. **Score the responses (weeks 6-7).** Have each evaluator score independently against the rubric before comparing notes, and set aside any vendor that misses a Must-have. Check every 'yes' for whether it needs an add-on license, a minimum agent version or a feature still in preview.
6. **Run a proof of concept with two or three vendors (weeks 7-10).** Place connectors in one data center and one cloud environment, and test with a pilot group on managed and unmanaged devices, including a contractor. Disable a test user and break a device's posture mid-session to see how quickly access ends, take a connector offline, and compare performance with your current VPN. Ask the help desk to diagnose a staged access failure. Call references that have switched off their VPN.
7. **Negotiate and award (weeks 10-11).** Use the pricing table to compare like for like, including contractor licensing and add-ons. Line up the subscription start with your migration waves and your VPN renewal date, and settle renewal caps and exit assistance before you sign.

ZTNA or full SASE: which RFP do you need?

ZTNA controls how users reach private applications in your data centers and cloud environments. On its own, it doesn't filter web traffic, control SaaS use or connect branch offices. Use this template when the job is retiring remote-access VPN, or giving contractors and partners access to specific internal applications.

If you also need a secure web gateway (SWG), a cloud access security broker (CASB), data loss prevention across all traffic, or SD-WAN, use the RFPhub SASE RFP template instead: it includes ZTNA as one of its services. If you're starting with ZTNA but expect to add those services later, keep this template and ask how your licenses carry over (requirement C6), so the first purchase doesn't box in the second.

Signs you need the SASE RFP rather than this one:

- You're also retiring on-premises web proxies, or need to control SaaS and generative AI use.
- Branch offices need new WAN connectivity, or branch firewalls are due for replacement.

- You want one agent, one console and one policy for web, SaaS and private-application traffic.
- You need data loss prevention on web and SaaS traffic, not only on private applications.

Contents

1. Introduction and Background
2. Project Objectives
3. Scope of Work
4. Requirements
5. Vendor Questions
6. Evaluation Criteria and Scoring
7. Pricing Response
8. Submission Guidelines
9. Timeline

1. Introduction and Background

[Company Name] is seeking proposals for a zero trust network access (ZTNA) solution that gives employees, contractors and partners per-application access to our private applications, based on identity and device posture, and replaces network-level remote-access VPN. This RFP describes our requirements, the questions we need answered, and how proposals will be evaluated.

Organization background

- [Describe your organization: industry, size, locations]
- [Regulatory or contractual requirements that apply]
- [Current remote-access setup: VPN products, concentrator locations, and what else the VPN carries (site-to-site links, server-initiated connections)]
- [Number of employees, contractors and partner users needing access, and their devices: managed, personally owned or unmanaged]
- [Private applications in scope, where they are hosted (data centers, cloud providers and regions, other sites) and the protocols they use]
- [Identity providers, MFA, endpoint management and EDR tools in use]
- [SIEM and security operations tooling]

2. Project Objectives

- Replace network-level remote-access VPN with per-application, least-privilege access to private applications
- Check identity and device posture on every connection, and re-check them during active sessions
- Remove inbound internet exposure of private applications and VPN concentrators
- Give contractors and partners time-limited access to specific applications without putting them on our network
- Improve remote-access reliability for users and reduce help-desk effort
- Give security operations a complete record of every access decision

3. Scope of Work

The selected vendor will be responsible for:

- Delivery of the ZTNA service from service locations serving [regions]
- Design and deployment of application connectors in [data centers, cloud environments and other sites]
- Deployment of the agent to [number] managed devices, and agentless access for [number] contractor and unmanaged-device users
- Application discovery, policy design and migration from VPN in waves agreed with [Company Name]
- Integration with our identity provider, endpoint management, EDR and SIEM
- Training for administrators and help-desk staff
- Ongoing support and service management for the contract term

4. Requirements

For each requirement, enter a response code and a short explanation. Y = available today in the proposed edition; P = partially met or needs configuration/services (explain); R = on the roadmap (give a date); N = not supported. Must-have requirements are pass/fail; Nice-to-have requirements add points.

4.1 Functional

ID	Requirement	Priority	Response	Vendor comments
F1	Access granted per application, never to the network: each policy names the	Must		

ID	Requirement	Priority	Response	Vendor comments
	applications (by host name, wildcard domain, IP address or range, port and protocol) and the users or groups allowed to reach them.			
F2	Policy rules that combine identity-provider attributes (user, group, department, employment type), device posture, location and time of day, evaluated on every new connection.	Must		
F3	Device posture checks for operating system version, disk encryption, host firewall, screen lock, a valid device certificate and a running EDR agent on Windows and macOS. State what can be checked on Linux, iOS, Android and ChromeOS.	Must		
F4	Continuous evaluation during active sessions: when a device falls out of compliance or a user is disabled, existing connections are ended or moved to a restricted policy. State how often re-evaluation runs and how quickly a change takes effect.	Must		
F5	Per-application re-authentication rules, such as requiring fresh MFA through our identity provider for sensitive applications or after a set interval.	Must		
F6	Agent-based access for any TCP or UDP application, including thick clients, file shares, SSH, RDP and real-time voice and video. State support for ICMP and for applications that use dynamic ports.	Must		
F7	Agentless access from a standard browser to internal web applications, for unmanaged devices and contractors, with nothing installed on the device. State whether RDP and SSH sessions can also be delivered in the browser.	Must		
F8	Controls for agentless and unmanaged-device sessions: blocking downloads, uploads, copy-and-paste and printing, browser isolation for sensitive applications, and recording of RDP and SSH sessions.	Nice		
F9	Third-party and contractor access with its own policies: external users sign in through our identity provider or their own organization's identity provider via federation, see only the applications assigned to them, and lose access automatically on an end date.	Must		

ID	Requirement	Priority	Response	Vendor comments
F10	Just-in-time access requests, approved by an application owner or sponsor, that grant access to a named application for a set time window.	Nice		
F11	Discovery of the private applications users reach, from observed traffic, to build our application inventory and show which applications still depend on the VPN.	Must		
F12	Policy recommendations based on observed access that narrow broad rules toward per-application least privilege, with a preview of the users affected before a change is applied.	Nice		
F13	An always-on connection that starts automatically and needs no user action after sign-in, plus pre-logon access on Windows so domain sign-in, group policy and device management work before a user logs in. State macOS support.	Must		
F14	A help-desk view of each user's recent access attempts and sessions, showing the device posture result, the policy applied and the reason any request was denied.	Must		
F15	Server-to-client connections, such as help-desk remote assistance or software deployment to a user's device, so these flows don't keep the VPN in service.	Nice		

4.2 Technical and architecture

ID	Requirement	Priority	Response	Vendor comments
T1	Outbound-only connectors: private applications need no inbound firewall rules, public IP addresses or listening ports exposed to the internet.	Must		
T2	Connectors deployable as virtual machines, as containers and as images for each cloud provider we use [list], with published sizing and supported throughput per connector.	Must		
T3	Connector groups with automatic load balancing and failover, and a recommendation for where to place connectors and how many to run in each of our data centers, cloud networks and regions.	Must		
T4	Central monitoring and upgrade of connectors, with health alerts and upgrades we can schedule and stage by	Must		

ID	Requirement	Priority	Response	Vendor comments
	connector group.			
T5	Resolution of internal DNS names through the connectors, including split DNS, so users reach applications by their usual host names.	Must		
T6	Service locations offering private-application access in [list your regions], with each user's connection routed to a nearby location automatically. State any location where private-application access isn't offered.	Must		
T7	Documented behavior when the vendor's control plane, a service location or a connector group is unavailable: what happens to new and established sessions, and how long failover takes.	Must		
T8	A business continuity option that keeps designated critical applications reachable through customer-hosted components if the vendor's cloud service can't be reached.	Nice		
T9	Local enforcement for users on the corporate network, so the same per-application policy applies on site without sending traffic to on-premises applications through the cloud.	Nice		
T10	Coexistence with our current VPN client and other security agents on the same device during migration, with documented handling of routing and DNS conflicts.	Must		
T11	Encryption of all traffic between agents, the service and connectors, with mutual authentication of each component. Describe the protocols used and how device and connector certificates are issued, stored and rotated.	Must		

4.3 Integration

ID	Requirement	Priority	Response	Vendor comments
I1	Sign-in through our identity provider via SAML 2.0 or OIDC, SCIM provisioning of users and groups, and support for more than one identity provider (for example, a separate one for partners).	Must		
I2	Device posture and risk signals from our endpoint management (MDM/UEM) and EDR tools, usable in access policy. List the tools with pre-built integrations.	Must		