timus

ZERO TRUST NETWORK PROTECTION

Technical FAQ

Q. What does Timus Networks do?

Timus Networks simplifies network security and access for SMBs and mid-market enterprises helping to significantly reduce business risks and bolster compliance. Our premier ZTNA product, Timus SASE, transforms complex setups involving multiple tools into a single, unified solution that secures networks and safeguards users, regardless of their location or device.

Developed by firewall experts with decades of cybersecurity experience, Timus SASE is purpose-built for the MSP/MSSP Channel. It offers simplicity and rapid deployment, with installation in under 30 minutes.

Always-on, Zero Trust Network Access

Adaptive Cloud Firewall on a Dedicated Gateway

Protect your SaaS Apps behind a Static IP address

Secure Web Gateway for Safe Browsing, and Compliance

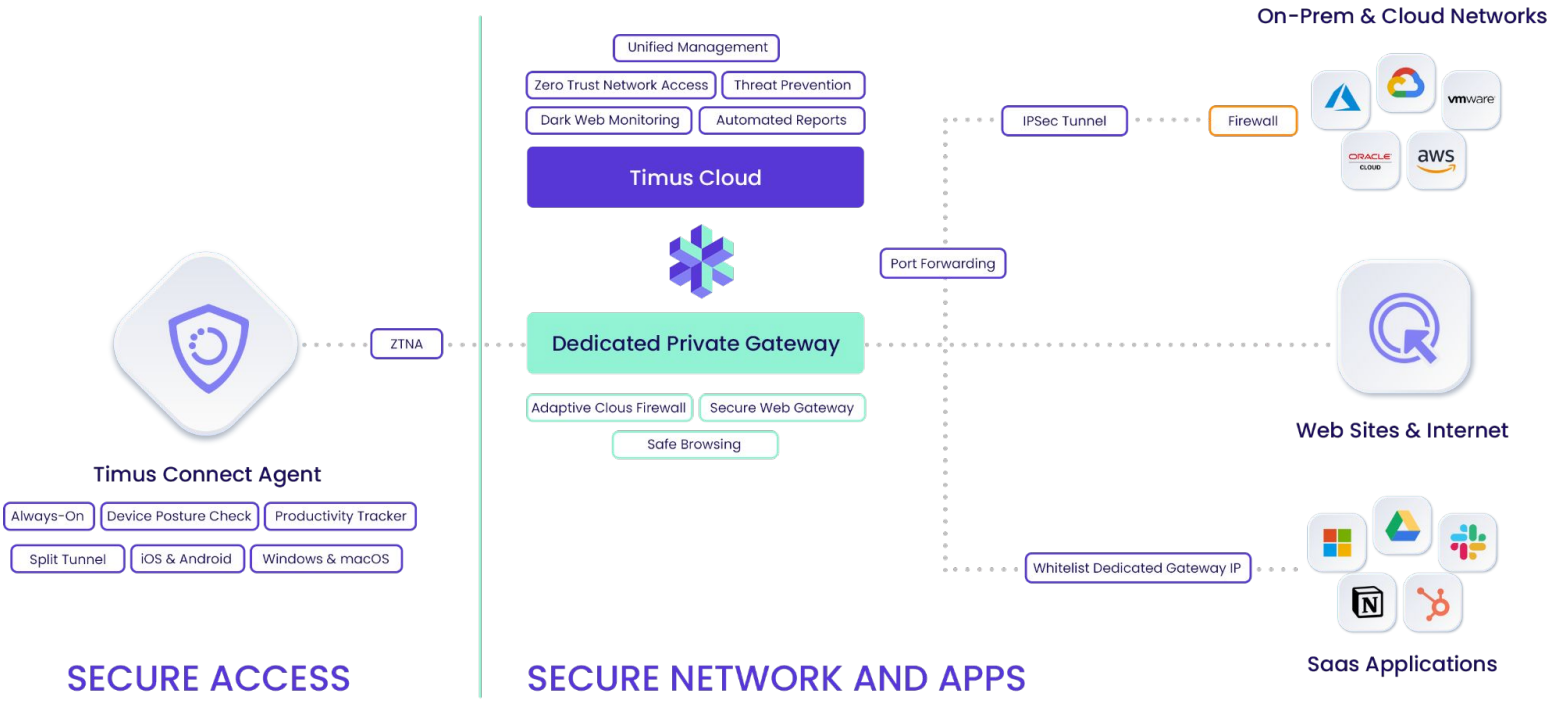
Q. How can we start with Timus SASE?

See the Timus Quick Setup Guide

Q. What services could potentially Timus SASE replace in my security stack?

VPNs, Dark Web Monitoring, Activity/Productivity Tracker, DNS filtering, network level malware and category & content filtering via SWG. Timus SASE also provides a cloud-based firewall that can be used in conjunction with or in lieu of an on-premise FW. Timus SASE also allows for using free MFA tools such as Google Authenticator. Timus SASE helps harden RDP connections via solid ZTNA as well.

Q. How does the high-level Timus SASE architecture for a Client look like?



Timus SASE uses zero-trust secure remote access and least privilege principles before granting any access to the network and data to protect against hackers, criminals, and ransomware. Additionally, Timus SASE uses URL/web filtering (at the network level) to protect users from malware, phishing, and malicious sites from wherever they may encounter it (any device, application, protocol or port). A user is protected against all of the below:

- Malicious software including drop servers and compromised websites, including drive by downloads and adware
- Fraudulent phishing websites that aim to trick users into handing over personal or financial information
- Command and Control botnet hosts
- Sites which serve files or host applications that force the web browser to mine cryptocurrency
- Parked sites & domains that may no longer be controlled by the original owner

Q. What intelligence services are utilized by Timus SASE for better protection?

Timus SASE uses best-in-class intelligence services for better protection. Intelligence data is used in firewall rules, ZTNA policies and logs. Some examples include:

- IP address intelligence for users' public IP addresses to see if they are part of abusive activities, a proxy or TOR network, a botnet, etc.
- Geo-location intelligence for users' location
- Malware, ransomware, phishing and many other suspicious domains
- Dark web monitoring for users' and administrators' email addresses daily to see if they are breached

Q. What is the maximum number of firewall rules we can create on your platform?

There is no limit on the number of firewall rules that can be created (subject to change).

Q. How many site-to-site tunnels can we create?

The number of gateways that you can create are dependent on your Timus plan, but the number of tunnels associated with the gateways are unlimited. You can build tunnels to as many sites as needed.

Q. Does Timus SASE provide shared or dedicated gateways?

Timus SASE provides dedicated gateways with static IP addresses. An MSP can allowlist the Static IP in SaaS applications for controlled access and additional security.

Q. Is there a limit on the amount of traffic passing through Timus SASE gateway?

No, traffic passing through the gateway is not limited.

Q. Is there a limit on the bandwidth of traffic passing through Timus SASE gateway?

Bandwidth through the gateway depends on your Timus plan. There are 500 mbps and 1000 mbps options.

Q. Can we create custom web categories and use them in firewall rules?

Yes. Timus SASE has 30 pre-defined web categories with frequent website list updates that can be used in firewall rules to allow/deny access. You can also create custom categories with your own website lists and keywords. Timus SASE also provides detailed web access logs at the user level.

Q. How long do you retain logs?

Depending on the pricing plan, we will retain logs for either 15 or 30 days.

Q. Do we still need to have an EDR solution if we use the Timus SASE platform?

While Timus SASE provides a suite of security services attached to our gateways, our domain is primarily in network security, with a very light-weight, OS agnostic agent installed on the device. Timus recommends that you maintain endpoint security in your stack in unison with our network security to provide a holistic protection of your customers' devices and resources.

Q. How do we download Timus Connect agent?

Download links to Timus Connect application are available in the following places:

- Inside Timus management portal manage.timusnetworks.com, Manager->Settings->Downloads page. Admins can access here.
- Inside my.timusnetworks.com user portal Downloads page. Users can access here with their Timus credentials
- Inside Timus Networks web site timusnetworks.com, Resources page Documents & Downloads section.

Q. Which tunneling protocols are supported by the Timus Connect agent?

WireGuard and OpenVPN tunneling protocols are supported.

Q. How does split tunneling work?

The tunnel for secure connections can be configured to pass all user traffic, or just part of it, through the tunnel. Split tunnel configurations can be created in the Manager->Settings-Tunnel Configuration page. Default configuration is all traffic passes through the tunnel. Timus Connect agent gets the tunnel configuration valid for the user and context, and passes traffic through the tunnel accordingly. This feature is currently available only for Windows and macOS releases of the Timus Connect app.

Q. Can we manage Timus Connect agent settings centrally?

Yes. Agent profiles can be created in Timus Manager. Settings can be configured as only the admin can edit, or users can edit as well.

Q. How is the Timus Connect app updated?

When a new update is available, the Timus Connect application will automatically notify you that there is an update, along with a button to start the update wizard.

Q. I have to periodically send out reports to my CTO regarding network traffic and utilization. Can I use your platform for this?

We allow organizations to send out automated reports on a scheduled basis.
These reports can be shared to whomever is required to view this information. All you need to do is provide their email address and the reports will automatically be sent out at a time of your choice.

Q. How many users are supported comfortably on your platform?

We can support about 100 users per gateway, depending on the traffic of the users. Of course, adding more than one gateway will optimize the experience and allow for more users. This will also further facilitate remote work as more gateways in more regions will minimize latency and increase available bandwidth.

Q. How can we reduce latency and have redundancy for gateway connections?

To reduce latency, you should have gateways close to your users as much as possible. Thus select the datacenter region accordingly while creating a site in Timus Manager. You can have multiple gateways for redundancy. Users can be allowed to access all or some of the sites. Timus Connect agent can be configured to connect to the gateway that has the fastest round-trip time, which means the fastest gateway connection to the user.

Q. How are ZTNA policies prioritized?

Only one policy will be valid for each sign-in attempt, and that will be the most specific policy with respect to the source items selected. Policies within Timus' Zero Trust Network Access (ZTNA) security framework are automatically prioritized from specific to general. More specific policies take precedence over general policies. The most specific policy with respect to the source items has the highest priority.

For example, if there is a specific policy that denies access to a specific user and a general policy that allows access to all users, the specific policy will take precedence, and the specific user will be denied access.

Q. I only want to be alerted of mission-critical sign-ins. How can I limit what is blowing up my inbox?

When creating a user sign-in policy, select the Alerts and Notifications tab and select Notifications. You can select a higher severity for notifications, so that you are only notified when something our system has determined to be high-risk has occurred.

Q. Which MFA methods are supported?

- MFA with an authenticator app like Google Authenticator, Microsoft Authenticator, Authy, Duo Mobile.
- MFA with email. A one-time code is sent to the user's email address.

Q. How do we set MFA policies for users or administrators?

MFA policies are set within ZTNA policies, both for users and admins. MFA can be configured adaptively based on certain behaviors like new devices, new country, etc. If no behavior is selected, MFA is applied to all sign-in attempts.

Q. I want to create a global rule to block all users from accessing certain websites. What should be selected as the source?

Our dynamic firewall can be used in a couple of ways to create global rules.
1. The source can be set to IP: Wireguard Client Subnet or IP: OpenVPN Client Subnet
2. A team can be created that includes all users within Timus and it can be used as the source.

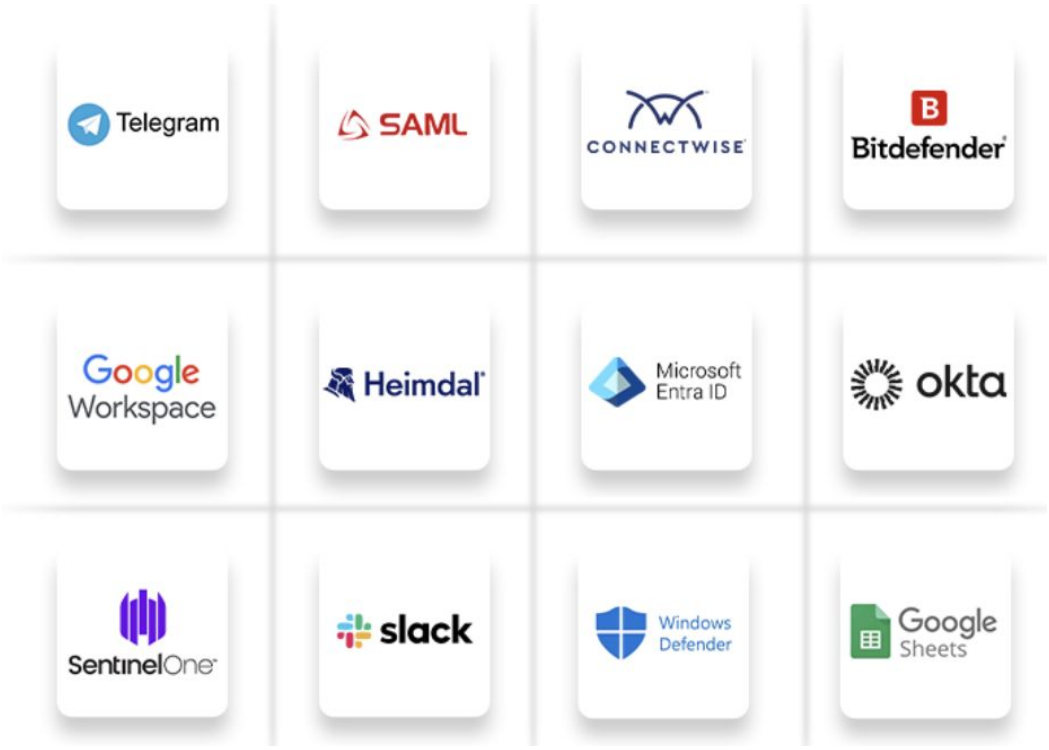
Q. If I am using my identity provider to sync users into Timus, will new users created within Timus also backwards sync into my IdP?

Identity integrations use your chosen IdP as a single source of truth. For this reason, two-way syncing can become messy, especially if more than one IdP is added to the SDN. If you need to add a new user into your IdP, it is required that the user be added from the IdP. From there, the user will be synced to Timus.

Q. I have several on-prem file shares and web servers that I need to have access to. Can I use your platform to enable remote access to them?

By utilizing the firewall functionality with IPSec site-to-site tunneling to on-prem environments, you can enable granular remote access to your resources by connecting the edges of the two networks and forwarding RDP or SSH traffic to the relevant devices.

Q. What does Timus SASE come integrated with?



Identity Providers & Authentication

- Active Directory (on-prem)
- Google Workspace
- Microsoft Entra ID (cloud)
- Okta
- SAML 2.0

Endpoint Protection Platforms

- BitDefender
- Heimdal
- Microsoft Defender
- SentinelOne

Notifications

- Slack
- Telegram

Data Synchronization

- Google Sheets

Billing Integration

- ConnectWise PSA

Q: How do I troubleshoot issues with syncing users from identity providers?

Ensure your identity provider credentials are up to date and correctly configured in Timus. For Azure AD, ensure the application ID and secret key have proper permissions. You can find in-depth troubleshooting guides for integrations here.

Q: What are the OS compatibility requirements for Timus Connect?

Windows: Windows 10 and above.
macOS: macOS 11 (Big Sur) and above.
Mobile Devices: iOS 14+ and Android 10+.
Legacy OS support may have limitations; see the Timus Compatibility Matrix.

Q: How do I debug split-tunneling issues for remote users?

- Verify the split-tunnel configuration in the Manager → Settings → Tunnel Configuration page.
- Confirm specific applications or IPs are correctly listed to bypass the tunnel. Ensure to include a wildcard if necessary for expanded coverage. For example, use *.reddit.com instead of reddit.com to include all subdomains.
- For client-side issues, check the Timus Connect logs located in the application under "Settings → Diagnostics".

Q: How can I optimize gateway configurations to reduce latency?

- Choose the datacenter region closest to your primary users while setting up the gateway.
- Enable automatic gateway selection for users in the Manager portal under "Settings → Integration -->Allowed Sites".

Answers to the questions in this FAQ are strictly subject to change based on roadmap, plans, and business direction.