SANGFOR

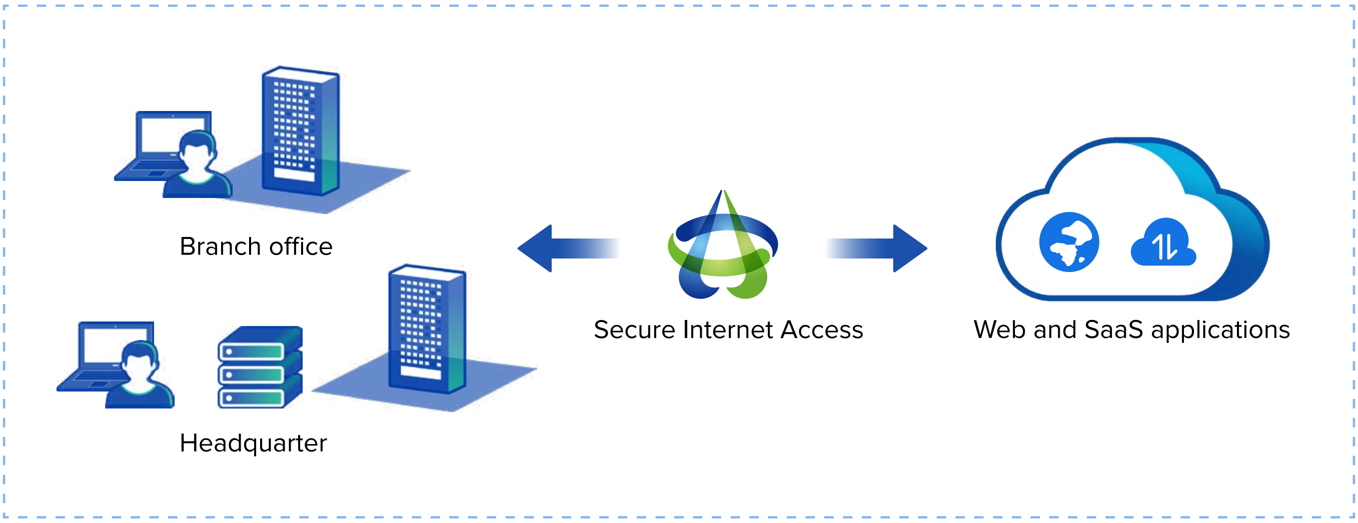
marketing@sangfor.com
www.sangfor.com

SOLUTION BRIEF
Secure Internet Access

Sangfor IAG

Internet Access Gateway

Internet Access Gateway (IAG) is secure internet access (SIA) solution designed as a cost-effective user-centric protection solution. By leveraging its purpose-built platform, IAG caters to customers' needs with a collective set of SIA solutions providing the first line of defence against threats on the internet.



Visibility	Identity	Control				Analytics
Encrypted traffic	User Identity & endpoints	Reduce risk exposure	Malware Protection	Data Loss Prevention	Identify & manage web & SaaS applications	Investigation & remediation with user and network analytics
What is the impact and why is it important?						
While encryption is necessary for the exchange of private business information, this can also leave organizations blind to hidden security threats.	Tracking IP address instead of username will undermine your ability to know who is the actual user identity with associated role and permissions.	Accessing inappropriate or llegal content will lead to productivity loss and penalty under cyberlaw.	Malware infections disrupt your business operation and damage company critical data.	Data loss will permanently damage company reputation damage customer trust and eventually go out of business.	Lack of SaaS application control will result in unauthorized application access and data exfiltration.	Inability to track user behavior and activities will allow malicious content or unauthorized activities to bypass your security perimeter undetected.
What can you do to protect yourself?						
SSL decryption allows you to inspect encrypted traffic and confirm no malicious activities or malware payloads are hiding and delivered in your network traffic.	User identity-centric policies focus on assigning, securing and controlling user access.	Web filtering to enforce company acceptable use policy and reduce time spent on non-work-related websites.	Network anti-malware protection can shield the users and intemal network from malicious content.	Data loss prevention detects, monitors and blocks sensitive data from leaking outside the corporate network.	Maintain control using lists of sanctioned and unsanctioned SaaS applications to minimize business risk and increase visibility.	Real-time analytics-based user internet activity dashboard and reports pinpoint abnormal user activities and provide clear remediation.

Challenges Solved

Securing users with comprehensive protection

- Gateway and client SSL decryption to ensure full visibility into your user internet access traffic.
- A user-driven solution to ensure all policies and protections provide granular control based on username and associated devices.
- SIA provides all the access control and web URL categories for blocking risky websites and unintended website access to reduce risk exposure.
- Anti-malware protection with the latest machine learning and deep learning capabilities identifies and blocks even the most advanced malware.
- Intuitive DLP engine monitors and prevents data exfiltration by clueless or rogue users.
- CASB control ensures accurate identification and granular control on sanctioned and unsanctioned SaaS applications.
- Comprehensive analytics and drill-down reporting enable rapid identification and remediation for users' internet access activities.

Secure Internet Access Differentiator

1. User identity-based policy

It enhances existing access control and security policy mechanisms by specifying users or groups when creating policy. This empowers any organization to easily identify user activities on network resources and simplifying user activity monitoring.

2. A single vendor with a unified management platform

SIA is managed by Platform-X enabling a familiar and seamless single pane of glass administration experience across Sangfor security products and solutions including the new Omnipoint Secure Agent (All-in-One agent) for ease of management and deployment. Furthermore, strong integration between IAG, Cyber Command, and NGAF ensures better threat detection, faster response, and ease of operation & management.

3. Secure onboarding devices network access

Any onboarding BYOD and IOT devices will go through a compliance check to ensure these devices are secure and keeping your network safe. SIA delivers agent and agentless visibility to continuously discover, assess and remediate devices without disrupting your business operations.

4. Stop proxy avoidance

Many organizations have users accessing proxy avoidance applications such as Ultrasurf, Freegate, etc. to circumvent security protection and access web content that should be filtered. SIA provides comprehensive proxy avoidance protection by using IAG with Endpoint Secure to deliver dynamic detection and blocking of proxy avoidance applications.