

Internet Access Management

As Asia's first technology brand to deliver an Internet management solution, SANGFOR's IAM series can help you achieve complete management of your organization's Internet access. By virtue of powerful functions and easy administration, SANGFOR's IAM family delivers the most effective solutions for P2P traffic management, prevention of unauthorized information disclosure, legal risk mitigation, Internet access usage monitoring, and online security, plus many other features.

SANGFOR's IAM has an industry-leading network behavior recognition ability, with an extensive built-in application recognition database. IAM products can govern up to 500 types of Internet applications. Statistics-based P2P smart recognition technologies can identify encrypted, newly-released or even unknown variants of P2P applications, providing technological assurance for complete governance of P2P applications.

Based on nine years of real world research and development in core networking technologies, as well as a fully optimized systems architecture and a high-performance hardware platform, the SANGFOR IAM series is significantly more advanced than comparable offerings. The IAM products can govern networks of more than 50,000 users.

Features

Function		Description
Authentication	User identification	An extensive range of user identification approaches to fit the needs of almost any organization. These include IP, MAC, IP?MAC binding, username / password, third-party authentication such as LDAP / AD / RADIUS / POP3 / PROXY, USB-KEY and hardware authentication; Single Sign-on (SSO) options include LDAP / POP3 / Proxy and forced SSO of designated network segment / account; account control via public / private accounts and account validity period; account import options include text list, IP / MAC scanning and even account and organization structures from Active Directory servers
	Authentication exception	Accounts can be renamed (in the IP / MAC / Computer name formats) based on new users' IP segments; authentication exception handling includes conflict detection, privileged control after authentication failure and page forward control after successful authentication
	Online access authorization	Multi-level user account management to align with organizational structure, allowing access control based on account IP, application, behavior, content, period and etc; Implements re-use, integration and forced inheritance of access privileges by combining object-based access policy templates; monitoring of accumulated duration and maximum traffic for specified user applications
Internet Access Control	Webpage control	Contains extensive built-in URL database that can be also manually customized; Support Webpage filtering based on URL / search word / keyword contained in Webpage; Support keyword-based filtering of outbound Webmail and Web post; fine-grained control such as allowing only reading post but not post thread, and only allowing receiving but not sending mail
	Advanced control	Encrypted SSL URL filtering, identifies and filters attempts to avoid management via public network proxies or encrypted proxy software; Capable to control behavior of sharing web access privileges with others via installed proxy software
	File control	Capable to control outbound file transmission via HTTP / FTP / email attachments, supports identification and blocking of outbound files based on file extensions and file types (to identify encrypted, compressed, extension name modified files)
	Application identification	Over 500 application identification rules conveniently built-in to identify and control popular network protocols, including IM chat, network games, Web-based stock trading, P2P, streaming media, remote control and proxy software
	Intelligent P2P identification	Identified over 30 popular P2P application protocols such as BitTorrent, eMule and etc, with deep packet inspection (DPI); SANGFOR's patented intelligent P2P identification technology can further comprehensively identify and manage other variant P2P protocols, encrypted P2P behaviors and unknown P2P behaviors
	Email control	Support complete blocking of email reception and sending, and filtering of outbound and inbound junk mail, filtering can be based on multiple conditions, such as keywords, sender and receiver addresses; Patented 'Postponed Sending after Audit' option intercepts outbound email per predefined criteria before allowing delivery after manual examination
Bandwidth management	Multiplexing and intelligent routing, bandwidth management based on wide range of criteria, including application type / Website type / file type, user, time, target IP and etc; extranet-to-intranet access flow control and bandwidth management	

Internet Access Management

Function		Description
Audit and Report	Real-time monitor	Real-time monitoring of CPU / harddisk / traffic / connection /session status, as well as online user information, traffic, ranking and connection ranking, real-time utilization visibility of bandwidth channels
	Access audit (Optional)	Records a wide variety of audit information including: URL, Webpage title and content accessed (can record only Webpage content containing specific keywords), outbound file transmissions via HTTP and FTP and file content, names and behavior of files downloaded, plain text thread posting and emails, chat sessions on MSN, MSN shell, Skype, Yahoo! Messenger, Google Talk and etc, also records application behavior such as network gaming, stock trading, entertainment, P2P downloads and Telnet, tallies user traffic and access duration and audits Webpage / file / email access of extranet users on intranet servers
	Reporting	Supports various kinds of reports, including scheduled reporting of statistics, behaviors, trend, comparison, plus customized reporting of traffic statistics, queries, ranking, times and behavior of users and user groups
	Data center features	Massed log storage with built-in and independent data center support; administrators can easily manage users based on a hierarchical permissions structure
	Audit-free key	Prevents access audits for users assigned audit-free keys. Audit-free status cannot be arbitrarily changed by system administrator (Optional)
	Log check key	Data center administrators can view recorded audit los only via audit check key (Optional)
Content search	Google-like log search tool to enable the manager to locate logs quickly by entering multiple keywords, including the search and location of the content of the log attachments, support the title subscription, and support automatically sending the search results to designated mailbox	
Network Security	Online access security	Built-in firewall threats a range of security, threats to gateway reliability, incliding DoS attacks, ARP spoofing and etc Identifies and filters viruses from external network (Optional) Built-in professional anti-virus engine in router mode
	End-point detection	Detects and end-point profile (including OS version / patch, system processes, disk files, registry and etc) and can prompt or reject access for end-points not meeting IT requirements or passing security tests
	Gateway anti-virus	Built-in professional anti-virus engine supports gateway virus elimination (Optional)
Equipment Management	Deployment mode	Deployable via router, bridge, bypass and multi-bridge topologies, with active-standby for HA
	Device management	Web based management access; functionality of different modules can be assigned to different administrators as needed, via a hierarchical management paradigm

