SANGFOR
INTERNET ACCESS GATEWAY

Secure User Internet Access Behaviour

- Detect and block unwanted behavior in encrypted traffic.
- Identify which applications are accessed by who and when.
- Boost user productivity through internet access compliance.
Sangfor
Internet Access Gateway Solution

Internet has become an increasingly vital platform for most businesses as an increasing number of business-critical applications are deployed over the Internet.

However, with great opportunities come great challenges. Improving user experience & work efficiency, blocking illegal endpoints, reducing bandwidth consumption, guarding intellectual property rights, protecting against malware and implementing internet access compliance have become the primary challenges for IT managers, who are often seen as an expense rather than an investment.

Furthermore, as BYOD (Bring Your Own Device) becomes more prevalent in the workplace, improved network management technologies are more important than ever for overwhelmed IT departments.

SANGFOR Internet Access Gateway (IAG) is a secure internet access solution that addresses enterprise network challenges by allowing users and networks to be managed in a simple and visible manner.
• **Advanced Report Center**: Accurate Traffic Reporting and Graphs

• **Content Visibility and Auditing**: Instant Messaging, Emails and Social Media

The old adage “You can’t manage what you can’t see” describes the challenges and risks of modern enterprise networks, making a comprehensive Report Center a critical component for IT departments to analyse network traffic. SANGFOR IAG includes an Advanced Report Center supporting numerous report customization options measuring traffic statistics, queries, ranking, times and behaviour of user & user groups, helping enterprises analyse the root causes of all network issues.

In addition, as information and data are becoming key business assets, enterprises are paying more attention to preventing potential information leakage and disruptive network activities. SANGFOR IAG boasts refined content and attachment auditing for corporate Instant Messaging programs.

• **Advanced Report Center**

IAG Advanced Report Center records, audits and counts all network behaviour to all unauthorized network behaviour of intranet users in easy-to-read graphical reports. With reports, curves and statistics, IT managers are provided with all the detailed information they need about their network, including Internet access activities, bandwidth consumption and viewed content. Reports are self-generating and sent automatically & regularly to an appointed e-mail address to effectively assist in the network design, security and optimization of bandwidth usage.

**Simple & Intuitive Reporting**

- User Report
- Application Report
- URL Report

These graphics are available in the Control Panel of IAG.
BM & User Access Management

- **Bandwidth Management**: Guaranteed Bandwidth for Critical Applications
- **User Access Management**: Avoid Abuse by Restricting Access & Devices
- **Application Control**: Protect Enterprises Against Unauthorized Applications
- **URL Filtering**: Monitor & Control Evasive Activities
- **Endpoint Control**: Management of Mobile Devices & Tablets
- **Illegal Wi-Fi Hotspot Detection**: Block Phishing Wi-Fi to Avoid Data Leakage

To solve these common issues SANGFOR IAG employs a URL & application database, which helps IT administrators effectively to enforce organization internet compliance by setting specific policies.

In addition, as the BYOD trend is becoming more and more popular, mobile devices should be also included in the enterprise network management policy. IAG empower IT administrators to ensure onboarding devices are identified and comply according to assigned acceptable user policy (AUP).

Sangfor IAG also detects and blocks illegal Wi-Fi hotspots to avoid any information leakage from laptops, smartphones or tablets. A wireless endpoint list will display which endpoint is using an illegal Wi-Fi hotspot allowing the IT team to decide whether to block it or not.

- **Authentication based on SMS, Portal, Social Media & QR Code**
- **Push Advertising based on SMS, Portal & Social Media**

**Authentication & Push Advertising based on SMS**
One of the quickest and most common way to collect customer information is by collecting phone numbers. When connecting to the Wi-Fi access point, the login page will ask the customer to insert a phone number to access the internet, allowing your business to send advertisements to your customers through SMS or phone call.

**Authentication & Push Advertising based on Portal**
Another common solution for collecting information is to redirect customers to a customized portal page after they have successfully connected to your Wi-Fi. This portal can be customized with any kind of information such as daily promotions, new products or services, etc.

**Authentication & Push Advertising based on Social Media**
Facebook, Line and WeChat are the fastest growing social media platforms in Asia. They can now be used as an authentication method for your Wi-Fi while simultaneously increasing your number of followers. More importantly, you can use push information to reach a larger potential customer base.
Authentication via QR Code

For companies receiving dozens of visitors per day, sharing the Wi-Fi password can become headache for the staffs. With Sangfor IAG, you can create a QR code to allow your visitors to connect to the Wi-Fi simply by opening any QR code software and scan it. With this type of authentication, there is no need to change your Wi-Fi password every time and you can generate the QR Code according to each visitor group.

Business Intelligence Platform

The Look of Innovation

Sangfor Business Intelligence Platform (BI) is the newest major innovation within Sangfor IAG. It is based on IAG’s massive internet log and conducts in-depth modelling analysis of internet usage trend. It constantly utilizes behavioural awareness applications in different scenarios and continuously uncovers valuable data, helping organizations understand behaviour risk and simplify O&M.
Work Smarter, Not Harder

**Report Center**

The Professional Report center has never been more simple, comprehensive or responsive. With a single dashboard and step-by-step analysis, you can simply see your network from top to bottom. Through analysis of traffic, duration, applications and URL’s you can easily see customized reports on keywords, uploads, email and application use. Finally, proactively monitor your network with monthly base reports in 10 seconds giving you the 20/20 hindsight you need to plan ahead.

**Bandwidth Analysis**

Give the people what they need! With Line Quality Analysis you can easily see what applications are utilizing the majority of your bandwidth and allocate or block bandwidth to individual applications with a single click.

**Leased Line Analytics**

It can provide a report on the quality of the leased line and help you with more informed decisions on when to expand the leased line bandwidth. It also provides visibility into the tunnel and the user to achieve awareness of the whole network.

**Electricity Waste Analytics**

We work 24/7 so you don’t need too! When the lights go out at night and the last employee leaves the building, Off Hours PC Scan allows you to monitor any network users, heightening your network security while also reducing business cost by monitoring power consumption outside business hours.

**Internet Access Analytics**

Reduce your IT expenditure and make IT more valuable. See and control information and traffic for all branches with SANGFOR Overall Status Display. With easy to read reports on bandwidth and traffic distribution as well as efficiency-reducing applications and websites at all your branches and locations, simply point and click to optimize your bandwidth consumption and user experience.

**Event Analytics**

Customise your view and see what is most important to you! Automatically scan for specific keywords indicative of malware or abnormal user behaviour and be proactive in managing your potential risk.
Manage the SaaS Application in the Right Way

1. Discover Know the Risk
IAG with the built-in SaaS application database, identifies the most used applications, and also categorize them in group according to their security risks (sent emails, high bandwidth consumption, unproductive websites and applications, data leakage risk, etc.). The dashboard directly shows the applications and how much data had been used and how much files are transferred, making the IT administrators have a clear understanding of the applications in the network.

<table>
<thead>
<tr>
<th>Applications</th>
<th>Users</th>
<th>App Category</th>
<th>Tags</th>
<th>Sanction Status</th>
<th>Outgoing Files</th>
<th>Outbound(Bytes)</th>
<th>Inbound(Bytes)</th>
<th>Users</th>
</tr>
</thead>
<tbody>
<tr>
<td>QQ Mail/brow...</td>
<td>Mail</td>
<td>Network storage</td>
<td>Disclosure Risk</td>
<td>New</td>
<td>31.89 KB</td>
<td>8.12 KB</td>
<td>1</td>
<td></td>
</tr>
<tr>
<td>Google Drive</td>
<td></td>
<td>Network storage</td>
<td>Reduce the Efficiency of Work</td>
<td>New</td>
<td>2.24 MB</td>
<td>16.61 MB</td>
<td>15</td>
<td></td>
</tr>
<tr>
<td>Baidu_Wangpeng</td>
<td>Mail</td>
<td>Network storage</td>
<td>Reduce the Efficiency of Work</td>
<td>New</td>
<td>1.05 MB</td>
<td>3.51 MB</td>
<td>1</td>
<td></td>
</tr>
<tr>
<td>Baidu_Wangpeng</td>
<td>Mail</td>
<td>Network storage</td>
<td>Reduce the Efficiency of Work</td>
<td>New</td>
<td>721.42 KB</td>
<td>3.27 MB</td>
<td>5</td>
<td></td>
</tr>
<tr>
<td>QQ Mail-Base</td>
<td>Mail</td>
<td>Network storage</td>
<td>Reduce the Efficiency of Work</td>
<td>New</td>
<td>707.45 KB</td>
<td>2.09 MB</td>
<td>1</td>
<td></td>
</tr>
<tr>
<td>Baidu_Wangpeng</td>
<td>Mail</td>
<td>Network storage</td>
<td>Reduce the Efficiency of Work</td>
<td>New</td>
<td>502.84 KB</td>
<td>441.16 KB</td>
<td>4</td>
<td></td>
</tr>
<tr>
<td>Baidu_Wangpeng</td>
<td>Mail</td>
<td>Network storage</td>
<td>Reduce the Efficiency of Work</td>
<td>New</td>
<td>464.88 KB</td>
<td>1.4 MB</td>
<td>2</td>
<td></td>
</tr>
<tr>
<td>Sina_Mail_Base</td>
<td>Mail</td>
<td>Network storage</td>
<td>Reduce the Efficiency of Work</td>
<td>New</td>
<td>113.78 KB</td>
<td>1.07 MB</td>
<td>1</td>
<td></td>
</tr>
<tr>
<td>Google Hangout</td>
<td>IM</td>
<td>Network storage</td>
<td>Reduce the Efficiency of Work</td>
<td>New</td>
<td>105.02 KB</td>
<td>2.06 MB</td>
<td>9</td>
<td></td>
</tr>
<tr>
<td>Baidu_Wangpeng</td>
<td>Network storage</td>
<td>Disclosure Risk</td>
<td>New</td>
<td>21.92 KB</td>
<td>44.67 KB</td>
<td>1</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Baidu_Wangpeng</td>
<td>Network storage</td>
<td>Reduce the Efficiency of Work</td>
<td>New</td>
<td>8.8 KB</td>
<td>1.88 KB</td>
<td>4</td>
<td></td>
<td></td>
</tr>
<tr>
<td>GitHub_Client</td>
<td>Network storage</td>
<td>Reduce the Efficiency of Work</td>
<td>New</td>
<td>5.33 KB</td>
<td>19.67 KB</td>
<td>1</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Dropbox</td>
<td>Network storage</td>
<td>Disclosure Risk</td>
<td>New</td>
<td>4.53 KB</td>
<td>13.53 KB</td>
<td>1</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Sohu Mail(san...</td>
<td>Mail</td>
<td>Send Email</td>
<td>New</td>
<td>3.45 KB</td>
<td>2.21 KB</td>
<td>1</td>
<td></td>
<td></td>
</tr>
<tr>
<td>NetEase Mail(Email)</td>
<td>Mail</td>
<td></td>
<td>New</td>
<td>587 B</td>
<td>585 B</td>
<td>1</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

2. Grouping – Manage the Applications

- **Sanctioned**– These applications provide IT teams with security guarantee and are allowed to be used by the user.
- **Unsanctioned**– These applications are potentially dangerous and the IT administrators do not want users to use them due to security risk and data leakage risk.

The sanction status makes it easier for managing the applications in a proper way. Sanctioned applications are the ones known and approved by the IT administrators, while the unsanctioned one are not known but may be used by the user, which may affect the user experience when all of them are blocked, or the ones that need to be monitored for a while.
3. Control the Risk

Sangfor IAG provides a granular control over the applications identified, together with the bandwidth control capabilities, providing much higher work productivity.

- **Control Policy**— Setup control policy over the applications.
- **Block**— These applications have been used in the network.

**Create A Space For Work**

The search engine is convenient to find the information you need, but it will also come out with inappropriate contents. Sangfor IAG can set Google, Bing and YouTube into default safe search mode, blocking inappropriate content that could affect the organization reputation.

**Improve Work Productivity**

The SaaS application brings convenience but also brings troubles. It allows users to access work resources freely but also entertainment resources.

IAG can improve user productivity by allowing the user to only access specified work resources such as login Google Workspace and Office 365 with the enterprise user account, access, access Facebook company page for work purposes only, and block all other Facebook content.
Unified Authentication and Wireless Controller Integration

Control Any Device - Anywhere
Success used to have its price, but now it doesn’t! The issue of centralization and unification has become common as businesses expand and open new branches. In the past, various branches were individually responsible for management of their wired and wireless authentication, WIFI network and control policies.

User experience varied from branch to branch and WIFI connectivity did not roam with the user. SANGFOR IAG now provides centralized management capabilities which allow policies, restrictions and control to be exercised from a central platform, reducing operating costs and simplifying the IT management process. With the Central Manager system user experience is also improved by allowing roaming WIFI connectivity and unifying the information visible on each branch platform.
Real-Time Asset Management

IOT devices especially those are unknown has become another major dilemma among the administrators. Without standardized monitoring and enforcement policy, there is no way administrators can have current holistic view of total onboarding devices and compliance check to determine overall status.

Sangfor real-time asset management is designed to tackle this problem with 2 main components:

Asset Discovery
It provides real-time status of what endpoint are running on your network and all this without any agent software. This allows administrators to build accurate inventory and up-to-date status about their network assets.

Asset Classification
One of the crucial elements in asset management is the ability to identify any unknown IOT devices and perform classification to determine asset type.

SSL Decryption

Typically, user always have to choose between having SSL decryption enabled with huge performance degradation and using internet access without any SSL decryption. IAG now provide another option to mitigate such performance degradation by using ingress client to perform SSL proxy decryption process.

With captive portal redirection, users will have the ability to deploy ingress client with ease along with root SSL certificate is distributed and installed together with ingress client. User can now plan their SSL decryption policy strategy without compromising performance loss by having use either IAG decryption, Ingress client decryption or running both for different network segments as an option.

Endpoint Security

Endpoints are the most common target of cybersecurity attacks. One compromised endpoint within your organization can lead to widespread effects and disruption to your business. With endpoint security posture from IAG, you will get a complete picture of your current endpoints, whether compliant and non-compliant according to the organization policies. Also, this will identify risks associated with your organization’s endpoint devices, such as using unauthorized network connections, changing MAC/IP addresses, and subsequently make a remediation action plan to address these risks.
Advanced Bandwidth Management

Separate Management of International & Domestic Bandwidth

As businesses cross borders, IT needs to be aware of usage patterns, bandwidth needs, potential risks and differing costs and challenges associated with individual international locations.

With Sangfor IAG, you can separate the bandwidth management for international and domestic internet access. This is especially important in countries where different fees for bandwidth usage apply but also improves international user experience and reduces risk of network security issues stemming from international locations by allowing full visibility and control of both domestic and international network traffic.

Proxy Avoidance Protection

Proxy avoidance is a tool constantly used by users to bypass network security perimeter and allowing them to access inappropriate content. Many organizations face issues where users access proxy avoidance applications to circumvent security protection and access web content that should be filtered.

Sangfor IAG working with Endpoint Secure to provide comprehensive detection and blocking capabilities on proxy avoidance protection. It has an extensive library of well-known anti-proxy applications, anonymous browsers and VPNs to create blocking/monitoring policies enforced by the Endpoint Secure Protect Agent.
Sangfor IAG – SK Series

Enterprises require a high speed and proficient Secure Web Gateway to stay ahead of ever-increasing network performance requirements as well as growing of heavy internet users at campus and data center premises. With designed higher throughput and low latency, Sangfor IAG – SK Series represents an excellent choice model for small and medium data centers to eliminate throughput bottleneck and keep pace with your users’ internet behavior.

Safeguard Your Data with Data Loss Prevention (DLP)

Sangfor IAG offers an innovative Data Loss Prevention (DLP) solution that prevents data breaches and leakage, such as IP theft caused by rogue employees. It monitors various electronic communication channels, both outbound and internal, to block any unauthorized data transfers. When used in tandem with security control and analysis, Sangfor DLP helps organizations promote secure working habits, maintain compliance with data protection regulations, and avoid fallout from data compromise.

Key Use Cases

<table>
<thead>
<tr>
<th>DLP Replacement</th>
<th>Prevent Data Loss Across Communication Channels</th>
</tr>
</thead>
</table>

Unified visibility and control for all communication channels

Remove Complexity and Increase Productivity
Comprehensive Data Detection and Prevention Across Communication Channels

Audit Attachment, screen capture, offline audit with logging
- Applications
  - Instant Messaging, email client, cloud storage, etc.
- Browsers
  - Google Chrome, Microsoft Edge, Firefox, etc.
- Removable Hard Disk Drive
- Printer
- Decryption

Outgoing Files
- Allow and Deny with notification and logging
- Applications
  - Instant Messaging, email client, cloud storage, etc.
- Browsers
  - Google Chrome, Microsoft Edge, Firefox, etc.

Secure Outbound Data

Unsanctioned Action
- Prevent file transfer to USB
- Prevent transferring sensitive file within Skype
- Prevent transfer Microsoft Office file through Internet Explorer

Sanctioned Action
- Upload files to the authorized cloud storage
- Only allow transfer PDF document within Microsoft Teams
- Access and transfer file to Salesforce.com with Microsoft Edge

Real-Time Blocking

Real-time blocking of unauthorized data movement, including:
A: Outgoing files through applications and browsers
B: Content blocking by file type, file size, and file name keyword

Benefits
- Continuous monitoring, capturing and recording events
- Reduce data breaches
- Comply with cybersecurity requirements and industry regulations
- Protect employees against accidental data loss
- Improve visibility and control over the organization’s data
- Protect brand reputation and customer trust

Deep coverage of supported communication channels, including applications, peripherals, printers, browsers, and decryption.
Secure User Internet Access Behaviour

SANGFOR IAG Product Family

**Profile 1U**

- **HD Capacity**: 128 GB SSD
- **Throughput Options**: 160Mbps, 600Mbps, 1Gbps, 1.2Gbps

**Profile 2U**

- **HD Capacity**: 200,000 SSD
- **Throughput Options**: 2Gbps, 4Gbps, 10Gbps

**Profile 2U**

- **HD Capacity**: 1.92TB SSD
- **Throughput Options**: 50Gbps (Bridge)

**Application Layer Throughput Options**

- 160Mbps
- 600Mbps
- 1Gbps
- 1.2Gbps
- 2Gbps
- 4Gbps
- 10Gbps
- 20Gbps
- 40Gbps

**Recommended Concurrent Users**

- 600
- 2,000
- 3,000
- 5,000
- 6,000
- 15,000
- 20,000
- 50,000
- 100,000
- 200,000
- 200,000

### Power and Physical Specifications

**Model**

- **Support Dual Power Supplies**: N/A, N/A, N/A, N/A, YES, YES, YES, YES, YES, YES, YES
- **Working Temperature**: 0°C~45°C, 0°C~45°C, 0°C~45°C, 0°C~45°C, 0°C~40°C, 0°C~40°C, 0°C~40°C, 0°C~40°C, 0°C~40°C, 0°C~45°C
- **System Dimensions (W x L x H in mm)**: 430 x 300 x 44.5, 430 x 375 x 44.5, 430 x 400 x 44.5, 430 x 400 x 44.5, 440 x 600 x 89, 440 x 600 x 89, 440 x 600 x 89, 440 x 600 x 89
- **System Weight**: 3.4 Kg, 6.6Kg, 6.6Kg, 7.5Kg, 9Kg, 18.5Kg, 18.5Kg, 20.0Kg, 20.0Kg, 20.0Kg, 24.0Kg
- **Relative Humidity**: 5%~90% non-condensing

### Network Interfaces

**Model**

- **Bypass (copper)**: 1 pair, 2 pairs, 2 pairs, 3 pairs, 3 pairs, 3 pairs, 2 pairs, 2 pairs, 2 pairs, 2 pairs
- **10/100/1000 Base-T**: 4, 6, 6, 6, 6, 6, 6, 4, 4, 4, 4
- **1G SFP**: N/A, 2, 2, 2, N/A, N/A, N/A, 4, 4, 4, /
- **10GbE SFP+**: N/A, N/A, N/A, N/A, 2, 2, 2, 2, 4, 4, 8
- **Extended Slot Number**: 1, 1, 1, 1, 1, 2, 2, 1, 1, 4, 1
- **Serial Port**: RJ45x1, RJ45x1, RJ45x1, RJ45x1, RJ45x1, RJ45x1, RJ45x1, RJ45x1, RJ45x1, RJ45x1
- **USB Port**: 2, 2, 2, 2, 2, 2, 2, 2, 2
- **40G Fiber QSFP+**: N/A, N/A, N/A, N/A, N/A, N/A, N/A, N/A, N/A, N/A, 2

### Compliance and Certificates

- **Compliance**: CE, FCC, IPv6 Ready
- **CE**

---

1. Represents the maximum bidirectional flow (max. inbound + outbound flow).
2. M6000-UPG is a license upgrade from M6000 with application layer bandwidth increased from 1G to 2G.
3. Products specifications described herein are subject to change without prior notification.
4. All performance values are “up to” and vary depending on the system configuration.
Sangfor IAG – SK Series

### HD Capacity
- **Model**
  - M5500-SK-AC-I: 128GB MSATA
  - M5800-SK-AC-I: 128GB MSATA + 480GB SSD

### Application Layer Throughput Options
- **Model**
  - M5500-SK-AC-I: 750Mbps
  - M5800-SK-AC-I: 1.5Gbps

### Recommended Concurrent Users
- **Model**
  - M5500-SK-AC-I: 1,000
  - M5800-SK-AC-I: 2,000

### Power and Physical Specifications

<table>
<thead>
<tr>
<th>Model</th>
<th>M5500-SK-AC-I</th>
<th>M5800-SK-AC-I</th>
</tr>
</thead>
<tbody>
<tr>
<td>Support Dual Power Supplies</td>
<td>N/A</td>
<td>N/A</td>
</tr>
<tr>
<td>Power (Watt) (Typical)</td>
<td>40W</td>
<td>60W</td>
</tr>
<tr>
<td>Working Temperature</td>
<td>0°C~45°C</td>
<td>0°C~45°C</td>
</tr>
<tr>
<td>System Dimensions (W x L x H in mm)</td>
<td>430 x 300 x 44.5</td>
<td>430 x 300 x 44.5</td>
</tr>
<tr>
<td>System Weight</td>
<td>6.2Kg</td>
<td>7.3Kg</td>
</tr>
<tr>
<td>Relative Humidity</td>
<td>5%/90% non-condensing</td>
<td>5%/90% non-condensing</td>
</tr>
</tbody>
</table>

### Network Interfaces

<table>
<thead>
<tr>
<th>Model</th>
<th>M5500-SK-AC-I</th>
<th>M5800-SK-AC-I</th>
</tr>
</thead>
<tbody>
<tr>
<td>Bypass (copper)</td>
<td>2 Pairs</td>
<td>2 Pairs</td>
</tr>
<tr>
<td>10/100/1000 Base-T</td>
<td>6</td>
<td>6</td>
</tr>
<tr>
<td>1G SFP</td>
<td>2</td>
<td>2</td>
</tr>
<tr>
<td>10Gbe SFP+</td>
<td>/</td>
<td>/</td>
</tr>
<tr>
<td>Extended Slot Number</td>
<td>1</td>
<td>1</td>
</tr>
<tr>
<td>Serial Port</td>
<td>RJ45x1</td>
<td>RJ45x1</td>
</tr>
<tr>
<td>USB Port</td>
<td>2</td>
<td>2</td>
</tr>
<tr>
<td>Compliance</td>
<td>CE, FCC</td>
<td>CE, FCC</td>
</tr>
</tbody>
</table>

1 Represents the maximum bidirectional flow (max. inbound + outbound flow).

- Products specifications described herein are subject to change without prior notification.
- All performance values are “up to” and vary depending on the system configuration.
Sangfor Virtual IAG (VMware & Sangfor HCI Platforms)

### System Requirements

<table>
<thead>
<tr>
<th>vIAG &amp; vmIAG System Requirements</th>
<th>vIAG-50 vmlAG-50</th>
<th>vIAG-100 vmlAG-100</th>
<th>vIAG-200 vmlAG-200</th>
</tr>
</thead>
<tbody>
<tr>
<td>Virtualization Platform</td>
<td>Sangfor HCI/ VMWare ESXi</td>
<td>Sangfor HCI/ VMWare ESXi</td>
<td>Sangfor HCI/ VMWare ESXi</td>
</tr>
<tr>
<td>CPU</td>
<td>Min. 1 Virtual Core</td>
<td>Min. 1 Virtual Core</td>
<td>Min. 2 Virtual Cores</td>
</tr>
<tr>
<td>Memory</td>
<td>2GB</td>
<td>2GB</td>
<td>4GB</td>
</tr>
<tr>
<td>Disk Space</td>
<td>250GB</td>
<td>250GB</td>
<td>250GB</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>vIAG &amp; vmIAG System Requirements</th>
<th>vIAG-300 vmlAG-300</th>
<th>vIAG-700 vmlAG-700</th>
<th>vIAG-1000, vIAG2000 vmlAG-1000</th>
</tr>
</thead>
<tbody>
<tr>
<td>Virtualization Platform</td>
<td>Sangfor HCI/ VMWare ESXi</td>
<td>Sangfor HCI/ VMWare ESXi</td>
<td>Sangfor HCI/ VMWare ESXi</td>
</tr>
<tr>
<td>CPU</td>
<td>Min. 2 Virtual Cores</td>
<td>Min. 4 Virtual Cores</td>
<td>Min. 8 Virtual Cores</td>
</tr>
<tr>
<td>Memory</td>
<td>4GB</td>
<td>8GB</td>
<td>16GB</td>
</tr>
<tr>
<td>Disk Space</td>
<td>250GB</td>
<td>250GB</td>
<td>250GB</td>
</tr>
</tbody>
</table>

*SANGFOR IAG can co-exist alongside another internet security system or any other Sangfor solutions.*

---

1. Represents the maximum bidirectional flow (max. inbound + outbound flow).
2. vIAG = Virtual IAG based on Sangfor HCI | vmIAG = Virtual IAG based on VMware ESXi.
## Sangfor IAG Product Features

### User Authentication and Management

<table>
<thead>
<tr>
<th>Mapping and Identifying Users</th>
<th>IP, MAC, IP/MAC binding, hostname, USB Key, SMS, QR-Code, Portal, WeChat, Facebook, Line, Gmail, Twitter.</th>
</tr>
</thead>
<tbody>
<tr>
<td>User Accounts Importing</td>
<td>- Import user accounts information using CSV file, LDAP Server.</td>
</tr>
<tr>
<td></td>
<td>- Synchronize user with LDAP, Database and H3C CAMS Server.</td>
</tr>
<tr>
<td>Integration and SSO Option</td>
<td>Active Directory/POP3/Proxy/Web Server, Radius, Third-party authentication device, Database Server, CAS, OAuth, SAML2.0</td>
</tr>
<tr>
<td>Two-Factor Authentication</td>
<td>- Microsoft Authenticator, Google Authenticator.</td>
</tr>
<tr>
<td></td>
<td>- Verification method via SMS, password.</td>
</tr>
<tr>
<td>New User Management</td>
<td>- Automatically map new user to its privileged groups in local database based on its IP range, subnet or external authentication server group.</td>
</tr>
<tr>
<td></td>
<td>- Automatically map new users to a pre-defined privileged group as temporary accounts.</td>
</tr>
<tr>
<td>Account Attribution</td>
<td>Public (Share user login)/ Private (Single user login) account option.</td>
</tr>
</tbody>
</table>

### Access Control

<table>
<thead>
<tr>
<th>Application Control</th>
<th>Identify and control applications through application DB or port.</th>
</tr>
</thead>
<tbody>
<tr>
<td>URL Filter</td>
<td>URL DB, keyword in web-page based control.</td>
</tr>
<tr>
<td>Search Engine Control</td>
<td>Managed by keywords.</td>
</tr>
<tr>
<td>Enhanced Email Control</td>
<td>Managed by source address, destination address, keywords in email, keywords in body/title, attachment, type/size/count based control.</td>
</tr>
<tr>
<td>File Filter</td>
<td>Control HTTP, FTP upload and download activity based on true file type.</td>
</tr>
<tr>
<td>SSL Traffic Control</td>
<td>Certificate, text content based control and filter.</td>
</tr>
<tr>
<td>SSL Decryption</td>
<td>Gateway decryption and ingress client decryption.</td>
</tr>
</tbody>
</table>

### Proxy Avoidance Protection

| Anti-Proxy                     | Detect and block proxy tools based on application signatures database and Endpoint Secure integration. |

### Asset Management

| Asset Discovery                | - Identify and list of IOT devices based on endpoint type.                                       |
|                               | - Advance search and filter based on endpoint parameter.                                         |
|                               | - Export to csv.                                                                                |
| Asset Classification          | Categorize endpoint type based on host, mobile endpoint, network device, dumb endpoint, medical equipment, network endpoint sharing and custom. |

### Ingress Security Posture

| Ingress Client-based (Agent)  | Antivirus software, login domain, operating system, process, file, registry, task, service pack, internet access, access control, device control, windows account, IP/MAC address change prevention, software check, desktop watermark, inbound port, app access control. |
| Traffic-based (Agentless)     | Endpoint verification and enforce update on outdated antivirus signatures including consumer-grade antivirus and corporate antivirus. |
| 802.1x                         | Dynamic VLAN assignment, secure Wi-Fi access, secure IoT and dumb endpoints, user auto-login.    |

### Illegal Wi-Fi Detection and Blocking

| Illegal Wi-Fi Detection and Blocking | Detect the endpoint information from every IP address. |
## Bandwidth Management (BM)

<table>
<thead>
<tr>
<th><strong>BM Policy</strong></th>
<th>Traffic guarantee/limit policy for uplink and/or downlink base on bandwidth percentage of the pipe, max bandwidth per user, user/application priority, exclusion policy.</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>BM Objects</strong></td>
<td>Application type, website type, file type, user, schedule, destination IP, etc.</td>
</tr>
<tr>
<td><strong>Separate BM Management</strong></td>
<td>For International &amp; Domestic Traffic.</td>
</tr>
<tr>
<td><strong>Bandwidth Guarantee &amp; Limitation</strong></td>
<td>Allocate bandwidth resource according to business type &amp; guarantee bandwidth for core business applications and restrict irrelevant traffic.</td>
</tr>
<tr>
<td><strong>Multi-level SON Channel</strong></td>
<td>Match the organizational structure to achieve fine-grained bandwidth management.</td>
</tr>
</tbody>
</table>
| **Dynamic Bandwidth Management** | - “Bandwidth Borrowing” among BM tunnel for full bandwidth utilization.  
- Specify a network flow thresholds as effective points of BM policy.  
- BM based on public IP (oversea).  
- Average allocation/free competition among users in a single traffic pipe. |
| **Virtual Line** | Manage and control to each physical line independently and effectively bridge mode.                                                  |
| **Multiplexing and Intelligent Routing** | Provide link load balancing in router mode.                                                                                       |

## Traffic Identification and Categorization

| **Sangfor URL Database** | - Leverage on-the-cloud infrastructure, dynamically categorizes millions URLs into the predefined categories.  
- Support configurable in-box cache footprint.  
- Regular update twice in a week. |
| **Application Database** | - Independent Internet application signatures database.  
- Regular update once in a week. |
| **Intelligent Identification Rules** | Identify P2P/Proxy tools/VOIP/SSL traffic intelligently through dynamic flow characteristics analysis. |
| **File Type Identification** | - By extension name.  
- By file type (data pattern). |

## Value-Added Services

| **Big Data Mining** | Record of online behavior data record, data modeling analysis and analytics report. |

## Report Center

| **Report Objects** | Application flow, user behavior counts, online duration per user & per application, virus and security, keywords, etc. |
| **Graphical Reports** | Counts, ranking, comparison, trends analysis with statistics, pie, bar, line chart, etc. |
| **Real-Time Report** | Real-time monitor of CPU/hard disk/traffic/connection/session status, online user information, traffic ranking, connection ranking, real-time utilization, visibility of bandwidth channels. |
| **Content Log** | Content log including corporate Instant Messaging (IM) chat, SMTP and webmail content and attachment (Gmail, etc), BBS posts (Facebook, Twitter, etc) |
| **Customizable Risk Report** | Employee turnover trend, disclosure, work efficiency, security risks and other risk reports. |
| **CIO Report** | Tailored reports of overall network analysis and risk management for CIO. |
| **Web-Access Connection Quality Report** | Used for clear evaluation of the overall network quality. Users with poor web access quality can be listed down. |
| **Report Format** | CSV, PDF. |
| **Report Center Storage** | Built-in internal report center and optional external report center. |
| **External Reports Storage Security** | - Option to protect the report center by using external authentication key for additional security.  
- “Google Like” search engine GUI for external report center.  
- Email subscription. |
### Control Tools for Manageability

<table>
<thead>
<tr>
<th>Notification (Reminder)</th>
<th>Notify end user for online time of specific application and the flow speed of specific application.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Flow/Duration Control</td>
<td>Daily/Monthly flow quota per user. Daily online duration quota per user with exception case based on specific application. Concurrent session quota per user.</td>
</tr>
<tr>
<td>Audit-Free Key</td>
<td>Prevents access audits and control for users that assigned with audit-free keys.</td>
</tr>
<tr>
<td>Hierarchical Administration</td>
<td>Functionality of different modules can be assigned to different administrators as needed, via a hierarchical management paradigm. Administration of different functions and modules can be delegated to different administrative groups.</td>
</tr>
</tbody>
</table>

### Network & Deployment

<table>
<thead>
<tr>
<th>Centralized Management</th>
<th>Unified the configuration and policy for multiple devices, remote control and monitor running status.</th>
</tr>
</thead>
<tbody>
<tr>
<td>LAN+WLAN Management</td>
<td>Set special control policy for mobile user based on user &amp; location. Suitable for BYOD office environment.</td>
</tr>
</tbody>
</table>
| Security Modules       | - Built-in IPsec VPN.  
- IPSec Protocol: AH, ESP.  
- IPSec Authentication Algorithm: MD5, SHA-1, SM3.  
| Proxy Functions        | Support explicit Proxy, including HTTP/HTTPS two-level Proxy, Sock4/Sock5 Proxy, Forwarding Proxy function and support ICAP protocol. |
| Deployment             | Route, Bridge, Double Bridge, Bypass, Single-arm. |
| Log Monitoring         | Support Syslog, SNMP V1/V2/V3 |

### Proxy

| Proxy Service | HTTP Proxy / SOCKS4 / SOCKS5 / PAC SCRIPT. |
| Policies      | Enables customers controller proxy data security. |
| Prevent Data Disclosure | - Send web content to content analysis  
- Support response and request modification with inspection mode of ICAP server grouping.  
- Support inspection type including round robin and concurrent options.  
- Visualization representation and statistics from forwarding log of ICAP server. |

### Business Intelligence

<table>
<thead>
<tr>
<th>Self-Customized Application</th>
<th>Be aware of trends and incidents using keyword related searches to monitor traffic in real-time.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Bandwidth Analysis</td>
<td>Monitor bandwidth status, availability and top bandwidth consuming applications to provide better user experience.</td>
</tr>
<tr>
<td>Overall Status Display</td>
<td>Identify threats quickly and easily through combined IAG and NGAF logs.</td>
</tr>
<tr>
<td>Leased Line Quality Analytics</td>
<td>Understand the load and real-time status of traffic by collectively analysing user trends and application use.</td>
</tr>
<tr>
<td>Off Hours PC Scan</td>
<td>Monitor PC usage outside business hours.</td>
</tr>
</tbody>
</table>

### Data Loss Prevention

| Audit Capabilities | - Internet Access Audit : Application, flow/online duration, webpage content  
- Ingress Client Audit : Application (desktop app, including instant messaging), peripherals, printers, browsers, decryption |
| Control Capabilities | - Outgoing File Control : Application (desktop apps, including instant messaging), browsers  
- Sensitive File Rules : File type, file size, file name keyword |
COMPANY PROFILE

Make Your Digital Transformation Simpler and Secure. This is Sangfor Technologies’ commitment to our customers. Since forming in 2000, Sangfor has been a global leader of IT infrastructure, security solutions and cloud computing. Five business groups deliver industry leading products for Hyper-Converged Infrastructure, Virtual Desktop Infrastructure, Next Generation Firewall, Secure Web Gateway, Endpoint Protection, Ransomware Protection, Incident Response, WAN Optimization, and SD-WAN. Constant innovation and dedication to creating value for our customers are the heart of our corporate strategy.

Sangfor’s 9500+ employees take customer’s business needs and user experience seriously by servicing and supporting them at over 60 branch offices globally in exciting locations like Hong Kong, Malaysia, Thailand, Indonesia, Singapore, Philippines, Vietnam, Myanmar, Pakistan, UAE, Italy, Türkiye and the USA.

INTERNATIONAL RECOGNITION & COOPERATION
CONTINUOUS INNOVATION & EXCELLENT SERVICE

Sangfor invests at least 20% of annual revenue in R&D to improve products and develop new solutions at our five R&D centers located. With over 2,200+ patents, Sangfor has more patent applications submitted in 2022. This dedication to innovation enables us to release product updates every quarter and launch new products annually.

We pride ourselves on our excellent service. Customers enjoy fast 24x7 online support 365 days a year and personalized on-site service support from over 10,000 certified engineers at our three Customer Service Centers in Malaysia & China.

Sangfor has more than 100,000 satisfied customers worldwide, including Fortune Global 500 companies. Governments, universities & schools, financial institutions, manufacturing, and other industries trust us to protect them from the next generation of cyberthreats and help them on their journey to digital transformation with a future-proof IT infrastructure.
SANGFOR INTERNET ACCESS GATEWAY

INTERNATIONAL OFFICES

SANGFOR SINGAPORE
10 Ubi Crescent, #04-26 Ubi Techpark (Lobby B), Singapore 408564
Tel: (+65) 6276-9133

SANGFOR HONG KONG (CHINA)
Unit 1612-16, 16/F, The Metropolis Tower, 10 Metropolis Drive, Hung Hom, Kowloon, Hong Kong
Tel: (+852) 3845-5410

SANGFOR MALAYSIA
MD Place 3rd Floor, Jl Setiabudi No.7, Jakarta Selatan 12910, Indonesia
Tel: (+62) 21-2966-9283

SANGFOR INDONESIA
No 45-10 The Boulevard Offices, Mid Valley City, Lingkaran Syed Putra, 59200 Kuala Lumpur, Malaysia
Tel: (+60) 3-2702-3644

SANGFOR THAILAND
141 Mayor Tower Thonglor (Thonglor10) Floor 11 Sukhumvit Road, Khlongtan Nues Wattana BKK, Thailand 10110
Tel: (+66) 02-002-0118

SANGFOR PHILIPPINES
7A, OPL Building, 100 Don Carlos Palanca, Legazpi, Makati, 122 Metro, Manila, Philippines.
Tel: (+63) 0916-267-7322

SANGFOR VIETNAM
4th Floor, M Building, Street C, Phu My Hung, Tan Phu Ward, District 7, HCMC, Vietnam
Tel: (+84) 287-1005018

SANGFOR SOUTH KOREA
Floor 17, Room 1703, Yuwon bldg. 116, Seosumun-ro, Jung-gu, Seoul, Republic of Korea
Tel: (+82) 2-6261-0999

SANGFOR EMEA
D-81 (D-Wing), Dubai Silicon Oasis HQ Building, Dubai, UAE.
Tel: (+971) 52855-2520

SANGFOR PAKISTAN
D-44, Navy Housing Scheme, ZamZamma, Karachi, Pakistan
Tel: (+92) 333-3365967

SANGFOR ITALY
Floor 8, Via Marsala, 36B, 21013 Gallarate VA, Italia
Tel: (+39) 0331-648773

SANGFOR TURKEY
Turgut Ozal Street, Zenta Istanbul, First Floor, Office. 20 Çekmekoy / Istanbul, Postal Code: 34788
Tel: (+90) 546-1615678

AVAILABLE SOLUTIONS

IAG - Internet Access Gateway
Secure User Internet Access Behaviour

NGAF - Next Generation Firewall
Smarter AI-Powered Perimeter Defence

Endpoint Secure - Endpoint Security
The Future of Endpoint Security

Cyber Command - Network Detection and Response
Smart Efficient Detection and Response

TIARA - Threat Identification, Analysis and Risk Assessment
Smart Threat Analysis and Assessment

IR - Incident Response
Sangfor Incident Response – One Call Away

Cyber Guardian - Managed Threat Detection & Response Service
Faster Response Through Human/Al Collaboration

HCI - Hyper-Converged Infrastructure
Fully Converge Your Data Center

MCS - Managed Cloud Services
Your Exclusive Digital Infrastructure

VDI - aDesk Virtual Desktop Infrastructure
Seamless Experience, Secure and Efficient

Access - Secure Access Service Edge
Simple Security for Branches & Remote Users

EDS - Enterprise Distributed Storage
The Only Secured Data Storage You Need

SD-WAN
Boost Your Branch with Sangfor

https://twitter.com/SANGFOR
https://www.linkedin.com/company/sangfor-technologies
https://www.facebook.com/Sangfor
https://www.instagram.com/sangfortechnologies/
https://www.youtube.com/user/SangforTechnologies

Sales: sales@sangfor.com
Marketing: marketing@sangfor.com
Global Service Center: +60 12711 7129 (or 7511)

www.sangfor.com