1. Sangfor IAG Security Background

IAG background

Behind the seemingly normal online behavior, there are many invisible risks hidden, and online management needs to be visually controllable.

While the Internet brings great convenience to the business, if there is no effective management, it will bring various risks to the business, and the enterprise needs to do effective online management.

Internet management faces more challenges and there are many invisible risks. It is impossible to control users and behaviors, so the goal of online management should be visual and controllable.

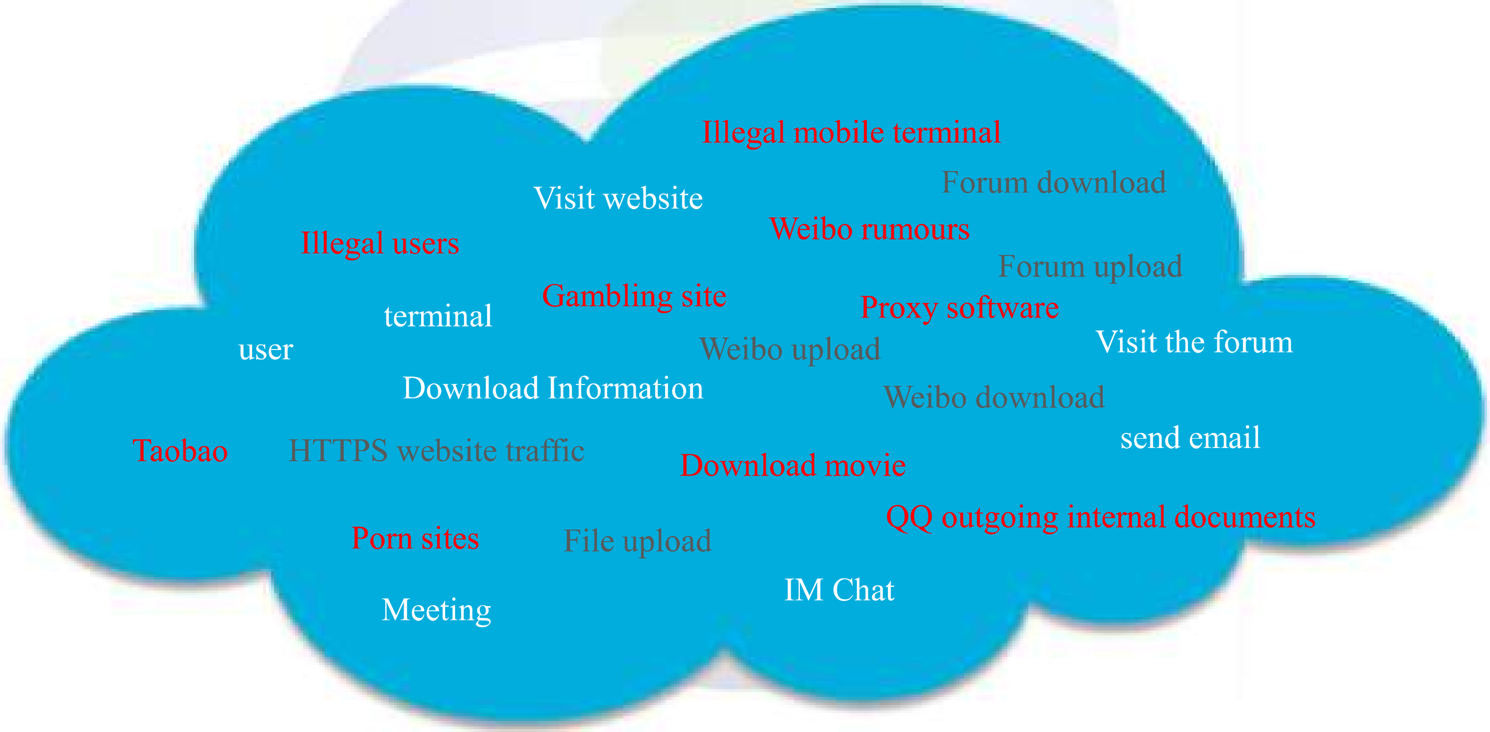
Because the elements of online behavior are: users, terminals, applications, content, traffic. Therefore, it is necessary to realize the visual controllability of the Internet: the user/terminal, the application and the content, and the visibility and control of the traffic.

Why need IAG ?

- The development and popularization of the Internet is changing people's work and lifestyle；
- The Internet is gradually becoming an important means of production, and organizational business is gradually migrating to the Internet；
- The Internet is a "double-edged sword", and the lack of management of the Internet brings many problems.

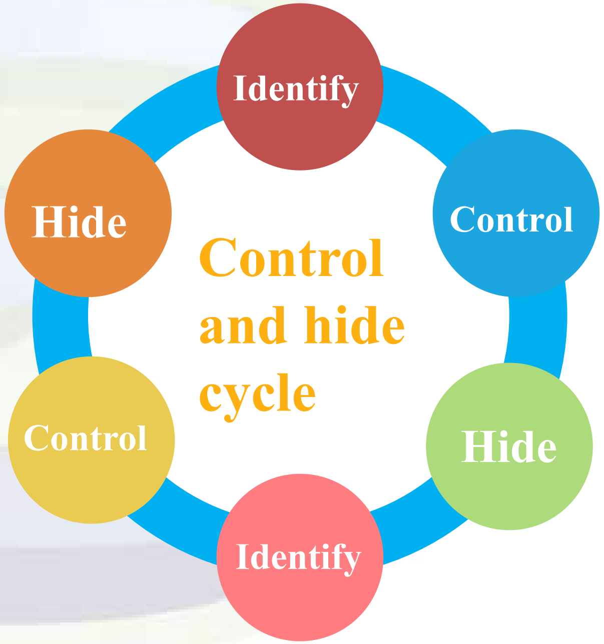
The Internet can't be seen or touched

The seemingly normal online behavior actually hides a huge "invisible and uncontrollable" risk



Challenge

- New Internet applications emerge one after another
- Mobile Internet and wireless make the environment more complex
- Various new technologies make it more difficult to identify and manage applications



Bandwidth abuse

Phenomena

- Poor Internet experience and slow data interaction between branches and headquarters;
- Voice and video conferencing systems are intermittent；
- Email sending and data download are seriously affected;
- Employees complain about the network environment, the core business cannot be guaranteed, the IT department has been repeatedly complained, and the performance of the department is affected.

Analysis

- P2P, streaming media and other traffic occupy more than 70% of the bandwidth；
- Lack of reasonable division and allocation of bandwidth；
- Simply expanding bandwidth will not cure the root cause

Difficult to monitor online behavior

Phenomena

- The corporate office has become a free Internet cafe, and the office efficiency is low；
- Unannounced visits and exposure of government officials to chat online, speculate in stocks, and play online games during working hours have affected the image of the organization；
- In the school's electronic reading room, students use IM to chat, watch online videos, and play online games, which affect learning.

Analysis

- Lack of management of user access rights;
- The proliferation, complexity and rapid updating of Internet applications increase the difficulty of management ；
- The rapid growth of mobile applications increases the difficulty of management.

Information leakage

Phenomena

- Leakage of important information such as email messages of senior leaders and company R&D codes；
- The company‘s business decisions and inside information are known in advance by competitors.

Analysis

- Lack of authorization to access the Internet, users want to surf the Internet, providing a channel for network leak；
- Actively leaking information, or being remotely controlled by hackers and passively leaking coexist；
- After the leak, there is no evidence to investigate, it is difficult to be held accountable, and it is difficult to form a deterrent 。

Internet violations

Phenomena

- Weibo, Baidu Tieba, etc. have become the hardest hit areas for online rumors and personal attacks；
- Wanted to send out reactionary, gambling, pornographic information, and be prosecuted by law；
- Popular Freegate, Unbounded Browser and other proxy circumvention software, bypassing company management.

Analysis

●Lack of online supervision, users surf the Internet simply;

●Web2.0 makes everyone an information publisher;

●Lack of logging, no evidence tracking.

Security threat

Phenomena

- Terminals without anti-virus software and potential security risks go online freely and are easily infected with threats;
- Visiting seemingly normal web pages may be infected with Trojans and malicious plug-ins;
- Threats have been infected, users do not know; even major problems such as viruses and ARP spoofing break out.

Analysis

- The management system is like empty text, and the lack of technical supervision leads to poor implementation;
- Internet threats are growing, stealth and infection techniques are becoming more advanced;
- Due to cost reasons, no security devices are deployed in the network.

2. Sangfor IAG Security Requirement

SANGFOR
深信服科技

Three elements of IAG

User	Traffic	Action	
	Streaming traffic	Porn sites	Technical forum
Illegal mobile terminal	Download traffic	Proxy	Download info
Illegal users	Send mail traffic	Taobao	Work Application
Legitimate terminal	Meeting traffic	Mail	
Legitimate user	SAAS application traffic	Wechat	Visit forum

Visible

Controllable

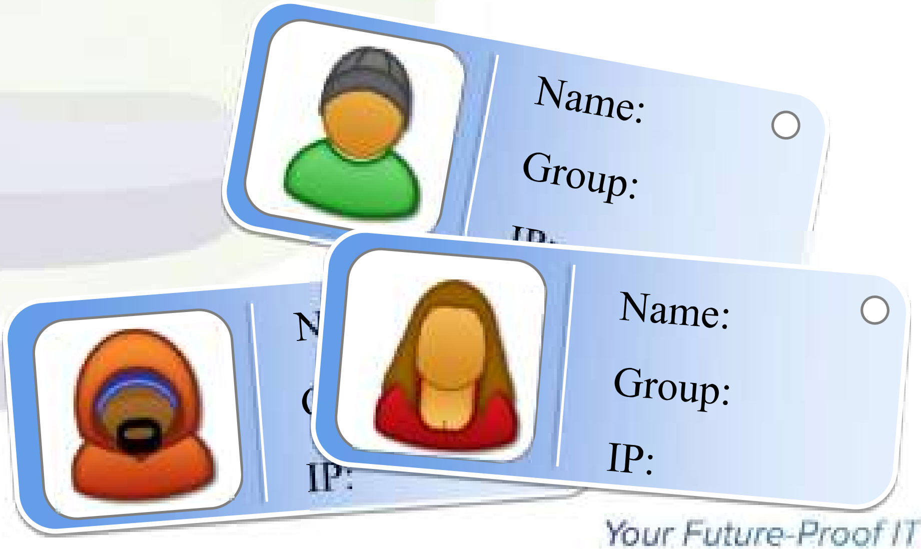
User Authentication

Purpose

- Establish the identity of Internet users and verify their legitimacy;
- Use this information as the user ID to control and audit the user's online behavior;

Function

- IP/MAC binding;
- Local password authentication;
- Third party server authentication;
- DKEY authentication;
- Sinigle Sign On;
- SMS/QR code authentication.
- Terminal Type Identification



Application Control

Purpose

- Block IM chat, stock trading, games, downloads, online videos and other applications, regulate online behaviour, and improve employee work efficiency;
- Block proxy and circumvention software to avoid legal risks caused by improper online behaviour;
- Block emails to prevent sensitive information from leaking；

Function

- Application feature library；
- App management tagging；
- Refinement control；
- Anti-proxy。

SANGFOR

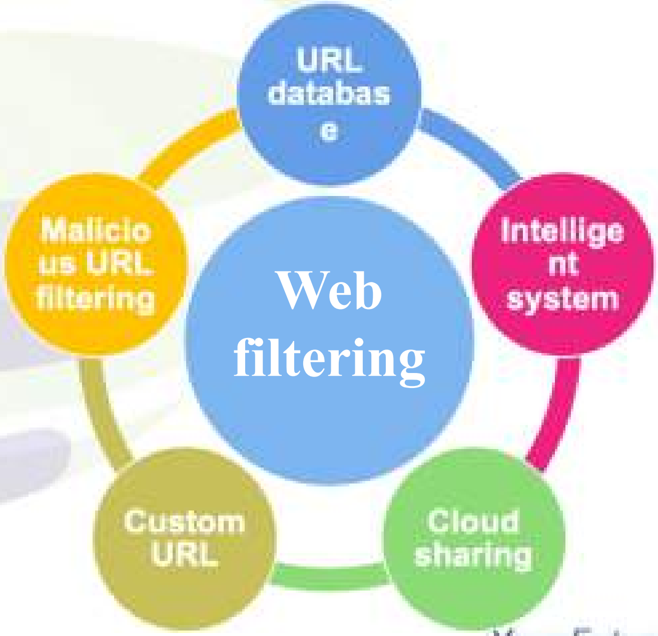
Web filtering

Purpose

- Filter illegal and bad websites to avoid legal risks；
- Improve employee productivity by filtering gaming, gambling, shopping, online videos, and more；
- Filter malicious web pages to ensure Internet security；

Function

- URL database；
- URL intelligent system；
- URL cloud sharing；
- Custom URL；
- Malicious URL filtering



Behavior Audit

Purpose

- Record the online behavior of intranet users, which can be used as traceable evidence in the event of network violations；
- Count users' online time, application traffic, application distribution for enterprise decision-making;
- Record intranet security events to help administrators discover security threats.

Function

- Web access audit；
- Email audit；
- IM chat audit；
- File audit；
- Forum post audit;

Bandwidth Management

Purpose

- Bandwidth is limited or guaranteed according to the type of service to ensure smooth operation of core services；
- Flexible allocation of bandwidth resources to achieve dynamic adjustment and improve bandwidth utilization；

Function

- Flow control based on user/usergroup/application/site type；
- Multi-level parent-child channel；
- Dynamic flow control；
- P2P intelligent flow control；
- Flow control blacklist

Path selection

Purpose

- Load balance for multi-operator lines；
- Accurate identification of applications, enabling effective drainage；
- Dynamic intelligent routing.

Function

- Application program；
- DNS transparent proxy；
- Application routing technology；
- Dynamic drainage technology；
- DSCP/tos tagging

3. Sangfor IAG Core Features

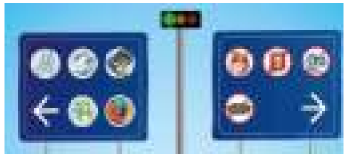
SANGFOR
深信服科技

Sangfor IAG Core Features

SANGFOR

Network visibility

- Monitor and identify problems; Preventive maintenance



Web filtering and application access control

- Control the unwanted Internet access to reduce risks

Bandwidth Management (BM)

- Perform traffic shaping base on domestic and international traffics

Additional features

- Quota control, simple and intuitive reporting, etc.

Sangfor IAG New Features

1. Bring Your Own Device

Due to smartphone and tablet are trending, some staffs might connect their personal devices to the network and this kind of traffics behaviour could be clearly identified and filtered

Sangfor IAG New Features

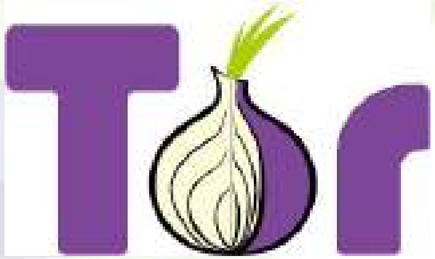
2. Connection Sharing

Portable Wifi and PC can share Internet access to the smart devices such as tablet and smartphone, the Internet connection sharing between PCs is very common and these behaviors are hardly detected by network administrator.

Sangfor IAG New Features

3. Proxytools Control

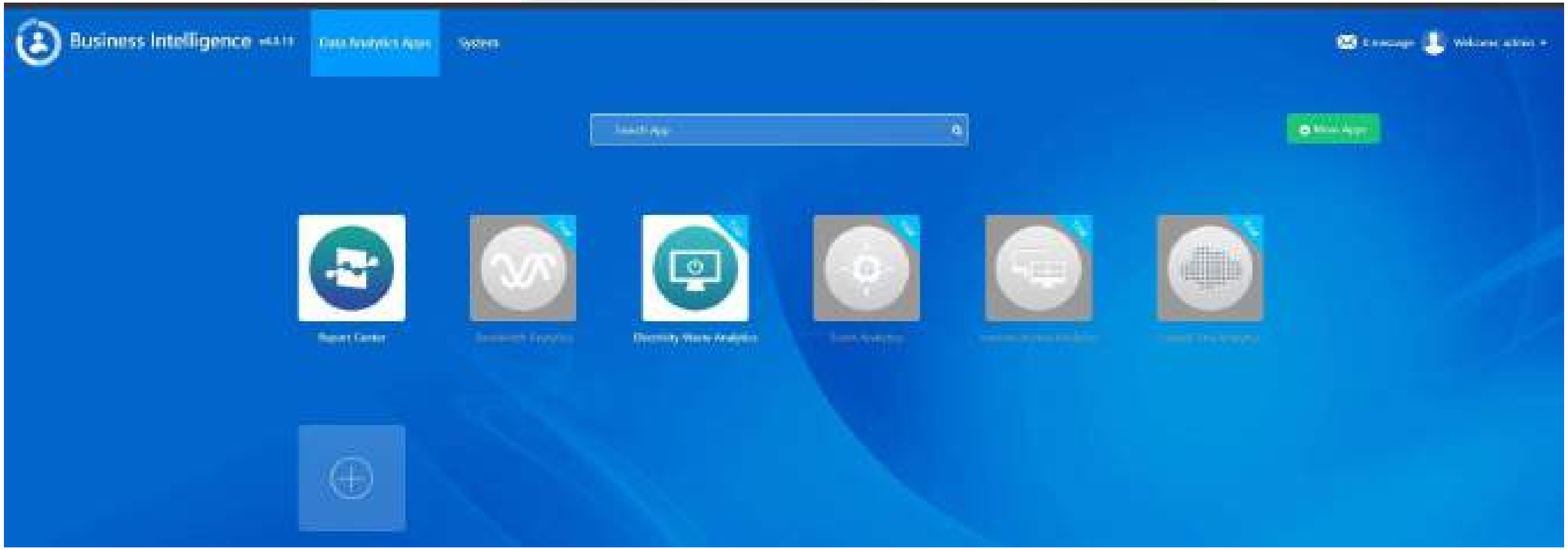
Free proxytool softwares such as UltraSurf, Encrypted VPN, etc. allow users to surf anonymously on the internet and bypass the access control in the network. IAG can identify these traffics and apply filtering control base on administrator configuration



Sangfor IAG New Features

4. Business Intelligence

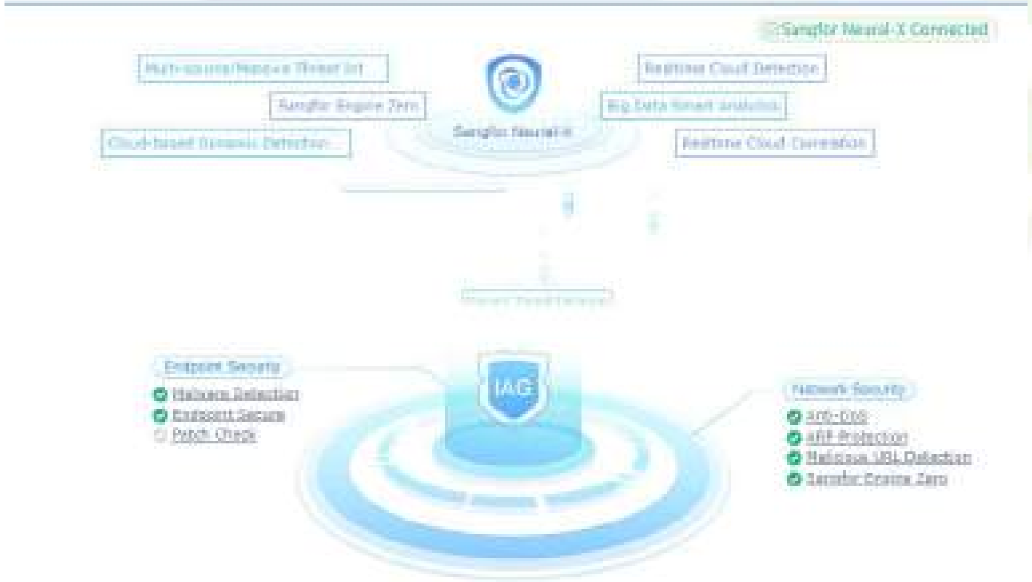
Sangfor BI is based on the new architecture of the original convinced IAG external data center, based on massive online logs, and provides a variety of behavior-aware applications based on the application store. Each application helps customers solve a business problem.



Sangfor IAG New Features

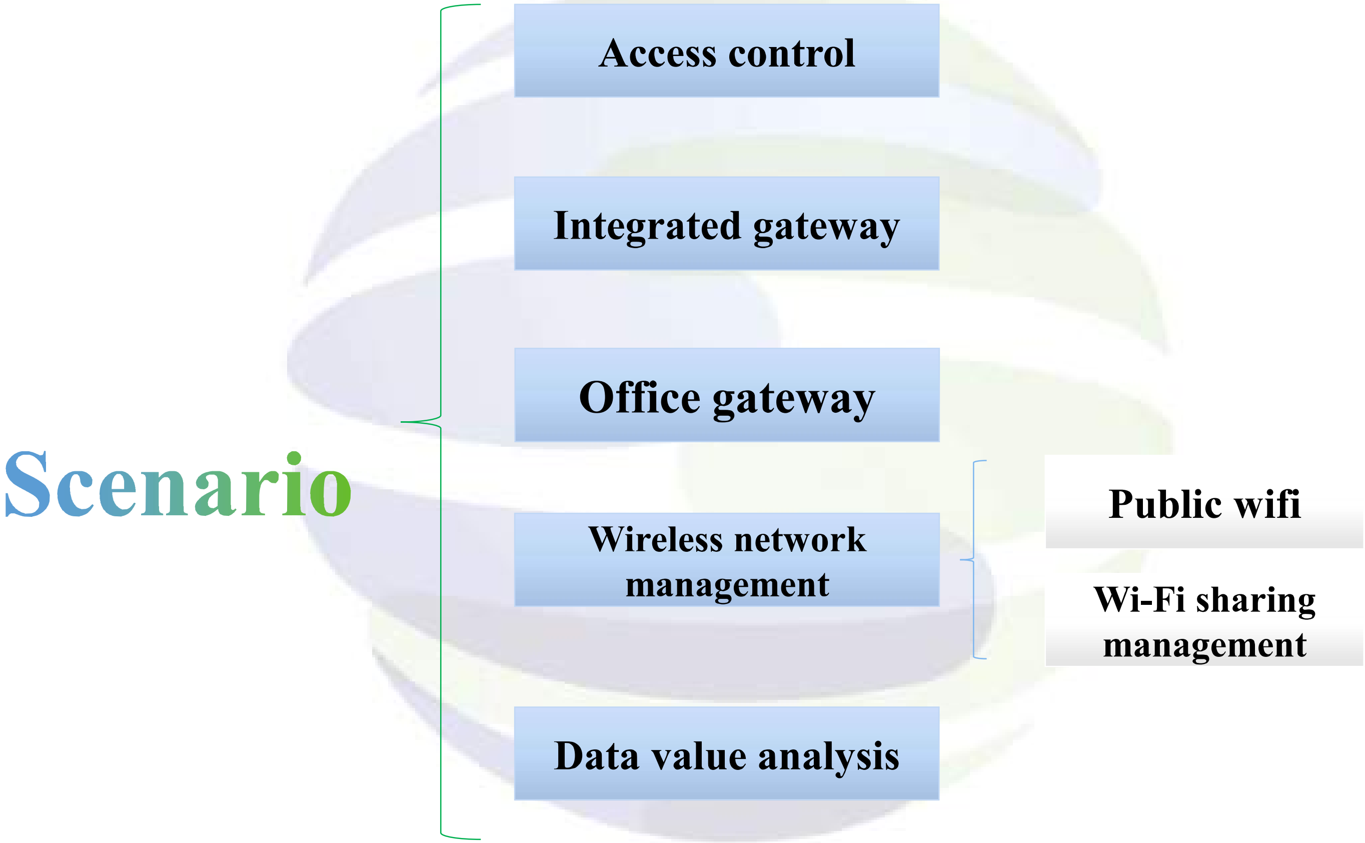
5. Sangfor Neural-X

The new security protection module, IAG and sangfor Neural-x maintain deep linkage, and the secure cloud brain continuously empowers IAG, enabling IAG to have the security ability to continuously discover unknown threats and advanced threats.



4. Sangfor IAG Security Scenarios

SANGFOR
深信服科技



Scenario

Access control

Integrated gateway

Office gateway

Wireless network management

- Public wifi
- Wi-Fi sharing management

Data value analysis

Access control

Target user

Whole industry，IAG as gateway

User requirement

1、 Employees use the Internet, requiring web filtering and application blocking to improve employee work efficiency;

2、 Poor Internet experience, need to control bandwidth traffic to ensure the smooth flow of core services;

3、 Online behaviour audit to meet cybersecurity laws；

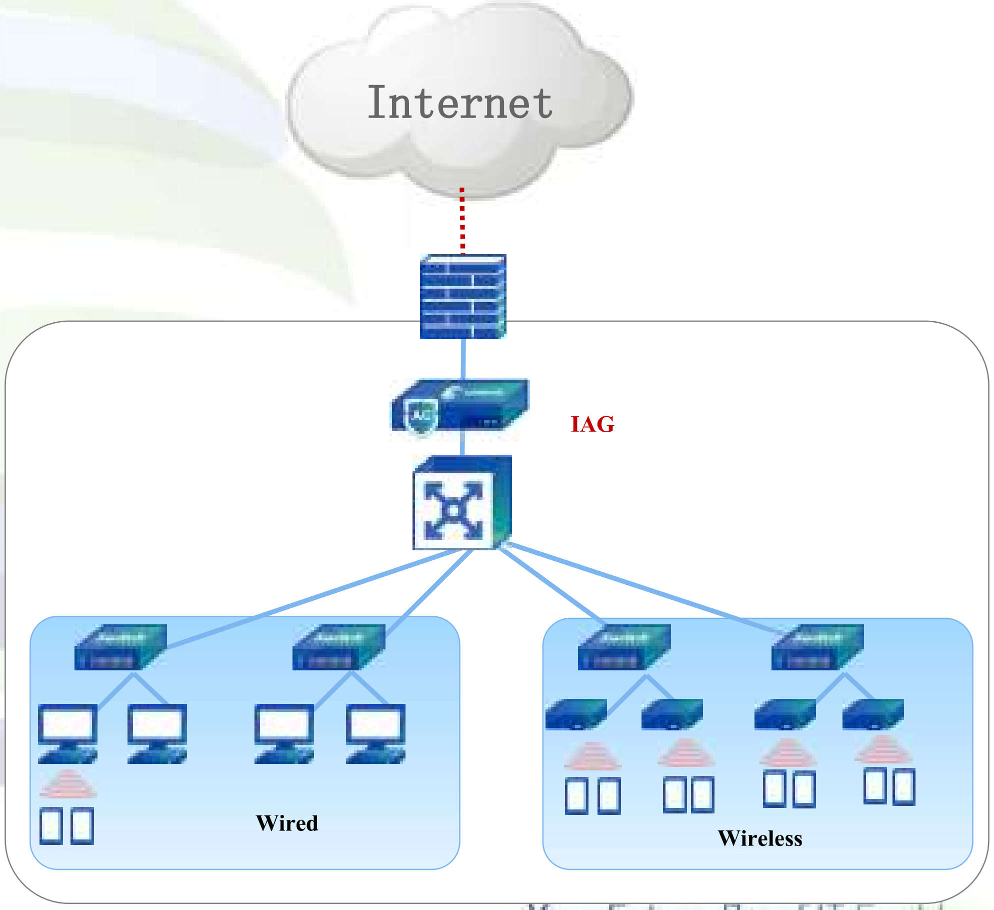
Plan

Routed or Bridge Mode Deployment

1、URL filter + application control

2、Dynamic flow control + P2P intelligent flow control

3、 Based on website, email, forum, Weibo, IM and other content audit and flexible report presentation.



Integrated gateway

Target user

Multi-branch enterprise, government, finance, etc

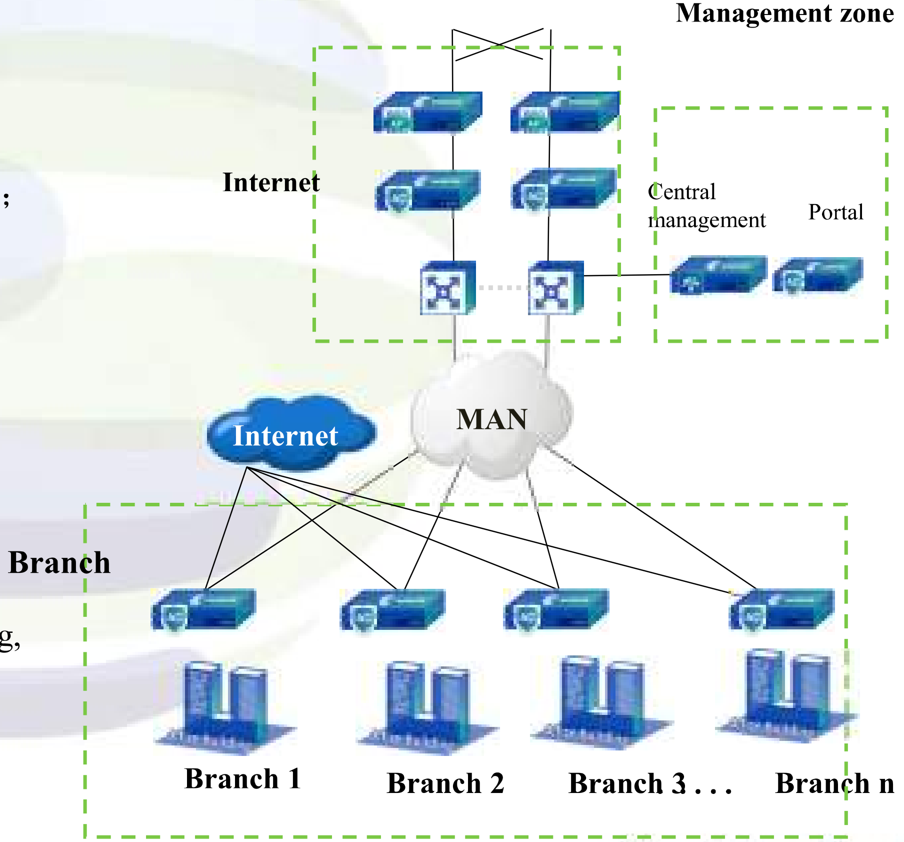
User requirement

1、 IPSEC networking is required between the branch and the headquarters；

2、 Branches need to control Internet behaviour；

3、 Need to have online behaviour audit to meet the network security law；

4、 Branches require basic firewall protection



Plan

1、 Save investment, integrate gateway, easily meet the needs of networking, security, behaviour control

2、 Comprehensive audit to meet the regulatory requirements of the public security department；

Wireless Wi-Fi Control Marketing

Client requirement

1、 Centralized authentication for branch Wi-Fi access

2、 Multiple authentication methods and interfaces are required to meet different scenarios

3、 Realize unified policy management

4、 To meet cybersecurity law audit requirements

Plan

1、 Before user authentication, use a browser to visit any website.

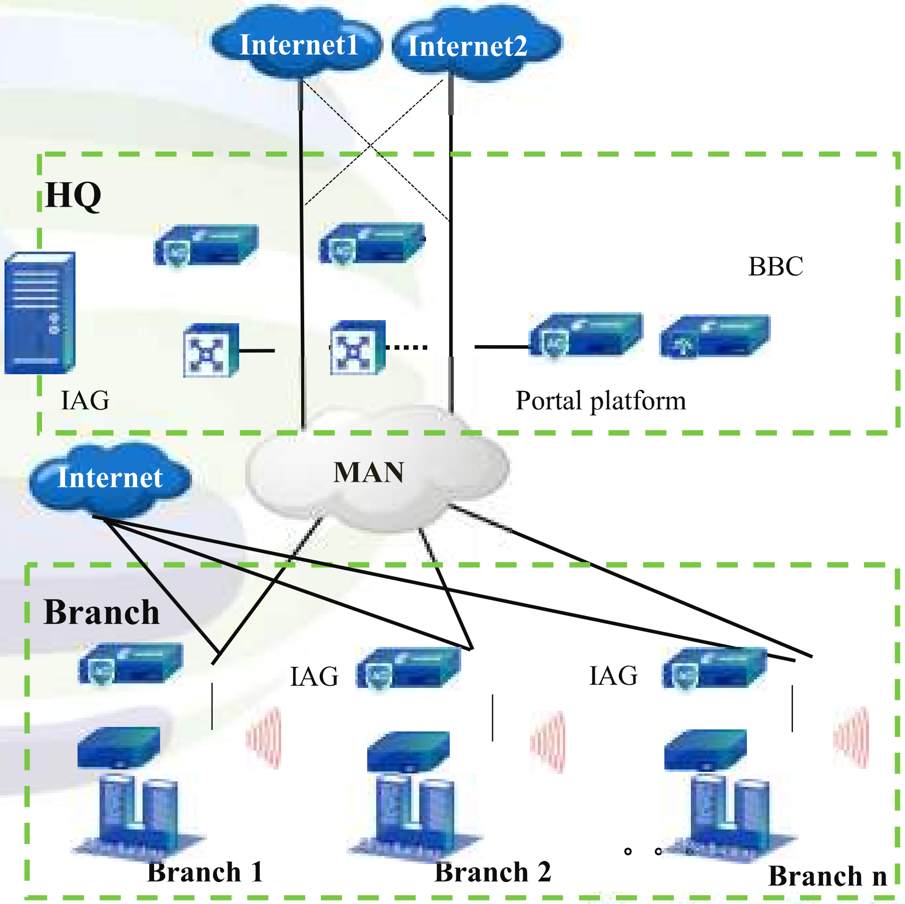
2、 The WLC finds that the user is not authenticated and redirects to the Portal server.

3、 Authentication on the Portal server with SMS, QR code authentication and other authentication methods.

4、 Through authentication, normal access to the network

5、 Audit and send logs to headquarters

6、 The behavior perception system shows the network situation on the whole network



Office gateway audit

Client requirement

1、Lack of measures to record online behaviour, once a network violation occurs, it is impossible to trace people.

2、 "Network Security Law" requires online auditing, and compliance requirements are more stringent.

3、 The organizational structure is complex and there are many people, so it is impossible to carry out effective real-name online authentication

Plan

1、Build an online identity authentication system to ensure the security of personnel online access

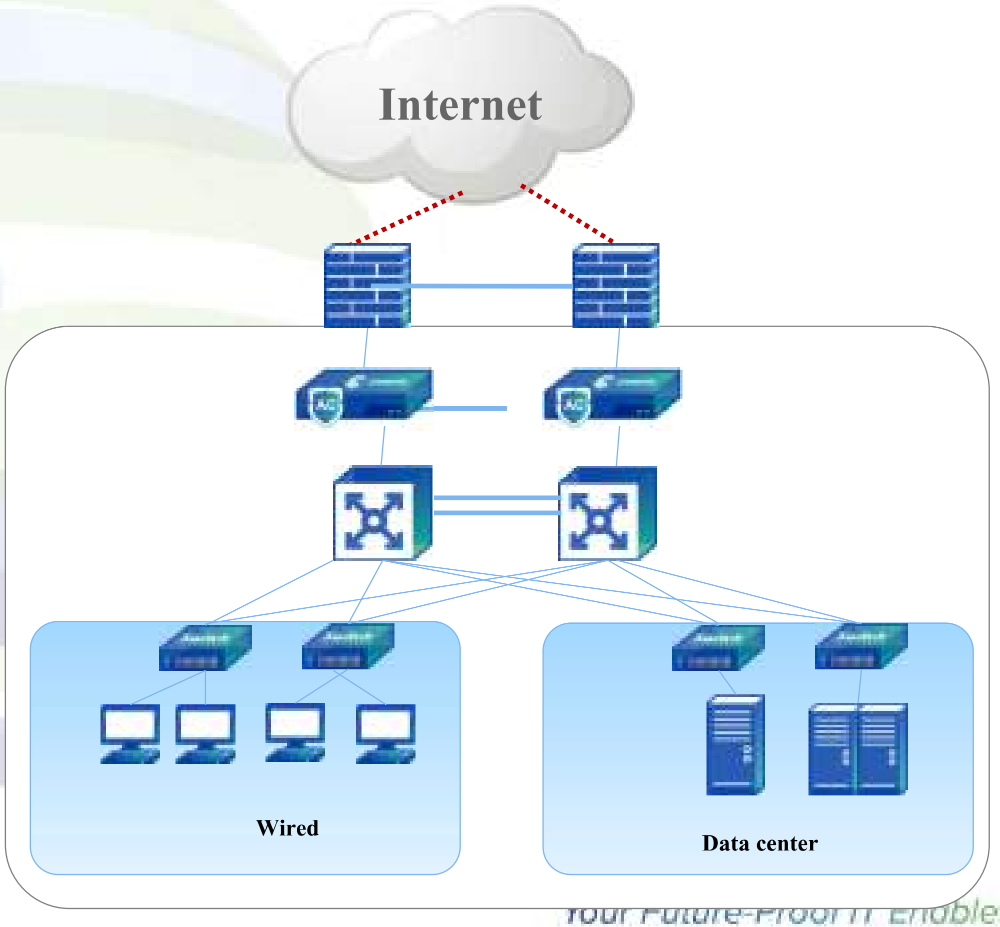
2、 Comprehensive audit of online behaviour

3、 [University] There is a need for precise flow control

4、 [Finance] Accurate identification and strategic control needs.

Target client

Government/Finance/University



Wireless Anti-Share Internet Access

Client requirement

1、Enterprise and government：Private access to Wi-Fi is easy to expose the intranet. Therefore, it is necessary to prohibit shared Internet access behaviours to prevent shared access users from bypassing the company's Internet access control and Internet behaviour monitoring.

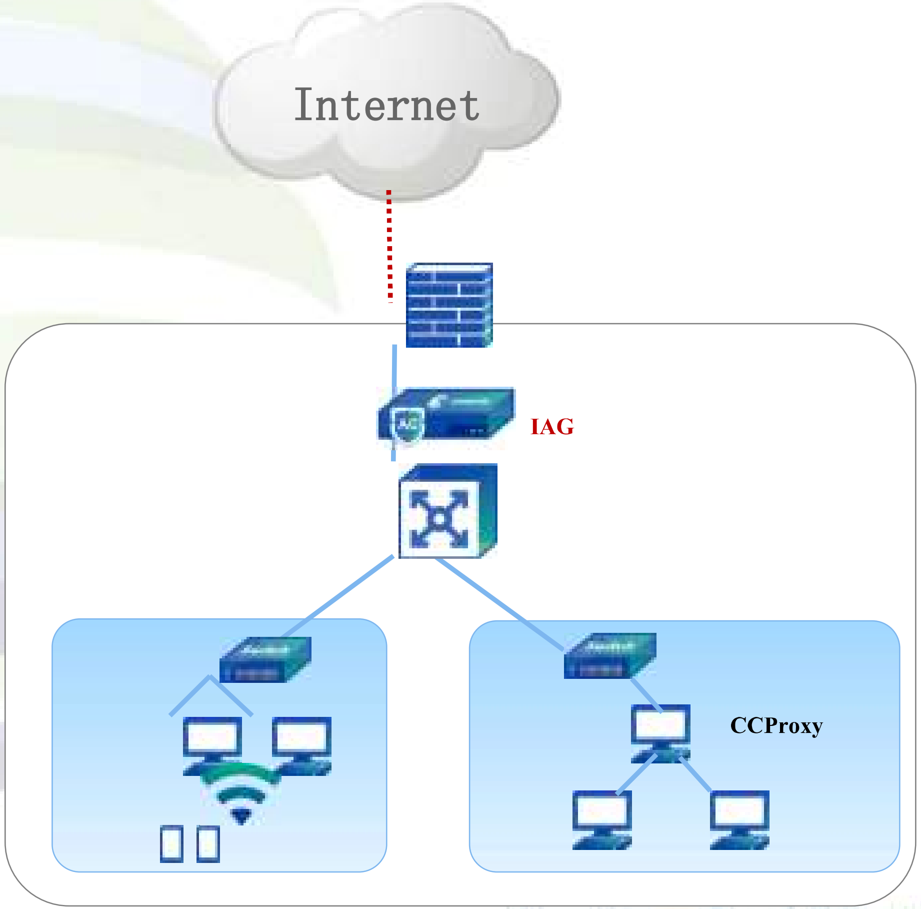
2、 The operator undertakes the construction of the campus network of the university and the wireless shared network in the student dormitory, which affects the operator's broadband account opening rate and income.

Plan

The device is deployed in the gateway or bridge mode. After detecting the sharing behaviour, it will alarm and block the sharing behaviour according to the policy.

Technical advantages

Low false positive rate



Analysis of the network situation on the whole network

Client requirement

●Multi-branch networks are complex and difficult to manage

●The status of the entire network cannot be seen

Value

●Report real-time data, and present the status of Internet access and security at the headquarters

Target client

Education（education network）、multi-branch enterprise.