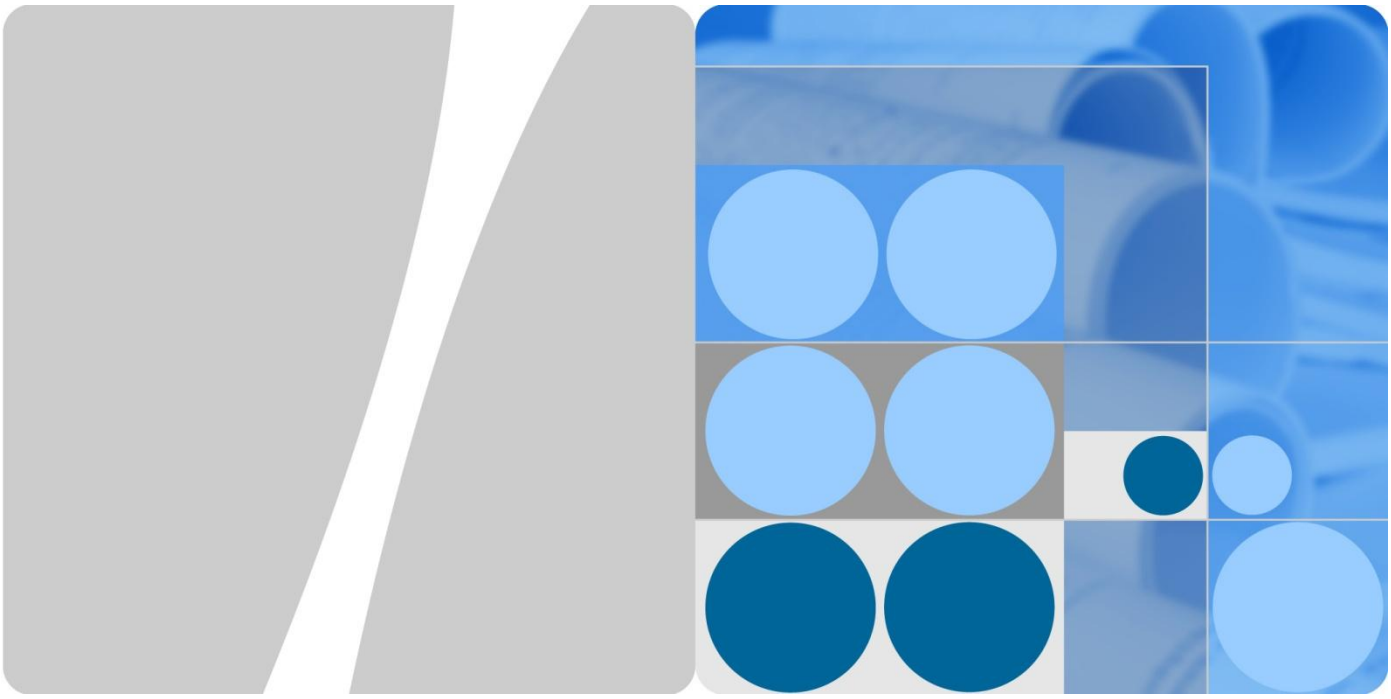


WLAN Application-Layer Security

Technology White Paper

Issue 01

Date 2016-09-14

HUAWEI TECHNOLOGIES CO., LTD.

Trademarks and Permissions


and other Huawei trademarks are trademarks of Huawei Technologies Co., Ltd.

All other trademarks and trade names mentioned in this document are the property of their respective holders.

Notice

The purchased products, services and features are stipulated by the contract made between Huawei and the customer. All or part of the products, services and features described in this document may not be within the purchase scope or the usage scope. Unless otherwise specified in the contract, all statements, information, and recommendations in this document are provided "AS IS" without warranties, guarantees or representations of any kind, either express or implied.

The information in this document is subject to change without notice. Every effort has been made in the preparation of this document to ensure accuracy of the contents, but all statements, information, and recommendations in this document do not constitute a warranty of any kind, express or implied.

Huawei Technologies Co., Ltd.

Address: Huawei Industrial Base
Bantian, Longgang
Shenzhen 518129
People's Republic of China

Website: http://www.huawei.com

Email: support@huawei.com

About This Document

Keywords

WLAN, application security, URL, IPS, antivirus

Abstract

With the network development, increasing new applications bring more conveniences to people's network life, but also cause more security risks. When internal hosts access the Internet, worms, Trojan horses, and other viruses may be introduced accidentally from the Internet and cause confidential data leakage and huge losses to enterprises. Traditional firewalls control traffic of terminals only using IP addresses and protocols. That is, network access is controlled using the protocol type, source IP address, source port, destination IP address, and destination port in ACL rules. To protect intranet security, enterprises need to control the traffic based on the source and destination as well as identify and monitor traffic contents. To enable enterprises to achieve security protection capabilities at the application layer, Huawei provides URL filtering, application identification and filtering, intrusion prevention system (IPS), and antivirus features.

Acronyms and Abbreviations

Acronym and Abbreviation	Full Name
STA	Station
AP	Access Point
URL	Uniform Resource Locator
ACL	Access Control List
IPS	Intrusion Prevention System
AV	Antivirus
FTP	File Transfer Protocol
HTTP	Hypertext Transfer Protocol
POP3	Post Office Protocol - Version 3
SMTP	Simple Mail Transfer Protocol

Acronym and Abbreviation	Full Name
IMAP	Internet Message Access Protocol
NFS	Network File System
SMB	Server Message Block

Contents

1 Application Security Overview

With the network development, increasing new applications bring more conveniences to people's network life, but also cause more security risks.

When internal hosts access the Internet, worms, Trojan horses, and other viruses may be introduced accidentally from the Internet and cause confidential data leakage and huge losses to enterprises. Traditional firewalls control traffic of terminals only using IP addresses and protocols. That is, network access is controlled using the protocol type, source IP address, source port, destination IP address, and destination port in ACL rules. This can hardly meet enterprises' requirements for a rich variety of diversified networks and applications. For example:

- An increasing number of services with different risk levels run on ports 80 and 443 using HTTP and HTTPS, for example, web instant messaging, web game, web video, and web chats.
- As new working modes such as telecommuting and mobile office emerge, IP addresses of hosts used by the same user may change at any time. Traffic control based on IP addresses cannot meet modern network requirements.
- The traditional single-packet detection mechanism only analyzes the security of a single packet, and cannot defend against network threats such as buffer overflow attacks, Trojan horses, and worms that occur during a normal network access process.

  To protect intranet security, enterprises need to control the traffic based on the source and destination as well as identify and monitor traffic contents.

  Huawei WLAN products provide the following application-layer security access control capabilities.

1.1 URL Filtering

In an enterprise, employees' uncontrolled access to the Internet where an abundance of applications and websites exist will definitely bring many potential problems and threats to the enterprise. The following are some examples:

- Visiting non-work-related websites during working hours reduces work efficiency.
- Visiting illegal or malicious websites may result in leaks of enterprise confidential information and threats such as worms, viruses, and Trojan horses.
- Failures to properly access work-related websites, such as the enterprise home page and search engines, impair employees' work efficiency.

To control website access of employees, an enterprise administrator can use URL filtering technology to prevent the employees from accessing illegal or malicious websites that contain gambling, entertainment, or pornography information. URL filtering technology can control URL access of users or user groups based on various information such as the user, user group, period, and security zone, thereby implementing precise management of users' online behavior.

1.2 Application Identification and Filtering

Among so many Internet applications, some applications carry key services of enterprises, some applications merely meet recreational demands of the people, and some applications consume a large number of network resources (such as P2P download). Additionally, illegal applications with security risks to enterprises exist on the Internet. Confronted with such challenges, enterprises are in need of refined management of network applications and services, visualized management and control over applications and services on smart terminals, and enhanced capabilities in controlling network bandwidth resources for network security.

Traditional firewalls identify applications by protocol and port number. If two applications use the same protocol and port number, for example, web game and web video that both use HTTP port 8080, a traditional firewall cannot distinguish these two applications. Existing network statistics collection and control means based on interfaces, IP addresses, or other original packet characteristics can hardly meet current network management requirements.

Based on the market competition and solution needs, enterprises need refined service management to achieve visualized management and control over services and applications on smart terminals in addition to enhanced security management and effective bandwidth control. The following are some security policies:

- Limit or block unexpected application traffic on the network to better utilize bandwidth resources.
- Improve the service level of key services by setting higher priorities to ensure the quality of key services.
- Collect traffic statistics based on applications so that a network administrator can easily identify network usage.

1.3 IPS

With the network development, increasing new applications bring more conveniences to people's network life, but also cause more security risks. When internal hosts access the Internet, worms, Trojan horses, and other viruses may be introduced accidentally from the Internet and cause confidential data leakage and huge losses to enterprises. Therefore, enterprises need to control the traffic based on the source and destination as well as identify and monitor traffic contents.

An intrusion prevention system (IPS) is a security mechanism. It detects intrusion behavior (such as buffer overflow attacks, Trojan horses, and worms) by analyzing network traffic, and terminates the intrusion behavior in real time through specific response methods. This protects enterprise information systems and network architectures against intrusions.

Server protection	Protects servers providing access to external networks against viruses and intrusions.	IPS: defends against attacks from the application layer to servers.
Web access protection	Protects internal users against viruses and intrusions when they access websites and download files.	IPS: blocks intrusions in web access.

IPS identifies various application-layer attacks by matching signature fields. Signature-based threat detection is achieved based on the following protection methods:

- Vulnerability attack defense: Vulnerabilities refer to security defects in a system, including the defects in computer hardware, software, protocol implementation, and system security policies. Intruders use vulnerabilities to access files, obtain confidential information, or even execute programs without authorization.
- Web security protection: Web services are generally applications running on HTTP. Attackers use HTTP/HTTPS-based applications to bypass traditional firewalls and HTML evasion technology to attack the web security server, such as SQL injection and cross site script (XSS) attacks. Additionally, more and more attacks are launched to ActiveX controls of desktop clients and plug-ins, components, and JavaScript of browsers.
- Malicious code prevention: This defends against attacks caused by malicious codes such as botnet, Trojan horse, worm, and spyware.

1.4 Antivirus

Virus is a kind of malicious code that may be attached in or infect application programs or files. In most cases, viruses are spread through email or file sharing protocols and pose threats on user hosts and networks. Some viruses exhaust host resources and occupy a lot of network bandwidth, some viruses may control the host permission and steal user data, and some viruses even do damage to host hardware.

Currently, most network threats such as viruses not only attack computer systems but also are used by hackers or criminals to earn profits. Traditional network threats such as computer viruses are being transformed into profit-driven and all-round network threats. Users are now confronted with combinations of network threats such as viruses, attacks, Trojan horses, botnets, and spyware, instead of sole virus attacks. The legacy defense cannot be as effective as expected.

Antivirus is a security mechanism that identifies and processes virus files to secure networks and prevent such problems as data damage, permission tampering, and system crashes. Huawei's WLAN systems are integrated with the antivirus function and have a large and up-to-update antivirus signature database to effectively protect network security and prevent virus files from corrupting system data. Virus detection devices are deployed at ingresses of enterprise networks to exclude viruses, providing a solid protection layer for the enterprise networks.

Note: The antivirus feature provided by network devices and the antivirus software on user hosts are complementary and cooperate with each other. As they are deployed in different

places and have different signature databases, the antivirus feature and the antivirus software can be used simultaneously to better ensure security of the network and user hosts.

2 Implementation

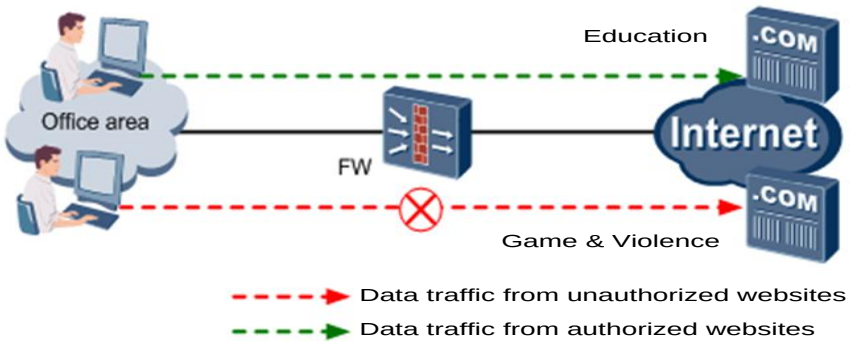
2.1 URL Filtering

The openness of the Internet enables any organization or individual to easily establish websites. The Internet is filled with hundreds of millions of websites, millions of which are newly registered each year. As laws, regulations and the supervision of different countries vary, the influx of web pages is diversified, covering online gaming, shopping, stock trading, online radio, video, and even contents with pornography, violence, and racism.

If users' web access is controlled at the egress gateway of an enterprise network, the enterprise can obtain abundant Internet resources, while mitigating the negative impacts caused by the Internet. In this way, enterprise's work efficiency is improved and network resources are properly utilized, ensuring the security of IT infrastructure and reducing legal risks for the enterprise.

If the egress gateway verifies web resources in advance and saves their URLs, when a user attempts to access a web resource URL, the gateway can determine whether to allow the user to access it by extracting the previously saved URLs. Therefore, users' web access rights can be effectively controlled.

Figure 2-1 URL filtering



2.1.2 URL Filtering Process

Figure 2-2 URL filtering process

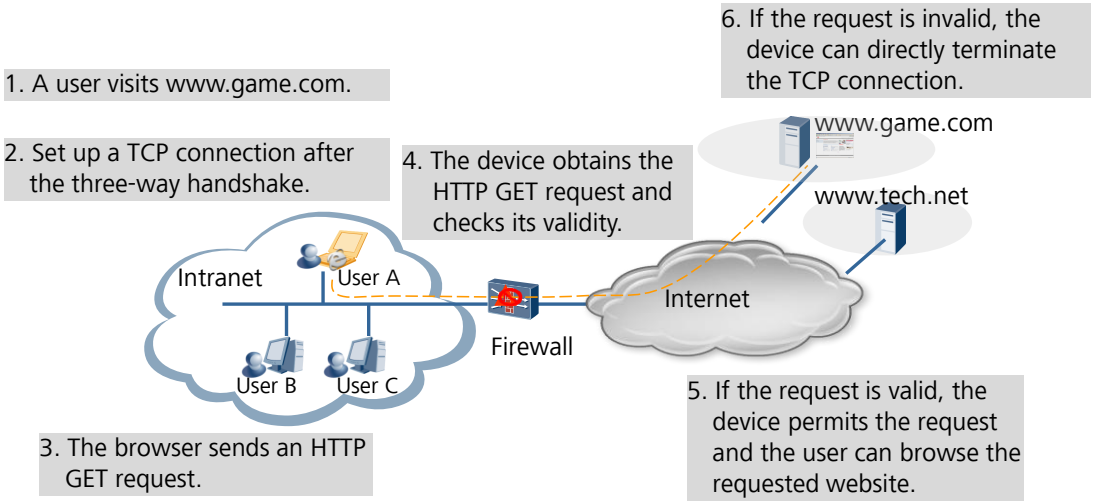


Figure 2-2 shows how the URL filtering is implemented.

1. A user enters the URL of a website in the browser.
2. The STA sets up a TCP connection with the website server.
3. The browser sends an HTTP GET request to the target website server.
4. The WLAN device supporting the application security firewall function obtains the HTTP GET request, and matches it against the URL blacklist and whitelist by keyword.
5. If the HTTP GET request is valid (in the URL whitelist), the WLAN device permits the request, so that the user can browse the requested website.
6. If the HTTP GET request is invalid (in the URL blacklist), the WLAN device blocks this request and terminates the TCP connection.

2.1.3 URL Filtering by Blacklist or Whitelist

An enterprise administrator can configure a URL blacklist and whitelist to permit or deny a URL.

The whitelist has a higher priority than the blacklist. The blacklist and whitelist are applicable to the following scenarios:

- Blacklist

  To improve work efficiency of employees and fully utilize network bandwidth, enterprises need to control online behavior of employees and prevent them from accessing entertainment, game, and video websites.

  A URL blacklist is configured to prevent users from accessing the blacklisted URLs.
- Whitelist

  Enterprises have special requirements and want to exempt certain websites from filtering.

  A URL whitelist is configured to allow users to access the whitelisted URLs.

URLs can be matched in various modes, as listed in the following table. The following table lists the comparison of these matching modes.

Matching Mode	Definition	Keyword	Result
Prefix matching	Matches URLs that start with a specified character string.	www.test.com*	All URLs that start with www.test.com are matched, for example, www.test.com and www.test.com/solutions.do.
Suffix matching	Matches URLs that end with a specified character string.	*aspx	All URLs that end with aspx are matched, for example, www.test.com/news/solutions.aspx and www.test.com/it/price.aspx.
Keyword matching	Matches URLs that include a specified character string.	*sport*	All URLs that include **sport** are matched, for example, sports.test.com/news/solutions.aspx and sports.test.com/it/.
Exact matching	Matches only an exact character string.	www.test.com/news	Only www.test.com/news is matched. www.test.com/news/solutions.aspx and www.test.com/news/en/ are not matched.

NOTE

1. The URL whitelist has a higher priority than the URL blacklist.
2. The priorities of URL matching modes are as follows: exact matching > suffix matching > prefix matching > keyword matching.

2.2 Application Identification and Filtering

Traditional WLAN devices can collect statistics on network traffic based only on the interface or user, but not the service type (such as Thunder, QQ, or Facebook). Therefore, these devices cannot identify applications, or implement application-level policy control.

Huawei's WLAN system supports application visualization, which can identify applications based on the following key technologies:

- Protocol port number
- Signature
- Protocol association
- Behavior analysis
- Multi-dimension combination

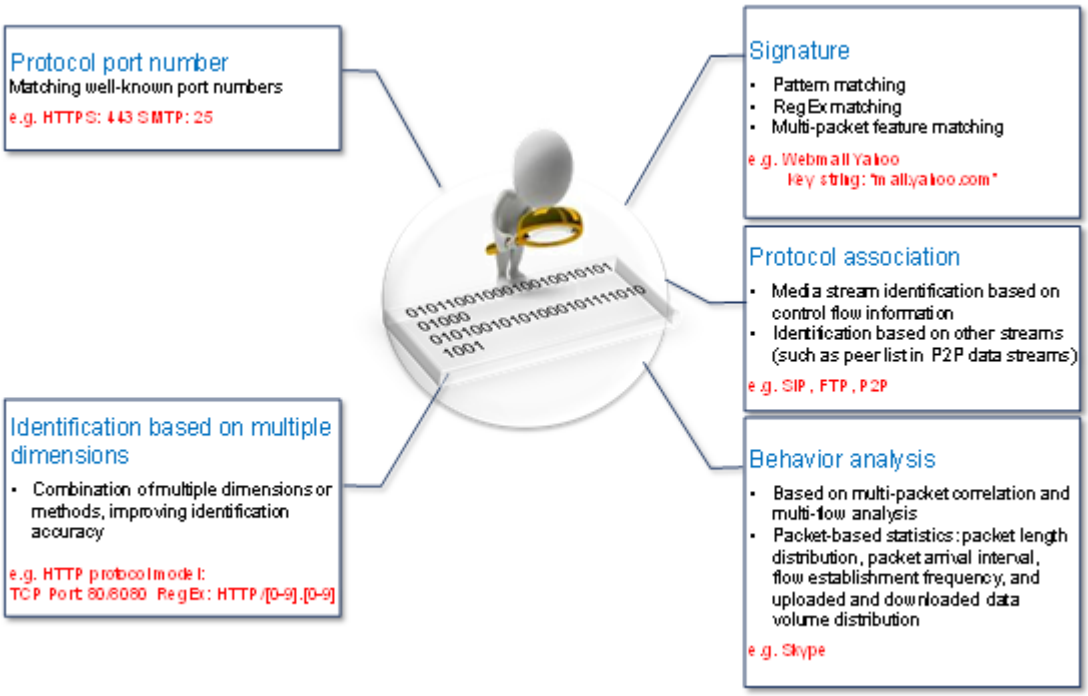
After the WLAN system completes application identification, the network administrator can develop and implement application-based control policies depending on enterprise regulations and/or network congestion status. The available policies include:

- Block traffic of specified applications
- Modify the priorities of specified applications
- Limit the rates of specified applications

2.2.1 Intelligent Application Identification

Huawei uses intelligent application and service identification technologies to visualize applications for identifying and collecting statistics on network traffic. The following figure shows the methods of network traffic identification supported by Huawei.

Figure 2-3 Application identification methods



- Protocol port number–based identification

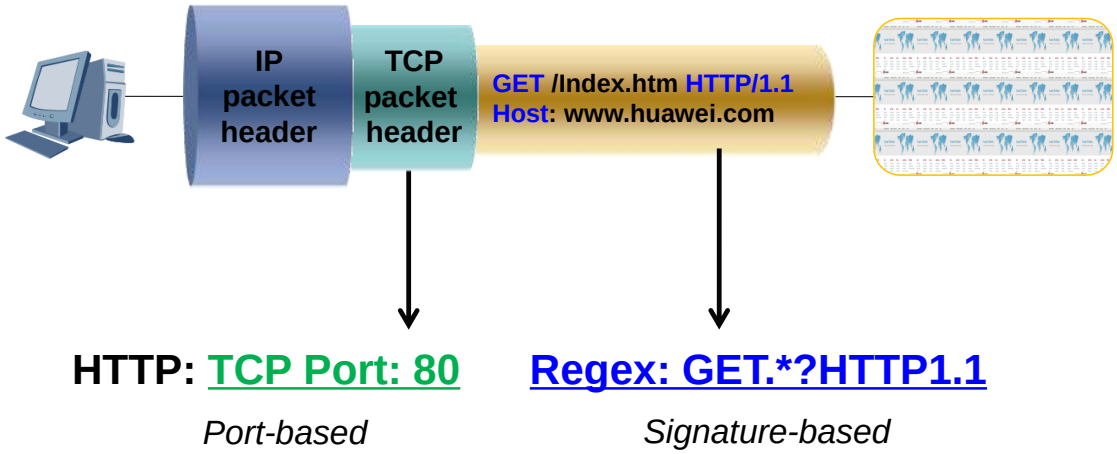
  The identification method is based on protocol port numbers, that is, matching well-known port numbers, for example, HTTP port 80, HTTPS port 443, and SMTP port 25.
- Signature-based identification

The identification method is based on feature codes, which include specific key strings in packets, and the combination of multiple key strings. The feature codes are classified into the following types:

- Pattern matching based on a single or multiple features
- RegEx matching
- Multi-packet feature matching

For example, the packets of Webmail Yahoo protocol may contain the key string **mail.yahoo.com**.

Figure 2-4 HTTP identification



- Protocol association–based identification

  The identification method is based on the analysis of specific application protocols, that is, identifying application streams by parsing the protocol interaction process. This type of identification consists of the following types:

  - Media stream identification based on control flow information
  - Identification based on other streams (such as P2P data streams)

    For example, regarding the port number used by SIP and FTP for media stream interconnection, analyze the control protocols to identify corresponding media streams.

- Behavior analysis–based identification

  The identification method is based on the statistics on intra-flow and inter-flow packets by dimensions such as packet length, interval, and direction.

  - Based on multi-packet correlation and multi-flow analysis
  - Packet-based statistics: packet length distribution, packet arrival interval, flow establishment frequency, and uploaded and downloaded data volume distribution

    This identification method is generally used in Skype. A small amount of traffic from Skype has signature strings, TCP traffic sometimes is destined for ports 80 and 443, and UDP traffic sometimes is destined for ports 12340 and 12350. Therefore, the identification method based on port, signature, and behavior analysis can effectively identify traffic from Skype.

- Identification based on multiple dimensions

The identification based on multiple dimensions or methods can improve identification accuracy. For example, HTTP-based identification is based only on the TCP protocol and well-known port 80. This method may incur incorrect judgment because other applications can also use TCP and port 80 to transmit data. To improve identification accuracy, you can use both port number–based and signature-based identification to define the HTTP protocol model, for example, **TCP Port: 80/8080 Regex: HTTP/[0-9].[0-9]**.

2.2.2 Application-based Policy

You can perform a specified application policy after identifying the application type of packets. WLAN products support three types of policies:

- Application blocking

  After the blocking policy is implemented on specified applications, all packets from the applications will be discarded.

- Priority setting

  The priority policy is implemented on specified applications, and the precedence field (DSCP or 802.1p) of the packets from the applications is set to the configured value. The administrator can set the priorities of different applications to ensure the service quality of important applications.

- Bandwidth restriction

  The bandwidth restriction policy can set the upper limit of the bandwidth occupied by a specific application. By setting the bandwidth upper limit for different applications, you can specify the traffic proportion for these applications on the network.

  This policy is used to prevent some applications from occupying a large number of network resources and affecting other applications. For example, the bandwidth of P2P applications can be limited to prevent their abuse of network resources.

2.3 IPS

The IPS consolidates intrusion features into a knowledge base and compares network data flows with the features in the knowledge base to detect threats and prevent attacks at the application layer.

- For vulnerability attack defense, the IPS analyzes vulnerability principles and extracts common signatures for pattern matching to detect vulnerabilities.
- For web security protection, security protection for HTTP applications is of great importance in addition to defense against common vulnerabilities. URL anti-evasion and HTML anti-confusion are required before pattern matching for HTTP application attack detection.
- The IPS analyzes Trojan horses, worms, and botnets, extracts communication features, and identifies roles based on the features to detect threats.

2.3.1 High-Precision Protocol Decoding

To detect intrusions and viruses in application-layer data and filter the data, a system must be able to identify application-layer protocol types before providing protocol-specific suggestions.

By dynamically analyzing the protocol features contained in packets, the IPS can automatically identify application-layer protocols running on non-standard ports.

For accurate attack identification, the IPS carries out in-depth application identification before protocol decoding and in-depth threat detection. As an essential part for in-depth detection, the protocol decoding specifications reduce signature matching workloads, identify and process anti-evasion technologies, and detect protocol anomaly attacks, improving threat detection accuracy.

The IPS supports the detailed decoding of about 100 protocol variable fields, including common protocol variable fields. The detailed decoding is performed on the basis of network attack research and analysis of protocol information in the signature database. Protocol decoding helps the IPS defend against protocol anomaly attacks. Hackers often exploit the less-perfect design of application servers (that is, vulnerabilities in inadequate consideration of protocol anomalies) to launch attacks. By sending non-standard or buffer-overflow protocol data to servers, the hackers seize the control power over servers or cause server crashes. The IPS supports anomaly detection for multiple protocols. It performs in-depth protocol analysis of RFC violations, excessively long fields, unreasonable protocol interaction sequences, and parameters of abnormal application protocols to evaluate the severity, based on which the IPS identifies potential intrusions targeted at application servers and clients.

Protocol Anomaly Detection (PAD) covers more than 40 types of protocols, including HTTP, SMTP, FTP, POP3, IMAP, MSRPC, NETBIOS, SMB, TDS, TNS, TELNET, IRC, and DNS.

2.3.2 File-based Detection Technology

The IPS engine can detect file anomalies by considering files as protocols. Therefore, the IPS can detect malicious files transmitted on the network.

The IPS can detect most types of files transmitted over the Internet protocols, including HTTP, SMB, FTP, SMTP, POP3, IMAP, and NFS. The built-in file type identification engine can identify hundreds of file types, such as PE, ZIP, OFFICE, PDF, JPG, AVI, and SWF, to detect malicious files transmitted on the network.

2.3.3 Network Feature–based Pattern Matching

Network traffic has behavior such as intrusion attacks, Trojan horse spread, vulnerability attacks, and botnet communications. The analysis of such behavior features helps form network behavior feature codes, which can be used to detect malicious network traffic and finally block malicious network behavior. Most malicious network behavior can be detected based on the features of one packet. The IPS provides multi-pattern matching technology and supports regular expressions to improve rule flexibility and accuracy.

2.3.4 Other Advanced Defense Technologies

- PAD

  PAD is a common intrusion detection method. Hackers often exploit the less-perfect design of application servers (that is, vulnerabilities in inadequate consideration of protocol anomalies) to launch attacks. By sending non-standard or buffer-overflow protocol data to servers, the hackers seize the control power over servers or cause server crashes.

  The IPS supports anomaly detection for multiple protocols. It performs in-depth protocol analysis of RFC violations, excessively long fields, unreasonable protocol interaction sequences, and parameters of abnormal application protocols to evaluate the severity, based on which the IPS identifies potential intrusions targeted at application servers and clients.

Similarly, the IPS considers an abnormal file structure a protocol anomaly. In this case, the IPS can detect buffer anomaly attacks or scripting attacks hidden in file content.

- Web attack behavior–based detection

  In addition to the detection on common HTTP traffic, the IPS can restore data for user-submitted information and then perform feature detection to identify attack behavior, such as SQL injection and XSS attacks.

- Comprehensive anti-evasion technology

  Taking advantage of network protocol complexity and TCP/IP openness, hackers may transform protocol traffic. As devices cannot identify the transformation cause, they cannot simply discard transformed traffic, which may interrupt services, or permit it, which may cause attack vulnerabilities. To resolve this problem, the engine must be able to shape the traffic. For example:

(1) Reassembly of IP fragments. The engine must cache and reassemble out-of-order fragments to ensure that the fragments start from the first one and arrive at the destination in sequence.

(2) TCP traffic reassembly. The engine must maintain TCP state, process overlapped TCP segments, discard overlapped parts, and check TCP options.

(3) RPC (DCERPC, SUNRPC) fragment reassembly and multi-request binding

(4) Normalized processing of URL insert characters, codes, and paths

(5) Processing of FTP insert characters

(6) NetBIOS and SMB anti-evasion technology

(7) HTTP anti-evasion technologies such as codes, folding, and abnormal header

2.4 Antivirus

Currently, enterprise users transfer and share files over networks more frequently, facing unprecedented virus threats. Enterprises have to keep viruses out of the networks to ensure data security and system stability. Therefore, preventing viruses from intruding hosts and network systems becomes a challenge to enterprises.

The antivirus function depends on the powerful and continuously updating virus signature database to secure the network and system data. The virus detection device deployed at the ingress of the enterprise network shields the networks from viruses.

Figure 2-5 Antivirus control

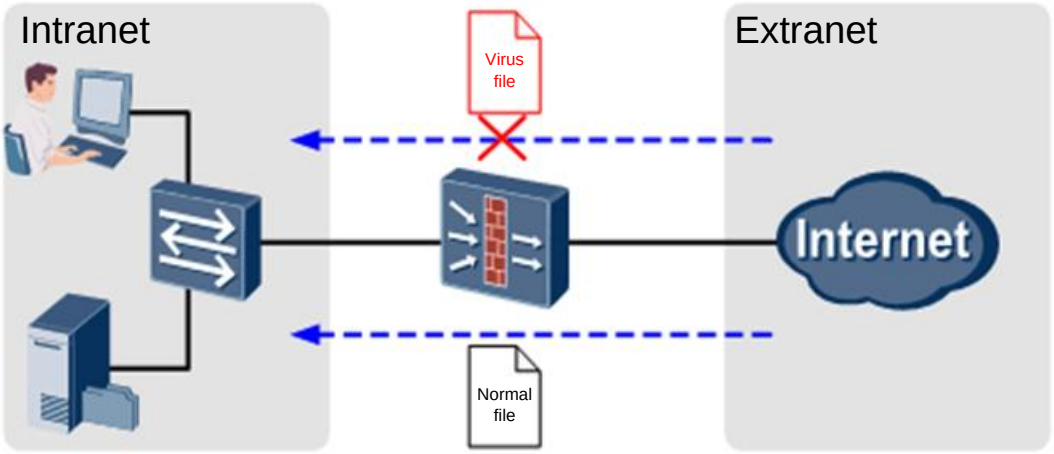
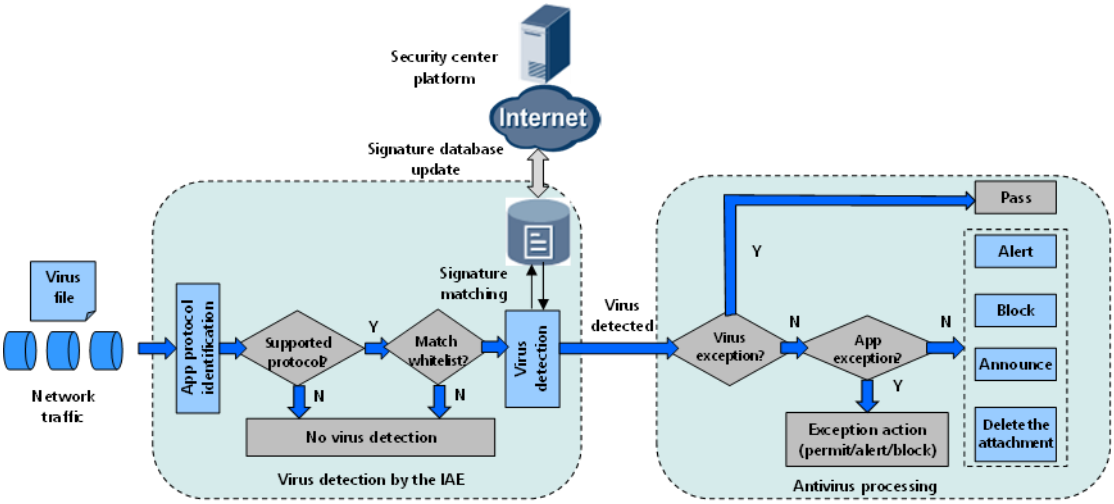


Figure 2-6 Antivirus mechanism



2.4.2 Virus Detection by the IAE

Virus detection is performed by the Intelligence Awareness Engine (IAE). After traffic enters into the IAE, the IAE:

1. Deeply analyzes network traffic to identify the protocol type and file transfer direction.
2. Checks whether this protocol type and file transfer direction support virus detection.

   Huawei's WLAN system performs antivirus for files transferred using the following protocols:

   - File Transfer Protocol (FTP)
   - Hypertext Transfer Protocol (HTTP)
   - Post Office Protocol - Version 3 (POP3)

- Simple Mail Transfer Protocol (SMTP)
- Internet Message Access Protocol (IMAP)
- Network File System (NFS)
- Server Message Block (SMB)

Huawei's WLAN system also supports antivirus for files that are transferred in the following directions:

- Upload: A client sends a file to a server.
- Download: A server sends a file to a client.

3. Implements virus detection.

   The IAE extracts signatures of a file for which antivirus is available and matches the extracted signatures with those in the antivirus signature database. If a match is found, the file is a virus and processed according to the response action specified in the configuration file. If no match is found, the file is permitted.

   Huawei analyzes various common virus signatures and forms a virus signature database. The database defines common virus signatures and assigns a unique virus ID to each virus signature. After being loaded with this database, the device can identify viruses defined in the database. To identify new viruses, the virus signature database needs to be continuously updated. For details, visit Huawei security center at sec.huawei.com.

2.4.3 Antivirus Procedure

After identifying a transferred file as a virus, the system performs the following operations:

1. Check whether the virus matches a virus exception. If yes, the file is permitted.

   To prevent file transfer failures due to incorrect reports, users can add the virus IDs that users identify to virus exceptions so that the corresponding virus rules do not take effect. If the detection result matches a virus exception, the file is permitted.

2. If the virus does not match any virus exception, check whether it matches an application exception. If yes, the file is processed according to the specified response action (permit, alert, or block).

   Response actions for application exceptions can be different from those for protocols. Various types of application traffic can be transmitted over the same protocol. For example, traffic of 163.com and yahoo.com is transmitted both over HTTP.

   For such applications and protocols, the configured response action takes effect based on the following rules:

   - If only the protocol response action is configured, all applications over this protocol inherit this response action.
   - If both protocol and application response actions are configured, the application response action is preferential.

   For example, HTTP can carry both traffic of 163.com and that of yahoo.com.

   - If you configure the response action for HTTP as **Block**, the response action block takes effect on both 163.com and yahoo.com.
   - If you need to configure an exception for 163.com, configure the response action for 163.com as **Alert** in **Application Exception**. Then the response action for yahoo.com is **Block** whereas the response action for 163.com is **Alert**.

3. If the virus matches neither virus exceptions nor application exceptions, deal with it based on the response action corresponding to its protocol and transfer direction specified in the configuration file.

The following table lists response actions supported by various protocols in various file transfer directions.

Protocol	Transfer Direction	Response Action	Description
HTTP	Upload/Download	Alert/Block. The default response action is Block.	Alert: The device permits the virus file and generates a virus log. Block: The device blocks the virus file and generates a virus log.
FTP	Upload/Download	Alert/Block. The default response action is Block.	
NFS	Upload/Download	Alert	
SMB	Upload/Download	Alert/Block. The default response action is Block.	
SMTP	Upload	Alert	
POP3	Download	Alert	
IMAP	Upload/Download	Alert	

NOTE

The virus signature database updates frequently. To ensure the effectiveness of the antivirus function, it is recommended that the antivirus signature database be updated every day.

3 Signature Database Update

Rapidly increasing intrusion methods, virus types, and applications on networks motive people's demand in identification efficiency and capability of devices. To enable devices to identify new applications and defend against emerging attacks and viruses, users need to constantly update signature databases.

Huawei's professional security team closely traces the security bulletins of renowned security organizations and software vendors, analyzes and verifies various applications and threats, and generates the signature database for protecting software and systems such as operating systems, applications, and databases. Additionally, an information collection system is deployed to capture the latest attacks, worms, and Trojan horses in real time, facilitating the generation of signatures and the discovery of threat trends. In this manner, the system can obtain the latest signatures and IPS engine in the shortest time, providing zero-day attack defense capability.

Huawei has deployed a dedicated security center (sec.huawei.com) for all Huawei security products to update their signature databases. You can visit Huawei security center to update signature databases to enhance your security products' capabilities of and efficiency in detecting the latest intrusions, viruses, applications, and malicious domain names.

The application security features in Huawei's WLAN system involve the following signature databases:

- IPS signature database
- Antivirus signature database
- Application identification signature database
- Malicious domain name signature database

The signature databases can be updated in any of the following modes, which apply to different scenarios:

1. Scheduled update: The update can be implemented in time, and new attacks can be defined quickly, requiring no manual intervention. This mode is applicable to devices that connect to the update server. To confirm the security and availability of a downloaded signature database, you can use the confirmation mechanism. That is, the latest version is downloaded periodically but is not immediately applied. Instead, it is applied after being confirmed.
2. Real-time update: When a new version is released but the automatic update time does not approach, you can update the signature database immediately. This mode features high timeliness and allows you to immediately know the update results.

3. Local update: If a device cannot connect to the update server or the version must be rolled back to an earlier version, use this update mode to switch the version to a specific version.
4. Version rollback: If the incorrect report rate is high and the detection rate is low, you can roll back the software version to the previous one.

The scheduled and real-time update modes require manual intervention. You only need to ensure that WLAN network devices can access Huawei's security center (sec.huawei.com), and that scheduled or real-time update is enabled on these devices. WLAN network devices can automatically access the security center and download the latest security signature and application signature database for update to protect the security of WLAN networks.

4 Products and Networking

The following table lists security features supported by WLAN products.

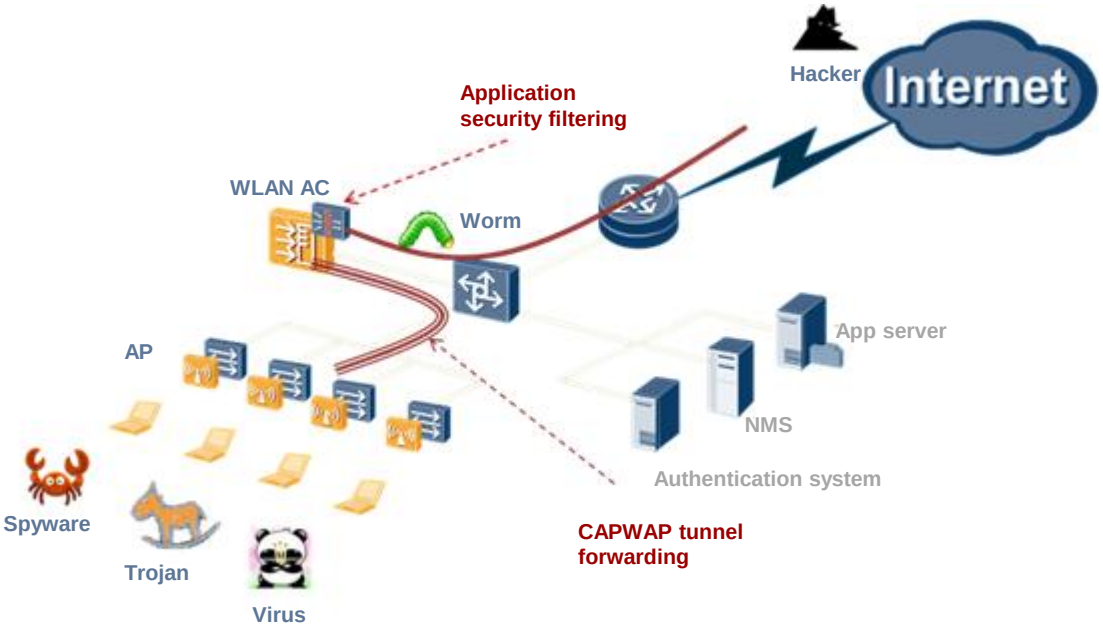
	AC	Fit AP	Fat AP	Central AP (Fat)	Central AP (Fit)
URL filtering	Y	N	Y	Y	N
SAC	Y	N	Y	Y	N
IPS	Y	N	N	Y	N
Antivirus	Y	N	N	Y	N

4.1 Campus Security Deployment

4.1.1 WLAN AC Deployment in Bypass Mode

In bypass mode, an AC is connected to a network device (usually an aggregation switch) to manage APs. Data flows can be forwarded by the AC over a Control and Provisioning of Wireless Access Points (CAPWAP) data tunnel, or forwarded to the upper-layer network by the aggregation switch and do not pass through the AC.

Figure 4-1 WLAN AC deployment in bypass mode



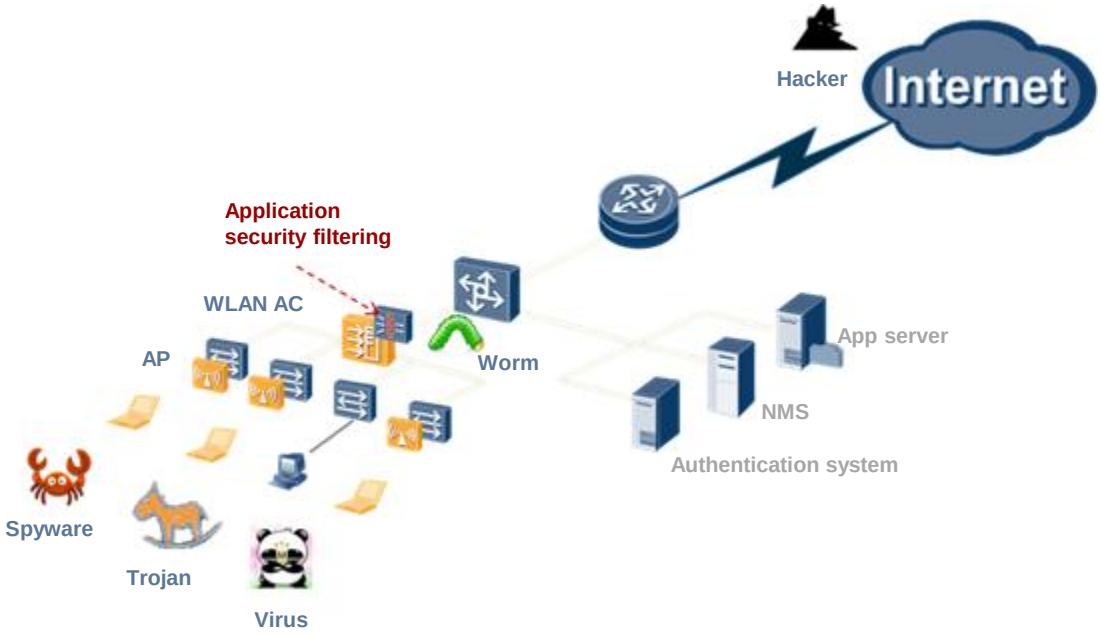
Fit APs do not support application-layer security features mentioned above. Therefore, to protect wireless access security, configure the tunnel forwarding mode so that wireless traffic is forcibly forwarded through a CAPWAP tunnel to the AC for security check and filtering at the application layer. Such a networking mode prevents viruses and Trojan horses of mobile STAs from entering the intranet, and regulates Internet access and applications of STAs according to the enterprise's requirements.

4.1.2 WLAN AC Deployment in Inline Mode

In inline mode, an AC is directly connected to APs or access switches. The AC serves both as an AC and an aggregation switch to forward and process data and management services of APs.

In inline mode, the AC sets up CAPWAP management tunnels with APs to configure and manage these APs over the CAPWAP management tunnels. Service data of wireless users can be forwarded between APs and the AC over CAPWAP data tunnels (in tunnel forwarding mode) or be directly forwarded by APs (in direct forwarding mode).

Figure 4-2 WLAN AC deployment in inline mode



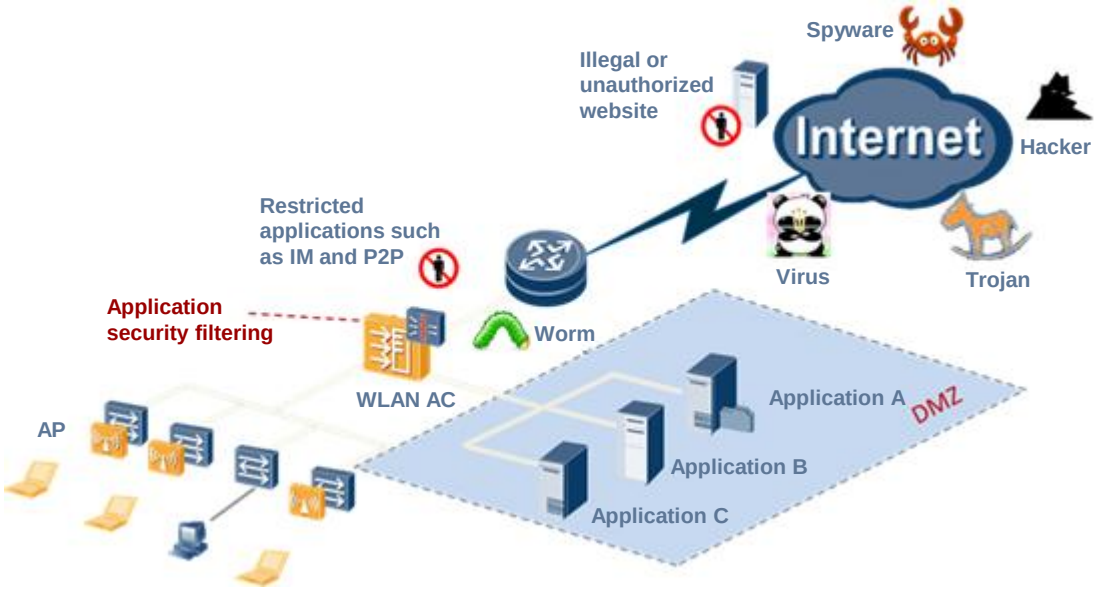
In this networking mode, all wireless traffic is forwarded by the AC regardless of the forwarding mode. Application-layer security protection features of the AC take effect not only on CAPWAP data tunnels but also on wired ports. Therefore, security check and filtering can be performed no matter what forwarding modes Fit APs use.

Another benefit is that all wired STAs connected to the AC are secured, that is, security check and filtering are performed on traffic from all STAs under the AC.

4.1.3 Full Integration Deployment for Small Campuses

Some small campuses may have no core/aggregation switches or independent firewall devices. In this case, a Huawei WLAN AC can be deployed to build a simple and fully integrated secure campus network.

Figure 4-3 Full integration deployment for a small campus



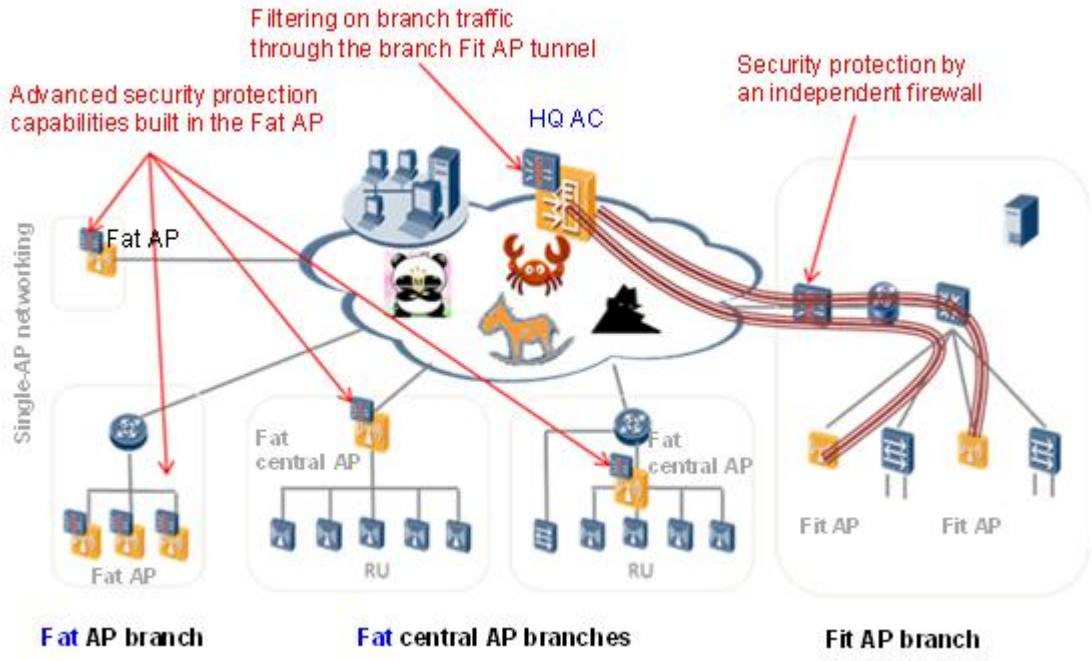
Based on wired ports and AP access capabilities of the AC, three zones can be constructed: intranet, extranet, and demilitarized zone (DMZ).

4.2 Branch Security Deployment

If a branch deploys an AC to manage local APs, the network topology can be considered as a small campus network, which is not described in this section.

This section discusses how to configure and deploy application-layer security features when no AC is not deployed in a branch. Branches can be classified into the branches having Fit APs, Fat APs, and Fat central APs.

Figure 4-4 Branch security deployment



4.2.1 Fit AP Deployment in a Branch

When Fit APs are deployed in a branch, they can be centrally managed by the HQ AC. Fit APs do not support application-layer security features and therefore cannot perform security detection or filtering on locally forwarded user traffic.

In this deployment scenario, the following SSIDs are configured on Fit APs to provide access services:

- SSID for STAs to access the HQ network

  Wireless user traffic is forwarded directly through the CAPWAP tunnel to the HQ AC. The firewall function built in the AC performs security check and filtering on the traffic.
- SSID for STAs to access the Internet through local branch egresses

  Wireless user traffic is directly forwarded in the branch. Fit APs cannot filter the traffic, so the branch needs to deploy an independent firewall at the branch egress. The firewall will filter incoming and outgoing traffic on the branch network.

4.2.2 Fat AP Deployment in a Branch

Certain small branch networks or even super-small branch offices (such as SOHO) can have Fat APs deployed to provide application-layer security protection capability.

4.2.3 Fat Central AP Deployment in a Branch

If a branch has multiple small office rooms or areas, Huawei agile distributed Wi-Fi network is recommended. The two-layer agile distributed Wi-Fi network architecture is suitable for SOHO, SMB, and multiple- branch networking scenarios.

On an agile distributed Wi-Fi network, central APs may work in Fat or Fit mode. To enable application-layer security features, users need to deploy Fat central APs.

When central APs work in Fat mode, the agile distributed Wi-Fi network architecture consists of only central APs and remote units (RUs).

- RU

  The functions of RUs are the same as those of the RUs when the central AP works as a Fit AP. For details, see the function descriptions of RUs when the central AP functions as a Fit AP.

- Central AP

  In addition to the functions of Fit central APs, a Fat central AP has the functions of the AC. A Fat central AP is equal to a Fit central AP + AC.

The two-layer agile distributed Wi-Fi network no longer depends on independent ACs. A Fat central AP functions as an AC and implements self-networking and self-management. The Fat central AP integrates the service gateway functions and provides users with related gateway functions. The Fat central AP also supports switch ports and provides PoE capability. In addition, the Fat central AP reserves the capability for abundant service evolution.

Therefore, branch networks constructed by Fat central APs may have two different network topologies. On one topology, a central AP serves as the branch egress. On the other topology, independent access routers (ARs) are deployed, and central APs serve as internal network devices. The topologies both support application-layer security check and filtering on wired and wireless STAs connected to Fat central APs.

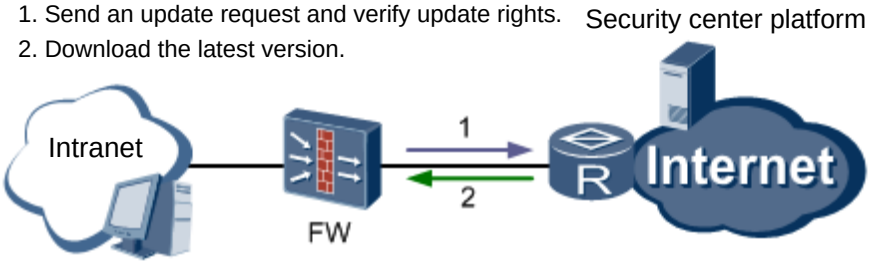
4.3 Signature Database Update Deployment

4.3.1 Direct Update

When an AC can directly communicate with the update center through the Internet, the signature database can be directly updated using the update center.

NOTE

In most cases, the update center is the security center platform. Only some enterprises build their own update centers due to special requirements.



A device sends an update request using HTTP and downloads the signature database using FTP. Therefore, you need to configure a security policy to permit HTTP and FTP protocol packets.

In this scenario, the signature database can be updated in the following modes:

- Scheduled update

  The AC connected to the update center periodically checks for the new signature database version. If a new version exists, the AC will automatically download it and update the local signature database at the preset time.

- Immediate update

  When a new signature database version is released but the scheduled update time does not approach or the AC is not enabled with scheduled update, you can update the signature database immediately.

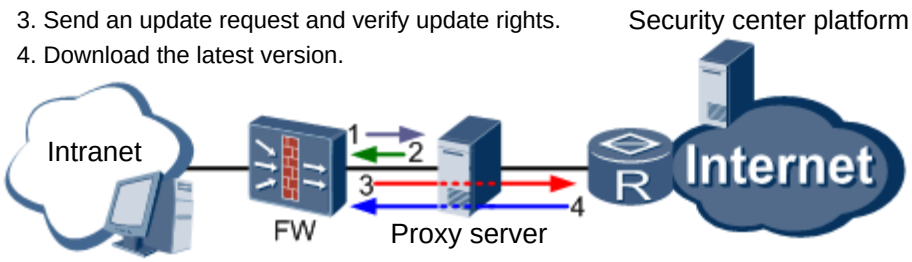
  In this update mode, the download address and update processes are the same as those in scheduled update mode. The only difference is that immediate update can be executed at any time.

4.3.2 Update Through a Proxy Server

When an AC cannot be directly connected to the update center through the Internet, deploy a proxy server between the AC and the update center to update the signature database.

NOTE

When the proxy server runs on the Windows operating system, the CCProxy software is recommended. When the proxy server runs on the Linux operating system, the Squid software is recommended. The proxy server must be enabled with HTTP ports as well as PUT, GET, CONNECT, and POST access modes.



The AC only supports HTTP proxy. Therefore, in an update through a proxy server, configure a security policy for permitting HTTP packets.

In this scenario, the signature database can be updated in the following modes:

- Scheduled update

  The AC connected to the update center periodically checks for the new signature database version. If a new version exists, the AC will automatically download it and update the local signature database at the preset time.

- Immediate update

  When a new signature database version is released but the scheduled update time does not approach or the AC is not enabled with scheduled update, you can update the signature database immediately.

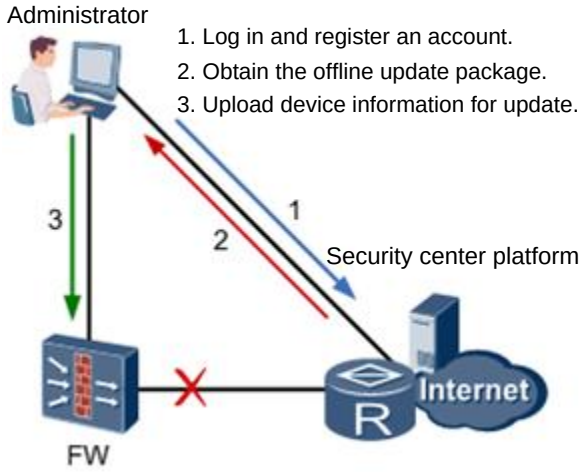
  In this update mode, the download address and update processes are the same as those in scheduled update mode. The only difference is that immediate update can be executed at any time.

4.3.3 Local Update

When an AC is physically isolated from the Internet and no proxy server is deployed on an intranet, use the local update mode.

NOTE

Currently, the regional identification signature database supports only local update. The latest regional identification signature database is released irregularly. You can download the upgrade file from Huawei's security center (sec.huawei.com). The signature database is referred to as REGION on the security center platform.



5 Appendix

5.1 Terms

5.1.1 Botnet

A Botnet is a network where a controller infects a large number of hosts with the bot program by means of one or more spreading methods. The controller and the infected hosts form a one-to-many control network.

1. Bot: is short for robot that can automatically execute predefined function and be controlled predefined commands. The bot is not necessarily malicious, but it is designed for malicious functions on a botnet.
2. Zombie: is a computer where malicious bots or other malicious remote control programs.
3. C&CS: is short for Command & Control Server. It is the IRC server connecting to IRC bots. The controller delivers commands to the C&CS for control.
4. Botnet: refers to a network composed of zombie computers where malicious bots are installed so that attackers can control the botnet. In recent years, driven by the huge economic benefits, botnets have been developing rapidly. The botnet architecture becomes more complicated, control methods are more diversified, and botnet attacks are difficult to find. These changes pose great challenges on Botnet detection and control technologies.

5.1.2 Trojan

Trojan is a malicious interception and control program that is secretly installed on computers by attackers. The Trojan program may provide some useful or interesting functions. However, Trojan also has many other functions of which users may be unaware, for example, Trojan can secretly copy files on a computer or intercept user passwords. Once implanted into a computer, Trojan not only intercepts important files and information on the computer but also listens on all user operations. Additionally, attackers can use Trojan to launch attacks to computers surrounding the Trojan-implanted computer.

5.1.3 Worm

Worm is a program that can run independently without manual intervention. Worms are spread by continuously taking part of or all control over computers with vulnerabilities on the network. The largest difference between worm and virus is that worms can autonomously replicate and spread without manual intervention.

5.1.4 Spyware

Spyware can install backdoors and collect user information on attacked computers without being found. Spyware can be leveraged by attackers to:

- Weaken users' control over their use experience, privacy, and system security.
- Use users' system resources, including programs installed on their computers.
- Collect, use, and disseminate users' personal or sensitive information.