2016

Confidentiality: INTERNAL

Product Whitepaper

Venusense Industrial Firewall (IFW-3000 Series)

Grow with users

Copyright Statement

Information Feedback

In case of any valuable suggestions, please contact us:

Mailbox: Venus Plaza, No. 21 Zhongguancun Software Park, No. 8 Dongbeiwang West Road, Haidian District, Beijing

Postal Code: 100193

Tel: (+86) 10 82779088

Fax: (+86) 1082779000

Please visitwww.venustech.com.cn to learn more about our new technologies and products.

Contents

1 Requirements and Challenges of Information Security in the Industrial Control System

The industrial network is a network based on the fieldbus technology that is evolved gradually from a distributed control system. Due to the lack of universal standards, many vendors propose their private fieldbus standards. This leads to the formation of "automation silos", which certainly does not meet the requirements of modern companies for data communication. Industrial Ethernet enables seamless integration of information from the onsite equipment layer to management layer, and provides an open infrastructure.

Industrial Ethernet features openness, low cost, and easy networking, and is able to improve the compatibility, interoperability, and information fluidity in industrial networks. However, due to the merge of management network and production network, the traditional network security threatsgradually migrate to the industrial control networks. Among them, the advance persistent threat (APTs), aiming at the industrial control systems, have caused a series of astonishing industrial network security events worldwide. This indicates that the network security threats have moved from the open Internet to the originally closed industrial control networks. According to statistics, more than 80% of key infrastructure related to people's livelihoodrelies on the industrial control system to achieve automatic operation. Therefore, China has regarded industrial control system security as a major part of the national security strategy.

1.1 Vulnerabilities Inherent in the Industrial Control System

The original industrial network is a closed network, and therefore its security is not considered as the most important factor in the initial design. In addition, due to the high reliability requirements of an industrial system, enterprises seldom or are difficult to updatetheir systems even though they find vulnerabilities in system components. Therefore, the inherent vulnerability is the biggest challenge of the existing industrial control system.

The PLC or RTU in a control system has severe vulnerabilities which can be directly exploited by hackers (such as the Stuxnet) to destroy the production network. Both overseas vendors like Siemens and Schneider and domestic manufacturers likeForcecon and WellinTechhave announced a large number of hardware vulnerabilities.

System platform software consists of the equipment OS, configuration software, and management system.

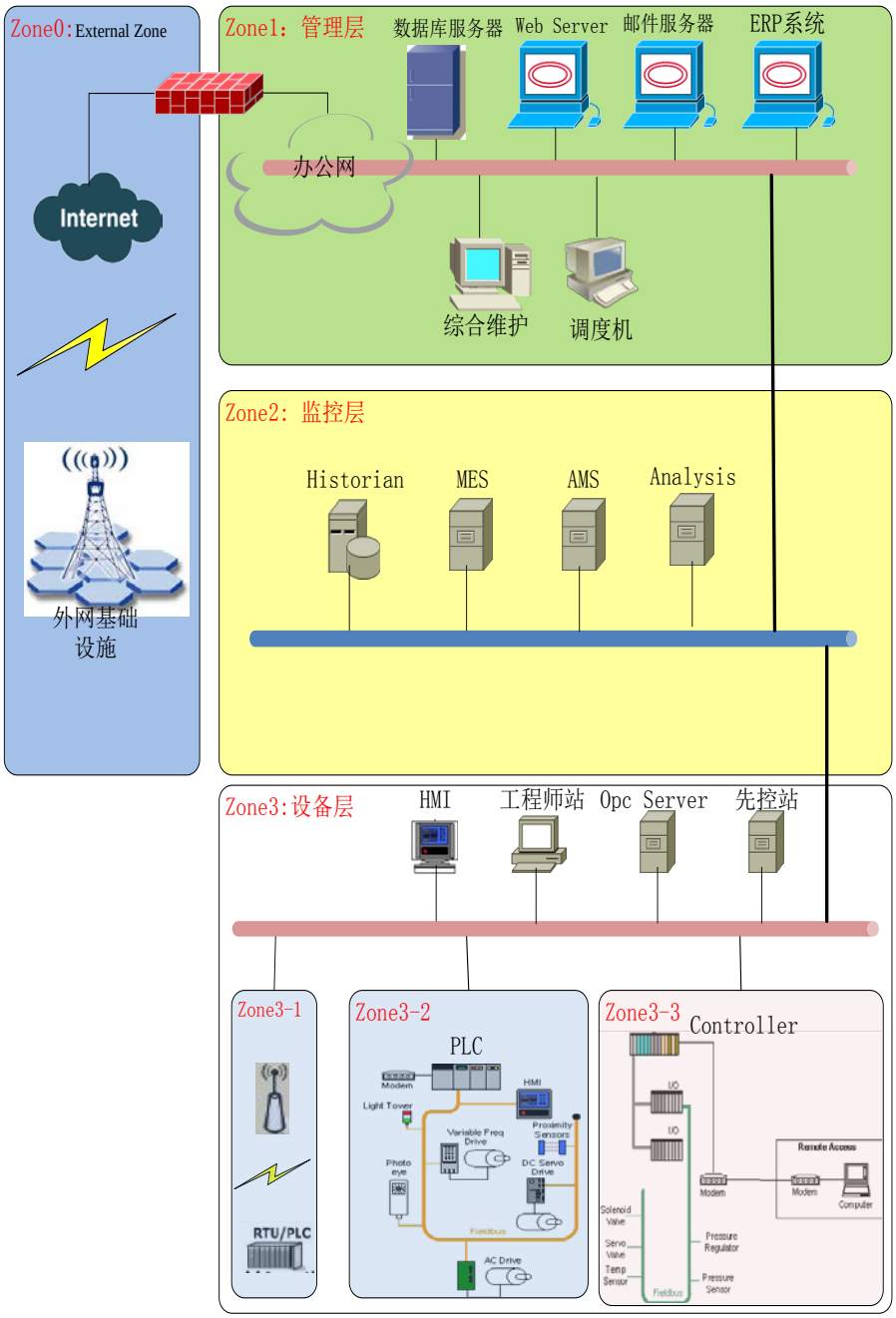
Currently, many engineering workstations, servers, HMIs, and embedded devicesare using the Windows XP as their operation system. After Microsoft stops providing security updates for Windows XP, the industrial control systems are exposing to larger security risks, and vulnerabilities occur on the embedded systems.

The configuration software and management system can directly control the production equipment. Therefore, their vulnerabilitiesmay cause direct threatsto devices in the industrial control networks.

1.2 Vulnerabilities Caused byInterconnection of Industrial Control Networks

Industrial Ethernet can help improve information intercommunication, but it also involves the OPC-based industrial data exchange and FTP-based DNC network directive transfer, which enable security threats in traditional networks to penetrate into industrial networks. However, the originally closed industrial networks do not have corresponding security protection measures, for example, encryption for data transmission, access control over data flows and control flows, user authentication mechanism, secure wireless connection, and security audit and monitoring. In addition, a large number of vendors and associations have published standards and details of industrial control protocols, such as Modbus, HSE, and Ethernet/IP, which enables attackers to further explore vulnerabilities and make full use of them.

Figure 1-1 Typical industrial control network



A typical industrial control network, as shown in Figure 1-1, consists of three layers: management layer, monitoring layer, and equipment layer.

- The management layer refers to the traditional office network. It includes the management information system with which managers can obtain the lower-layer production information and data. In this way, managers can learn about the operating status of manufacturing processes and changes in technological parameters, to better monitor and control the manufacturing processes.
- The monitoring layer is used to monitor and maintain the equipment layer.

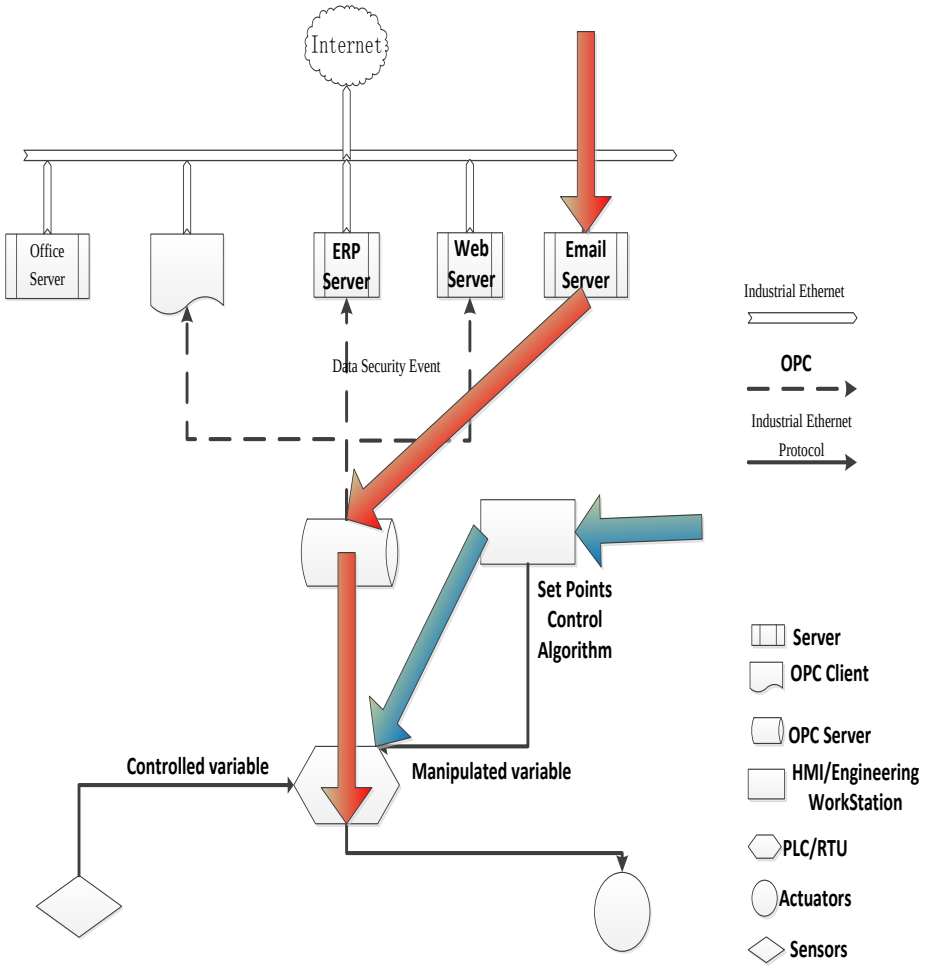
- The equipment layer is the core of manufacturing. Instructions are delivered through this layer to control onsite equipment and complete production tasks. Hardware on this layer includes the PLC, RTU, and controller as well as O&M equipment such as HMI and engineeringworkstation. The equipment layer performs the following functions:
  - ☐ Configures the PLC;
  - ☐ Displays configuration images;
  - ☐ Compiles PLC programs;
  - ☐ Changes tasks.

  These functions are implemented by software, including the upper configuration software and application software.

Production lines are directly exposed to attackers due to the lack of border protection in interconnected networks. Figure 1-2 shows the typical attack pathswith the red and blue arrows. Hackers make use of vulnerabilities to attack a serve or engineering workstation and then penetrate into the process control network using the compromisedserver or engineeringworkstation as the pivot point. The possible attack pathsare described as follows:

- Attacks the Historian to destroy the health and security records of the enterprise, modifies the status reports of factories, and initiates attacks on the next target by taking this as the pivot.
- Attacks the HMI to make factories work in blind, modifies control parameters to destroy devices, and initiates attacks on the next target by taking this as the pivot.
- Attacks the application server, tampers images that display onsite operations, blocks synchronization of onsite data, tampers databases, and initiates attacks on the next target by taking this as the pivot.
- Attacks the engineering workstation, deletes the predefined security logics, steals PLC codes, tampers PLC logics, and initiates attacks on the next target by taking this as the pivot.
- Attacks the PLC and writes any contents to destroy the PLC.

Figure 1-2 Typical attack routes in an industrial control network



The existing industrial networks are facing great risks and threats, and therefore comprehensive security policies are required. Border protection is the most critical part. Currently, most control networks seldom have or lack the isolation function between subsystems. If errorsoccur due to configuration, hardware faults, or viruses occur on some devices in a network, the problem will spread to the entire network in seconds. In this case, the professional firewalls that are applicable to the industrial environment that can be deployed to divide the network into secure zones and provideholisticprotection for borders, zones, and endpoints, thus effectively decreasing network attacks possibilities and holding the spread of threats.

2 Product Overview

2.1 Product Positioning

Venusense industrial firewall is a professional information protection product dedicated for industrial control systems. It applies to the supervisory control and data acquisition system (SCADA), distributed control system (DCS), PCS, and programmable logic controller (PLC). The firewall can be widely used in the industrial control systems that relate to people's livelihood, such as nuclear facilities, steel and iron, nonferrous metal, chemical industry, petroleum and petrochemical industry, electric power, natural gas, advanced manufacturing, water control projects, environmental protection, railway, urban mass transit, civil aviation, and urban supply of water, heat, and gas.

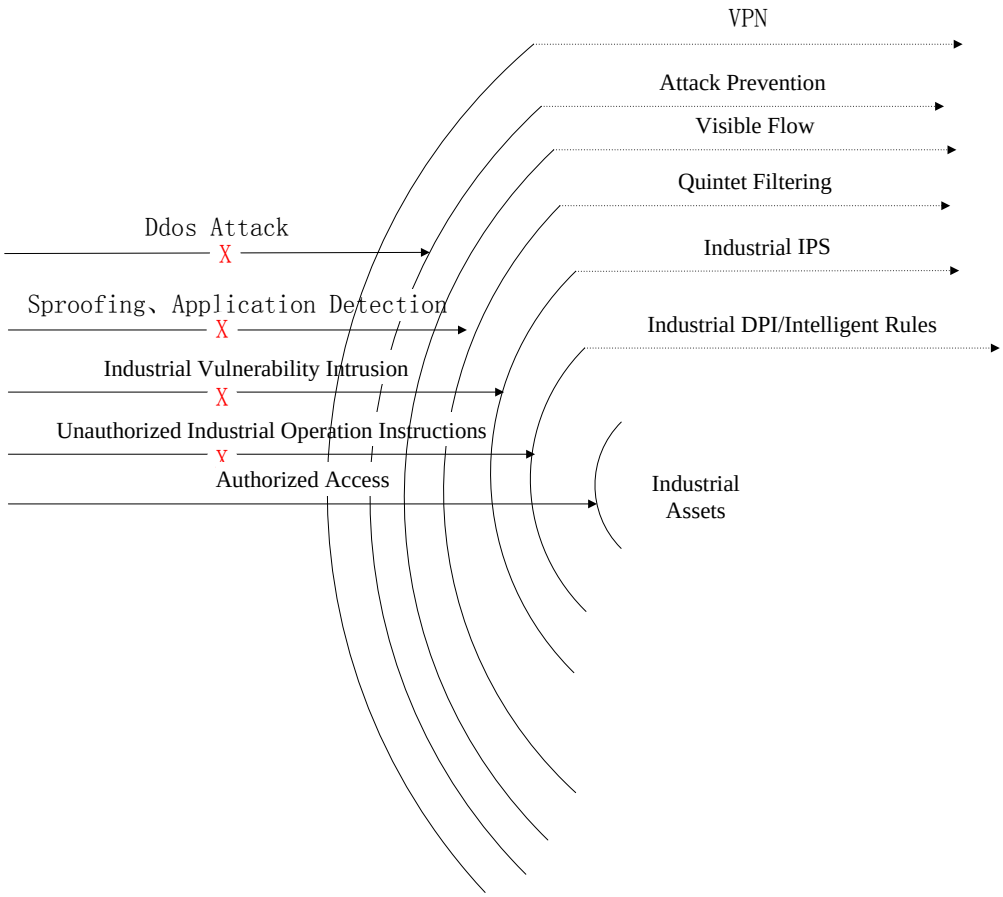
The firewall can be deployed in the border of each layer of an industrial network. The firewall can filter the collected data if being deployed in the border of the monitoring layer and can logically isolate different factories if being deployed in the border of the equipment layer.

The firewall can also protect key positions. For example, the firewall can be deployed before key engineering workstations or PLCs to perform logic isolation protection.

2.2 Protection Model

Figure 2-1 shows the protection model of Venusense industrial firewall.

Figure 2-1 Protection model



Venusense industrial firewall protects the security of target assets by using the multi-level protection mechanism, and supports such functions as attack prevention, stateful firewall, industrial intrusion prevention, and industrial protocol deep parsing and control.

2.3 ProductFunctions

Venusense industrial firewall has the following functions:

- Basic functions: integrated multi-tuple access control based on traditional 5-tuple, protocol, asset, and time; deployment in transparent, routing, and hybrid modes; multiple built-in industrial protection modules; customized protection rules
- Industrial DPI: deep parsingof multiple industrial protocols, including the OPC, Modbus/TCP, Modbus/RTU, Ethernet/IP, IEC104, EIP, S7, and DNP3; support for instruction-level access control
- Flowlearning: intelligent learning of network flow, to form a network relationship with assets as the communication subjects; instruction learning at the industrial protocol level, to precisely grasp the operation instructions delivered to the industrial control equipment; automatic recommendation of security policies based on learning results to administrators for easy O&M, to enable visible flow, and help administrators gain insights into industrial networks

- Intelligent rules: automatic generation of whitelist rules of security operation instructions for industrial controllers based on the learning results of instructions at the industrial protocol level
- Industrial IPS: predefined attack event database for improving the security protection capability; scalable rule engine based on natural language descriptions; customized packet analysis with outstanding and extensible security protection capability
- Predefined scenario-based rules: In actual application deployment, extracting scenario-based rules that are verified through real-world examinations for security demands of common industry characteristics and predefining such rules in the firewall system for administrators to choose on demand, thus simplifying user configurations.
- Industrial VPN: encryption of data transmission based on industrial protocols
- Centralized management: support for large-scale deployment of the industrial firewall, unified delivery of policies to the entire network, unified display of equipment status, and centralized display of logs and alarms
- Log audit: recording and sending of equipment management logs and system logs

2.4 Differences from Traditional Firewalls

Traditional firewalls cannot effectively protect industrial networks due to the following limitations:

- The industrial networks use various dedicated industrial protocols, such as protocols based on industrial Ethernet (layer 2 and layer 3) and protocols based on serial links (RS232 and RS485). However, the traditional firewalls cannot fully support the whitelist-based filtering of industrial protocols.
- Traditional firewalls cannot deeply parse or control the industrial protocols, and therefore are incapable of handling illegal instructions.
- Most firewalls are deployed by using theDin-railon the industrial site, which poses high requirements of environment compatibility, such as fanless and wide temperature range. Traditional firewalls can hardly meet the harsh environment requirements.

3 Product Features

3.1 Adaptability with Military Industry Qualities

Industrial manufacturingasks for high adaptability of the network security device, and some industrial sites are even unattended. Therefore, industrial firewalls must be able to adapt to the predictable environment and eliminate interference in extremely harsh environment.

Owning to the rich experience of Venustech in the military industry, IFW-3000 can better meet such requirements in the industrial environment as mechanical requirements (shock, vibration, and stretching), climate protection (operating temperature, storage temperature, humidity, and ultraviolet ray), intrusion protection (protection level and pollution level), electromagnetic radiation and immunization (transmission and immunization) and network- and equipment-level reliability.

- Climate protection: tolerable for extreme cold and hot condition; operating temperature from -40℃ to 70℃; storage temperaturefrom -40℃ to 85℃, and humidity of 5-95% without condensation
- Intrusion protection: fanless design with full metal shell;ingress protection rating of IP40, which can effective keep away from dirt (diameter>1mm) and fully adapt to the dust-blowing industrial environment
- High reliability: support for redundantpower supply and bypass function, preventing single point of failures

3.2 Support for Industrial Control Network Protocols

3.2.1 Access Control of Industrial Protocols

Industrial firewalls can perform access control for dedicated industrial protocols by using the whitelist or blacklist.

- The industrial firewall has hundreds of types of built-in industrial protocols, to protectthe security of whitelisted industrial protocols.

- The industrial firewall is built with common PLC protection models, to quickly protect the security of whitelisted controllers.
- The industrial firewall supports the customized protection of whitelisted industrial protocols based on the layer 2 protocol No. and layer 3 network port number..

3.2.2 In-Depth Filtering of Industrial Protocols

Besides the basic whitelist-based access control function, IFW-3000 also controls industrial protocols at the application layer to filter industrial directives. IFW-3000 supports the in-depth filtering based on Modbus/TCP, Modbus/RTU, and IEC104.

OPC Deep Parsing and Protection

The OPC Classic specifications are based on Microsoft Windows technology using the distribution component object model (DCOM) for exchange of data between software components in the industrial field. The OPC is an industrial dedicated standard and therefore cannot be protected via traditional firewalls.

Firstly, the TCP port used by the OPC is determined from time to time through server-client negotiation, which is totally different from that of the traditional IT protocol (using a fixed TCP port). Therefore, firewalls based on static port filtering cannot protect the OPC.

IFW-3000 can check, track, and protect each link created based on the OPC program, with only the dynamic port used for OPC data communication open and without changing any configurations on the OPC client and server. IFW-3000 supports the following functions:

- Uses the dynamic connection and tracing technologies to protect the OPC.
- Protects the security of OPC DA, HAD, and A&E.
- Tracks the dynamic port of OPC data links.
- Checks and blocks OPC requests that do not meet the DCE/RPC standards.

Secondly, the remote procedure call (RPC) mechanism of DCOM is somewhat vulnerable, and security vulnerabilities have been frequently found and reported in recent years, thus providing opportunities for virus and Trojan as well as hacker attacks. To this end, packets that are sent over the DCOM protocol must be deeply parsed, to help block the security threats targeting at DCOM vulnerabilities, such as viruses, Trojan, and malicious codes.

The in-depth packet parsing module of IFW-3000 supports the following functions:

- Filtering based on operation methods.
- Content filtering based on items.
- Content audit based on items.

Modbus/TCP Deep Parsing and Protection

Industrial protocols are not designed with inherent security mechanism. As a widely used industrial protocol, Modbus also has inherent vulnerabilities,

such as lack of authentication, authorization, and encryption. The abuse of function codes is a common problem on the Modbus networks.

The Modbus/TCP deep parsing module of IFW-3000 supports detailed control at the application layer:

- Access control over function codes
- Access control over device addresses
- Read and write control over coil range
- Read and write control over register range
- Access control over input addresses

In addition, IFW-3000 supports the following functions:

- Responding with the Reset command when **Block** is selected
- Responding with the exception code when **Block** is selected
- Whitelist and blacklist

The preceding functions ensure that exceptions do not occur when the security device is blocked.

IFW-3000 can also check the status and compliance, which can effectively detect and block the exceptionModbus packets in time.

Administrators can create a Modbus directive table for valid services by analyzing the services and production networks. Administrators can also use the Modbus deep parsing and protection module to create a whitelist to block unauthorized packets and intrusion packets, thereby improving the security protection capability of Modbus networks.

Modbus/RTU Deep Parsing and Protection

Although the industrial Ethernet is developing rapidly, many production lines still communicate based on serial links. IFW-3000 supports data communication based on RS232/440/485 links and supports the deep parsing and protection policy that references Modbus/RTU.

IFW-3000 allows configuration of serial communication parameters including the bit rate, data bit, parity check, stop bit, and flow control.

Modbus/RTU directives can be filtered and controlled after the communicationparameters are configured.

IEC104 Deep Parsing and Protection

The IEC 60870-5-104 CDT (hereinafter referred to as IEC104) is applicable to Ethernet data transmission between the master station and transformer station or between the master station and RTU. The IEC104 is a supporting standard of the IEC60870-5 serial standards and is widely used in power generation and rail transit industries.

IFW-3000 supports the detailed filtering and control for the IEC104 to allow the authorized directives to pass through:

- Access control over the APCI (S frame, I frame, and U frame)
- Access control over data that are proactively sent to the upper layer

- Access control over remote-regulated informosomeaddress and control values
- Access control over remotely-controlled informosome address and control values
- Access control over remote pulse directives

EIP Deep Parsing and Protection

The Ethernet Industry Protocol (EIP) is specifically used for networks of industrial automation applications. The protocol is widely used in fields such as tobacco, electric power, and automobile, supporting connection of a large number of devices in an open area.

The Venusense industrial firewall can deeply parse the EIP with control of read only or read and write, and controls access to instruction codes and services.

S7 Deep Parsing and Protection

The S7 protocol is specifically used for communication of Siemens S7 PLC series, which are widely used in such industrial control sectors as tobacco, aerospace, nuclear power, and automobile.

IFW-3000 supports the detailed parsing and deep filtering of the S7 protocol, and blocks unauthorized instructions or operations.

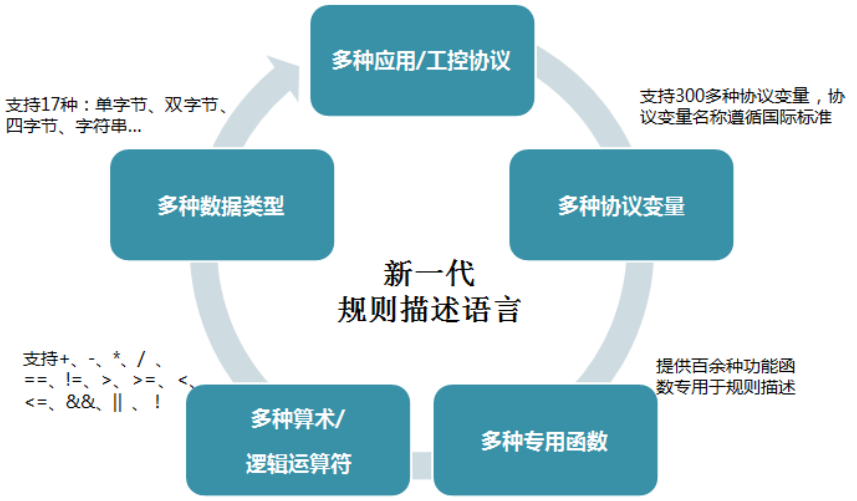
- Read/write protection
- Downloading/installation protection
- Prevention of PLC-based unauthorized parking
- Prevention of abnormal function start-stop
- Prevention of authorized access to CPU information

3.3 Industrial Intrusion Prevention

The Venusense industrial firewall integrates the professional intrusion prevention engine, which can protect proprietary protocols of industrial systems or protect the industrial systems from specific attacks. The event database is created based on the research findings of Venustech ADLab and features fast upgrade speed and more accurate data, making it best suit theintegration of IP application and industrialization.

The engine uses its proprietarynew-generation rule-defined languagestoprovide the flexible and powerful detection capabilities.This set of rule-definedlanguages can be used to parse than 60 protocols, including theTCP, UDP, HTTP, and DNS, and supports interpretation of more than 300 protocol variables whose names comply with international standards. This set of rule-defined languages provides more than 100 functions dedicated to rule description to simplify the definition of complex rule functions. In addition, it also supports 24 kinds of arithmetic operators, logical operators, and a variety of data types. This set of rule-defined languages can accurately express rich detection requirements similar to natural languages, reducing false positives as well as enhancing the detection of a variety of diverse, complex, and hidden attacks.

Figure 3-1 Intrusion prevention engine



With this powerful detection engine, users can detectnormal and abnormal network service behaviors which they concerned based on their dedicated network characteristics, to greatly extend the detection scope. Furthermore, users can ask experts to customize the intrusion prevention policies according to the actual environment.

3.4 Industrial VPN

The firewall integrates the professional VPN module developed by Venustech, and therefore supports the professional tunnel encryption and protection of industrial protocols. The VPN module has undergone market tests for a long time, which proves to be highly stable and easy to use with high adaptability and performance. The VPN module is able to protect the confidentiality, integrity, and availability of production and operation data of users.

3.5 Flow Self-Learning

In case the onsite engineers are not familiar with industrial control network protocols, flow self-learningcan be enabled in the industrial control environment before a prevention policy is added to the device.

The device first obtains the IP address, MAC address, and industrial protocol of the industrial control device through self-learning, automatically names the device to vividly sort and display the status of the industrial control network in terms of asset and protocol, and recommends security policies in a wizard guide style.

This significantly simplifies deployment procedures and reduces the impact of device onboarding on production. In addition, engineers who are not familiar with industrial control protocols can easily customize security policies that better meet actual service requirements.

3.6 Multiple Working Modes

The industrial network has the highest requirement for availability. The administrator must fully learn about the operating condition of the industrial network to effectively customize the security policy. IFW-3000 supports the following working modes:

- Passivemode: All packets are allowed to pass through, to ensure normal network communication.
- Debug mode: Packets to be blocked are not directly discarded. Instead, a log alarm is reported to notify the administrator of the blocked packets, so that the administrator can learn whether the policy effect meets expectations.
- Protection mode: After the security policy undergoes the testing mode, the administrator optimizes the security policy based on the evaluation results. In this case, IFW-3000 can switch to the protection mode to protect the industrial network.
- One-armmode: The preceding three modes are deployed serially. IFW-3000 works in bypass mode at the network debugging stage when the firewall is initially connected to the network, so as to demonstrate the security protection functions of the firewall to users without compromising network performance.

The preceding modes can gradually guide the administrator to develop the optimal security protection policy. All security modules of IFW-3000 can operate in the preceding working modes.

3.7 Centralized Management

The industrial network is deployed with various devices and runs many protocols. Most tasks are performed manually, such as unified configuration of devices, performance monitoring, and policy configuration and delivery, which consumes numerous manpower and resources. The inconsistent policy configuration commands for different types of devices may also lead to inconsistentpolicies in the network, which may cause potential security vulnerabilities.

In scenarios where industrial firewalls are deployed in a large scale, users can choose the centralized management system to develop a unified security policy. The centralized management system supports management of up to 50 industrial firewalls in a centralized way and has the following functions:

- Device status monitoring: monitors the availability of industrial firewalls. Indicators to be monitored include the port traffic and state, CPU usage, memory usage, and disk usage, which can reflect the health status of the device. The centralized management system savesthe monitoring data for users to query.
- Device log collection: collects and analyzes logs of industrial firewalls.
- Alarm: extracts device status monitoring information that users concern most, and reports an alarm or action prompt when an intrusion behavior is detected.
- Policy management: allows users to log in without client certificates, user name or password, and provides batch upgrade, batch backup and recovery, as well as batch policy delivery.

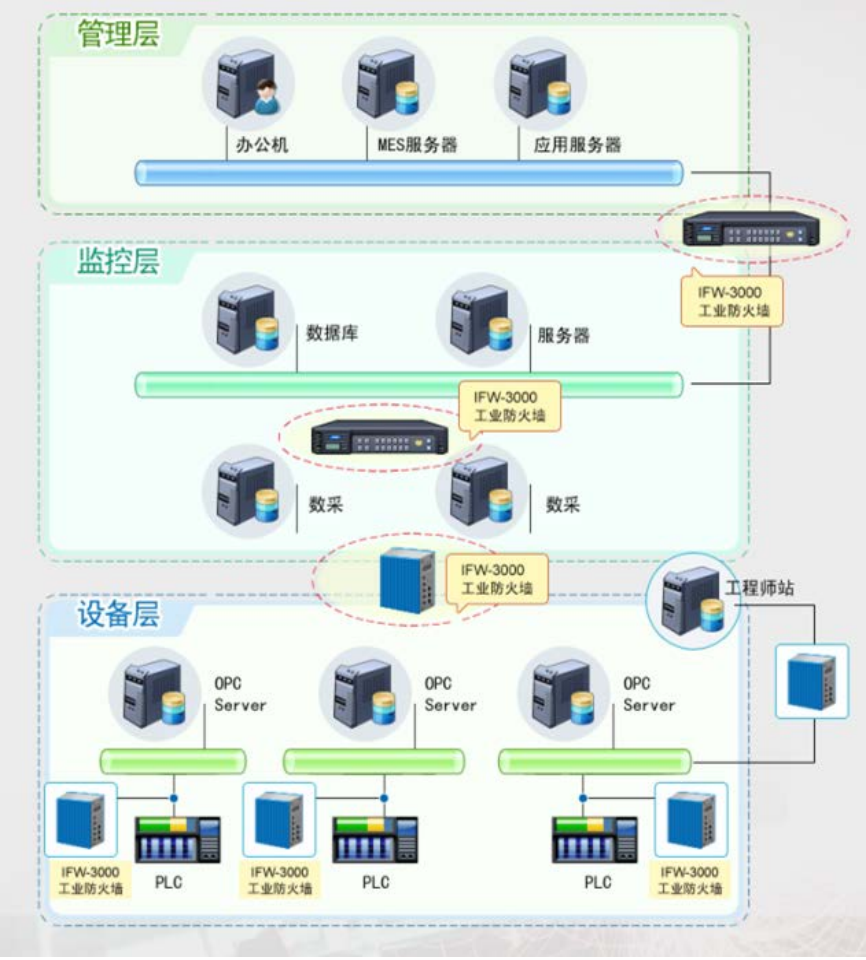
- Data maintenance: periodically exports data stored in the system, and supports data recovery in addition to data uploading and downloading through FTP.
- Device management: automatically fills in device information through the SNMP, and supports batch adding of devices.

4 Product Deployment and Values

4.1 Product Deployment

Figure 4-1 shows the firewall deployment, which facilitates the in-depth security protection of industrial networks.

Figure 4-1 Product deployment

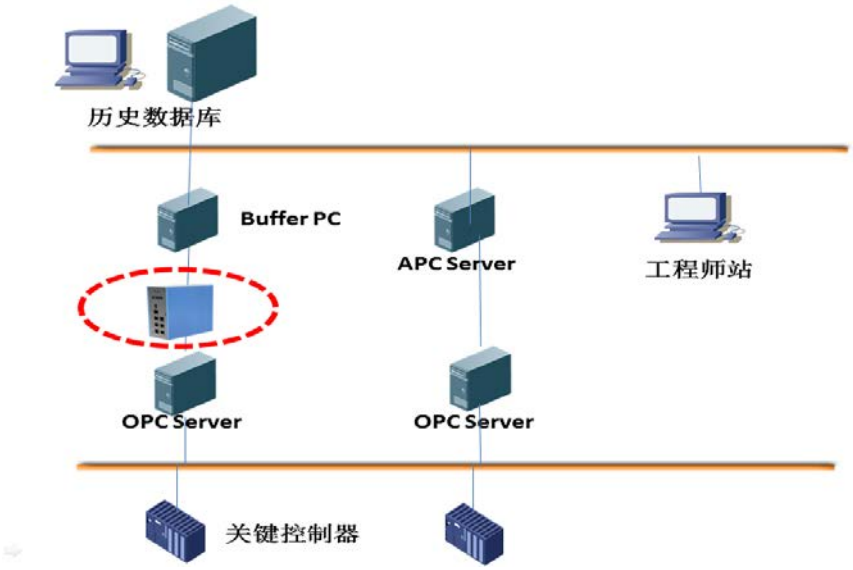


4.2 Application Scenarios

The industrial firewall applies to the following scenarios:

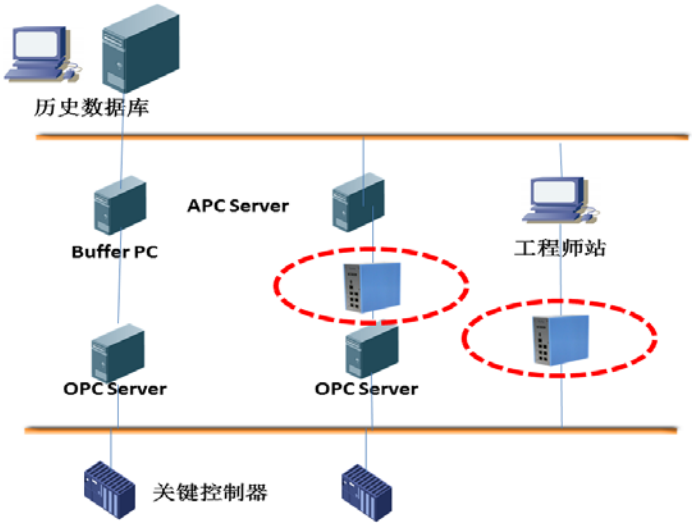
The industrial firewall can be used to isolate the data acquisition networkfrom thecontrol network, as shown in Figure 4-2.

Figure 4-2 Isolating the data acquisition network from the control network



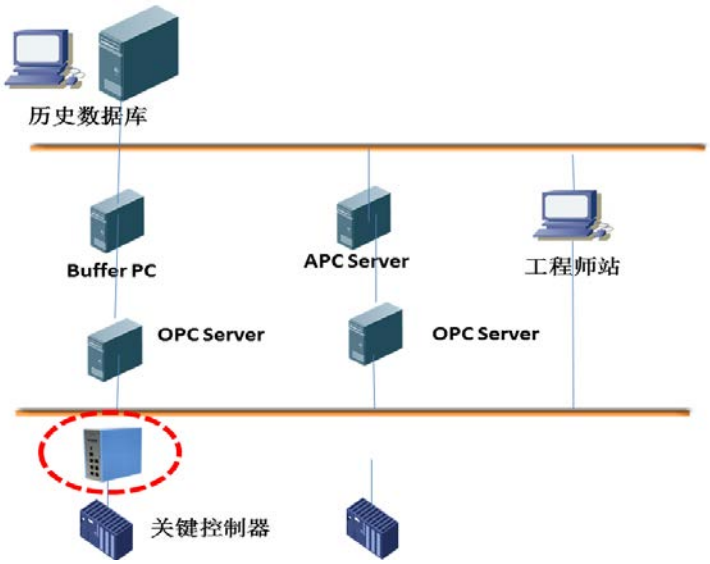
The industrial firewall can be used to isolate the APC server from the engineeringworkstation, as shown in Figure 4-3.

Figure 4-3 Isolating the APC server from the engineering workstation



The industrial firewall can be used to protect critical PLCs, as shown in Figure 4-4.

Figure 4-4 Protecting critical PLCs



5 Company Profile

Found in 1996 by Dr. Jane Yan, who received her PhD degree in the United States, Venustech Group Inc. (hereinafter referred to as Venustech) is China's most powerful vendor of network security products, trusted security management platforms, and security services and solutions with independent intellectual property rights. Headquartered in Venus Plaza, Zhongguancun Software Park, Venustech has over 30 branches and offices across China with the nationwide channel systems and technical support centers.

On June 23, 2010, Venustech was listed in Shenzhen Stock Exchange Small and Medium Enterprise Board, becoming China's first private information security company entering the capital market. In 2012, Venustech completed the acquisition of Beijing Leadsec Inc. In 2014, Venustech acquired Hangzhou UNIMAS Information Technology Co., Ltd. and Beijing Sursen Electronic Technology Co., Ltd., and planned to acquire 100% stocks of Beijing Anfanggaoke Electromagnetic Security Technology (Beijing) Co., Ltd. using cash and share issuing. In 2015, Beijing Venustech Inc. was officially renamed Venustech Group Co., Ltd. It holds share in over 30 companies, including Beijing Integrity Tech, T1 Networks, EverSec, and Shenzhen UNNOO.

Currently, Venustech has four wholly owned subsidiaries, named as, Venustech Security, Leadsec, Hangzhou Unimas, and Sursen, spanning areas of network security, data security, and application service security.

Venustech has a complete professional security product line covering technical fields including firewall/UTM, intrusion detection and management, network audit, endpoint management, and encryption and authentication. In addition, Venustech is an enterprise-level technology center certified by the country and a key software enterprise in the national program, with the highest-level qualification of computer information system integration involving national secrets.

Leadsec has many core technologies and has successively applied for nearly 50 invention patents. Its product portfolio includes the security gateway, GAP, VPN, and IPS across fields such as network security prevention, application security prevention, and security risk management. Leadsec has held a leading place in market share among national brands for five consecutive years.

Hangzhou Unimas is a well-known product supplier and system integration vendor dedicated in information security and big data. It is among the earliest Hangzhou enterprises that have obtained both software product and software enterprise certifications from Zhejiang Province Economic and Information Commission. Unimas takes the rejuvenation of national information industry

as its responsibility and endeavors to protect information security and promote information sharing. Currently, the company has become the most dynamic and representative leading enterprise in China's security exchange and data processing fields with utmost creativity.

Sursen has been dedicated to replacing the use of traditional paper with digital products through related technologies and services. Sursen is globally competitive as one of the few software companies in China that have mastered core IT industry technologies. The SEP digital paper technology of Sursen can create a technical platform providing the characteristics of traditional paper, thereby achieving comprehensive electronic paper application. In addition to SEP, Sursen has unique techniques in electronic stamp, information security, DRM, anti-counterfeit print, electronic form, data collection, and exchange.

Venustech has been blessed with the care and encouragement from the Party and country leaders all these years. In January 2000, top Chinese leaders Jiang Zemin, Li Lanqing, Zeng Qinghong visited Venustech. In January 2003, General Secretary Hu Jintao met with Dr. Jan Yan, CEO of Venustech.

2000年1月24日，江泽民、李岚清、曾庆红等党和国家领导人亲切视察启明星辰公司

2003年1月24日，胡锦涛总书记亲切接见启明星辰公司CEO严望佳博士

图片译文：

In January 2000, Chinese government leaders Jiang Zemin, Li Lanqing, Zeng Qinghong visited Venustech.

In January 2003, General Secretary Hu Jintao met with Dr. Jan Yan, CEO of Venustech.

As a leading enterprise in the information security industry, Venustech has developed a complete professional security product line to meet users’requirements. After continued hard work and dedication, Venustech has become the first choice for high-end enterprise customers in the government and industries of telecommunication, finance, energy, transportation, military, defense and manufacturing. Venustech enjoys an 80% share in the government and military market, and provides security products and services for 60% of Chinese enterprises that are among the Global500 Companies. In the financial area, Venustech has a 90% coverage in policy banks, state-owned commercial banks, and national joint-equity commercial banks. In the telecommunication area, Venustech provides security products, security services, and solutions for China Mobile, China Telecom, and Chine Unicom.

Venustech was the sole provider of core information security products, services, and solutions for the Beijing Organizing Committee of Olympic Games (BOCOG) and was the only information security supplier of the Olympic Sailing Committee. Venustech was solely authorized to be responsible for the security of the main network system of the Olympic Games, and was greatly honored by national authorities for that.

In April 2014, Venustech has established a special industrial control security team that coordinates between the front, middle, and back courts, effectively communicates with customers, and directly reacts to customer requirements. The team is made up of over 50 members working to meet industrial control security requirements and develop related products for customers in industries such as petroleum refinery, tobacco, military defense, advanced manufacturing, rail transportation, electric power, steel, fuel transfer, and coal.

Typical achievements of Venustech in industrial control security include:

- Obtains support for the industrial control firewall and vulnerability scanning systems from the National Development and Reform Commission.
- Provides technical support for two pilot security projects of the National Development and Reform Commission.
- Builds a secondary operation and maintenance system for a power grid dispatch system.
- Delivers industrial control security projects for industries such as tobacco, electric power, fuel transfer, steel, coal, and petrochemical.
- Participates in the compilation of industry security standards, including a railway industry level wireless security standard, a security design requirement for industrial control system level protection, and multiple TC124/TC260 industrial control security standards.
- Proactively involves in industrial control security activities.
- Establishes close partnership with industrial control vendors and integration vendors.

Since the founding of the special industrial control security team, Venustech has invested a large amount of money and manpower in the research and development of industrial control products. Venustech has created an industrial control information security product system with the industrial control information security management system at its core, supported by bypass detection, series protection, and onsite protection. The product system implements unified security monitoring and protection as well as security risk analysis and display for the industrial control devices on the entire network. Assisted by the industrial control security risk assessment platform that covers the full lifecycle of industrial control system demands, design, construction, operation, and abolition, this system can dynamically manage the information security risks. Figure 4-1 shows the product architecture.

Figure 5-1 Product architecture