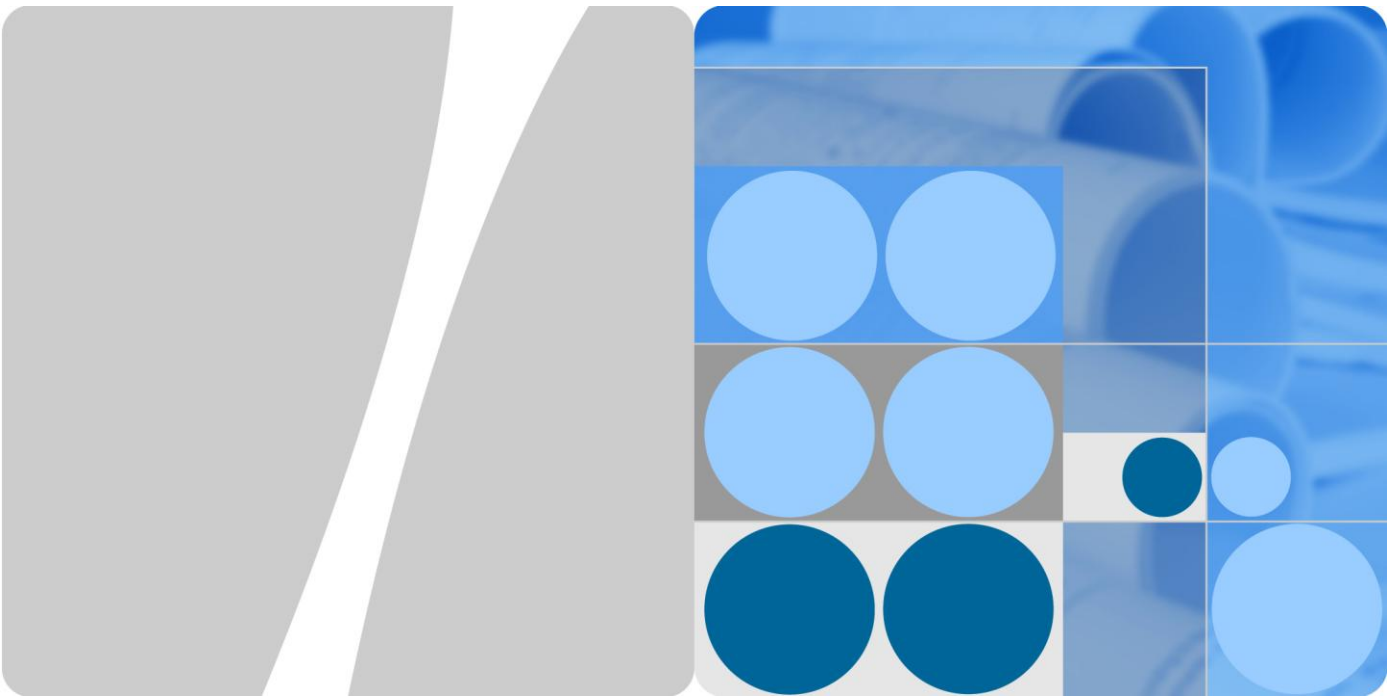


HUAWEI NIP2000/5000 Network Intelligent Protection System V100R002C00

Product Description

Issue	01
Date	2013-03-27

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://enterprise.huawei.com

About This Document

Related Version

The following table lists the product version related to this document.

Product Name	Version
HUAWEI NIP2000/5000 Network Intelligent Protection System	V100R002C00

Intended Audience

This document describes the product positioning and features, product architecture, functions, typical application scenarios, operation and maintenance methods, technical specifications, and ordering guidance of the HUAWEI NIP2000/5000 Network Intelligent Protection System (NIP for short).

It provides a quick reference about the product literature of the NIP.

This document is intended for:

- Network planning engineers
- Data configuration engineers
- Onsite maintenance engineers
- Network management administrators

Feature Conventions

The threat prevention feature may involve collecting users' communication contents. Huawei Technologies Co., Ltd. alone is unable to collect or save the content of users' communications. It is suggested that you activate the interception-related functions based on the applicable laws and regulations in terms of purpose and scope of usage. You are obligated to take considerable measures to ensure that the content of users' communications is fully protected when the content is being used and saved.

- The threat prevention feature may involve the collection of attack traffic contents. The product provides administrator permission control function to avoid the leaks of user's

communication content. You are advised to clear unnecessary sensitive logs in a timely manner.

Symbol Conventions

The symbols that may be found in this document are defined as follows.

Symbol	Description
 DANGER	Indicates a hazard with a high level or medium level of risk which, if not avoided, could result in death or serious injury.
 WARNING	Indicates a hazard with a low level of risk which, if not avoided, could result in minor or moderate injury.
 CAUTION	Indicates a potentially hazardous situation that, if not avoided, could result in equipment damage, data loss, performance deterioration, or unanticipated results.
TIP	Provides a tip that may help you solve a problem or save time.
NOTE	Provides additional information to emphasize or supplement important points in the main text.

Update History

Updates between document issues are cumulative. Therefore, the latest document issue contains all updates made in previous issues.

Updates in Issue 01 (2013-03-27)

Initial commercial release.

Contents

About This Document ii

1 Product Positioning and Features 1

1.1 Product Positioning 1

1.2 Product Features 2

1.2.1 Timely Signature Release Against the Latest Threats, Delivering Zero-Day Defense 3

1.2.2 Extremely Low False Negatives, Ensuring Service Continuity 3

1.2.3 Plug-and-Play, Easy to Deploy 3

1.2.4 Separate Structure, Ensuring Flexibility and Performance 4

1.2.5 Professional Anti-Virus Function to Protect Networks from Virus Infection 4

1.2.6 Superb Defense Against Application-Layer DDoS Attacks, Protecting Legitimate Services 4

1.2.7 Industry-Leading Application Recognition, Providing Control over Applications 5

2 Product Architecture 6

2.1 System Components 6

2.2 NIP Hardware Structure 8

2.2.1 Appearance of the NIP2000 Series 8

2.2.2 Appearance of the NIP5000 Series 11

2.2.3 Fixed Interfaces and Expansion Interface Cards 16

2.3 Software Structure 19

2.4 Configuration Requirements of the NIP Manager 20

3 Product Functions 23

3.1 Function List 24

3.2 Virtual Patch 32

3.3 Client Protection 33

3.4 Web Applications Protection 34

3.5 Malware Prevention 34

3.6 Anti-Virus 34

3.7 Application Identification and Control 35

3.8 Abnormal Traffic Prevention 36

3.9 Logs and Reports 38

3.10 High Availability 39

4 Application Scenario 41

4.1 At Enterprise Internet Edge (IPS Device) 41
4.2 At the Edge of a Server Farm (IPS Device)....44
4.3 Next to the Switch of the Intranet (IDS Devices or Off-line Deployed IPS Devices)....46
4.4 At the Network Edge (IPS Device)....48
5 Operation and Maintenance 49
5.1 Configuration and Management....49
5.2 System Maintenance....50
5.3 Security....50
6 Technical Specifications....52
6.1 System Specifications....52
6.2 Environment Requirements....56
6.3 Compliant Standards and Protocols....57
7 Ordering Guide 61
7.1 Chassis Ordering....61
7.2 Interface Module Ordering....62

1 Product Positioning and Features

About This Chapter

This chapter describes the positioning and features of the NIP.

1.1 Product Positioning

1.2 Product Features

NIP is a network intelligent detection and protection system built on the full understanding of the customer demands in the marketplace. It leverages the mature system design and is capable of preventing the latest threats with extremely low false negatives and is easy to deploy.

1.1 Product Positioning

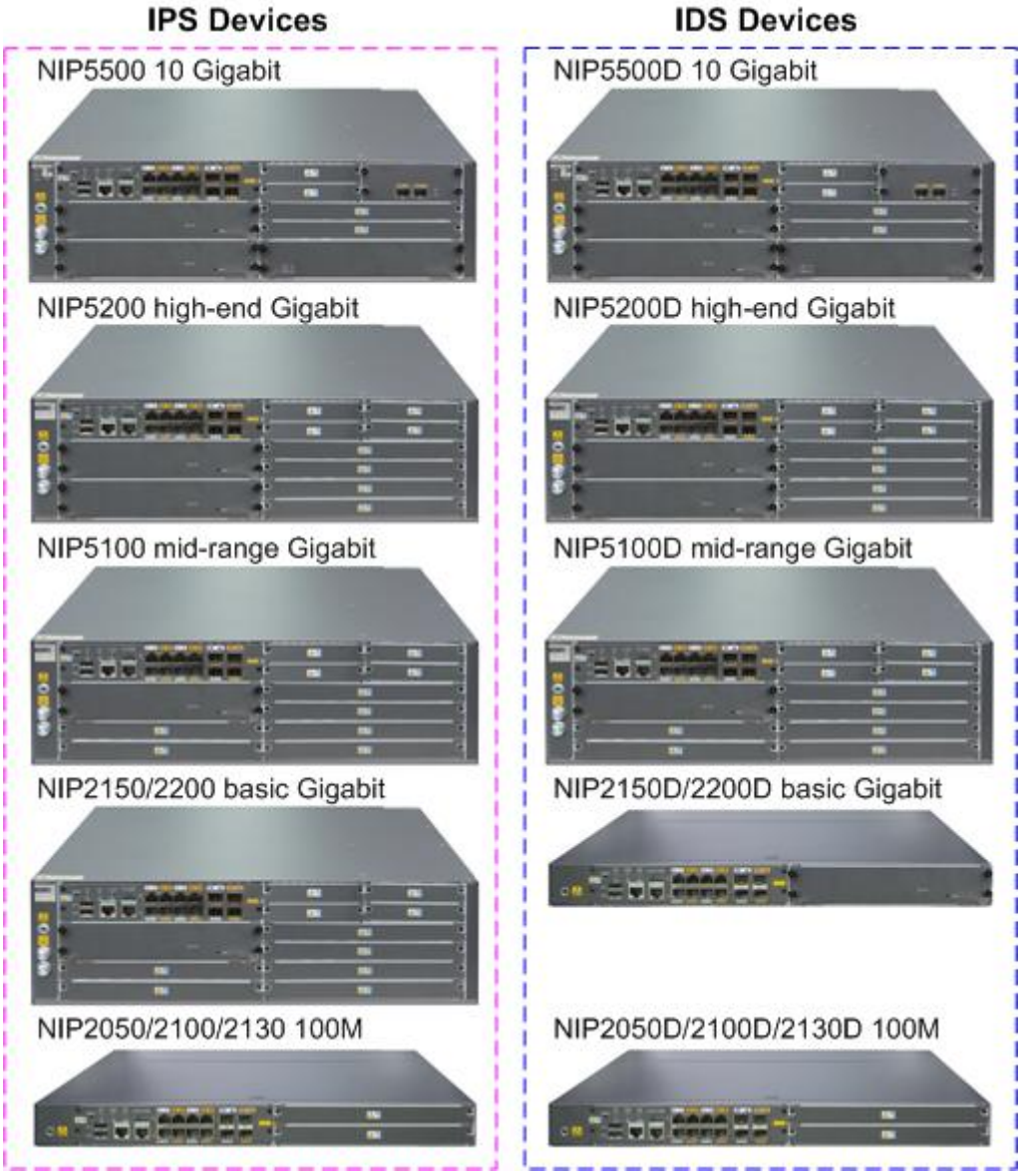
NIP is a new generation of network intelligent protection system (NIP for short) developed by Huawei Technologies Co., Ltd. (Huawei for short). NIP products fall into Intrusion Prevention System (IPS) and Intrusion Detection System (IDS) devices, which are designed to provide traffic and application security for enterprise networks, Internet Data Centers (IDCs), and campus networks.

With the rapid development of the Internet, the importance of the Internet is growing, and so are the attacks and threats it faces. This drives the emergence of the Intrusion Detection System (IDS) devices, which can detect, and analyze exploits and threats. The IDS evolves to the IPS to proactively and promptly detect the exploits and threats. IDS and IPS are two typical threat management products and an integral part of security solution.

The sophisticated NIP IDS and IPS devices are built on many years of experience of Huawei in networking and security. They can control network access, identify and control undesired applications, prevent threats that taking advantage of application vulnerabilities, file virus scanning and removal and defend against Denial of Service (DoS) and Distributed Denial of Service (DDoS) attacks.

NIP comes in NIP2000 and NIP5000 series. Figure 1-1 shows the appearance of different product models and types.

Figure 1-1 Appearance of the NIP



1.2 Product Features

NIP is a network intelligent detection and protection system built on the full understanding of the customer demands in the marketplace. It leverages the mature system design and is capable of preventing the latest threats with extremely low false negatives and is easy to deploy.

1.2.1 Timely Signature Release Against the Latest Threats, Delivering Zero-Day Defense

To identify the emerging exploits and threats, Huawei will immediately release the signatures upon the discovery of new vulnerabilities to prevent known and unknown exploits targeting the vulnerabilities and deliver zero-day defense.

The professional security team of Huawei closely traces the security bulletins of the renowned security organizations and software vendors, analyzes and verifies the threats to generate a signature database that protects software systems including operating systems, application programs, and databases. The signature database meets the compatibility requirements of International authority Common Vulnerabilities and Exposures (CVE). Additionally, the worldwide honey pot networks can capture the latest attacks, worms, and Trojan horses in real time, facilitating the generation of signatures and the discovery of threat trends. By using the techniques, Huawei can release the latest signatures in the shortest time and promptly update the detecting engine and signature database to deliver zero-day defense.

Common Vulnerabilities and Exposures (CVE®) is a list/dictionary of common names (i.e., CVE Identifiers) for publicly known information security vulnerabilities.

CVE is now the industry standard for vulnerability and exposure names. CVE Identifiers provide reference points for data exchange so that information security products and services can speak with each other. CVE Identifiers also provides a baseline for evaluating the coverage of tools and services so that users can determine which tools are most effective and appropriate for their organization's needs. In short, products and services compatible with CVE provide better coverage, easier interoperability, and enhanced security.

1.2.2 Extremely Low False Negatives, Ensuring Service Continuity

False positive rate is an important metric of the accuracy of signatures and the quality of the signature database. False positives compromise legitimate services and bury valuable information in the false information, making it harder to isolate real attacks.

A false positive occurs when the IPS regards legitimate traffic as attack traffic or mistakenly regards one type of attack as another. False positives are usually caused by inaccurate signatures or detecting mechanisms.

Huawei has a host of security professionals and data sources to analyze more samples, create signatures, and perform false negative tests to achieve near-zero false negative rate. Due to the extremely low false negative rate, a large percentage of the signatures of the NIP are enabled by default to maximize protection with compromising legitimate services. The administrators do not need to check a bunch of logs for false negatives or to determine whether some signatures should be disabled.

1.2.3 Plug-and-Play, Easy to Deploy

The service interfaces of the NIP operate at Layer 2 and can be transparently connected without changing the existing network topology. The NIP is configured with pre-defined default threat prevention policies to provide plug-and-play protection.

With the growth of networks and increase of network devices, ease of deployment and configuration is most needed among administrators.

Therefore, the fixed interfaces on the NIP and expansion interface cards are grouped into pairs. Each interface pair has an incoming and an outgoing interface. When the NIP is deployed in-line as an IPS, one interface of a pair is connected to the upstream device and the other to

the downstream device. When the NIP is deployed one-armed as an IPS or off-line as an IDS, only one of an interface pair is connected off-line at the edge of the network to be protected.

During IPS deployment, a common practice is to set the action to alert and test the IPS for a period, and then set the action to block if no noticeable false positives are observed. This practice is complex and reduces deployment efficiency.

NIP is a plug-and-play design. All policies and signatures are applied upon the startup of the device and no tuning is required. Of course, you can create security policies on the Web interface using the policy templates in a few minutes to accommodate your special situations.

Each NIP is shipped with the latest possible knowledge base and can start to work upon deployment without waiting for online update.

1.2.4 Separate Structure, Ensuring Flexibility and Performance

The packet forwarding and inspection functions of the NIP are separated to ensure both performance and flexibility.

ASIC-based devices are efficient in packet forwarding but weak in packet detecting; Intel architecture (IA, or x86)-based devices are efficient in packet detecting, but slow in packet forwarding. IPS devices must be efficient in both packet forwarding and inspecting. Therefore, both ASIC-based and x86-based devices have performance bottleneck, either in packet detecting or in packet forwarding.

The NIP uses multi-core network process unit (NPU) and multithreading design to deliver superior packet forwarding and the x86-based ESP to deliver efficient packet detecting. The separate architecture provides both flexibility and performance, ensuring stable performances of the NIP in complex network environments.

1.2.5 Professional Anti-Virus Function to Protect Networks from Virus Infection

The NIP rapidly and precisely scans and removes viruses to enhance the network anti-virus capacity without sacrificing network performance.

The Internet facilitates information sharing and communication, and increases productivity of enterprises. However, the Internet access also brings threats, such as viruses.

The NIP provides 99% detection ratio using the AV engine that has file-level scanning capability, world-leading emulation environment, and virtual execution technology. It supports virus scanning by protocol, such as HTTP, SMTP, POP3, and FTP. Besides, the dedicated virus analysis team traces latest viruses to facilitate virus database update.

NOTE

The IPS device in off-line mode and the IDS device do not provide the anti-virus function.

1.2.6 Superb Defense Against Application-Layer DDoS Attacks, Protecting Legitimate Services

The NIP can prevent DDoS attacks in network, transport, and application layers to protect legitimate traffic and services.

In the past, SYN flood is the typical flood attack. Nowadays, UDP and ICMP floods are the most common flood attacks. Application-layer DDoS attacks are also major DDoS attacks, and the most common application-layer DDoS attacks are those targeting Web and DNS servers. These attacks, particularly DNS flood attacks, have wider impact than other ones.

NIP can learn the traffic model and implement multiple layers of inspecting and cleaning to prevent application-layer DDoS attacks, such as DNS flood, HTTP flood, and HTTPS flood.

NOTE

IDS devices and IPS devices that are deployed off-line can detect and log attack events, but do not clean the traffic.

1.2.7 Industry-Leading Application Recognition, Providing Control over Applications

The NIP uses Service Awareness technology to analyze the traffic of different applications and the traffic directions. The Service Awareness technology can provide visibility into traffic, protocols, services, and their distribution so that administrators can make informed decisions in network planning and the creation of flow control policies.

The NIP uses the Service Awareness technology to perform inspection, recognize application-layer protocols, and control the traffic of specific types. The application control rule base contains a wide range of protocol features. The NIP analyzes packets and compares the features against the application control rule base to identify traffic of applications such as games, stock transaction, P2P, IM, and VoIP and implement control policies accordingly.

NOTE

IDS devices and IPS devices that are deployed off-line cannot control application traffic, but can provide visibility into applications through the analysis and report functions.

2 Product Architecture

About This Chapter

This chapter describes the components of the NIP system, the software and hardware structures, and the NIP Manager configuration requirements.

2.1 System Components

The Network Intelligent Protection (NIP) system consists of the NIP and the NIP Manager centralized management environment.

2.2 NIP Hardware Structure

The NIP consists of an integrated chassis with fan and power supply modules, and expansion slots for interface cards.

2.3 Software Structure

The software system is composed of modules that perform specific functions and collaborate with each other.

2.4 Configuration Requirements of the NIP Manager

This section describes the hardware and software requirements of the NIP Manager.

2.1 System Components

The Network Intelligent Protection (NIP) system consists of the NIP and the NIP Manager centralized management environment.

Figure 2-1 shows the components of the NIP system. Table 2-1 provides the description for each component.

Figure 2-1 System components

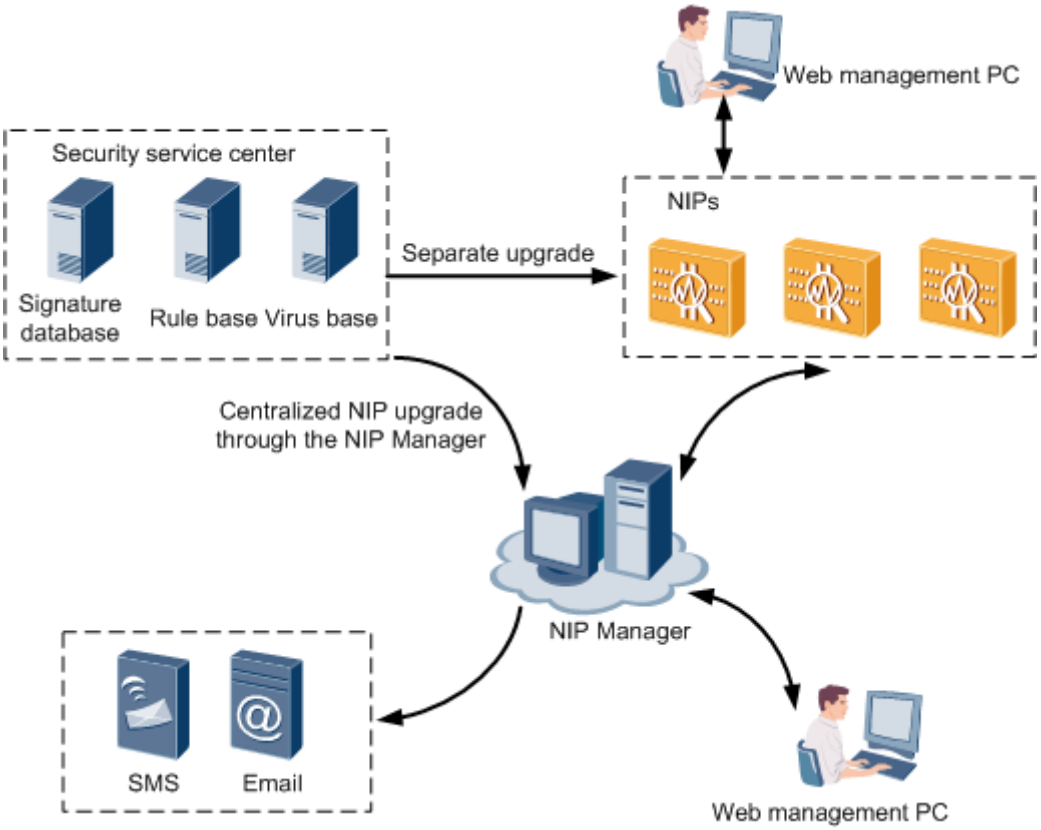


Table 2-1 System component description

Item	Description
NIP device	The NIP series falls into IPS devices (NIP2050/2100/2130/2150/2200/5100/5200/5500) and IDS devices (NIP2050D/2100D/2130D/2150D/2200D/5100D/5200D/5500D). The two differs from each other in deployment location and functions. The IPS device is usually deployed in in-line mode on the existing network to block the connections with attacks. On the contrary, the IDS device is deployed in off-line mode to record and analyze the attack events for subsequent network assessment and auditing. The IPS device can be deployed in off-line mode as well, and supports mixed deployment in in-line and off-line modes. In this case, an IPS device can function as the IPS device and IDS device at the same time. The NIP has a embedded Web system, through which the administrator can perform separate management on the NIP.
NIP Manager	Serving as the management software for the NIP, the NIP Manager provides centralized management for multiple NIPs, such as monitoring their running status, managing the alarms generated by them, configuring services, and checking logs and reports.
Security service center	The security service center provides the latest threat prevention signature database, application control rule base, and virus database.

Item	Description
	Timely updates of the threat prevention signature database and application control rule base ensure the device to obtain the latest attack defense capabilities. You can use the built-in Web-based management system of the NIP to update the threat prevention signature database, application control rule base, and virus database on a single device, or perform the centralized update of the two databases through the NIP Manager.
Alarm notification	The NIP performs remote alarm notification in following modes: • Email The NIP Manager can notify the maintenance personnel of the alarm by sending emails. After the notification email arrives at the specified email address, the maintenance personnel can learn about the alarm information received by the NIP Manager. • SMS The NIP Manager can notify the maintenance personnel of the alarm by sending short messages. Upon receiving the short message sent through the SMS provided by the ISP or the SMS modem connected to the NIP Manager, the maintenance personnel can learn about the alarm information received by the NIP Manager.
Web management PC	The built-in Web-based management system of the NIP and the NIP Manager provide user-friendly configuration and management interface on the Web. Using the user interface, you can perform individual and centralized configuration and management for the NIP.

2.2 NIP Hardware Structure

The NIP consists of an integrated chassis with fan and power supply modules, and expansion slots for interface cards.

2.2.1 Appearance of the NIP2000 Series

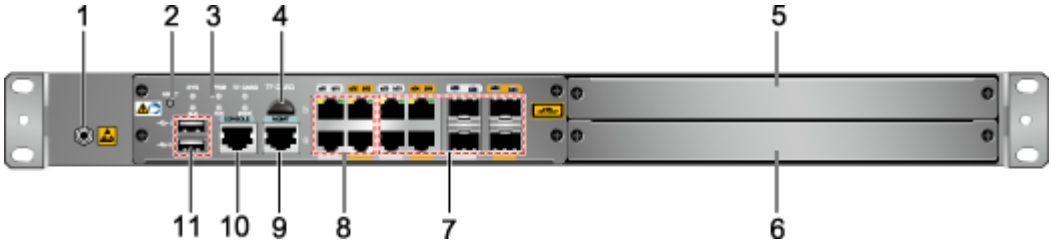
NIP2000 series consist of NIP2050/2100/2130/2150/2200 and NIP2050D/2100D/2130D/2150D/2200D. NIP2050/2050D/2100/2100D/2130/2130D and NIP2150D/2200D are 1U products and NIP2150/2200 is a 3U product. The ports, LEDs, and expansion slots are located on the front panel of the NIP, and the power receptacles and switches are located on the rear panel.

NIP2050/2050D/2100/2100D/2130/2130D

The NIP2050/2050D/2100/2100D/2130/2130D consist of the integrated chassis and expansion interface cards. The dimensions (H x W x D) of such chassis are 43.6 mm x 442 mm x 560 mm. The chassis can be installed in a 19-inch standard cabinet.

Figure 2-2 shows the front panel of the NIP2050/2050D/2100/2100D/2130/2130D.

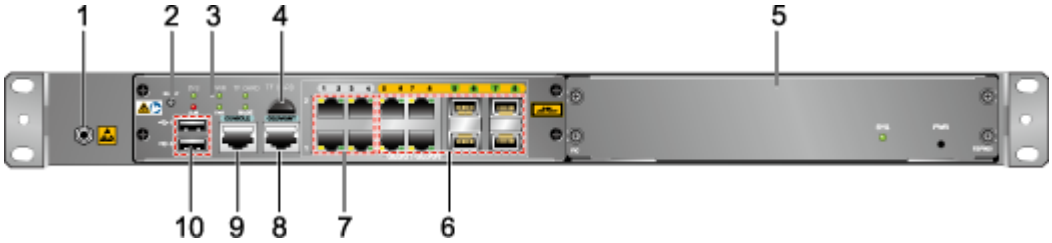
Figure 2-2 Front panel of the NIP2050/2050D/2100/2100D/2130/2130D



1. ESD wrist strap socket	2. System reset button	3. Indicator area
4. microSD card slot	5. FIC2	6. FIC1
7. Optical or electrical (mutually exclusive) interfaces	8. 10/100/1000M adaptive electrical Ethernet interface	9. Management interface
10. Console port	11. USB 2.0 interface	

Figure 2-3 shows the front panel of the NIP2150D/2200D.

Figure 2-3 Front panel of the NIP2150D/2200D



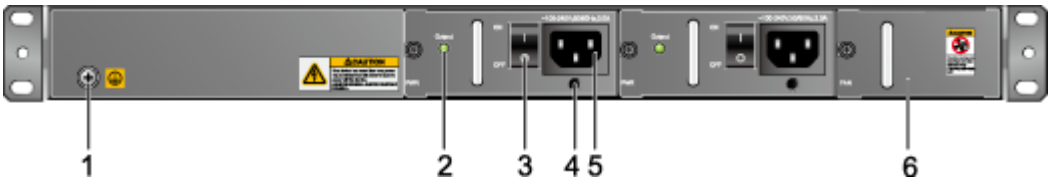
1. ESD wrist strap socket	2. System reset button	3. Indicator area
4. microSD card slot	5. ESP800 card	6. Optical or electrical (mutually exclusive) interfaces
7. 10/100/1000M adaptive electrical Ethernet interface	8. Management interface	9. Console port
10. USB 2.0 interface		

NOTE

- The microSD card slot of the NIP2050/2050D/2100/2100D/2130/2130D/2150D/2200D do not support microSD cards and is reserved for expansion.
- The FIC1 and FIC2 slots of the NIP2050D/2100D/2130D do not support FIC interface cards and are reserved for expansion.
- The NIP2150D/2200D have an ESP800 card in standard configuration. The ESP800 card is used to accelerate service processing and the card is installed on the NIP before shipment.

Figure 2-4 shows the rear panel of the NIP2050/2050D/2100/2100D/2130/2130D/2150D/2200D.

Figure 2-4 Rear panel of the NIP2050/2050D/2100/2100D/2130/2130D/2150D/2200D



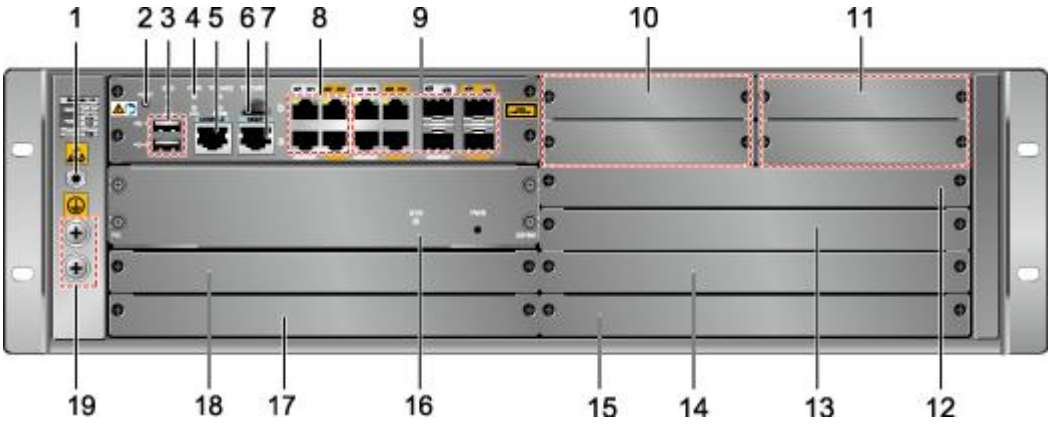
1. Grounding terminal	2. Power indicator	3. Power switch
4. AC power cable clip jack	5. Power socket	6. Fan frame

NIP2150/2200

The NIP2150/2200 consist of an integrated chassis and expansion slots. The dimensions (H x W x D) of the chassis are 130.5 mm x 442 mm x 414.1 mm, and the chassis can be installed in a 19-inch standard cabinet.

Figure 2-5 shows the front panel of the NIP2150/2200.

Figure 2-5 Front panel of the NIP2150/2200



1. ESD wrist strap socket	2. System reset button	3. USB 2.0 interface
4. Indicator area	5. Console port	6. microSD card slot
7. Management interface	8. 10/100/1000M adaptive electrical Ethernet interface	9. Optical or electrical (mutually exclusive) interfaces
10. Filler panel (inapplicable to interface cards)	11. Filler panel (inapplicable to interface cards)	12. FIC9
13. FIC7	14. Filler panel (inapplicable to interface cards)	15. FIC5
16. ESP card	17. Filler panel (inapplicable to interface cards)	18. Filler panel (inapplicable to interface cards)
19. Grounding terminal		

NOTE

- The microSD card slot of the NIP2150/2200 do not support microSD cards and is reserved for expansion.
- The NIP2150/2200 have two hardware versions that use one ESP710 card and one ESP800 card respectively for service accelerating. The devices of the two versions have identical performance and functions.

Figure 2-6 shows the rear panel of the NIP2150/2200.

Figure 2-6 Rear panel of the NIP2150/2200

1. Air filter
2. Power switch
3. AC power cable jack
4. Power socket
5. Fan filter
6. Power indicator
7. ESD wrist strap socket
8. Fan frame

2.2.2 Appearance of the NIP5000 Series

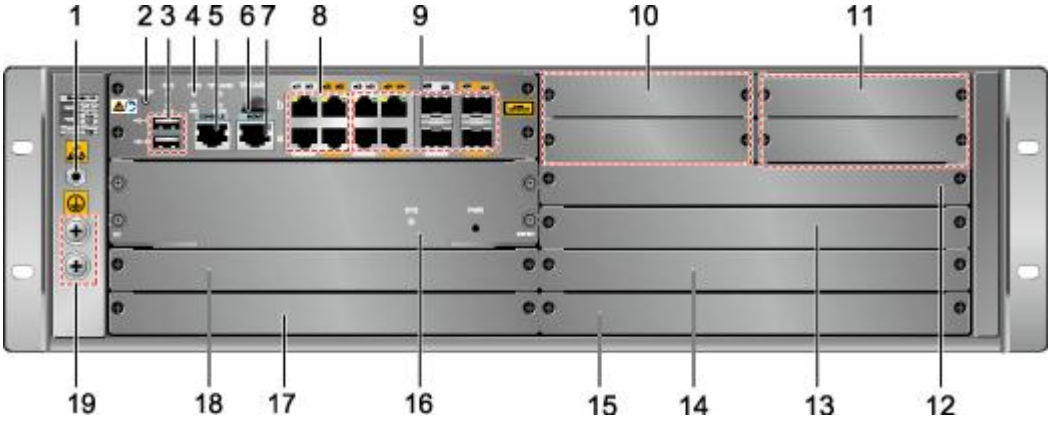
The NIP5000 series consists of NIP5100/5100D, NIP5200/5200D, and NIP5500/5500D, which are all 3U models.The ports, LEDs, and expansion slots are located on the front panel of the NIP, and the power receptacles and switches are located on the rear panel.

NIP5100/5100D

The NIP5100/5100D consists of the integrated chassis and expansion interface cards. The dimensions (H x W x D) of such chassis are 130.5 mm x 442 mm x 414.1 mm.

Figure 2-7 shows the front panel of the NIP5100/5100D.

Figure 2-7 Front panel of the NIP5100/5100D



1. ESD wrist strap socket	2. System reset button	3. USB 2.0 interface
4. Indicator area	5. Console port	6. microSD card slot
7. Management interface	8. 10/100/1000M adaptive electrical Ethernet interface	9. Optical or electrical (mutually exclusive) interfaces
10. Filler panel (inapplicable to interface cards)	11. Filler panel (inapplicable to interface cards)	12. FIC9
13. FIC7	14. Filler panel (inapplicable to interface cards)	15. FIC5
16. ESP801 card	17. Filler panel (inapplicable to interface cards)	18. Filler panel (inapplicable to interface cards)
19. Grounding terminal		

NOTE

- The microSD card slot of the NIP5100/5100D does not support microSD cards and is reserved for expansion.
- The NIP5100 has two hardware versions that use two ESP710 cards and one ESP801 card respectively for service accelerating. The devices of the two versions have identical performance and functions.

Figure 2-8 shows the rear panel of the NIP5100/5100D.

Figure 2-8 Rear panel of the NIP5100/5100D

1. Air filter	2. Power switch	3. AC power cable jack
4. Power socket	5. Fan filter	6. Power indicator
7. ESD wrist strap socket	8. Fan frame	

NIP5200/5200D

The NIP5200/5200D consists of the integrated chassis and expansion interface cards. The dimensions (H x W x D) of such chassis are 130.5 mm x 442 mm x 414.1 mm.

Figure 2-7 shows the front panel of the NIP5200/5200D.

Figure 2-9 Front panel of the NIP5200/5200D

1. ESD wrist strap socket	2. System reset button	3. USB 2.0 interface
4. Indicator area	5. Console port	6. microSD card slot
7. Management interface	8. 10/100/1000M adaptive electrical Ethernet interface	9. Optical or electrical (mutually exclusive) interfaces
10. Filler panel (inapplicable to interface cards)	11. Filler panel (inapplicable to interface cards)	12. FIC9
13. FIC7	14. Filler panel (inapplicable	15. FIC5

to interface cards)

16. 2 x ESP801 17. Grounding terminal

NOTE

- The microSD card slot of the NIP5200/5200D does not support microSD cards and is reserved for expansion.
- The NIP5200/5200D has two ESP801 cards in standard configuration. The ESP801 card is used to accelerate service processing. The card is inserted in the slot of the device upon shipment.

Figure 2-10 and Figure 2-11 show the rear panel of the AC and DC models of the NIP5200 and NIP5200D.

Figure 2-10 Rear panel of the AC model of the NIP5200/5200D

Figure 2-11 Rear panel of the DC model of the NIP5200/5200D

1. Air filter
2. Power switch
3. AC power cable jack
4. Power socket
5. Fan filter
6. Power indicator
7. ESD wrist strap socket
8. Fan frame

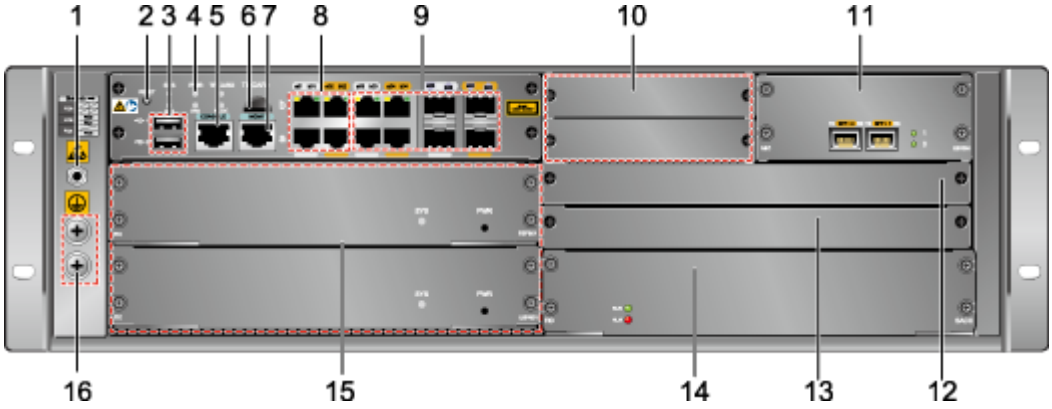
NOTE

The DC and AC models of the NIP5200/5200D employ the same panel. Jack 3 of the DC model is not required.

NIP5500/5500D

Figure 2-12 shows the front panel of the NIP5500/5500D.

Figure 2-12 Front panel of the NIP5500/5500D



1. ESD wrist strap socket	2. System reset button	3. USB 2.0 interface
4. Indicator area	5. Console port	6. microSD card slot
7. Management interface	8. 10/100/1000M adaptive electrical Ethernet interface	9. Optical or electrical (mutually exclusive) interfaces
10. Filler panel (inapplicable to interface cards)	11. 2 x 10GE Optical Interface Card (standard configuration)	12. FIC9
13. FIC7	14. FPGA Accelerator	15. ESP801 cards (2 cards)
16. Grounding terminal		

NOTE

- The microSD card slot of the NIP5500/5500D does not support microSD cards and is reserved for expansion.
- The NIP5500/5500D has two ESP801 cards in standard configuration. The ESP801 card is used to accelerate service processing. The card is inserted in the slot of the device upon shipment.
- The NIP5500/5500D has one FPGA accelerator to accelerate packet forwarding. The card is inserted in the slot of the device upon shipment.

Figure 2-13 and Figure 2-14 show the rear panel of the AC and DC models of the NIP5500/5500D.

Figure 2-13 Rear panel of the AC model of the NIP5500/5500D

Figure 2-14 Rear panel of the DC model of the NIP5500/5500D

1. ESN	2. Fan frame	3. ESD wrist strap socket
4. Power indicator	5. Fan filter	6. Power socket
7. AC power cable jack	8. Power switch	9. Air filter

NOTE
The DC and AC models of the NIP5500/5500D employ the same panel. Jack 3 of the DC model is not required.

2.2.3 Fixed Interfaces and Expansion Interface Cards

The NIP2000/5000 series (except NIP2050D/2100D/2130D/2150D/2200D) provide fixed interfaces and support a wide range of expansion interface cards to deliver expansion capability.

Fixed Interfaces

The fixed interfaces supported by the NIP are shown as follows:

- One console port
- One management interface (10/100/1000M auto-sensing electrical Ethernet interface)
- Two USB 2.0 ports
- Four 10/100/1000M auto-sensing electrical Ethernet interfaces
- Four Combo interfaces

Expansion Interface Cards

Table 2-2-Table 2-6 show the expansion interface cards supported by the NIP.

Table 2-2 Expansion interface card of the NIP2050/2100/2130/2150/2200

Type	Interface Card	Interface	Function
FIC	Eight-port GE electrical interface card	Eight 10/100/1000M auto-sensing electrical Ethernet interfaces	Provides electrical interfaces for communication with other network devices.
FIC	Eight-port GE optical interface	Eight GE optical interfaces	Provides optical interfaces for communication with other network

Type	Interface Card	Interface	Function
	card		devices.
FIC	Four-port GE electrical bypass interface card	Four 10/100/1000M auto-sensing electrical Ethernet interfaces	When the four interfaces work in non-bypass state, they function the same as common GE electrical interfaces. In bypass state, adjacent bypass interfaces (GE0 and GE1, GE2 and GE3) are directly connected.
FIC	Optical bypass interface card	An optical bypass interface card has two bypass link-layer subcards. Each link-layer subcard provides four optical interfaces.	The bypass link-layer subcard can operate in working or protection mode. In working mode, the subcard diverts the traffic from an upstream device to the NIP. After the traffic is processed, the subcard diverts the processed traffic to the downstream device. In protection mode, the NIP connects the upstream and downstream devices.

Table 2-3 Expansion interface card of the NIP5100/5200

Type	Interface Card	Interface	Function
FIC	Eight-port GE electrical interface card	Eight 10/100/1000M auto-sensing electrical Ethernet interfaces	Provides electrical interfaces for communication with other network devices.
FIC	Eight-port GE optical interface card	Eight GE optical interfaces	Provides optical interfaces for communication with other network devices.
FIC	Eight-port GE electrical interface and two-port 10 GE optical interface card	Eight 10/100/1000M auto-sensing electrical Ethernet interfaces and two 10000M optical interfaces	Provides electrical and optical interfaces for communication with other network devices.
FIC	Two-port 10 GE optical interface card	Two 10000M optical interfaces	Provides optical interfaces for communication with other network devices.
FIC	Four-port GE electrical bypass interface card	Four 10/100/1000M auto-sensing electrical Ethernet interfaces	When the four interfaces work in non-bypass state, they function the same as common GE electrical interfaces. In bypass state, adjacent bypass interfaces (GE0 and GE1, GE2 and GE3) are directly connected.

Type	Interface Card	Interface	Function
FIC	Optical bypass interface card	An optical bypass interface card has two bypass link-layer subcards. Each link-layer subcard provides four optical interfaces.	The bypass link-layer subcard can operate in working or protection mode. In working mode, the subcard diverts the traffic from an upstream device to the NIP. After the traffic is processed, the subcard diverts the processed traffic to the downstream device. In protection mode, the NIP connects the upstream and downstream devices.

Table 2-4 Expansion interface card of the NIP5100D/5200D

Type	Interface Card	Interface	Function
FIC	Eight-port GE electrical interface card	Eight 10/100/1000M auto-sensing electrical Ethernet interfaces	Provides electrical interfaces for communication with other network devices.
FIC	Eight-port GE optical interface card	Eight GE optical interfaces	Provides optical interfaces for communication with other network devices.
FIC	Eight-port GE electrical interface and two-port 10 GE optical interface card	Eight 10/100/1000M auto-sensing electrical Ethernet interfaces and two 10000M optical interfaces	Provides electrical and optical interfaces for communication with other network devices.
FIC	Two-port 10 GE optical interface card	Two 10000M optical interfaces	Provides optical interfaces for communication with other network devices.

Table 2-5 Expansion interface card of the NIP5500

Type	Interface Card	Interface	Function
FIC	Eight-port GE electrical interface card	Eight 10/100/1000M auto-sensing electrical Ethernet interfaces	Provides electrical interfaces for communication with other network devices.
FIC	Eight-port GE optical interface card	Eight GE optical interfaces	Provides optical interfaces for communication with other network devices.
FIC	Two-port 10 GE optical interface card	Two 10000M optical interfaces	Provides optical interfaces for communication with other network devices.

Type	Interface Card	Interface	Function
FIC	Four-port GE electrical bypass interface card	Four 10/100/1000M auto-sensing electrical Ethernet interfaces	When the four interfaces work in non-bypass state, they function the same as common GE electrical interfaces. In bypass state, adjacent bypass interfaces (GE0 and GE1, GE2 and GE3) are directly connected.
FIC	Optical bypass interface card	An optical bypass interface card has two bypass link-layer subcards. Each link-layer subcard provides four optical interfaces.	The bypass link-layer subcard can operate in working or protection mode. In working mode, the subcard diverts the traffic from an upstream device to the NIP. After the traffic is processed, the subcard diverts the processed traffic to the downstream device. In protection mode, the NIP connects the upstream and downstream devices.

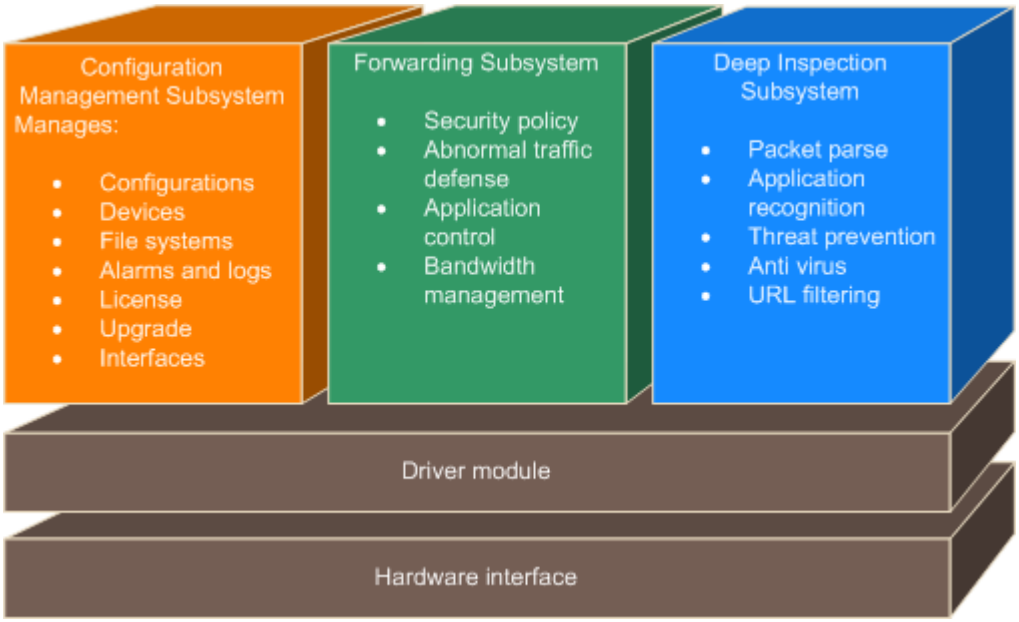
Table 2-6 Expansion interface card of the NIP5500D

Type	Interface Card	Interface	Function
FIC	Eight-port GE electrical interface card	Eight 10/100/1000M auto-sensing electrical Ethernet interfaces	Provides electrical interfaces for communication with other network devices.
FIC	Eight-port GE optical interface card	Eight GE optical interfaces	Provides optical interfaces for communication with other network devices.
FIC	Two-port 10 GE optical interface card	Two 10000M optical interfaces	Provides optical interfaces for communication with other network devices.

2.3 Software Structure

The software system is composed of modules that perform specific functions and collaborate with each other.

Figure 2-15 Modular software structure



Configuration Management Subsystem

The configuration management subsystem supports the entire system and interacts with users. This subsystem also provides interfaces for configuration, testing, and maintenance to manage devices, configurations, file systems, interfaces, alarms and logs, software patches, licenses, knowledge base and virus database updates.

Forwarding Subsystem

The forwarding subsystem forwards packets based on blacklists and whitelists and packet-filtering, abnormal traffic prevention, flow control policies, and bandwidth management.

Deep Inspection Subsystem

The deep inspection subsystem detects and prevents attacks at the application layer. It reassembles packets, analyzes the application-layer information, prevents application-layer exploits and threats, virus scanning and removal, and URL filtering.

Driver Module and Hardware Interface

The driver module and hardware interface provide basic support for the communication between software and hardware.

2.4 Configuration Requirements of the NIP Manager

This section describes the hardware and software requirements of the NIP Manager.

Hardware Requirement

Table 2-7 shows hardware requirements of NIP Manager.

Table 2-7 Hardware requirements of NIP Manager

Item	Requirements
Recommended configuration (For smaller than or equal to 20 managed NIP devices)	IBM X3650M3 server • CPU: Xeon quad-core E5506 2.13 GHz or higher • Memory: 8 GB To ensure the normal startup of the NIP Manager, the server must have a minimum of 3.0 GB free memory space. • Hard disk: 2 x 300 GB RAID1 Recommended RAID card model: ServeRAID card (M5015). RAID 5 is recommended when the number of hard disks is 3 or greater. **NOTE** Configuration for connecting an external disk cabinet: Huawei OceanStor S2600F that supports FC port is recommended. HBAs and optical jumpers need to be configured independently.
Minimum configuration (For 1 or 2 managed NIP devices)	• CPU: Dual-core X86 processor • Memory: 4 GB To ensure the normal startup of the NIP Manager, the server must have a minimum of 1.2 GB free memory space. • Hard disk: 100 GB To improve system reliability and security, you are advised to partition the disk into at least two logical drives. The storage capacity of a drive is 30 GB and is only for the installation of the operating system. The remaining space is allocated to the other drive for the installation of the database software and the NIP Manager as well as the storage of database files.

Software Requirement

Table 2-8 shows software requirements of NIP Manager.

Table 2-8 Software requirements of NIP Manager

Hardware Platform	Software Type	Software Version
x86 (Windows 64bit)	Operating system	Windows Server 2008 R2 Standard
	Database	MSSQL Server 2008 Standard with SP2
	Web browsers that can access the server	Internet Explorer 6.0/7.0/8.0 Mozilla Firefox 3.6.X to 4.X

Hardware Platform	Software Type	Software Version
x86 (Windows 64bit)	Operating system	Windows 7 Professional
	Database	MSSQL Server 2005 Express with SP4
	Web browsers that can access the server	Internet Explorer 6.0/7.0/8.0 Mozilla Firefox 3.6.X to 4.X
x86 (Windows 32bit)	Operating system	Windows Server 2003 R2 Standard
	Database	MSSQL Server 2005 Standard with SP3
	Web browsers that can access the server	Internet Explorer 6.0/7.0/8.0 Mozilla Firefox 3.6.X to 4.X
x86 (Windows 32bit)	Operating system	Windows 7 Professional
	Database	MSSQL Server 2005 Express with SP4
	Web browsers that can access the server	Internet Explorer 6.0/7.0/8.0 Mozilla Firefox 3.6.X to 4.X
x86 (Windows 32bit)	Operating system	Windows XP
	Database	MSSQL Server 2005 Express with SP4
	Web browsers that can access the server	Internet Explorer 6.0/7.0/8.0 Mozilla Firefox 3.6.X to 4.X

3 Product Functions

About This Chapter

This chapter describes the functions of the NIP.

3.1 Function List

This section lists the functions of the NIP for quick reference.

3.2 Virtual Patch

The signatures of the NIP are advanced and are based on vulnerabilities instead of attacks. All attacks that target at the same vulnerability are prevented. Therefore, the signatures function as virtual patches to the system.

3.3 Client Protection

The NIP uses Huawei threat prevention engine, which is accurate and has inherent advantages in client protection.

3.4 Web Applications Protection

The NIP uses accurate content analysis and recognition technologies to prevent attacks on Web servers, such as cross-site scripting and SQL injection.

3.5 Malware Prevention

The NIP can identify infected system based on the data sending of the malware, locate the data exchanged between the botnet and the controlled programs, and prevent the automatic upgrade of malware, the sending of confidential information such as browser history by malware, and the sending of spam from zombies.

3.6 Anti-Virus

The NIP provides professional anti-virus functions to protect enterprise networks from virus infection.

3.7 Application Identification and Control

The NIP uses the Service Awareness technology to inspect and recognize the application-layer protocols of the packets to control and manage the packets.

3.8 Abnormal Traffic Prevention

Based on multi-layer filtering, the NIP learns the traffic model and uses static filtering, source validity authentication, behavior analysis, session monitoring, and signature recognition to implement accurate traffic cleaning against DoS/DDoS attacks.

3.9 Logs and Reports

The logs generated on the NIP are sent to the NIP Manager, which summarizes and analyzes the logs and generate reports to provide visibility into the network status.

3.10 High Availability

The NIP delivers device-level and network-level availability to ensure service continuity.

3.1 Function List

This section lists the functions of the NIP for quick reference.

The functions of NIP vary with deployment modes. Table 3-1 shows the functions of in-line deployed IPS devices, and Table 3-1 shows the functions of IDS devices and off-line deployed IPS devices.

Table 3-1 Functions of the NIP

Function	Sub-function	Description	Whether Supported by the IDS Device or IPS Device in Off-line Deployment
Threat prevention	Virtual patch	Defends against exploits to eliminate the dependence of IT systems on software patches, improve the security of servers and terminals, and reduce maintenance efforts and system downtime.	This function is used to detect and record the attack events. The IDS device or IPS device in off-line deployment can block the connection by sending TCP RST with limited capability. Supports the interworking with the firewall for blocking connections.
	Client protection	• Protects browsers and plug-ins such as JavaScript and ActiveX. • Protects files such as Word, PDF, Flash, and AVI. • Defends against exploits. • Detects spyware and adware. • Defends against drive-by downloads. • Defends against deceptive software.	
	Web applications protection	• Protects Web applications, including Web2.0 and background databases.	

Function	Sub-function	Description	Whether Supported by the IDS Device or IPS Device in Off-line Deployment
		• Defends against major attacks such as SQL injection and cross-site scripting.	
	Malware prevention	Defends against Trojan horses, backdoor software, adware, and malware.	
Application identification and control	Application identification	• Provides a rule base, which can identify over 850 types of applications, including P2P, IM, online game, stock, voice, online video, web mail, mobile terminal, and remote login applications. • Supports the update of the rule base to identify the latest applications.	Identifies and monitors applications, but does not perform any control.
	Application control	• Supports the limiting on traffic and the number of connections by protocol to control game, stock, P2P, IM, and VoIP traffic. • Supports application control based on user-defined application protocol set. • Supports application control based on schedule and IP address range.	
Anti-Virus	Anti-Virus	• Supports virus scanning for files transmitted through HTTP, SMTP, POP3, and FTP. • Supports processing the special files and configuring policy for different protocols.	Not supported.
URL filtering	URL filtering	The NIP controls users' HTTP requests by generating an alarm or denying users to access certain network resources, therefore regulating online behaviors.	This function is used to detect and record the HTTP access events. The IDS device or IPS device in off-line deployment can block the connection by

Function	Sub-function	Description	Whether Supported by the IDS Device or IPS Device in Off-line Deployment
			sending TCP RST with limited capability.
Basic network access control	Basic network access control	The NIP provides such a function as packet filtering of the firewall. It determines whether packets are allowed by their source IP addresses, destination IP addresses, services, and control actions. Then the NIP performs subsequent operations on the packets that are allowed through. The denied packets are directly blocked.	The NIP in off-line mode does not forward traffic. Therefore no basic access control actions are required. However, you can configure attack and application protocol detection based on IP addresses and service types
Abnormal traffic prevention	Flood type attack defense	• Supports traffic model learning. • Defense against the following flood type attacks is supported: – TCP flood attacks – TCP connection flood attacks – UDP flood attacks – HTTP flood attac	Detects and records the attack events, but does not clean the abnormal traffic.

Function	Sub-function	Description	Whether Supported by the IDS Device or IPS Device in Off-line Deployment
		ks – HTTPS flood attacks – DNS flood attacks – SIP flood attacks – ICMP flood attacks	
	Packet type attack defense	Defense against the following packet type attacks is supported: • Scanning attack: IP address scanning and port scanning. • Malformed packet attack: multiple malformed packet attacks is supported, such as Teardrop, Ping of Death, and WinNuke attacks. • Special packet attack: multiple special packet attacks is supported, such as oversized ICMP packets, ICMP unreachable packets, ICMP redirection packets, and Tracert attacks.	
Bandwidth management	Per-IP traffic limiting and global traffic limiting	Supports IP address-based traffic control, including traffic control on individual IP address and multiple IP addresses, which ensures minimum bandwidth and	Not supported.

Function	Sub-function	Description	Whether Supported by the IDS Device or IPS Device in Off-line Deployment
		supports idle time bandwidth borrowing.	
Logs and reports	Log display	• The NIP records and displays logs on intrusion events, operations on the NIP, and system messages, so that you can know the network security status and the NIP operating status. This plays an important role in operation maintenance and fault locating. • The memory only records limited logs, and logs can be exported to the NIP Manager or other log hosts. • Supports the download of packet capture files for attack analysis.	Supported.
	Statistical report	• The Web page provides five types of statistics, namely, abnormal traffic statistics, threat prevention severity statistics, major application category proportion statistics, top 10 threat prevention attack events and top 10 virus events. • The reports provided by the Web page are rather simple. Complicated ones need to be displayed by the NIP Manager in a centralized way. • The NIP Manager provides reports on abnormal traffic, threat intrusions, anti-virus, and Web applications. In addition, it provides an integrated report, which enables you to know the network security status and monitor user online behaviors in a timely manner, therefore providing reference for threat identification and elimination.	

Function	Sub-function	Description	Whether Supported by the IDS Device or IPS Device in Off-line Deployment
High availability	Dual-system hot backup	The NIP supports dual-system hot backup, so that if one NIP fails, the other can take over services, which ensures service continuity.	Not supported.
	Traffic bypass	Supports bypass cards to allow traffic to bypass a failed (regardless of software failure, hardware failure, or power failure) NIP system to ensure service continuity.	
Operation and maintenance	Configuration management	• Separate management – Through the Web interface The NIP can be managed through the Web interface that supports both HTTP and HTTPS. – Through command lines When the Web interface is unavailable, you can log in to the NIP through the console port and configure the NIP through command lines to restore the Web interface. • Centralized management The NIP Manager is the NIP management software that can manage multiple NIPs and provide the following functions: – Service configur	Supported.

Function	Sub-function	Description	Whether Supported by the IDS Device or IPS Device in Off-line Deployment
		ation – Running status monitoring – Alarm management – Logs and reports viewing	
	System software upgrade	• Through the Web interface The Web interface is a preferred upgrade tool to upgrade the NIP software. It provides one-touch upgrade function to easily upgrade the system software of the NIP • Through the BootROM When the system software of the NIP is corrupted and cannot be started, you can upgrade the system software through the BootROM.	Supported.
	Updating the knowledge base and virus database	• Supports Internet online update, intranet online update, local update, version rollback, and restoration to the factory default version of the knowledge base and virus database. • Supports the knowledge base and virus database update through the embedded Web interface of the NIP. • Supports individual or batch	Supported.

Function	Sub-function	Description	Whether Supported by the IDS Device or IPS Device in Off-line Deployment
		knowledge base and virus database update of the managed NIPs through the NIP Manager.	
	SNMP	• Supports the sending of alarms to third-party NMS software. • Supports SNMPv1, SNMPv2c, and SNMPv3.	Supported.
	Fault diagnosis	• Supports ping and tracert. • Supports viewing and downloading of diagnosis information. • Provides diagnosis function to diagnose the communication between the NIP and the NMS software or log host. • Provides the ESP card diagnosis function.	Supported.
	Security	• Supports hierarchical and domain-based management for NIP Manager administrators. • Provides administrative access control. • Provides logging function. • Provides protection for the sensitive information of users. • Defends against brute-force cracking. • Supports screen lock.	Supported.
Interworking	Interworking with firewalls	Supports the interworking with Huawei Eudemon firewalls.	Supported.
Deployment mode	In-line deployment	Supports the blocking of malicious connections by using a transparently connected interface pair.	Not supported.
	One-armed deployment	The NIP is deployed in one-armed mode over the trunk link of the switch. In this case, the NIP detects the traffic	Not supported.

Function	Sub-function	Description	Whether Supported by the IDS Device or IPS Device in Off-line Deployment
		originated from the switch and analyses the data flows matching the VLAN pair. After processing the data packets matching the configured policy, the IPS device converts these packets based on the VLAN pair mapping and sends the traffic along the original link.	
	Off-line deployment	Either interface in an interface pair can be off-line deployed to analyze the traffic and log attack events for future network assessment and auditing.	Supported.
	Composite deployment	The NIP provides massive interfaces and flexible working modes, serving both as an IPS and an IDS. Therefore, users do not need to purchase two separate devices.	Not supported.
	Asymmetrical traffic deployment	The NIP allocates a interface pair for the traffic in each direction and then binds the interface pairs to transparently access networks and successfully detect threats.	Supported.

3.2 Virtual Patch

The signatures of the NIP are advanced and are based on vulnerabilities instead of attacks. All attacks that target at the same vulnerability are prevented. Therefore, the signatures function as virtual patches to the system.

Just as that a key of a specific pattern can open a lock of the same pattern, only the worms of specific signatures can attack exploits of the specific patterns. The NIP protects unpatched operating systems and applications as follows:

1. Identify the signature of a vulnerability.
2. Scan the network traffic against the signature to block all packets of the same signature. Therefore, all worms that target at the vulnerability can be blocked, regardless of the features of the worms.

Huawei tracks and studies the evolution of every exploit (one exploit can evolve into many variants) to provide protection against the latest attack with a single signature. The signatures

are created in a generic way because the more generic the signatures, the more likely the NIP can prevent future exploits or variants targeting at known vulnerabilities.

3.3 Client Protection

The NIP uses Huawei threat prevention engine, which is accurate and has inherent advantages in client protection.

The majority of Internet attacks target at the clients. A client can be infected with malicious codes any time if the client accesses the Internet. The clients in most enterprises can access the Internet, increasing the threats to clients. Most attacks take advantage of the vulnerabilities of browsers and files.

Drive-by Download Prevention

The drive-by download is subtle. If the network is running properly, the computer automatically downloads executable data from the Internet without being noticed. The drive-by download is one of the most severe intrusions on the live network.

Mainstream websites are targets of drive-by download attacks. The NIP uses the virtual patch technology to protect browsers and plug-ins from drive-by downloads. Drive-by downloads use the advanced obfuscation technology with well-designed attacks. Therefore, the NIP uses advanced anti-evasion technologies to detect drive-by downloads.

- Prevent attacks that target at Web 2.0, browsers, and plug-ins.
- Prevent malicious codes in formats such as JavaScripts, VB scripts, Flash, and HTML.
- Prevent exploits that target at vulnerabilities of clients, applications such as PDF reader, and browsers (such as Microsoft Internet Explorer and Mozilla Firefox).

Spoofing Application Prevention

Hackers exploit vulnerabilities to intrude operating systems and application software, and other methods such as social engineering to cheat users into implementing unexpected operations. The social engineering spoofing includes attacks of misleading applications and rogue security software. The NIP supports the network signature rules for detecting and preventing misleading applications. Common misleading applications are listed as follows:

- Fake virus scanning software and related scams and hoaxes.
- Fake malware scanning Web pages.
- Fake decoder component installation programs.
- Executable files disguised in improper contents.

Spyware and Adware Detection

The NIP can detect the spyware and adware to alleviate security threats to enterprises. Enterprises prefer IPS products that can detect the spyware and adware although spyware and adware may not spread among intranet hosts. Alarms for the spyware and adware can be ignored if the security strategy of an enterprise permits.

3.4 Web Applications Protection

The NIP uses accurate content analysis and recognition technologies to prevent attacks on Web servers, such as cross-site scripting and SQL injection.

Web-based services are increasingly popular on the Internet. Interruption of these services has severe impact on economic and reputation losses and the life of end users.

Exploits targeting at vulnerabilities of Web-based applications account for half of attacks on Web applications, and the most common attacks are SQL injection and cross-site scripting. In addition, scanning, guess, sniffing, and DoS and DDoS attacks are threatening Web-based applications.

The NIP provides a wide range of signatures to protect Web servers against SQL injection and cross-site scripting.

3.5 Malware Prevention

The NIP can identify infected system based on the data sending of the malware, locate the data exchanged between the botnet and the controlled programs, and prevent the automatic upgrade of malware, the sending of confidential information such as browser history by malware, and the sending of spam from zombies.

Malware writers usually disguise malware in adult Web sites or video or audio instructions to trick users to click the play button. After users click the play button, the users will be prompted to download and install a codec. However, the codec is a disguised malware file.

The NIP can inspect and block the connections to these types of Web sites. Two types of signature databases are provided against such Web sites: One for inspection before the malware is detected, and the other for host inspection after the hosts are infected.

The signature database of the NIP focuses on the following aspects against fraudulent Web sites:

- HTTP-based disguised applications
- HTTP-based disguised download requests
- HTTP-based disguised file downloads
- HTTP-based disguised malware download requests

3.6 Anti-Virus

The NIP provides professional anti-virus functions to protect enterprise networks from virus infection.

The NIP scans Web access, email, and FTP traffic for viruses and forwards the traffic only if no virus is detected. In addition, the NIP can scan compressed files of multiple formats, packed files, and attachments in emails to prevent virus spread.

The NIP can scan files transmitted through HTTP, SMTP, POP3 and FTP. You can configure different virus scanning policies for application protocols based on the features of the network. For example, you can configure response mode, and restrict the size and types of files to be scanned. Upon detecting a virus, the NIP notifies users using email or pushing a web page.

Scanning policies can be applied between desired security zones to avoid the impact of global scanning on performance.

The NIP supports manual or scheduled update of the virus database from the security service center. If the NIP cannot be connected to the security service center on the Internet, you can download the update package in other ways, upload the update package to the NIP, and update the virus database offline. The virus database can be rolled back if necessary.

NOTE
The IPS device in off-line mode and the IDS device do not provide the anti-virus function.

3.7 Application Identification and Control

The NIP uses the Service Awareness technology to inspect and recognize the application-layer protocols of the packets to control and manage the packets.

Bandwidth is usually a limited resource in most enterprises and organizations. If non-work-related applications (such as download of online video and games) occupy the bandwidth, the network may be unavailable for mission-critical applications and services.

The NIP analyzes packets and compares the features against the application control rule base to identify traffic of applications such as games, stock, P2P, IM, and VoIP applications, providing visibility into and control over the applications.

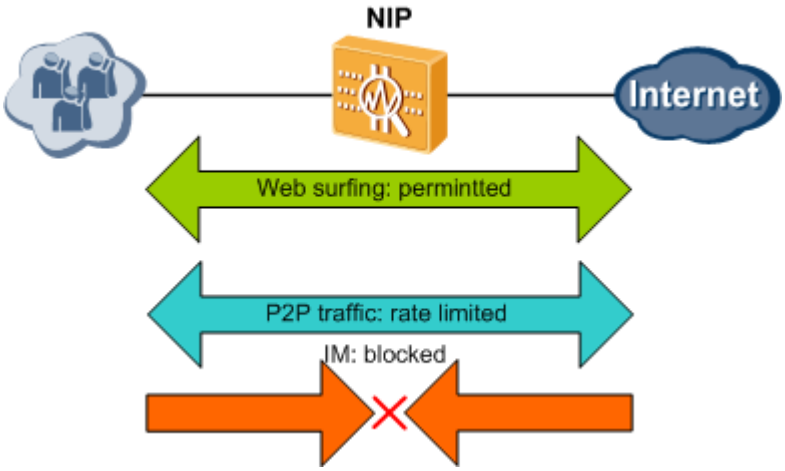
The NIP provides flexible application traffic control. The administrator can specify users to use an application at a specified time. In this way, the network administrator maximizes visualized network traffic.

The application traffic control prevents and restricts traffic. The administrator can set whether to allow an application and set the maximum bandwidth for an application. In this way, the administrator can prevent employees from using applications that may lower the work efficiency such as watching online videos, and can set the maximum bandwidth of an application available for employees to ensure that the key service of the enterprise runs properly.

Enterprises vary in organizational structures, network classification, and business hours. Therefore, the NIP allows administrators to set different application traffic control policies for different users in different time segments. For example, the sales department is allowed to use all network resources except online videos and stock applications and the R&D department is not allowed to use P2P downloads and IM applications during working hours.

As shown in Figure 3-1, legitimate Web browsing is allowed, the rates of applications (such as P2P) that compete bandwidth with mission-critical applications are limited, and undesired applications (such as IM) are blocked.

Figure 3-1 Application control



NOTE

IDS devices and IPS devices that are deployed off-line cannot control application traffic, but can provide visibility into applications through the analysis and report functions.

3.8 Abnormal Traffic Prevention

Based on multi-layer filtering, the NIP learns the traffic model and uses static filtering, source validity authentication, behavior analysis, session monitoring, and signature recognition to implement accurate traffic cleaning against DoS/DDoS attacks.

DoS attacks paralyze target victims by exhausting bandwidth and system resources of the victims, attacking the program defects, and providing false routes or DNS information.

DDoS attacks are DoS attacks launched from distributed sources by multiple attacks or from distributed zombies controlled by attackers. DDoS attacks are used in unfair business competition, financial crimes, and release of political views.

The NIP uses multiple advanced detection technologies and algorithms to better defend against DoS and DDoS attacks. The following describes some advanced protection technologies against DDoS attacks.

CAUTION

In-line deployed IPS devices can prevent attacks; whereas IDS devices and off-line deployed IPS devices can detect, but cannot prevent attacks.

Dynamic Traffic Baseline

Traditional IPS devices calculate traffic based on traffic types and compare the results with the preconfigured thresholds. The IPS devices detect DDoS attacks if the results exceed the thresholds. This method is called the static traffic baseline. In this method, the thresholds must

be properly configured to ensure accurate attack detection. Proper threshold configuration depends on experience of configuration personnel.

The NIP calculates and compares network traffic by time and sets the base value to the maximum value obtained during a learning period. The NIP calculates the detection threshold using the following formula:

Detection threshold = Base value + Tolerance for false positives caused by traffic jitters

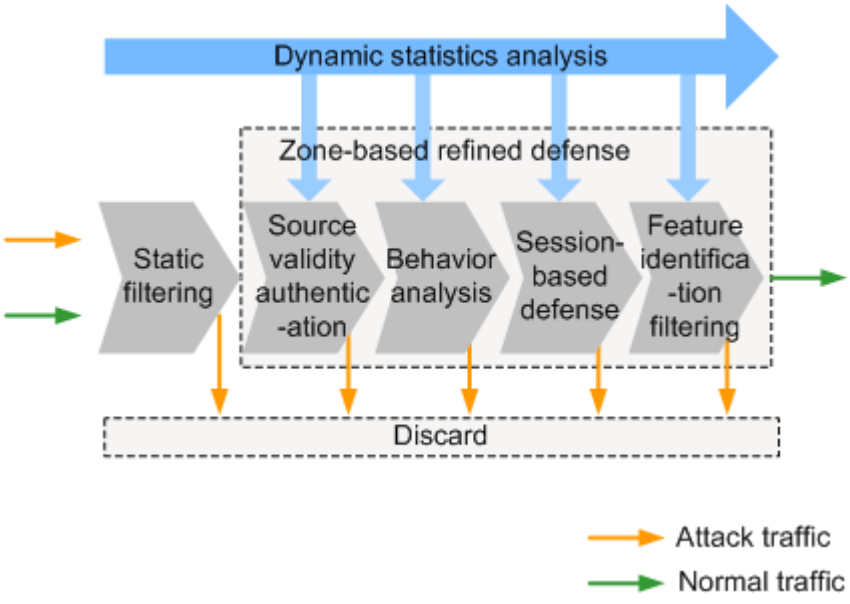
The NIP restarts the learning process to obtain new detection thresholds when the network traffic model changes. Therefore, this method is called the dynamic traffic baseline.

Using the dynamic traffic baseline greatly improves the accuracy of detection and protection and makes it easier to deploy and use the NIP.

Multi-layer Filtering

The NIP defends against DoS and DDoS attacks by using multi-layer filtering to provide granular protection, as shown in Figure 3-2.

Figure 3-2 Multi-layer filtering



The layers shown in the previous figure provide the following functions:

1. Static filtering

   Static filtering is performed on the basis of the blacklist and whitelist.

   The NIP supports the dynamic generation of blacklist and whitelist entries. Packets from IP addresses that match the blacklist are discarded, and those match the whitelist are directly forwarded.

2. Zone-based refined defense

   The refined defense is performed on the basis of all destination IP addresses. The NIP first identifies the destination IP addresses of packets, and then performs source validity authentication, behavior analysis, session monitoring, and feature identification on the packets in turn.

a. Source validity authentication

Source validity authentication is performed based on transport-layer and application-layer protocols to defend against the attacks initiated from forged source IP addresses or Botnets, for example, the SYN flood, SYN-ACK flood, ACK flood, DNS Request flood, DNS Reply flood, SIP flood, HTTP flood, and HTTPS flood attacks.

b. Behavior analysis

Both the attack behaviors of Botnets and the access of normal users are learned to defend against attacks from Botnets, for example, the TCP low-rate attack with continuous light traffic.

c. Session-based attack defense

Session-based attack defense is to defend against connection flood attacks, for example, abnormal session check and FIN/RST flood attack defense.

d. Feature identification filtering

Feature identification filtering identifies abnormal traffic based on attack features, and is to defend against non-service flood attacks on ports. For example, feature identification filtering performs fingerprint filtering on UDP flood attacks and HTTP flood attacks.

3.9 Logs and Reports

The logs generated on the NIP are sent to the NIP Manager, which summarizes and analyzes the logs and generate reports to provide visibility into the network status.

The logs record the operations (such as configuration on a Web interface) to the device and specific events (such as connection failure and matching of a signature). Logs keep a track of security events for system diagnosis, maintenance, and fault locating.

The NIP can buffer the logs or send the logs to the specified NIP Manager or third-party log host. By analyzing the logs, administrators can monitor network traffic, check the security vulnerabilities, security breaches, and attack types. Real-time logs provide visibility into ongoing instructions.

The NIP delivers visualized management through its embedded Web interface, which can generate reports on the statistics on abnormal traffic flows, threat severalties, application categories (in percentage), top 10 attack events and top 10 virus events to provide visibility into network status. The NIP Manager is a sophisticated network management system in B/S structure. It can generate advanced reports in different formats, charts (including bar charts, pie charts, and curve charts), and dimensions (including abnormal traffic, threat prevention, application control, and anti-virus). It can also generate consolidated reports in different granularities about the real-time network status, historical data, ranking of the detected attacks, and traffic changing trend to provide visibility into network traffic and threats.

For example, Figure 3-3 is a report about the worms on the victim hosts.

Figure 3-3 Reports on the victim hosts

	Threated Host	Number of Events (Entries)	Percentage to Total Entries
1	1.1.1.25	53,610	43.48%
2	1.1.1.26	53,600	43.47%
3	14.0.0.2	10,720	8.69%
4	61.178.77.171	5,362	4.34%

Details of threated host Top 10

Threated Host	Number of Events (Entries)
1.1.1.25	53610
Threat Events Top 10	
DDOS TFN Probe	53610

Threated Host	Number of Events (Entries)
1.1.1.26	53600
Threat Events Top 10	
DDOS TFN Probe	53600

Threated Host	Number of Events (Entries)
14.0.0.2	10720
Threat Events Top 10	
user_defined	10720

Threated Host	Number of Events (Entries)
61.178.77.171	5362
Threat Events Top 10	
field Host too long	5362

3.10 High Availability

The NIP delivers device-level and network-level availability to ensure service continuity.

System-Level Availability

The dedicated hardware system of the NIP supports temperature monitoring and hot-swap of fans to accommodate harsh environments. The power supply modules support 1+1 backup and hot swap. The switchover between the power supply modules has no impact on system running. The NIP is designed to deliver carrier-class high availability.

Network-Level Availability

NOTE

The IDS device and the IPS device in off-line or one-armed mode do not provide network-level availability.

- Dual-system hot backup

  The NIP supports Huawei Redundancy Protocol (HRP) to implement dual-system hot backup. A backup group includes an active device and a standby device. HRP synchronizes important configuration information and session table information between the active and standby devices to ensure smooth failover.

- Bypass interface card

  The NIP can hold bypass interface cards, which can directly connect upstream and downstream devices of the NIP when the NIP fails to ensure service continuity. When the faulty NIP is recovered, all traffic is switched back to the NIP to ensure security.

4 Application Scenario

About This Chapter

As a professional IPS product or IDS product, the NIP can be used on enterprise networks, IDCs, and campus networks to provide all-dimensional detection and protection.

4.1 At Enterprise Internet Edge (IPS Device)

In-line deployment at the enterprise Internet edge is a common deployment for small- and medium-sized enterprises to secure the hosts of the enterprise networks.

4.2 At the Edge of a Server Farm (IPS Device)

In-line deployment at the edge of a server farm is the most popular deployment of IPS products and is usually used at the edge of the server farms of enterprise networks and IDCs. In this scenario, the IPS product protects not only the software, but also the platforms (such as operating systems, hosts, and network infrastructure) of the software.

4.3 Next to the Switch of the Intranet (IDS Devices or Off-line Deployed IPS Devices)

Off-line deployment next to the switch of the intranet is a common deployment for enterprise networks to monitor, analyze, and audit network events.

4.4 At the Network Edge (IPS Device)

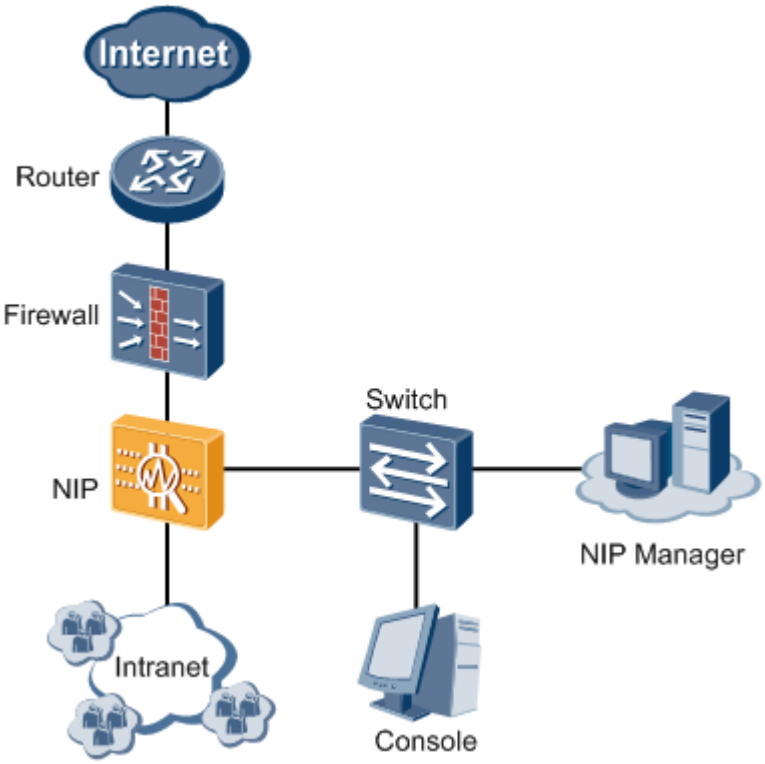
In-line deployment at network edges is a common deployment to secure the communication between subnets of an intranet or between the network at the headquarters and the branch networks. This deployment is similar to the deployment at Internet edge, but is used to isolate risks between subnets of an intranet.

4.1 At Enterprise Internet Edge (IPS Device)

In-line deployment at the enterprise Internet edge is a common deployment for small- and medium-sized enterprises to secure the hosts of the enterprise networks.

Figure 4-1 shows a typical network topology of small- and medium-sized enterprises. The NIP is deployed between the firewall and the intranet to secure the hosts on the intranet.

Figure 4-1 NIP deployed at enterprise Internet edge



The benefits of this type of implementation include:

- Blocking undesired P2P and video traffic to ensure the bandwidth for legitimate services.
- Preventing IM, on-line gaming, and stock exchange applications to avoid improper consumption of network resources.
- Preventing online storage, Web mail, and IM applications to avoid disclosure of internal documents or confidential information.
- Protecting internal hosts and browsers from threats to avoid data loss or damage or turning the hosts into zombies.
- Protect intranet PCs against viruses by scanning the files downloaded from the Internet.
- Regulating online behaviors by controlling accessible URLs to prevent network threats caused by employees' access to websites at will.
- Preventing DoS and DDoS attacks to avoid network interruptions.

To improve bandwidth or availability, enterprises may use multiple links to connect to the Internet. In this case, two deployment methods are applicable, based on whether the access links are located in the same place.

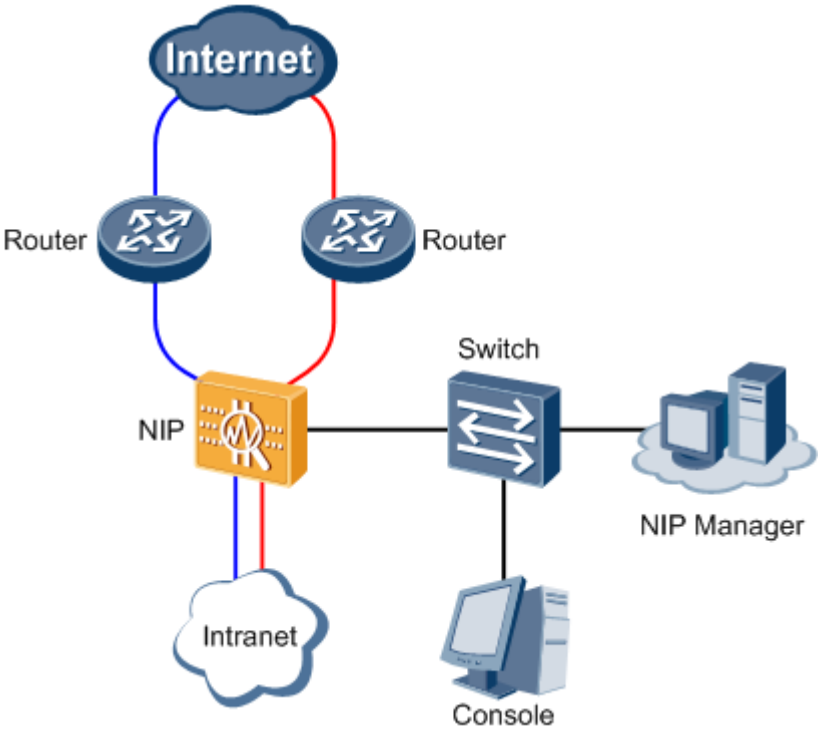
NOTE

Assume that there are two links in this example. The deployment methods are similar if there are more than two links.

- If the two links are located in the same place:

  As shown in Figure 4-2, only one NIP is needed. The two links are connected to two interfaces pairs on the NIP.

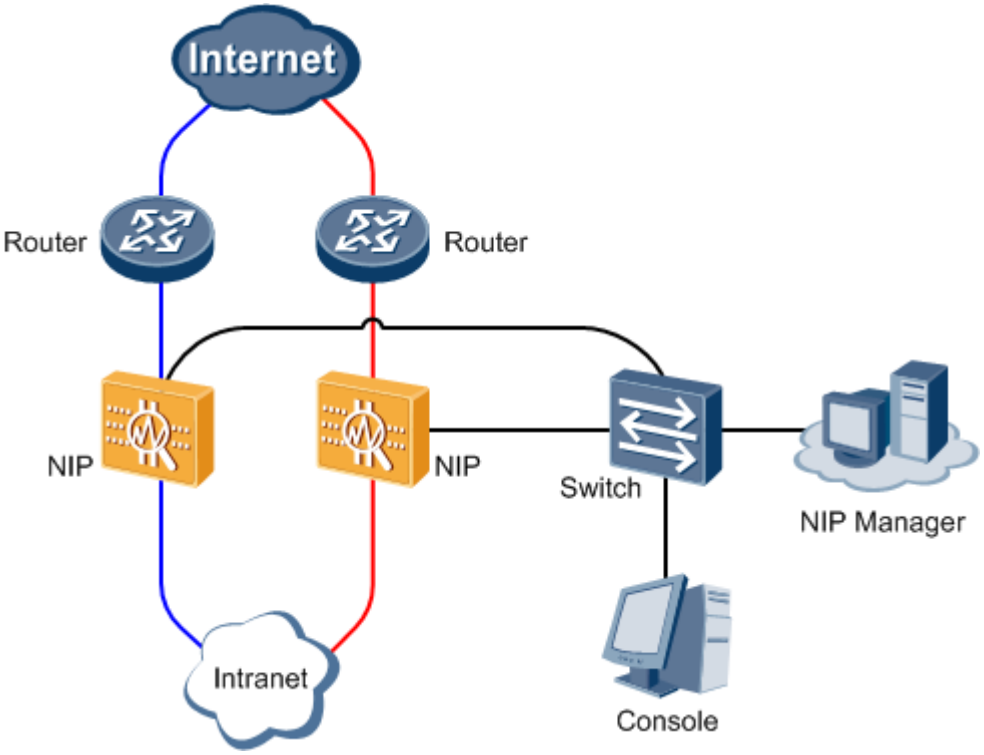
Figure 4-2 Two links connected to the Internet are located in the same place



- If the two links are located in different places:

  As shown in Figure 4-3, one NIP is needed in each place and the deployment method is similar to that when only one link is connected to the Internet.

Figure 4-3 Two links connected to the Internet are located in different places

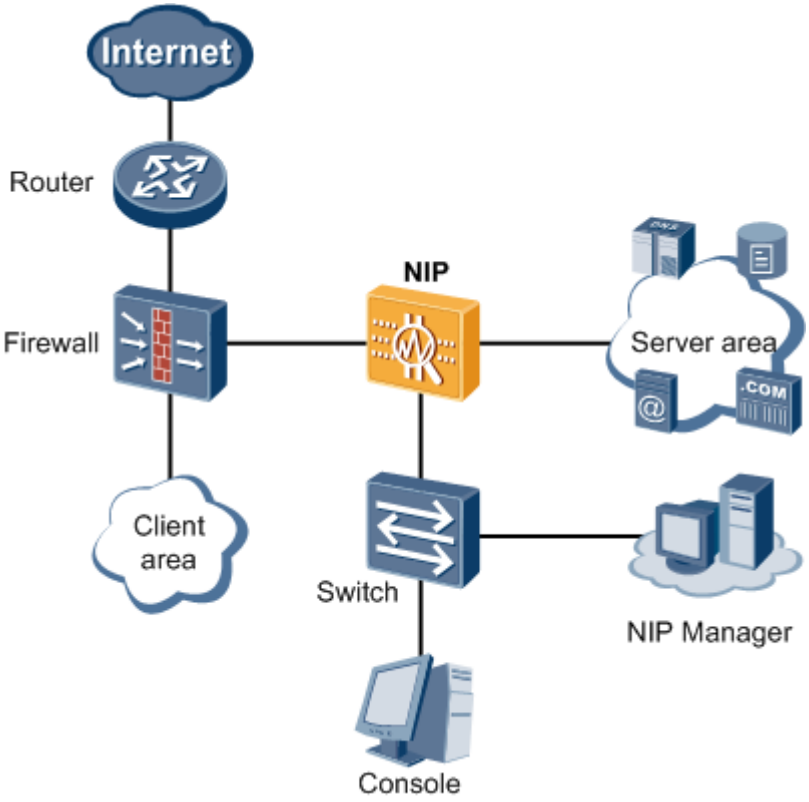


4.2 At the Edge of a Server Farm (IPS Device)

In-line deployment at the edge of a server farm is the most popular deployment of IPS products and is usually used at the edge of the server farms of enterprise networks and IDCs. In this scenario, the IPS product protects not only the software, but also the platforms (such as operating systems, hosts, and network infrastructure) of the software.

As shown in Figure 4-4, the NIP is deployed at the edge of a server farm on an enterprise network to secure the information systems (databases, DNS servers, Web servers, and mail servers). The NIP also provides reports to give intuitive visibility into network health.

Figure 4-4 NIP deployed at the edge of a server farm

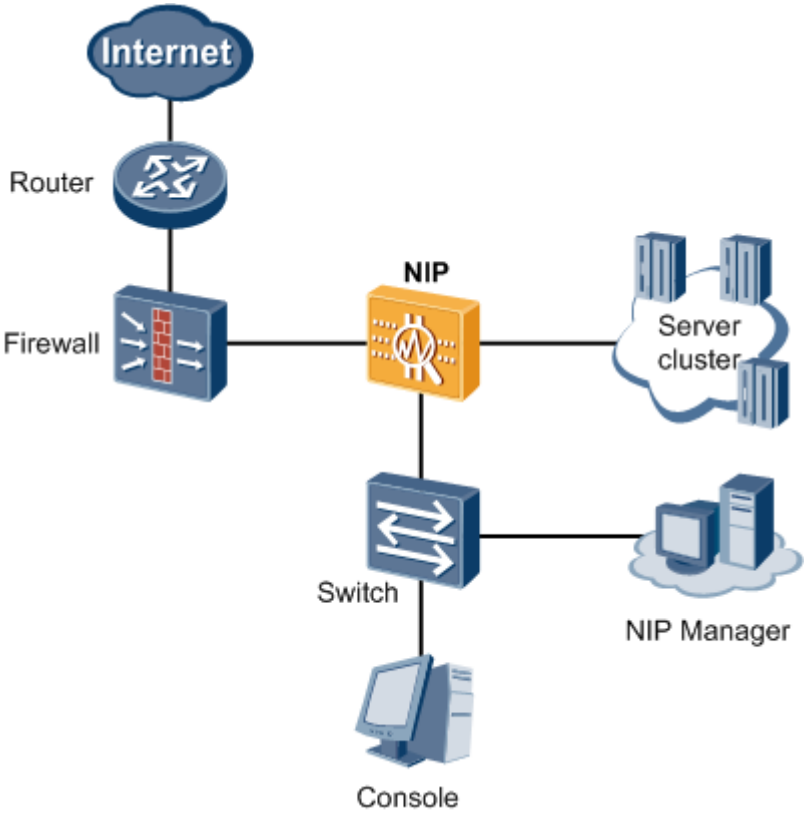


The benefits of this type of implementation include:

- Preventing worms and exploits targeting at service and platform vulnerabilities to avoid possible damage, tampering, or loss of data or turning the servers into zombies.
- Preventing service interruption caused by DoS or DDoS attacks.
- Preventing virus infection by scanning files or email messages sent to the server.
- Preventing emerging attacks targeting at Web applications, such as SQL injection, cross-site scripting, scanning, password guessing, and sniffing.

IDCs are special enterprises that make profits from providing servers and network resources for other enterprises. As shown in Figure 4-5, the NIP is deployed at the edge of a server cluster of an IDC to secure the servers. The NIP also provides reports to give intuitive visibility into network health and help the administrators to make informed decisions in IT implementation.

Figure 4-5 NIP deployed at the edge of a server cluster of an IDC



NOTE

- Service availability and reliability are important metrics of service quality. To ensures service continuity, use dual-system hot backup deployment or the bypass interface cards.
- The NIP provides a management interface to allow out-of-band management, which means that the management network is separated from the production network.

4.3 Next to the Switch of the Intranet (IDS Devices or Off-line Deployed IPS Devices)

Off-line deployment next to the switch of the intranet is a common deployment for enterprise networks to monitor, analyze, and audit network events.

Preventing improper use of network resources and intrusion from internal hosts are as important as preventing external threats. In fact, statistics indicates that the most common attacks are launched from internal networks. The activities of worms and Trojan horses, abnormal network access, and misuse or abuse of network services are difficult to evaluate. IDS devices can resolve these problems because the essence of IDS devices is security events management.

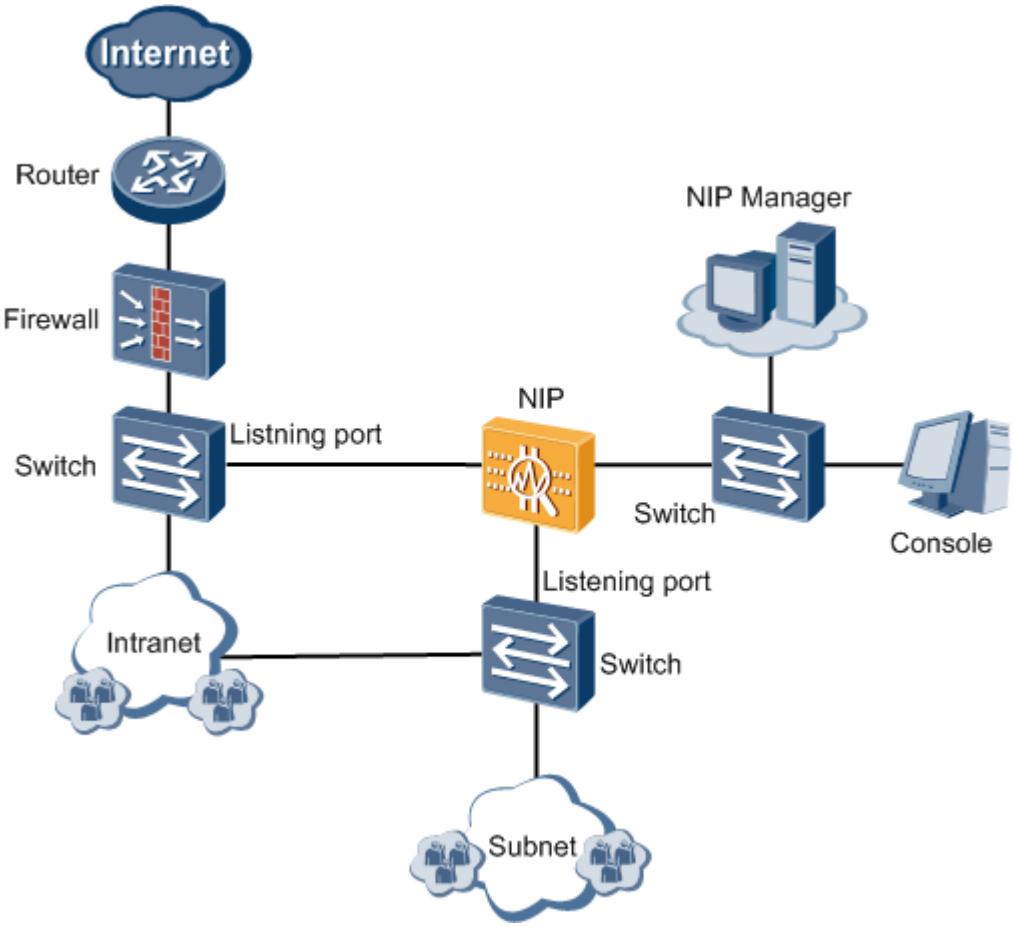
IDS devices use off-line deployment. IDS devices sample packets from the listening ports of the switches or the listening devices (such as optical splitters) on the networks. Each switch can monitor only the traffic from or to the directly connected hosts. If switches are deployed hierarchically, the traffic through the switches on the network to be monitored must be copied to the IDS devices through the listening ports of the switches.

As shown in Figure 4-6, the NIP is connected offline to the switches to analyze the traffic for attacks and abnormal behaviors and log them.

NOTE

For IPS devices, configure the interfaces to work in IDS mode and connect the interfaces in off-line mode. For IDS devices, connect the interfaces in off-line mode, which is the only deployment mode for IDS devices.

Figure 4-6 NIP deployed next to the switch of the intranet



The benefits of this type of deployment include:

- Detecting intrusion behaviors.
- Detecting behaviors that violate the IT policies of the enterprise.
- Providing important information to facilitate network maintenance and troubleshooting.
- Displaying network security events in real time or on daily, weekly, or monthly basis and providing suggestions about IT systems through automatic analysis.
- In offline deployment, the NIP is still capable of responding to threats by blocking a TCP flow through sending RST packets to minimize the impact of attacks.

4.4 At the Network Edge (IPS Device)

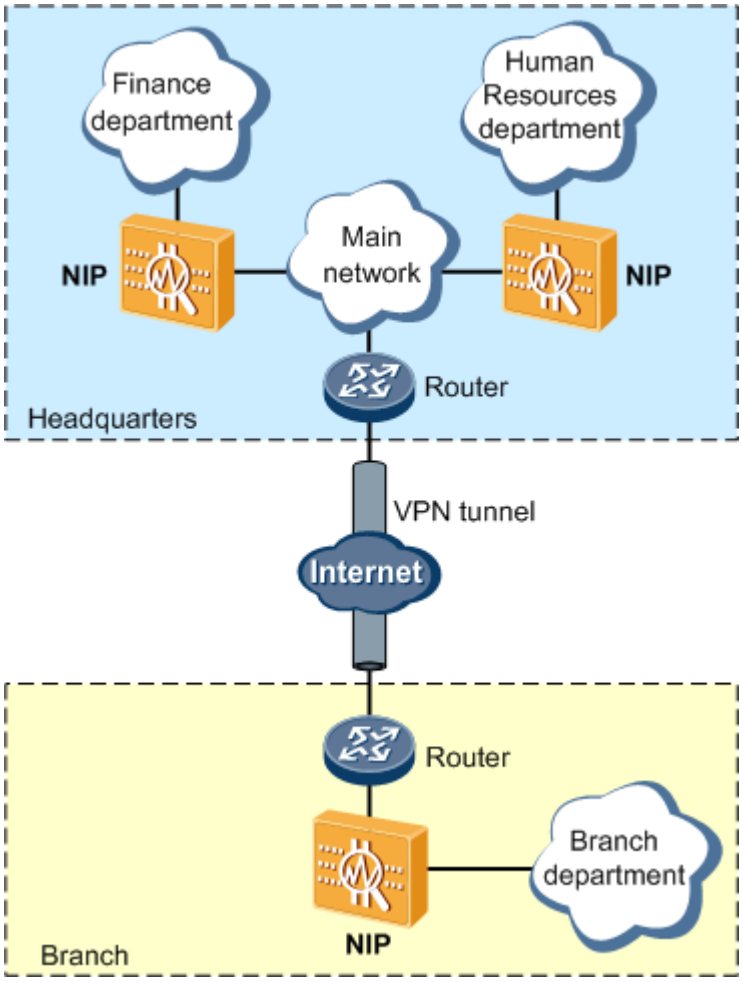
In-line deployment at network edges is a common deployment to secure the communication between subnets of an intranet or between the network at the headquarters and the branch networks. This deployment is similar to the deployment at Internet edge, but is used to isolate risks between subnets of an intranet.

As shown in Figure 4-7, the NIPs are deployed between subnets of different departments (such as the financial and HR departments) and between the network at the headquarters and the branch networks to protect the subnets and prevent the spread of risks.

NOTE

The NIPs still work well when the network at the headquarters and the branch networks are connected through VPN because the NIPs are connected offline to the perimeter routers or firewalls and the packets received by the NIPs are already decrypted.

Figure 4-7 NIP deployed at network edge



The benefits of this type of implementation include:

- Prevents the spread of worms and Trojan horses from external networks.
- Monitors violations on internal networks.
- Detects and prevents sniffing and reconnaissance from external networks.

5 Operation and Maintenance

About This Chapter

This chapter describes the operation and maintenance of the NIP.

5.1 Configuration and Management

The NIP and NIP Manager provide a user-friendly Web Graphic User Interface (GUI)-based configuration and management interface.

5.2 System Maintenance

The NIP provides easy-to-use maintenance functions.

5.3 Security

The NIP provides multi-dimensional security mechanism to ensure the security of the operation and maintenance in network management.

5.1 Configuration and Management

The NIP and NIP Manager provide a user-friendly Web Graphic User Interface (GUI)-based configuration and management interface.

You can perform the separate or centralized configuration and management for the NIP through the embedded Web system of the NIP or the NIP Manager. You can configure all features and functions of the NIP and view statistics in the visualized management system.

You can log in to the NIP in following ways:

- Unencrypted

  The Web browser communicates with the NIP through HTTP.
- Encrypted

  The Web browser communicates with the NIP through Hypertext Transfer Protocol Secure (HTTPS) to secure user information.

  To log in to the embedded Web system of the NIP with encryption, you need to log in to the system without encryption in the first place to enable the HTTPS service and configure the port for the service.

By default, you can log in to the NIP Manager in the encrypted way, that is, the Web browser communicates with the NIP Manager through Hypertext Transfer Protocol Secure (HTTPS).

HTTP transfer data in plain text and the data is easy to be eavesdropped; whereas HTTPS establish an SSL tunnel between the client and the server to encrypt data to avoid eavesdropping.

5.2 System Maintenance

The NIP provides easy-to-use maintenance functions.

- System software upgrade

  Provides one-touch upgrade function.
- Threat prevention signature database, application control rule base, and virus database update.

  The NIP support scheduled and manual online update, local update, version rollback of the threat prevention signature database, application control rule base, and virus database, and restoring the threat prevention signature database and application control rule base to the factory default version.
- Configuration backup and recovery

  The current configuration file can be backed up to the device or exported to the administrator PC for recovery. In addition, the device can be restored to the default settings.
- Restoration of Web interface connection

  When the Web interface connection of the NIP is lost, you can log in to the NIP through the console port and restore the Web interface connection.
- Fault diagnosis

  The NIP provides the following functions for the administrator to diagnose faults across networks:
  - Detection through Ping and Tracert for network connectivity
  - Check and download of the diagnosis information, including the information about the running status and configurations of each module of the device
  - Channel diagnosis for the the check of the communication between the NIP and the NMS software or that between the NIP and the log host
  - Management of diagnosis files for the check of the causes for the anomalies and alarms generated on the ESP card

5.3 Security

The NIP provides multi-dimensional security mechanism to ensure the security of the operation and maintenance in network management.

- Hierarchical and domain based management for the NIP Manager administrator

  The NIP Manager implements hierarchical and domain based management by setting up various administrator groups. An administrator group is the combination of various permissions. The available permissions are different among administrator groups. If an administrator is allocated to an administrator group, the administrator obtains the permissions defined for the group. To log in to the system, the administrator must

provide a correct user name and password. After successfully logging in to the system, the administrator can perform operations with the assigned permissions.

- Administrative access control

  The NIP provides a dedicated out-of-band management port instead of using the service ports for management.

  In addition, the NIP supports the configuration of trusted hosts. Administrators can log in to the NIP only from trusted hosts within the specified IP address range. Otherwise, the access to the NIP and NIP Manager is denied.

  The communication between the NIP and NIP Manager or that between the NIP and a third-party NMS is implemented through security protocols.

  You can enable the services of the security protocols, such as HTTPS.

  You can disable the services of insecure protocols, such as HTTP and Telnet.

- Security logging

  The system can log important operations such as login and logout for auditing.

- Protection mechanism for the sensitive user information

  The system authenticates users through password and identity authentication, and protects the key user information through the strong encryption algorithm. Every user is allocated with a password for the verification before the system provides services for the user, protecting the security of user information. The NIP has only one **admin** user, whereas the NIP Manager has multiple administrators.

- Anti-brute-force mechanism

  Some unauthorized users attempt to hack into the system by conjecturing the administrator's user name and password. The NIP records the failed login attempts. If the number of failed login attempts reaches the upper limit, the system adds the IP address of the user to the isolation list and blocks the access from the user for a certain period of time.

- Automatic screen lock mechanism

  If the administrator does not perform any operations in the system, the Web-based management system automatically logs out the administrator to avoid the access from illegitimate users. The administrator must enter the user name and password again to log in to the Web system.

6 Technical Specifications

About This Chapter

This chapter describes the system specifications, environment requirements, and the standard and protocol compliance of the NIP.

6.1 System Specifications

This section describes the system specifications of the NIP.

6.2 Environment Requirements

This section describes the environment requirements of the NIP.

6.3 Compliant Standards and Protocols

This section describes the compliant standards and protocols of the NIP.

6.1 System Specifications

This section describes the system specifications of the NIP.

Table 6-1 System and chassis specifications of the NIP2050/2100/2130/2150/2200/5100/5200/5500 series (IPS device)

Item	NIP2050/2100/2130	NIP2150/2200	NIP5100	NIP5200	NIP5500
Expansion slot	Two FIC slots	Three FIC slots	Three FIC slots	Three FIC slots	Two FIC slots
Fixed interfaces	• One console port • One management interface (10/100/1000M	• One console port • One management interface (10/100/1000M	• One console port • One management interface (10/100/1000M	• One console port • One management interface (10/100/1000M	• One console port • One management interface (10/100/1000M

Item	NIP2050/2100/2130	NIP2150/2200	NIP5100	NIP5200	NIP5500
	auto-sensing electrical Ethernet interface) • Two USB 2.0 ports • Four 10/100/1000M auto-sensing electrical Ethernet interfaces • Four combo interfaces, which can be used as 10/100/1000M auto-sensing electrical Ethernet interfaces or hold 100M or 1000M optical transceivers to function as optical interfaces.	auto-sensing electrical Ethernet interface) • Two USB 2.0 ports • Four 10/100/1000M auto-sensing electrical Ethernet interfaces • Four combo interfaces, which can be used as 10/100/1000M auto-sensing electrical Ethernet interfaces or hold 100M or 1000M optical transceivers to function as optical interfaces.	auto-sensing electrical Ethernet interface) • Two USB 2.0 ports • Four 10/100/1000M auto-sensing electrical Ethernet interfaces • Four combo interfaces, which can be used as 10/100/1000M auto-sensing electrical Ethernet interfaces or hold 100M or 1000M optical transceivers to function as optical interfaces.	auto-sensing electrical Ethernet interface) • Two USB 2.0 ports • Four 10/100/1000M auto-sensing electrical Ethernet interfaces • Four combo interfaces, which can be used as 10/100/1000M auto-sensing electrical Ethernet interfaces or hold 100M or 1000M optical transceivers to function as optical interfaces.	auto-sensing electrical Ethernet interface) • Two USB 2.0 ports • Four 10/100/1000M auto-sensing electrical Ethernet interfaces • Four combo interfaces, which can be used as 10/100/1000M auto-sensing electrical Ethernet interfaces or hold 100M or 1000M optical transceivers to function as optical interfaces.
Dimensions (H x W x D)	43.6 mm x 442 mm x 560 mm	130.5 mm x 442 mm x 414.1 mm	130.5 mm x 442 mm x 414.1 mm	130.5 mm x 442 mm x 414.1 mm	130.5 mm x 442 mm x 414.1 mm
Weight (fully configured)	9 kg	18 kg	18 kg	18 kg	18.8 kg
NVRAM	512 KB	512 KB	512 KB	512 KB	512KB
Flash memory	64 MB	64 MB	64 MB	64 MB	64MB

Item	NIP2050/2100/2130	NIP2150/2200	NIP5100	NIP5200	NIP5500
CF card	2 GB	2 GB	2 GB	2 GB	2 GB
ESP card	0	NIP2150: 1 x ESP800 card NIP2200: 1 x ESP800 card or 1 x ESP710 card	1 x ESP801 card or 2 x ESP710 card	2 x ESP801 card	2 x ESP801 card
FPGA card	0	0	0	0	1 x FPGA card
Rated input voltage	AC: 100 to 240 V (50/60 Hz)	AC: 100 to 240 V (50/60 Hz)	AC: 100 to 240 V (50/60 Hz)	AC: 100 to 240 V (50/60 Hz) DC: -48 to -60 V	AC: 100 to 240 V (50/60 Hz) DC: -48 to -60 V
Maximum input voltage	AC: 90 to 264 V (47/63 Hz)	AC: 90 to 264 V (47/63 Hz)	AC: 90 to 264 V (47/63 Hz)	AC: 90 to 264 V (47/63 Hz) DC: -36 to -72 V	AC: 90 to 264 V (47/63 Hz) DC: -36 to -72 V
Maximum output power of the power supply	150 W	300 W	300 W	300 W	300 W

Table 6-2 System and chassis specifications of the NIP2050D/2100D/2130D/2150D/2200D/5100D/5200D/5500D series (IDS device)

Item	NIP2050D/2100D/2130D	NIP2150D/2200D	NIP5100D	NIP5200D	NIP5500D
Expansion slot	None	None	Three FIC slots	Three FIC slots	Two FIC slots
Fixed interfaces	• One console port • One management interface (10/100/1000M	• One console port • One management interface (10/100/1000M	• One console port • One management interface (10/100/1000M	• One console port • One management interface (10/100/1000M	• One console port • One management interface (10/100/1000M

Item	NIP2050D/2100D/2130D	NIP2150D/2200D	NIP5100D	NIP5200D	NIP5500D
	auto-sensing electrical Ethernet interface) • Two USB 2.0 ports • Four 10/100/1000M auto-sensing electrical Ethernet interfaces • Four combo interfaces, which can be used as 10/100/1000M auto-sensing electrical Ethernet interfaces or hold 100M or 1000M optical transceivers to function as optical interfaces.	auto-sensing electrical Ethernet interface) • Two USB 2.0 ports • Four 10/100/1000M auto-sensing electrical Ethernet interfaces • Four combo interfaces, which can be used as 10/100/1000M auto-sensing electrical Ethernet interfaces or hold 100M or 1000M optical transceivers to function as optical interfaces.	auto-sensing electrical Ethernet interface) • Two USB 2.0 ports • Four 10/100/1000M auto-sensing electrical Ethernet interfaces • Four combo interfaces, which can be used as 10/100/1000M auto-sensing electrical Ethernet interfaces or hold 100M or 1000M optical transceivers to function as optical interfaces.	auto-sensing electrical Ethernet interface) • Two USB 2.0 ports • Four 10/100/1000M auto-sensing electrical Ethernet interfaces • Four combo interfaces, which can be used as 10/100/1000M auto-sensing electrical Ethernet interfaces or hold 100M or 1000M optical transceivers to function as optical interfaces.	auto-sensing electrical Ethernet interface) • Two USB 2.0 ports • Four 10/100/1000M auto-sensing electrical Ethernet interfaces • Four combo interfaces, which can be used as 10/100/1000M auto-sensing electrical Ethernet interfaces or hold 100M or 1000M optical transceivers to function as optical interfaces.
Dimensions (H x W x D)	43.6 mm x 442 mm x 560 mm	43.6 mm x 442 mm x 560 mm	130.5 mm x 442 mm x 414.1 mm	130.5 mm x 442 mm x 414.1 mm	130.5 mm x 442 mm x 414.1 mm
Weight (fully configured)	8.2 kg	9 kg	18 kg	18 kg	18.8 kg
NVRAM	512 KB	512 KB	512 KB	512 KB	512 KB
Flash Memor	64 MB	64 MB	64 MB	64 MB	64 MB

Item	NIP2050D/2100D/2130D	NIP2150D/2200D	NIP5100D	NIP5200D	NIP5500D
y					
CF card	2 GB	2 GB	2 GB	2 GB	2 GB
ESP card	0	1 x ESP800 card	1 x ESP801 card	2 x ESP801 card	2 x ESP801 card
FPGA card	0	0	0	0	1 x FPGA card
Rated input voltage	AC: 100 to 240 V (50/60 Hz)	AC: 100 to 240 V (50/60 Hz)	AC: 100 to 240 V (50/60 Hz)	AC: 100 to 240 V (50/60 Hz) DC: -48 to -60 V	AC: 100 to 240 V (50/60 Hz) DC: -48 to -60 V
Maximum input voltage	AC: 90 to 264 V (47/63 Hz)	AC: 90 to 264 V (47/63 Hz)	AC: 90 to 264 V (47/63 Hz)	AC: 90 to 264 V (47/63 Hz) DC: -36 to -72 V	AC: 90 to 264 V (47/63 Hz) DC: -36 to -72 V
Maximum output power of the power supply	150 W	150 W	300 W	300 W	300 W

6.2 Environment Requirements

This section describes the environment requirements of the NIP.

Table 6-3 Environment requirements of the NIP

Item	Description
Atmospheric pressure	70 kPa to 106 kPa
Altitude	-60 m (- 197 ft.) to 1800 m (6000 ft.) at 50 ℃ 1800 m (6000 ft.) to 4000 m (13000 ft.) at 40 ℃
Working temperature	Long term: 0 ℃ to 40 ℃ Short term: -5 ℃ to 45 ℃
Working humidity	Long term: 10% RH to 85% RH (non-condensing) Short term: 5% RH to 95% RH (non-condensing)

Item	Description
Storage temperature	-40 ℃ to 70 ℃

6.3 Compliant Standards and Protocols

This section describes the compliant standards and protocols of the NIP.

Table 6-4 ETS standards

Standard	Description
ETS 300 019-2-2	Equipment Engineering; Environmental conditions and environmental tests for telecommunications equipment. part2-2: specification of environmental tests transportation
ETS 300 119-3	European telecommunication standard for equipment practice Part 3: Engineering requirements for miscellaneous racks and cabinets
EN 300 386 Version 1.2.1	Electromagnetic compatibility and Radio spectrum Matters (ERM); Telecommunication network equipment; ElectroMagnetic Compatibility (EMC) requirements

Table 6-5 IEC standards

Standard	Description
IEC 61000	Electromagnetic compatibility (EMC)
IEC 61000-4-2	Electromagnetic compatibility (EMC) - Part 4: Testing and measuring techniques - Section 2: Electrostatic discharge immunity test - Basic EMC publication
IEC 61000-4-3	Electromagnetic compatibility (EMC) - Part 4-3: Testing and measurement techniques; Radiated, radio-frequency, electromagnetic field immunity tes
IEC 61000-4-4	Electromagnetic compatibility (EMC) - Part 4: Testing and measuring techniques - Section 4: Electrical fast transient/burst immunity test - Basic EMC publication
IEC 61000-4-5	Electromagnetic compatibility (EMC) - Part 4: Testing and measurement techniques - Section 5: Surge immunity test
IEC 61000-4-6	Electromagnetic compatibility (EMC) - Part 4: Testing and measurement techniques - Section 6: Immunity to conducted disturbances, induced by radio-frequency fields
IEC 61000-3-2	Electromagnetic compatibility (EMC) - Part 3-2: Limits; Limits for harmonic current emissions (equipment input current <kleiner =>16 A per phase)

Standard	Description
IEC 61000-3-3	Electromagnetic compatibility (EMC) - Part 3: Limits; section 3: Limitation of voltage fluctuations and flicker in low-voltage supply systems for equipment with rated current <kleiner =>16 A
IEC 62151	Safety of equipment electrically connected to a telecommunication network

Table 6-6 ISO standards

Standard	Description
ISO/IEC 11801	Information technology - Generic cabling for customer premises
ISO/IEC 15802-2	Information technology - Telecommunications and information exchange between systems - Local and metropolitan area networks - Common specifications - Part 2: LAN/MAN management

Table 6-7 CISPR standards

Standard	Description
CISPR 22	Information technology equipment - Radio disturbance characteristics - Limits and methods of measurement

Table 6-8 ITU-T standards

Standard	Description
I.430	[I.430] Recommendation I.430 (11/95) - Basic user-network interface - Layer 1 specification
I.431	[I.431] Recommendation I.431 (03/93) - Primary rate user-network interface - Layer 1 specification

Table 6-9 IEEE standard

Standard	Description
IEEE802.3	Carrier sense multiple access with collision detection (CSMA/CD) access method and physical layer specification
IEEE802.3u	Media Access Control (MAC) parameters, physical Layer, medium attachment units, and repeater for 100 Mb/s operation, type 100Base-T

Standard	Description
IEEE802.1D	Media Access Control (MAC) Bridges
IEEE802.3af	DTE Power via MDI

Table 6-10 National standards

Standard	Description
YDN028-1997	SDH optical fiber system and device linear MSP — linear multiplex section, self-healing ring, and other types of structures
YDN 062-1997	Fault detection and location procedure for PDH channel, section, and transmission system, and SDH channel and multiplex section
GB/T 13543-92	Environmental test methods for digital communication equipment
GB 2421-89	Environmental testing for electric and electronic products-General requirements
GB 2423.1-89	Basic environmental testing procedures for electric and electronic products Tests A: Cold
GB 2423.2-89	Basic environmental testing procedures for electric and electronic products Tests B: Dry heat
GB/T 2423.3-93	Basic environmental testing procedures for electric and electronic products Test Ca: Damp heat, steady state
GB/T 2423.5-1995	Environmental testing for electric and electronic products-Part 2: Test methods Test Ea and guidance: Shock
GB/T 2423.6-1995	Environmental testing for electric and electronic products-Part 2: Test methods Test Eb and guidance: Bump
GB 2423.9-89	Environmental testing for electric and electronic products Part 2: Test methods Test Cb: Damp heat, steady state, primarily for equipment
GB/T 2423.10-1995	Environmental testing for electric and electronic products-Part 2: Test methods Test Fc and guidance: Vibration (Sinusoidal)
GB 2423.22-87	Basic environmental testing procedures for electric and electronic products — Test N: change of temperature
GB 2423.43-1995	Environmental testing for electric and electronic products — Part 2: Test methods — Mounting of components, equipment and other articles for dynamic tests including shock (Ea), bump (Eb), vibration (Fc and Fd) and steady-state acceleration (Ca) and guidance
GB2424.1-89	Basic environmental testing procedures for electric and electronic products — Guidance for high temperature and low temperature tests
GB/T2424.2-93	Basic environmental testing procedures for electric and electronic products — Guidance for damp heat tests

Standard	Description
GB2424.13-81	Electric and electronic products — Basic environmental test regulations for electricians — Guidelines for temperature variation tests
SJ2170-82-SJ2175-82	Basic test method for common electronic product transport package
SJ 3213-89-SJ 3215-89	Basic test method for common electronic product transport package
SJ/Z 3216-89	Electronic product protection, package, and packing level
GB 3873-83	General Technical Conditions for Communication Equipment Product Package
GB/T 4857.1-92	Marking methods for package, transport package tests
GB/T 14013-92	Mobile communication device — transport package
GB191-1990	Packaging-Pictorial markings for handling of goods
GB6388-1986	Transport package shipping mark
GB/T 13426-1992	Reliability Requirements and Test Methods for Digital Communication Equipment

7 Ordering Guide

About This Chapter

This chapter describes factors you must consider when ordering the NIP.

7.1 Chassis Ordering

The NIP2000/5000 series fall into IPS and IDS devices. A larger model number implies a higher performance. You are advised to purchase a proper model of the device according to the requirements on the performance and the deployment mode.

7.2 Interface Module Ordering

The interface modules of the NIP are separately ordered and delivered. Select the type and number of interface modules according to the networking scale and reliability requirements.

7.1 Chassis Ordering

The NIP2000/5000 series fall into IPS and IDS devices. A larger model number implies a higher performance. You are advised to purchase a proper model of the device according to the requirements on the performance and the deployment mode.

An IPS device distinguishes itself from an IDS device by the deployment location and function. The IPS device is deployed in in-line mode on the existing network and blocks the connections with attacks. However, the IDS device is deployed in off-line mode and analyzes and records the attack events for subsequent network assessment and auditing.

The IPS device can be deployed in off-line mode as well, and supports mixed deployment in in-line and off-line modes. Then one IPS device can provide the capabilities of both the IPS device and IDS device.

Table 7-1 and Table 7-2 show the number of flash memories, CF cards, FIC slots, and ESP cards of the models.

Table 7-1 Chassis ordering information of the IPS device

Model	Flash memory	CF card	FIC slot	ESP card	FPGA card
NIP2050/21	64 MB	2 GB	2	0	0

Model	Flash memory	CF card	FIC slot	ESP card	FPGA card
00/2130					
NIP2150	64MB	2GB	3	1 x ESP800 card	0
NIP2200	64 MB	2 GB	3	1 x ESP800 card or 1 x ESP710 card	0
NIP5100	64 MB	2 GB	3	1 x ESP801 card or 2 x ESP710 card	0
NIP5200	64 MB	2 GB	3	2 x ESP801 card	0
NIP5500	64 MB	2 GB	2	2 x ESP801 card	1 x FPGA card

Table 7-2 Chassis ordering information of the IDS device

Model	Flash memory	CF card	FIC slot	ESP card	FPGA card
NIP2050D/2100D/2130D	64 MB	2 GB	0	0	0
NIP2150D/2200D	64 MB	2 GB	0	1 x ESP800 card	0
NIP5100D	64 MB	2 GB	3	1 x ESP801 card	0
NIP5200D	64 MB	2 GB	3	2 x ESP801 card	0
NIP5500D	64 MB	2 GB	2	2 x ESP801 card	1 x FPGA card

7.2 Interface Module Ordering

The interface modules of the NIP are separately ordered and delivered. Select the type and number of interface modules according to the networking scale and reliability requirements.

In addition to the interface modules, electric/fiber cables must also be ordered according to the selected interface modules. For details, see Table 7-3-Table 7-7.

NOTE
The NIP2050D/2100D/2130D/2150D/2200D does not support the interface module ordering.

Table 7-3 Interface module ordering information of the NIP2050/2100/2130/2150/2200

Type	Name	Cable	Remarks
FIC	Eight-port GE electrical interface card	Ethernet cable	The cables are optional.
FIC	Eight-port GE optical interface card	Single-mode or multi-mode fiber cable	The fiber cables are optional and can be selected from the external cable installation suite.
FIC	Four-port GE electrical bypass interface card	Ethernet cable	The cables are optional.
FIC	Optical bypass interface card (single-mode or multi-mode)	Single-mode or multi-mode fiber cable	The fiber cables are optional and can be selected from the external cable installation suite.
SFP transceiver module	Multi-mode optical transceiver module	Multi-mode fiber cable	The fiber cables are optional and can be selected from the external cable installation suite.
SFP transceiver module	Single-mode optical transceiver module	Single-mode fiber cable	The fiber cables are optional and can be selected from the external cable installation suite.

Table 7-4 Interface module ordering information of the NIP5100/5200

Type	Name	Cable	Remarks
FIC	Eight-port GE electrical interface card	Ethernet cable	The cables are optional.
FIC	Eight-port GE optical interface card	Single-mode or multi-mode fiber cable	The fiber cables are optional and can be selected from the external cable installation suite.
FIC	Eight-port GE electrical interface and two-port 10 GE optical interface card	Ethernet cable, multi-mode or single-mode fiber cable	The cables are optional. The fiber cables are optional and can be selected from the external cable installation suite.
FIC	Two-port 10 GE optical interface card	Multi-mode or single-mode	The fiber cables are optional and can be

Type	Name	Cable	Remarks
		fiber cable	selected from the external cable installation suite.
FIC	Four-port GE electrical bypass interface card	Ethernet cable	The cables are optional.
FIC	Optical bypass interface card (single-mode or multi-mode)	Single-mode or multi-mode fiber cable	The fiber cables are optional and can be selected from the external cable installation suite.
SFP transceiver module	Multi-mode optical transceiver module	Multi-mode fiber cable	The fiber cables are optional and can be selected from the external cable installation suite.
SFP transceiver module	Single-mode optical transceiver module	Single-mode fiber cable	The fiber cables are optional and can be selected from the external cable installation suite.

Table 7-5 Interface module ordering information of the NIP5100D/5200D

Type	Name	Cable	Remarks
FIC	Eight-port GE electrical interface card	Ethernet cable	The cables are optional.
FIC	Eight-port GE optical interface card	Single-mode or multi-mode fiber cable	The fiber cables are optional and can be selected from the external cable installation suite.
FIC	Eight-port GE electrical interface and two-port 10 GE optical interface card	Ethernet cable, multi-mode or single-mode fiber cable	The cables are optional. The fiber cables are optional and can be selected from the external cable installation suite.
FIC	Two-port 10 GE optical interface card	Multi-mode or single-mode fiber cable	The fiber cables are optional and can be selected from the external cable installation suite.
SFP transceiver module	Multi-mode optical transceiver module	Multi-mode fiber cable	The fiber cables are optional and can be selected from the

Type	Name	Cable	Remarks
			external cable installation suite.
SFP transceiver module	Single-mode optical transceiver module	Single-mode fiber cable	The fiber cables are optional and can be selected from the external cable installation suite.

Table 7-6 Interface module ordering information of the NIP5500

Type	Name	Cable	Remarks
FIC	Eight-port GE electrical interface card	Ethernet cable	The cables are optional.
FIC	Eight-port GE optical interface card	Single-mode or multi-mode fiber cable	The fiber cables are optional and can be selected from the external cable installation suite.
FIC	Two-port 10 GE optical interface card	Multi-mode or single-mode fiber cable	The fiber cables are optional and can be selected from the external cable installation suite.
FIC	Four-port GE electrical bypass interface card	Ethernet cable	The cables are optional.
FIC	Optical bypass interface card (single-mode or multi-mode)	Single-mode or multi-mode fiber cable	The fiber cables are optional and can be selected from the external cable installation suite.
SFP transceiver module	Multi-mode optical transceiver module	Multi-mode fiber cable	The fiber cables are optional and can be selected from the external cable installation suite.
SFP transceiver module	Single-mode optical transceiver module	Single-mode fiber cable	The fiber cables are optional and can be selected from the external cable installation suite.

Table 7-7 Interface module ordering information of the NIP5500D

Type	Name	Cable	Remarks
FIC	Eight-port GE electrical interface card	Ethernet cable	The cables are optional.
FIC	Eight-port GE optical interface card	Single-mode or multi-mode fiber cable	The fiber cables are optional and can be selected from the external cable installation suite.
FIC	Two-port 10 GE optical interface card	Multi-mode or single-mode fiber cable	The fiber cables are optional and can be selected from the external cable installation suite.
SFP transceiver module	Multi-mode optical transceiver module	Multi-mode fiber cable	The fiber cables are optional and can be selected from the external cable installation suite.
SFP transceiver module	Single-mode optical transceiver module	Single-mode fiber cable	The fiber cables are optional and can be selected from the external cable installation suite.