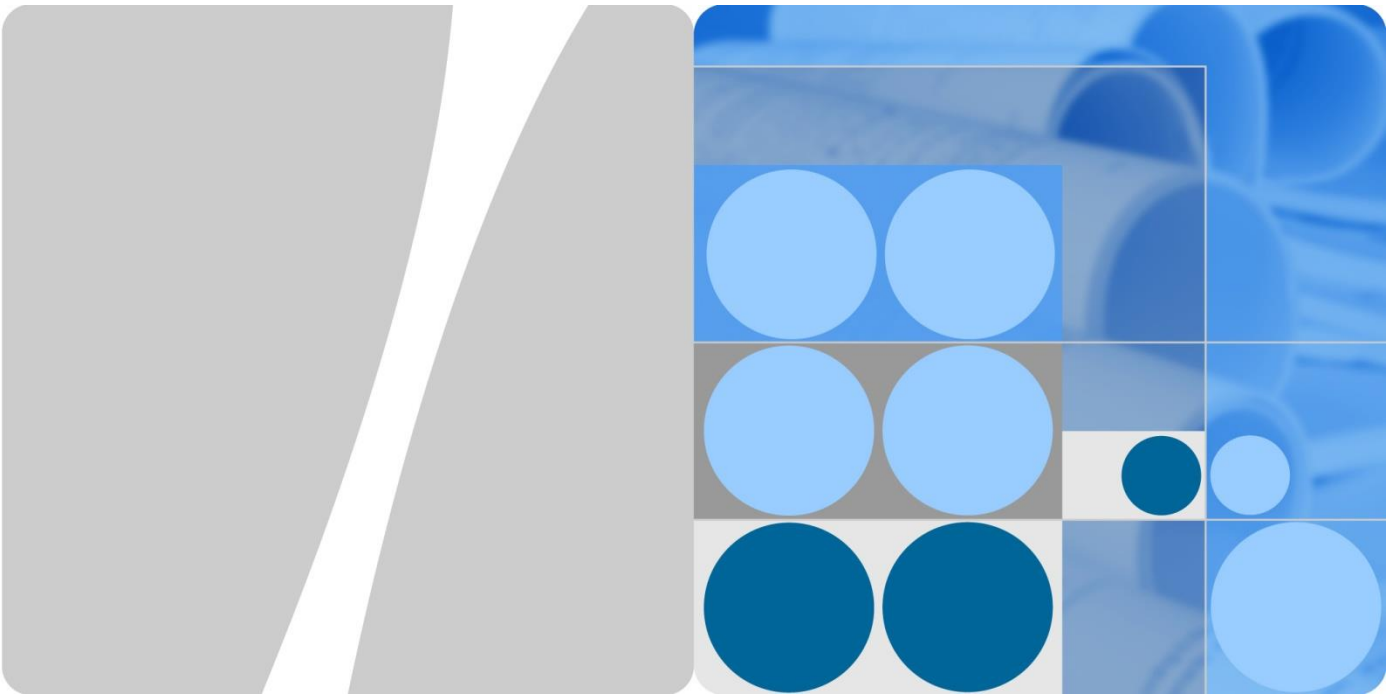


Huawei NIP6000 Intrusion Prevention & Detection System Technical White Paper

Issue 1.2

Date 2017-3-14

HUAWEI TECHNOLOGIES CO., LTD.

Trademarks and Permissions


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

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

Notice

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

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

Huawei Technologies Co., Ltd.

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

Website: http://enterprise.huawei.com

Email: ask_FW_MKT@huawei.com

Contents

1 Internet Security Trend 1

2 Customers Need More Advanced Intrusion Prevention Products 2

2.1 Disadvantages of Traditional Firewalls 2
2.2 Shortcomings of Traditional IPSs 2
2.3 Evaluating and Selecting IPS Products 4

3 NIP Technical Strengths 6

3.1 Advanced Application-Layer Threat Defense 6
3.1.1 Signature-based Threat Detection 6
3.1.2 User-Defined Threat Signature Detection 8
3.1.3 Real Protocol Identification 8
3.1.4 Precise Protocol Decoding Specifications 8
3.1.5 File-based Detection 9
3.1.6 Network Feature-based Pattern Matching 9
3.1.7 Correlation Analysis-based Detection 9
3.1.8 Protocol Anomaly-based Detection 9
3.1.9 Hardware Acceleration-based Detection 9
3.1.10 Web Attack Behavior-based Detection 10
3.1.11 Comprehensive Anti-Evasion Technology 10
3.1.12 User-Defined Signature 10
3.1.13 Signature Database Update 10
3.2 Powerful Anti-DDoS Capabilities 11
3.2.1 Excellent Necessary Capabilities for Defending Against DoS Attacks 11
3.2.2 Abundant Anti-DoS Measures 12
3.2.3 Defense Against Scanning and Sniffing Attacks 12
3.2.4 Malformed-Packet Attack Prevention 12
3.2.5 Application-Layer Anti-DDoS 12
3.2.6 Dynamic Traffic Baseline 13
3.3 Advanced Application Identification 13
3.3.1 Feature Identification Technology 14
3.3.2 Association Identification Technology 15
3.3.3 Behavior-based Identification Technology 15
3.3.4 Application Tracking and Analysis 15

3.4 Efficient Antivirus 16
3.4.1 PE Virus Detection 16
3.4.2 Immediate Coverage over Viruses 17
3.4.3 File Identification 17
3.4.4 Flow-based Virus Signature Matching 17
3.4.5 Flow-based Heuristic Virus Detection 19
3.4.6 Virus Exception 19
3.4.7 Virus Signature Database Update 19
3.5 Security Reputation 20
3.6 Fine-Grained Configuration of Unified Policies 20
3.7 IPv6 and Tunnel Detection 20
3.8 HTTPS Traffic Protection 21
3.9 Flexible Installation and Use 21
3.9.1 Plug-and-Play Installation 21
3.9.2 Flexible Update Modes 21
3.10 Layered High Availability 22
3.11 Comprehensive Maintenance and Management System 26
3.11.1 Diversified Management Methods 26
3.11.2 SNMP-based Terminal System Management 27
3.12 Comprehensive Log System 27
3.12.1 Local Log Storage 27
3.12.2 Log Server 27
3.12.3 Log Export Modes 28
3.12.4 Diversified Reports 28
4 Flexible Deployment 29
4.1 Comprehensive Border Protection for Enterprise Networks 29
4.2 IDS/IPS Hybrid Deployment 31
4.3 Deployment for Asymmetric Traffic 31
5 Conclusion 33

1 Internet Security Trend

With rapid growth of the Internet, enterprises and users have to face increasing threats.

On one hand, the software systems installed on servers become large in scale and complex in functions, inevitably resulting in the emergence of massive vulnerabilities. On the other hand, abundant computer techniques and tricks beyond thought are available on the Web for common users to expose and exploit the vulnerabilities on various software systems. Against this backdrop, even professional enterprises in the field of network security cannot provide comprehensive and effective solutions for network protection. The preceding factors and their combinations are accelerating the spread of security threats. The threats include illegitimate attacks, worms, viruses, Trojan horses and spyware as well as possible disclosure, tempering, and loss of secret information. Each of these threats would bring huge amount of economic loss to enterprises.

Emerging applications such as social networks, video streaming websites, and microblogs expose network users on the Internet accessible to almost everyone. In addition, a great number of vulnerabilities are exposed and exploited by attackers. Therefore, users also become the target of network attacks. By targeting at common network users, attackers obtain private information such as credit card numbers and private accounts for their own interests. These facts indicate that every server, including the ones that belong to enterprises and common users, will be adversely affected.

However, available network security products on the market still resolve network problems on the basis of the OSI model and ignore the emerging threats that focus on applications or even the content that are transmitted among them.

To defend against the traditional threats, users need an intrusion prevention system. But for emerging threats, users need more, especially a system capable of detecting the possible threats encoded in the content and transmitted among applications.

2 Customers Need More Advanced Intrusion Prevention Products

2.1 Disadvantages of Traditional Firewalls

Traditional firewalls are basic network security devices and play an important role in network security protection. However, they are vulnerable to new network security problems.

In most cases, they function as access control devices to permit traffic that matches security policies. Advanced firewalls detect the robustness of protocols and allow only valid traffic. However, new attack methods spring up and a large amount of attacks penetrate to the application layer or content layer. Traditional firewalls are impotent because these attacks seem to be secure on the network layer.

Due to the firewall positioning, the firewall architecture is designed for high-speed access control. Therefore, firewalls, even the most advanced stateful inspection firewalls, are defective in flexibility. Threats on the Internet change promptly. To deal with these threats, enterprises require an intrusion prevention product that can rapidly detect new threats in addition to firewalls.

2.2 Shortcomings of Traditional IPSs

Traditional IPSs enhance network security in certain aspects.

They can be deployed at the egress of an intranet or ahead of important servers to supplement firewalls, providing proactive and real-time defense. They can accurately identify suspect network traffic at Layer 2 to Layer 7 and block the traffic of various attacks, especially the threats targeting at the application layer, in real time.

An IPS provides defense as follows:

1. Captures network data packets.
2. Re-assembles the received packets at the network layer.
3. Re-assembles the packets (or traffic for TCP) at the transport layer.
4. Compares the patterns of captured packets and the signature database.
5. Takes actions for matched packets.

This type of IPS performs well when tackling the threats in network security in early years.

However, the situation is constantly changing and the traditional IPS becomes incapable of tackling emerging threats. The major causes of this are as follows:

False positive

The traditional IPSs are usually based on the intrusion detection systems (IDSs) and reuse their signature databases. This signature reuse, however, tends to cause false positives, as the IPSs differ from the IDSs in deployment and functionalities. To minimize false positives, the default policy of newly-deployed IPS only has a few signatures enabled, which can function to block a few threats. After correction of false positives, some signatures may have to be manually disabled.

In a complex IT environment, users and administrators demand more intelligent devices that help save their efforts. Specifically, they demand a plug-and-play product designed for security defense. Such an IPS enables all defense functions on a real network without impacting any applications.

Most IPSs cannot do this.

- **Less effective evasion prevention**

  According to a collection of known IPS manuals, even high-end IPSs can prevent evasion only by the following means:

  1 IP packet segmentation and TCP traffic segmentation

  2 Remote procedure call (RPC) packet fragmentation

  3 URL confusion

  4 FTP command evasion

  The traditional IPSs cannot defend against the emerging serious threats at all, though they may be functional with regard to evasion prevention.

  Most web threats target at HTTP applications, such as the top 10 web security threats listed by OWASP in 2010 and the top 10 web-based attacks. The traditional evasion prevention techniques do not function when dealing with these attacks. Attackers may easily evade detection using new methods.

  To provide effective evasion prevention, the traditional IPSs have to integrate many new evasion prevention techniques specific to the content in dissemination, including advanced URL confusion, HTTP Base64 coding, HTML arbitrary tag insertion, JavaScript confusion, HTTP chunked transmission, HTTP content compression, and HTTP header confusion.

- **Intranet traffic abuse**

  When the traditional IPSs were designed, there was no sign of P2P getting so popular that web applications are now an important part of Internet. For enterprises and organizations, traffic abuse by their staff becomes a major threat to their networks, which affects working efficiency and even brings risks of interruption to their services.

  A new IPS has to deal with external threats and traffic abuse, intentional or unintentional. Such a typical IPS has to visualize traffic and implement refined controls for each terminal user.

- **Threats from Web 2.0 and various client applications**

  Few IPSs are adaptive to web 2.0. Most traditional IPSs can detect only worms, spyware, and server software vulnerabilities. Some even pass traffic destined to clients without any check, by default. Most threats are hidden in such traffic, such as drive-by download, social engineering attack, and privacy theft.

  Noticing the rise of client threats, the well-known NSS and ICSA are focusing on client threat tests.

However, the traditional NIPs lack effective solutions to client threats in the Web 2.0 era, resulting in ineffective user protection.

- **Web application protection**

  The emerging Web 2.0 applications, such as virtualization applications, BBS, and social networking, appeal to massive users. Protecting these applications from being attacked by cybercriminals becomes the top priority. Without protection, massive users of such applications as Twitter or Facebook will become victims once these applications are under attack. In the April of 2011, Sony's PSN service was hit by a series of crippling attacks and the privacy data of tens of millions of users was stolen, including many credit card numbers. Not long after that, Sony's movie and music websites experienced SQL injection attacks. These attacks caused a huge loss of over hundred million US dollars.

  Timely patching is effective for the defense against traditional attacks. According to the statistics released by OWASP, SQL injection and cross-site scripting (XSS) become the most serious threats to Web applications.

  Most traditional IPSs are incapable of protecting web applications or weak in protection.

- **Emerging threats**

  Traditional IPSs detect and block vulnerability-specific attacks based on signatures. Signature-based attack detection is effective to known, long-term, and widely spread attacks. However, attackers now exploit social engineering to launch zero-day, botnet, and APT attacks. Vulnerability signature-based in-depth packet inspection used by traditional IPSs cannot effectively defend against emerging advanced attacks. Combination of signature-based attack detection with sandbox, event association, security reputation, and even big data analysis becomes the development trend of IPSs.

2.3 Evaluating and Selecting IPS Products

- **Applications that require protection**

  Before purchasing IPS products, determine the scenarios and applications that require protection. For example, determine whether servers need to be protected so that employees do not suffer from Internet attacks. After determining the scenario to be protected, determine the specific applications to be protected, for example, to protect the mail server and web server, or to prevent DDoS attacks. In addition, check the current traffic of the network to be protected and the possible increase of the traffic within the service life of the IPS products.

  After determining applications to be protected, evaluate an IPS product from the following aspects:

- **Engine capability**

  The engine must be application-aware and content-aware instead of just a modified Snort. You do not need to manually specify TCP ports for HTTP traffic, because an intelligent engine can identify applications and their contents.

  The engine can implement vulnerability-based signatures.

  The engine must be of high performance. Do not use the packet throughput to measure the performance of IPS products because the packet throughput cannot demonstrate the capability of handling abundant traffic content on live networks. The HTTP-based performance indicator is more useful to express the product performance than the packet throughput.

- **Signature database quality**

  Evaluate the quality of a signature database from the following aspects:

False positive rate

As traditional IDS products only listen to traffic in out-of-path mode, they slightly affect user networks. Therefore, their signature quality and detection efficiency are low. IPSs must be able to block attacks in real time, and therefore false positives greatly affect user services. Inheriting the knowledge base from traditional intrusion detection products, IPSs often have the signatures with high false positives disabled. Administrators may spend time on identifying such signatures, finding useful information from massive logs, or even repeatedly modifying device configurations. In a word, IPSs require high-quality signatures for accurate detection, which also reduces network maintenance costs.

Update frequency of the signature database

Query the update records on the update website. Generally, the signature database of an IPS is updated at least once a week because new vulnerabilities and patches are generated every week.

Research team

The research team of a vendor usually is assessed based on the public praise. For example, the security research team of Huawei is widely recognized because Huawei is leading in the network security field.

- **Usability**

  Usually, users are concerned about time and product maintenance cost. Therefore, a qualified IPS product is plug-and-play and easy to be deployed.

  Users require that the IPS be used immediately after deployment. No adjusting, commissioning, or complicated management software is required.

  In addition, how to identify effective attacks, help users adjust policy configurations, and reduce network maintenance costs are imported to users.

- **High availability**

  Except the duplicate power supply and BYPASS interface capability at the physical layer, users usually do not pay attention to the overall manufacturing performance and the quality system. Generally, IPS vendors do not develop hardware. They purchase the hardware from third-party vendors, where the quality system is uncontrollable. In this case, the quality of the IPS products is not guaranteed.

  In conclusion, vendors that can develop hardware and are familiar with the carrier-class reliability design are recommended. These vendors will not sacrifice the hardware reliability because of the high cost or incapability of hardware design.

3 NIP Technical Strengths

The Network Intelligent Protection (NIP) is a new IPS product that has basic functions of traditional IPS products and the capability of coping with new threats.

The intelligent attack defense system of the NIP falls into two product forms of intrusion detection system and intrusion prevention system. The intrusion prevention system can be deployed in-line to block attacks in real time. The intrusion detection system can be deployed off-line to detect network attack behaviors by receiving mirrored traffic. The intrusion detection system can also interwork with the network security device and send RST packets to block attack behaviors. In addition, with flexible interface deployment modes, the intrusion prevention system also applies to the usage scenario of the intrusion detection system.

3.1 Advanced Application-Layer Threat Defense

3.1.1 Signature-based Threat Detection

Signature-based threat detection mainly applies to vulnerability attack defense, web security protection, and malicious code defense.

- **Vulnerability attack defense**

  Vulnerabilities refer to security defects in systems. Defects in computer hardware, software, and protocol implementation or system security policies can be called vulnerabilities. Attackers may exploit vulnerabilities on device assets to access unauthorized files, obtain confidential information, or even execute programs.

  Zero-day vulnerability refers to the vulnerability information that has been obtained or exploited before the system provider is aware of the vulnerability and releases a related patch. This type of vulnerability information has not been widely spread. Most users are unaware of the vulnerability, and the vendor has not released the vulnerability fix. Hackers may exploit the vulnerability to launch attacks.

- **Web security protection**

  Web services are faced with the same security vulnerabilities as web application programs, such as SQL injection and XSS attacks. Unlike traditional web pages, web service programs are more open, incurring a lot of attacks specific to desktop client software. Moreover, web service programs often connect to enterprise core application programs and data. This characteristic significantly increases attack risks and makes web services an attractive attack target. Web services are running over HTTP and allow cross-website communications without requiring firewall reconfiguration. This

implementation threatens networks with traditional firewalls deployed, which cannot analyze web service communications transmitted over HTTP networks.

Attackers use HTTP or HTTPS applications to evade firewall detection and HTML evasion technologies to attack web security servers. Many insecure desktop programs are developed. There are more attacks specific to the ActiveX control and browser plug-ins/components/JavaScripts of desktop clients. Therefore, the security protection focus shifts from the service end to the client end. Hackers obtain the control permissions on web servers to tamper with web page contents or intercept sensitive data. They may even embed malicious code in web pages to infect more clients through Trojan horse-infected web pages. Hackers control the clients that access the infected web pages or even the computers of website employees to steal bank accounts and confidential information. Due to the simplicity of website Trojan horse making and the inevitability of website vulnerabilities, Trojan horse-infected web pages are the most popular website attack method used by hackers to spread Trojan horses.

- **Malicious code defense**

  A Botnet is a network where a controller infects many hosts with malicious Bot programs by various measures. The controller and zombie hosts form a 1-to-N control network.

  Bot is short for Robet, which can automatically execute pre-defined functions or controlled by pre-defined commands. Bot may not be malicious, but the Bot used on a botnet is defined with malicious purposes.

  Zombie indicates the host that is running with malicious Bot or other remote control programs.

  Command & Control Server refers to the IRC server that connects IRC Bot. The controller uses this server to deliver commands for control.

  Botnet is a network consisting of zombie hosts that have malicious Bot installed and controlled by hackers.

  Driven by huge economic interests, botnets are rapidly developed in recent years. Botnet structures become more complicated, and control means are more abundant and hidden. Botnet detection and control technologies are faced with great challenges.

  Trojan horse is an interception and control program that an attacker secretly installs on a victim computer. Trojan horse programs provide useful or interesting functions. However, they also have user-unknown functions, for example, copying files without notification or stealing passwords. One a PC is infected with a Trojan horse, important files and information may be stolen; user operations are closely monitored; and the computer may be controlled by the hacker to launch attacks on adjacent PCs.

  A worm is an independently running program without the intervention of PC users. A worm spreads by continuously obtaining the partial or whole control permission of the PCs with vulnerabilities on the network. The most significant difference between worms and viruses is that worms do not require human intervention and can continuously copy themselves and spread.

  Spyware installs backdoors and collects user information without user consent or awareness. It can:

  Weaken users' control over their use experience, privacy, and system security.

  Use users' system resources, including programs installed on their PCs.

  Collect, use, and disseminate users' personal or sensitive information.

  The NIP device uses the misuse detection model to consolidate intrusion signatures into a knowledge base and compare network data flows with signatures in the knowledge base to detect threats. This method features high detection efficiency, low false positive rate, and low detection costs. As this method relies on the accumulation of signatures, the

signature database must be continuously maintained, and unknown threats cannot be detected.

The NIP device analyzes vulnerability principles, extracts common signatures, and matches them with patterns to detect vulnerabilities. For web security protection, in addition to common system vulnerabilities, security protection for HTTP applications is more important. URL anti-evasion and HTML anti-confusion are required before pattern matching for HTTP application attack detection. The NIP device analyzes Trojan horses, worms, and botnets, extracts communication features, and identifies roles based on the features to discover threats.

3.1.2 User-Defined Threat Signature Detection

In practice, signatures are released some time after new attacks emerge. Users who are familiar with new attacks can define signatures to defend against such attacks.

3.1.3 Real Protocol Identification

To detect intrusions on and viruses in application-layer data and filter the data, we must first identify application-layer protocol types before providing protocol-specific suggestions. A common method is to use the default protocol port defined in RFCs to determine the protocol type, but this method is not accurate in some cases. The NIP device also checks the data packets to determine the protocol type.

For application-layer threat defense, the NIP device introduces real protocols. Protocol identification and threat scan happen at the same time. The advantage of this implementation is that the system can detect threats using unusual ports, for example, attacks using HTTP on port 3128. The IPS supports the identification and analysis of multiple protocol and file types. It can identify hundreds of real transmission protocols based on the SA service capability.

3.1.4 Precise Protocol Decoding Specifications

For accurate attack identification, the NIP device carries out in-depth application identification before protocol decoding and in-depth threat detection. The protocol decoding specifications are necessary for in-depth detection. They reduce signature matching calculation workloads, identify and process anti-evasion technologies, detect protocol anomaly attacks, and improve threat detection accuracy.

The NIP device supports the detailed decoding of about 100 protocol variable fields, including common protocol variable fields. The detailed decoding is on the basis of network attack research and analysis of protocol information in the signature database.

During protocol decoding, the system needs to normalize anti-evasion technologies, such as application protocol packet fragments, flow segments, RPC fragments, HTML confusion, URL confusion, and FTP-based Telnet code insertion.

Protocol decoding helps the system defend against protocol anomaly attacks. Hackers often exploit the less-perfect design of application servers (that is, vulnerabilities in inadequate consideration of protocol anomalies) to launch attacks. They send non-standard or overflowed protocol data to the servers to take control over the servers or break the servers down. The NIP device supports anomaly detection for multiple protocols. It performs in-depth protocol analysis of RFC violations, excessively long fields, unreasonable protocol interaction sequences, and parameters of abnormal application protocols to evaluate the severity, based on which it identifies potential intrusions targeted at application servers and clients.

Protocol anomaly detection covers more than 40 types of protocols, including HTTP, SMTP, FTP, POP3, IMAP, MSRPC, NETBIOS, SMB, TDS, TNS, TELNET, IRC, and DNS.

3.1.5 File-based Detection

The detection engine can detect file anomalies by considering files as protocols. Therefore, the NIP device can detect malicious files transmitted over the network. The NIP device can identify real file types (see file type filtering related services). File identification and threat scan happen at the same time. In this manner, the NIP device can detect threats even if hackers changed the file name extensions to evade detection. For example, the NIP device can detect attack.pdf even if the file name is changed to attack.txt.

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

3.1.6 Network Feature-based Pattern Matching

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

3.1.7 Correlation Analysis-based Detection

Single-packet network feature pattern matching may not accurately detect intrusion attacks and the spread of some botnets, Trojan horses, and worms. For accurate detection, one flow or even multiple packets of different flows must be correlatively analyzed. First, build a model for attack behavior to form multiple feature rules. Then, check the compliance of network traffic and attack behavior. The features can be the features of protocol fields, such as length, value, and content, the sequence of key positions in a protocol, number of times a feature appears, or a specific relationship among features. The comprehensive detection based on multiple feature rules makes the detection result more accurate.

3.1.8 Protocol Anomaly-based Detection

Protocol anomaly detection is a common intrusion detection means. Hackers often exploit the less-perfect design of application servers (that is, vulnerabilities in inadequate consideration of protocol anomalies) to launch attacks. They send non-standard or overflowed protocol data to the servers to take control over the servers or break the servers down.

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

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

3.1.9 Hardware Acceleration-based Detection

High detection precision and performance require the high-performance processor as well as high-speed multi-mode pattern matching engine and packet decompression engine. The NIP device adopts the MIPS64 processor provided by Cavium, the world-leading multi-core MIPS

and ARM processor provider. This processor provides a high-performance pattern matching engine and hardware decompression capabilities for compressed files such as in ZIP format. Therefore, IPS detection can be performed on ZIP files in high performance.

3.1.10 Web Attack Behavior-based Detection

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

3.1.11 Comprehensive Anti-Evasion Technology

Making use of network protocol complexity and TCP/IP openness, hackers may transform protocol traffic. As devices cannot identify the transformation cause, they should not simply discard transformed traffic (if the traffic is normally transformed, traffic discard will interrupt services) or permit it (if the traffic is transformed by a hacker, an attack occurs). To resolve this problem, the engine must be able to shape the traffic. For example:

1. Reassembly of IP fragments. The engine must cache and reassemble out-of-order fragments.
2. TCP traffic reassembly. The engine must maintain TCP status, process overlapped TCP segments, discard overlapped parts, and check TCP options.
3. RPC (DCERPC, SUNRPC) fragment reassembly and multiple request binding.
4. Normalized processing of URL insert characters, codes, and paths.
5. Processing of FTP insert characters
6. NetBIOS and SMB anti-evasion technology
7. HTTP anti-evasion technology

3.1.12 User-Defined Signature

In addition to predefined rules, the engine allows users to define signatures specific to common fields of common protocols, including HTTP, FTP, DNS, SMTP, POP3, IMAP, NETBIOS, SMB, DCERPC, SUNRPC, MYSQL, TNS, TDS, and FILE.

3.1.13 Signature Database Update

The IPS security team of Huawei closely traces the security bulletins of the renowned security organizations and software vendors, and analyzes and verifies the threats to generate the signature database that protects the software systems including operating systems, application programs, and databases. Additionally, an information collection system is deployed to capture the latest attacks, worms, and Trojan horses in real time, facilitating the generation of signatures and the discovery of threat trends. The system can obtain the latest signature in the shortest time to prevent attacks exploiting zero-day vulnerabilities.

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

- **Automatic and scheduled update**

  In this mode, the signature database is promptly updated without human intervention to defend against new threats. This mode applies to the devices that can connect to update servers. If the security of a downloaded signature database must be confirmed, the confirmation mechanism can be used. That is, the latest version is downloaded periodically but is not immediately applied. Instead, it is applied after being confirmed.

- **Real-time update**

  When a version is released but the automatic update time does not approach, you can update the signature database immediately. The advantage is high timeliness. You can know the update results immediately.

- **Local update**

  If the device cannot connect to the update server or the version must be rolled back to an earlier version, you can adopt local update to switch the version to a specific local version.

- **Version rollback**

  The software version can be rolled back to the previous normal version. If the false positive rate is high and the detection rate is low or there are other reasons, you can roll back the software version.

- **Context awareness-based event grading**

  Security events reported by the IPS may contain invalid attacks. The IPS detects threat events based on attack signatures in data packets. This detection method is not accurate every time. Hackers may succeed only when the protected system has the vulnerabilities that the hackers exploited. The validity cannot be determined merely based on the attack signatures in data packets. Therefore, it is difficult for administrators to grasp real threats from massive network attack logs.

  The NIP device addresses this problem. It can analyze the vulnerable environments that attacks targeted and score risk levels of attack events based on the OS, application, service, port, and vulnerability information about the attacked assets in real IT environments. It lowers the risk levels of the events that do not match asset environments. This information helps administrators adjust IPS policies, exempting the administrators from identifying valuable logs among massive logs. This implementation accurately identifies serious security events, improves security management efficiency, relieves administrators from heavy workloads, and reduces network maintenance costs.

3.2 Powerful Anti-DDoS Capabilities

3.2.1 Excellent Necessary Capabilities for Defending Against DoS Attacks

DoS attacks are common attacks over the Internet. During a DoS attack, an attacker sends various attack packets to devices to cause network breakdown or congestion. IP communication is connectionless. Taking advantage of this feature, attackers invent various attack means. Launching DoS attacks is extremely simple. For example, a PC and a packet sending tool are enough. Consequently, DoS attacks prevail the Internet and pose severe impacts on intranets and even backbone networks, causing serious network accidents. Therefore, an excellent anti-DoS capability is indispensable to intrusion prevention and detection systems.

Nearly all IPS devices in the industry claim to deliver anti-DoS functions, but network corruption events still continuously occur. An excellent anti-DoS system must have the following basic features:

Has rich attack defense means to defend against DoS attacks.

Has high processing performance. A DoS attack causes traffic bursts. Therefore, the system must have high traffic processing performance to defend against DoS attacks. Otherwise, the system is broken down by the attacks. Network breakdown is an important aim of DoS attacks.

Therefore, the network security device must have high traffic forwarding and processing capabilities. The number of new connections per second becomes an important index for network performance. During DoS attacks, attackers randomly change source addresses contained in sent packets. Therefore, all connections between the attackers and target devices are newly built.

Has an accurate attack identification capability. When processing DoS attacks, many IPS devices can only ensure that the traffic volume is within the acceptable range but cannot accurately identify attack packets. In this way, the servers are not broken down but packets sent by authorized users to go online may be denied. As a result, the devices cannot effectively defend against DoS attacks.

Huawei NIP series has taken all the above aspects into consideration, so it has prominent advantages over counterpart products in anti-DoS performance and features.

3.2.2 Abundant Anti-DoS Measures

Based on the features of data packets and specific DoS attack methods, the NIP device can defend against various DoS attacks, such as ICMP flood, SYN flood, CC, DNS attacks, and UDP flood. The NIP device identifies a dozen of common attack types, many among which may result in DoS attacks. The NIP device proactively detects and isolates these illegitimate attacks, and therefore prevents the intranet from being attacked. With these anti-DoS means, the NIP device constructs a secure defense system against DoS attacks.

It uses differentiated defense technologies for different attacks. Therefore, it provides dedicated DoS attack defense and delivers a comprehensive defense feature.

In addition to the consideration of attack means, the NIP device has enhanced its usability and network adaptability. It allows users to flexibly set the defense scope to a specific host or all hosts in a security zone.

3.2.3 Defense Against Scanning and Sniffing Attacks

Scanning and sniffing attacks identify active systems on a network by ping scanning, including ICMP and TCP scanning, to accurately locate targets. Then attackers can detect the monitored potential services and operating systems by scanning TCP and UDP ports. Through scanning and sniffing, attackers can learn about potential security vulnerabilities of and service types provided by the target system, preparing for further attacks.

Huawei NIP devices can flexibly and efficiently detect such scanning and sniffing packets through comparative analysis and therefore prevent the subsequent attacks. Scanning and sniffing attacks include address scanning, port scanning, IP source routing options, IP route record options, and network structure sniffing through Tracert.

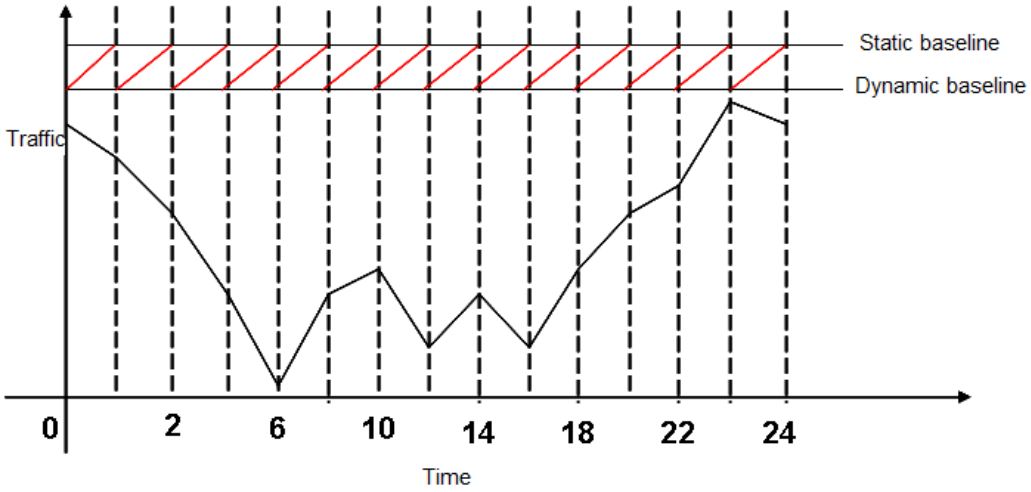
3.2.4 Malformed-Packet Attack Prevention

Huawei NIP devices defend against various attacks through abnormal packets, including Land, Smurf, Fraggle, WinNuke, ICMP redirect or unreachable packet, invalid TCP flag bits (for example, ACK, SYN, and FIN), Ping of Death, and Tear Drop.

3.2.5 Application-Layer Anti-DDoS

Huawei NIP devices can defend against DDoS attacks at the IP layer, transport layer, and application layer, including SIP-Flood, HTTP Flood, HTTPS Flood, DNS-Request Flood, and DNS-Reply Flood. Once a NIP device detects a DDoS attack, it enables the anti-DDoS function to block attack traffic.

3.2.6 Dynamic Traffic Baseline



DDoS attack detection provided by a traditional intrusion prevention product is actually traffic classification and statistics and then the comparison with preset thresholds. If the statistical result exceeds the threshold, the product considers that an anomaly occurs and takes a defense action. This method is based on a static baseline. The accuracy of attack detection depends on the reasonability of detection thresholds, which fully rely on the experience of configuration personnel.

The NIP device collects statistics on and compares the traffic by time. The detection threshold is specified based on the maximum value of the traffic within the learning period and tolerance (avoiding mistaken identification caused by sudden traffic jitter). When the traffic model changes, the device re-learns the traffic to obtain a proper detecting threshold.

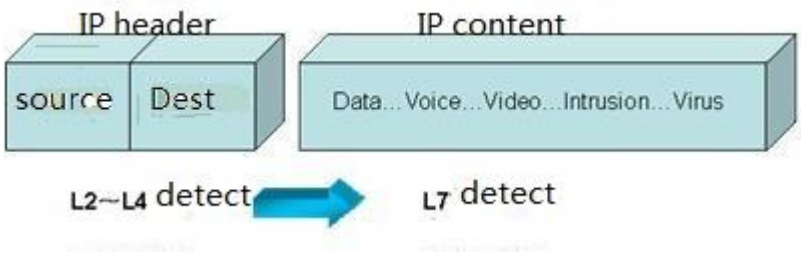
The dynamic traffic baseline helps improve detection and prevention accuracy and reduce deployment and use difficulties.

3.3 Advanced Application Identification

Traditional firewalls and IPS devices configure policies based on Layer-3 and Layer-4 information, such as IP addresses and ports. With the rapid development of Internet applications, an increasing number of IM, P2P, and online videos use port 80 for data transmission. Without the application identification capability, the firewalls and IPS devices cannot distinguish such applications from web browsing. In addition, many applications use dynamic ports, which frustrate the traditional firewalls and IPS devices.

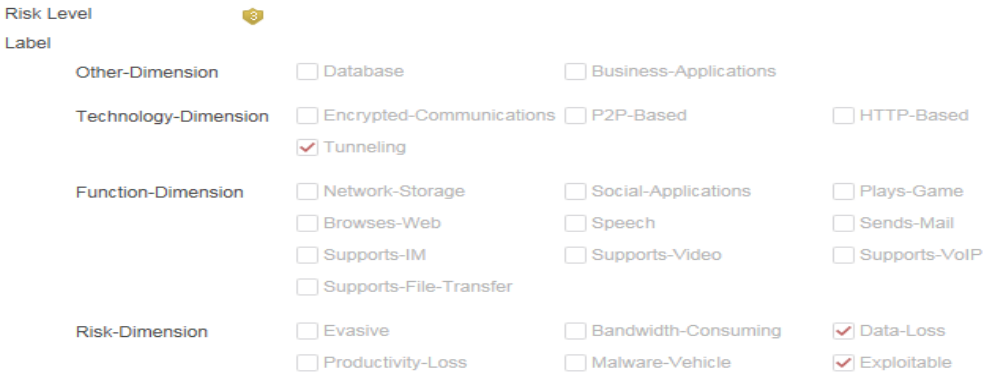
To resolve this problem, the Service Awareness (SA) function of the NIP6000 not only supports traditional packet detection and also application layer analysis to identify applications and the real services carried by the packets. Figure 3-1 shows the schematic diagram of the SA mechanism.

Figure 3-1 Schematic diagram of SA



The NIP6000 series provide application-specific policies. The SA function of the NIP6000 identifies the applications of packets based on the application-layer data of packets. Then the system configures policies based on the identified applications to prevent application identification failures caused by port reuse or dynamic ports.

Huawei SA can identify various applications, covering the common protocols and applications in China, Europe, Middle East, and Latin America regions. The identification rate and accuracy are especially high in identifying encrypted P2P, IM, and VoIP applications. Huawei SA sets several labels for each application so that customers can easily filter out the applications that compromise productivity and the applications that consume a large amount of network bandwidth. Customers can also sets a security risk level for each application based on these labels. Customers can filter applications based on the risk levels and labels.



3.3.1 Feature Identification Technology

Feature identification identifies protocols and applications based on the features of Layer-7 packet data, such as "GET" and "HTTP/1.1" features of HTTP packets, regardless of the ports being used. Huawei SA uses the layer-by-layer identification technology to identify layered applications and protocols. For example, Huawei SA can identify BT and MSN applications that use HTTP for data transmission.

Feature identification supports PCRE regular expressions to express complicated matching logic and employs a hardware acceleration engine for pattern matching to ensure high performance of SA.

Customers can customize applications and rules. The custom-made rules also support PCRE regular expressions. When new applications emerge or the applications are updated, causing signature changes, but the new signature data is not yet released, customers can define rules for complementary. In addition, user-defined rules can help customers to identify proprietary applications on enterprise networks.

With the rapid development of IPv6 networks, SA needs to support IPv6 networks. SA focuses on Layer-7 applications. Therefore, in general cases, the bottom-layer differences between IPv4 and IPv6 are transparent to SA. However, in specific scenarios, such as in IP address-involved operations like resolving addresses in the signaling channel of multi-channel protocols, operating association tables, and querying IP-domain name mapping tables, IPv4 and IPv6 addresses must be differentiated. Therefore, SA must support the operations specific to IPv6 addresses.

3.3.2 Association Identification Technology

Huawei NIP6000 identifies applications based on the association relationship between connections. For example, the FTP protocol has a control channel. The control channel can identify signatures of applications and create a temporary data channel during file transfer. The data channel does not have any characteristics and cannot be identified. However, when the data channel is created, the control channel will negotiate the IP address and port information of the data channel. SA can analyze such information and associate it with the source and destination addresses of the control channel, so that the data channel can be identified. Currently, the NIP6000 supports such multi-protocols as MSN, H323, SIP, MGCP, MEGACO, FTP, MMS, RTSP, GoogleTalk, and H245.

3.3.3 Behavior-based Identification Technology

Behavior-based identification is mainly used to identify the applications of encrypted traffic. For encrypted data, the pattern signatures are blurred and cannot be identified through feature identification. For some applications, the encryption starts from the first packet, and the applications cannot be distinguished based on the mapping relationships between control and data channels. Therefore, behavior-based identification requires more extensive information. Usually, the connection number of a single IP address, proportion of upstream and downstream traffic, datagram sending frequency, and packet length changes need to be analyzed. For example, for VoIP applications, the voice data packet length is usually stable, and the sending frequency is constant. For P2P applications, a single IP address may have a large number of connections; each connection has a different port number; and the shared file data is large in size but the size usually keeps the same.

With heuristic identification, Huawei SA can identify encrypted BT, eDonkey/eMule, and Thunder based on the multi-dimensional traffic characteristics and mapping relationships.

3.3.4 Application Tracking and Analysis

To identify the emerging new applications, the SA module must keep tracking the changes of applications, constantly focus on traffic changes, analyze unidentifiable updated applications and new applications in a timely manner, and update the signature database.

Huawei security intelligence center has an automatic application tracking system and a large number of professional application analysis engineers. The application tracking system can automatically track software releases, download and install the software, simulate the use of software, and identify traffic generated by the software. Once detecting any unidentifiable traffic, the system sends the captured traffic to the automatic signature extraction system. If the signatures cannot be extracted, professional technical engineers will manually extract signatures. Then the signatures are imported to the automatic verification system for verification.

The SA on Huawei devices can monitor network traffic changes. Once detecting any unidentifiable traffic, the device will notify the security intelligence center with customer consent. The security intelligence center then manually or automatically analyzes and extracts signatures from the unidentifiable traffic.

Huawei releases an SA signature database every month to update the signatures of changed applications and add new application signatures. The professional technical engineers provide 7x24 emergency response services.

3.4 Efficient Antivirus

According to ICSA statistics reports, 93% viruses come from email, 2% from Internet downloads, 1% spread by disks, and the other 4% from other means.

No doubts that email is the most frequently-used business communication tool in the world. Statistics show that over 50 billion email messages are sent every day in the world. However, some malicious people see this as a target for attacks.

Hackers use advanced means to open email attachment, including using double file name extensions, password-protected .zip files, and text spoofing. This is what people usually say, the social engineering for fraud. Users are tricked to perform the operations that they do not want to. These social engineering-based attack behaviors mainly include the behaviors called misleading applications and Badware. Common worms and viruses, such as ILOVEYOU worm and Klez virus, also exploit this for spreading. The recipient is lured to click the virus file by mistake. Then the virus file is executed. Common Trojan horse programs can live in drive programs. When users download the drive programs, the Trojan horses infect the user computers.

The intelligent attack defense system of the NIP6000 scans file viruses based on real file types, not on file name extensions. In this case, disguised attacks and viruses can be suppressed.

3.4.1 PE Virus Detection

According to statistics on virus file types, PE viruses take up a large proportion among all file type viruses. According to the network virus trend, PE file viruses are most destructive, whereas other types of viruses basically are used to assist the spreading of PE virus files. Specific virus functions and behavior are implemented by the PE file viruses.

In conclusion, if PE file viruses can be effectively prevented, network security conditions can be improved.

The antivirus function of the NIP6000 can detect popular PE file viruses on networks, including:

- Trojan
- Worm
- Backdoor
- Downloader
- Dropper
- Dialer
- Bot
- Clicker
- RootKit
- Adware
- Spyware

3.4.2 Immediate Coverage over Viruses

The antivirus function of the NIP6000 immediately covers popular viruses and updates virus signatures without compromising the high performance.

- Huawei cooperates with many security vendors and organizations around the world and can obtain the latest threat information promptly.
- Huawei virus analysis team studies new network vulnerabilities and new viruses, analyzes the latest threat data, and uses multiple types of threat analysis technologies to sum up the data and generate virus signatures.
- The new virus signatures are then released to the update center and distributed to live network devices.

The systematic threat analysis system ensures that the latest virus signature database that Huawei provides covers the latest, most popular, and most harmful viruses, so that the security status protected by live network devices can be improved.

3.4.3 File Identification

The antivirus function on gateway devices detects files transmitted over the network and must identify file data to identify network traffic. Huawei antivirus can identify mainstream network transmission and file sharing protocols, such as HTTP/HTTPS, FTP, SMTP, POP3, IMAP, SMB, and NFS, and decode these protocols to obtain file data. Then it identifies file types based on the file formats. Huawei antivirus can implement virus detection specific to PE files.

3.4.4 Flow-based Virus Signature Matching

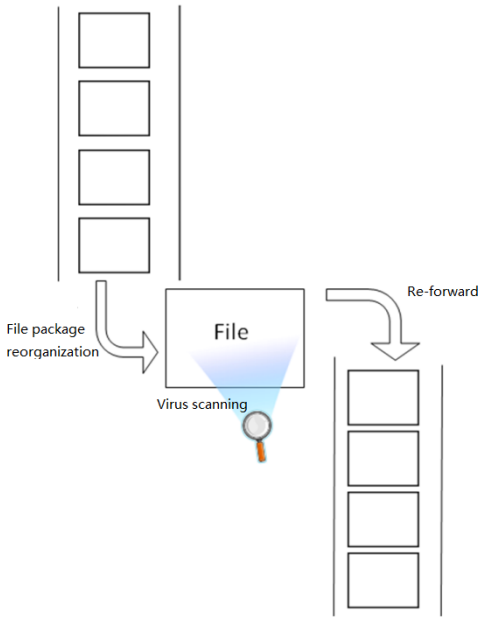
Currently, signature-based virus detection is implemented on complete files. Figure 3-2 shows the procedure. The detection engine first opens a file, extracts data from a specific position in the file based on signature description, and then compares the data with the signature.

To detect viruses on a gateway device, the gateway device must first reassemble the files sent in data packet format to a complete file.

First, the gateway device needs massive memory and CPU resources for file reassembly.

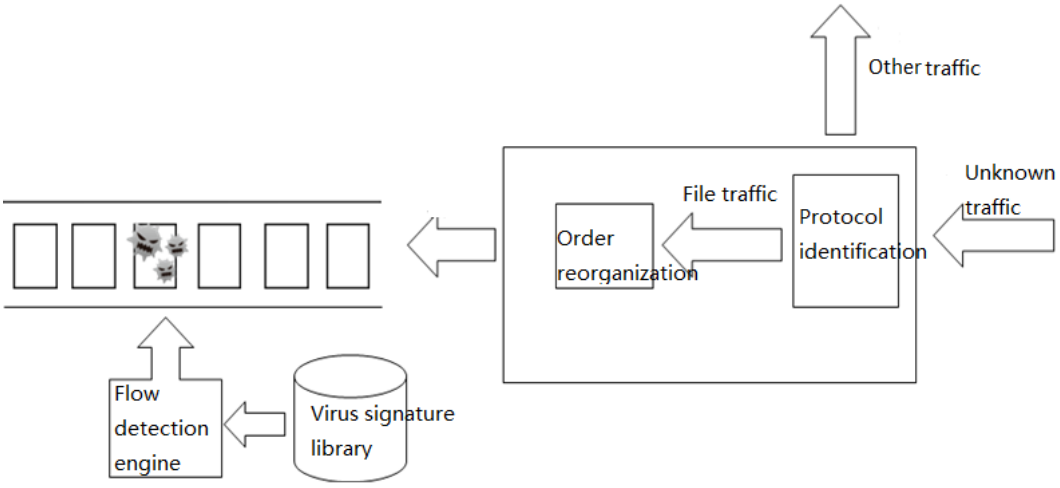
Second, each file must be reassembled, scanned, and resent on the gateway device, which greatly postpones the file transfer time, compromises the data throughput, and degrades user experience.

Figure 3-2 Schematic diagram of file-based virus scanning



The flow-based virus signature extraction technology developed by Huawei can resolve the preceding problems. With this technology, it is possible to detect viruses directly on network data packets. It helps the NIP6000 to obtain signatures from the data packets of virus files. When detecting network traffic for viruses, the NIP6000 identifies virus files if the packets match a virus signature. Compared with the traditional detection method, this technology does not compromise device performance because it does not require file reassembly or file resending. As a result, the detection performance is greatly improved. Figure 3-3 shows the flow-based antivirus scanning procedure.

Figure 3-3 Schematic diagram of flow-based virus scanning



Network devices employ protocol identification to identify the traffic of the file transfer protocols. The file traffic is reassembled based on the packet sequences corresponding to the file offset sequences. Then reassembled data packets are sent to the detection engine. The detection engine then matches the signatures of the data packets with the signatures in the

antivirus signature database. If the signatures of a data packet is the same as the signatures in the antivirus signature database, the file corresponding to the data packet is virus file, and the device will take a response action (block or alert) for the virus file data packet according to the customer's configuration. If the data packet does not match any signature in the antivirus signature database, the data packet will be forwarded towards the destination.

3.4.5 Flow-based Heuristic Virus Detection

Heuristic virus detection is developed on the basis of signature-based matching. Compared with the traditional signature-based virus detection technology, heuristic virus detection detects unknown viruses. This technology is the primary means against unknown threats currently. It comprises static and dynamic heuristic detection. Limited by the flow-based detection, Huawei antivirus supports only static heuristic detection. It analyzes tens of millions of malicious program samples, extracts the code logic of the malicious files, and completes threat modeling. During static file data analysis, if a virus file code logic is the same as the code logic of any modeling, the file can be identified as a virus file.

3.4.6 Virus Exception

To reduce virus detection false positives (which may prevents files from being transmitted to end users), Huawei antivirus provides the virus exception function. If a false positive is reported due to a detection rule, the customer can enter the detection rule ID to invalidate the detection rule, so that the file can be properly forwarded to the end user.

3.4.7 Virus Signature Database Update

The antivirus signature database is updated at least once every 24 hours. New virus signatures with the 24 hours are pushed to gateway devices in a timely manner, so that the gateway devices can promptly block detected new viruses.

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

- **Automatic and scheduled update**

  In this mode, the signature database is promptly updated without human intervention to defend against new threats. This mode applies to the devices that can connect to update servers. If the security of a downloaded signature database must be confirmed, the confirmation mechanism can be used. That is, the latest version is downloaded periodically but is not immediately applied. Instead, it is applied after being confirmed.

- **Real-time update**

  When a version is released but the automatic update time does not approach, you can update the signature database immediately. The advantage is high timeliness. You can know the update results immediately.

- **Local update**

  If the device cannot connect the update server, you can download the update package of the signature database from the update website and load the update package directly to the device.

- **Incremental update**

  Only incremental virus signatures are updated, so that you do not need to download the large antivirus signature database, which improves the update efficiency and decreases the bandwidth consumption during the update.

3.5 Security Reputation

Reputation-based security systems attract more attention in recent years. Reputation systems can evaluate the security status of dynamically changing entities. As an effective enhancement method of network security detection, reputation systems enable network security devices to block or filter out the connections to entities with bad reputation, which effectively improves the blocking accuracy, reduces false positives, and minimizes impact on service continuity.

The NIP6000 employs security technologies, such as IP reputation and C&C reputation, to monitor such attack behavior as junk email and botnet behavior and identify and filter out malicious traffic.

Based on the cloud security technology, Huawei NIP6000 detects global botnet variants and collects IP reputations globally to obtain the IP reputation and C&C reputation databases. The signature databases can be updated online or offline. The latest threat signatures can be updated and synchronized in real time to local devices.

3.6 Fine-Grained Configuration of Unified Policies

The NIP6000 supports not only 5-tupe-based security policies but also the security policies specific to such conditions as application, time, and location. The NIP6000 provides unified policies to integrate the preceding policy conditions. Policy unification is mainly reflected by the following aspects:

- Unified configuration page

  All policy conditions, including the 5-tupe, application, time, and location, can be configured in the same policy rule. A unified configuration page is provided, which facilitates policy configuration and maintenance.

  A policy rule can reference application-layer profiles, such as the IPS and antivirus profiles.

- Unified processing flow

  The NIP6000 provides a unified processing flow for the unified policies. For the functions of the same level, the NIP6000 scans and resolves packets only once and implements policy matching only once as well.

3.7 IPv6 and Tunnel Detection

With the rapid development of the Internet, the number of hosts on the Internet has being increasing exponentially, and new services emerge. Consequently, the Internet is thrown into a dilemma. Although temporary IPv4 addresses and network address translation (NAT) can alleviate the IPv4 address shortage, the address exhaustion problem is inevitable. IPv6 is the resolution to this problem. It greatly improves the address capacity, security, and network management and service qualities and is a core standard for next generation Internet protocols.

However, IPv4-to-IPv6 transition is a long-lasting process, and in a long time, IPv4 and IPv6 will coexist. Therefore, protecting IPv6 and IPv4-to-IPv6 transition network security has become the goal and challenge of next generation Internet security devices.

The NIP6000 supports dual-stack vulnerability protection and enables the defense against application-layer attacks and DDoS attacks on IPv6, IPv6 over IPv4, and IPv6-and-IPv4

hybrid networks. It applies to IPv6 networks and all networks in transition. Furthermore, the NIP6000 is also capable of analyzing and processing the traffic within VLAN 802.1Q, QINQ, MPLS, and GRE tunnels. Specifically, the NIP6000 identifies tunnel traffic and parses the encapsulated packets for security detection, which makes the NIP6000 compatible with complex network situations.

3.8 HTTPS Traffic Protection

With HTTPS traffic defense, the NIP6000 can decrypt HTTPS traffic for application-layer security.

With HTTPS traffic defense, the NIP6000 can decrypt the HTTPS traffic and perform security detection, such as intrusion prevention and antivirus.

Only proxied SSL traffic can be decrypted. The procedure is described as follows:

The NIP6000 intercepts the SSL negotiation requests from the client, works as a proxy server to negotiate with the client using its own certificate, and establishes an SSL tunnel with the client.

The NIP6000 initiates and establishes an SSL tunnel with the real server.

The NIP6000 transparently forwards data between the client and server. The USG decrypts the received traffic from one tunnel end, performs application-layer detection, and encrypts and forwards the inspected traffic.

3.9 Flexible Installation and Use

3.9.1 Plug-and-Play Installation

The NIP6000 provides default configurations upon delivery. It configures service interfaces as interface pairs by default and provides pre-defined policies. Customers need only to connect the interface pairs to the links 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.

The NIP6000 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, customers can create security policies on the web UI using the policy templates in a few minutes to accommodate special situations.

Each NIP6000 is shipped with the latest possible knowledge base and can start to work upon deployment without waiting for online update.

3.9.2 Flexible Update Modes

The NIP constantly updates the signature databases to obtain the latest detection capabilities and provides up-to-date protection for customer networks.

Since each customer may have different requirements on the IPS and customer networks are also different, the NIP6000 provides flexible update modes, including:

- **Online update**

  The NIP6000 connects to Huawei update server and downloads the latest update package. Online update can be implemented manually or automatically.

  In manual update, customers need to update the signature databases manually on the web UI. Usually, experienced network administrators hope to update the signature databases manually by themselves instead of waiting for the NIP to automatically connect to the update server.

  In automatic update, the customer can specify a time. Then the NIP6000 will automatically download the latest signature database to the NIP6000. The automatic update time can be set to a specified time every day or every week.

  If automatic online update is enabled, no manual prevention is required. The NIP6000 possesses the latest protection capabilities at all time.

- **Local update**

  If the customer does not allow the NIP6000 to directly connect to the update server or the network administrator does not want the NIP6000 to automatically connect to an external server, the local update mode can be used.

  In local update, the administrator needs to manually download the latest signature database file from the update website and then loads the file to the NIP6000.

3.10 Layered High Availability

- **Carrier-class hardware design**

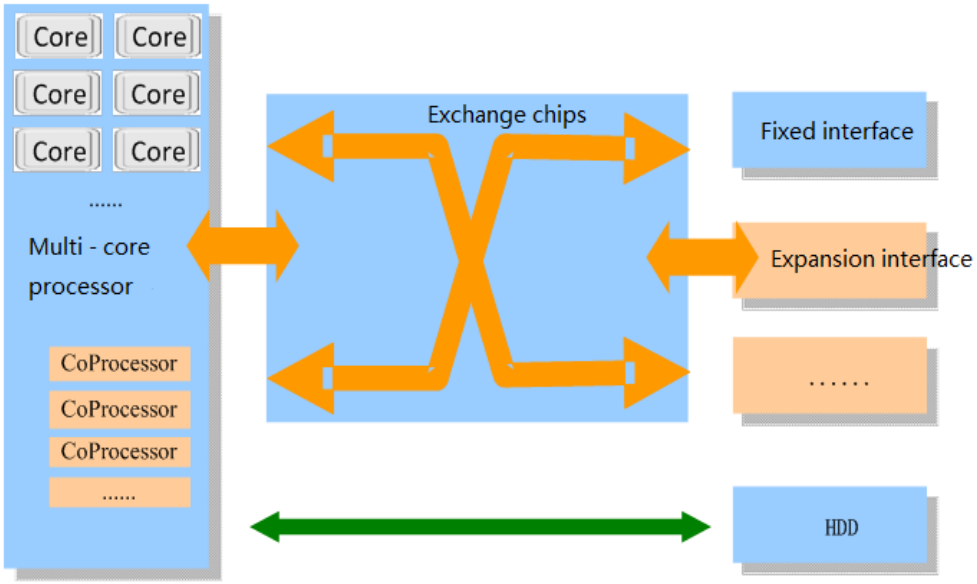
  With the ability to develop carrier-class hardware platforms, Huawei develops the reliable and stable NIP6000. The hardware and integrated design of the NIP6000 passed the strictest climate, environment, electrical, and mechanical tests, and all components are from suppliers with good quality assurance systems.

  The NIP6000 series provide dual power supplies to provide stable and reliable security protection for customers.

- **Huawei next generation security hardware platform**

  The next generation security (NG_Security) hardware platform is the hardware platform of all Huawei new generation high-performance security products. This platform, with a "Multi-core MIPS+Hardware co-processor acceleration+High-speed Switch Fabric" architecture, uses a high-speed bus to implement the communications between the multi-core CPU and the service processing and interface expansion modules. In addition, the redundancy design of this platform improves hardware reliability, enhances system performance and function expandability, and expands the storage, fulfilling the requirements for the local storage of logs generated by network security devices.

Figure 3-4 Huawei NG_Security hardware architecture



- **Multi-core MIPS CPU**

  Huawei NG_Security hardware platform uses a 64-bit multi-core MIPS architecture that has high performance and is based on the regularly encoded instruction set of a fixed length. The MIPS architecture provides streamlined instruction sets, hierarchical design of the instruction and high-speed data cache, concurrent multi-level flow lines, and dedicated high-speed interfaces and DMA capabilities for traffic throughput, and incorporates Huawei carrier-class embedded real-time operating system to ensure the high performance of the platform.

  In addition, the high-end model of this hardware platform has two CPU boards, which implements 1+1 CPU redundancy. Each CPU is a multi-core MIPS CPU, which doubles the processing capability of the hardware platform.

  The NIP6000 uses a new intelligent awareness engine (IAE) for threat detection. Traditional threat detection engine matches each packet to the threat signatures, which can easily lead to detection evasion. Instead of using the same method, the IAE reassembles packets based on sessions, decodes protocols, and matches the signatures, which detects threats more accurately. On the basis of the multi-core CPU architecture, the IAE resolves packets once for concurrent service processing during threat detection. The core application resolution and signature matching are completed by the hardware acceleration module. Each security service concurrently tracks the processing result and updates the status. If all threat signature conditions are matched, the IAE immediately takes the response action specified in the security policy. If some conditions are not matched, the IAE automatically adjusts the tracking status and ensure that secure traffic is rapidly forwarded. Such a architecture ensures that impact on the overall performance is minimized when multiple security services are enabled concurrently.

  The device uses the dedicated multi-core platform for multiple CPUs to process services concurrently. The hardware acceleration technology enables the IAE on application resolution and signature matching, greatly improves the detection efficiency.

- **High-speed bus**

  Huawei NG_Security hardware platform uses the switch fabric of 480 Gbit/s as the interconnection bus between the multi-core CPUs, service modules, and expandable interface modules. The high-speed switch fabric ensures sufficient bandwidth for service exchange among various modules.

- **Storage module**

  Huawei NG_Security hardware platform supports 300 GB high-speed SAS disk drives for the storage of real-time logs and reports.

  Dual disk drives can be configured as RAID1 for reliable data backup.

  Hard disk drives are hot swappable, which facilitates expansions and upgrades.

- **Scalability**

  The flexible hardware architecture ensures easy performance expansion by inserting various types of SPUs as required. The combination between the IAE and elastic hardware architecture ensures 10gigabit threat prevention performance and meets the security protection requirements of large enterprise data centers.

  The NIP provides multiple interface card slots, which support various types of interface cards, such as GE electrical/optical interface cards and 10GE interface cards. The administrators can expand the hardware forwarding capability and device performance by inserting appropriate interface cards into the slots.

  Hard disk drives are optional and can be configured as required.

  For the expandability, customers can determine the configuration as required at the deployment phase and expand the configuration as required by purchasing relevant modules, protecting existing investment.

- **High availability**

  The power supply modules work in 1 + 1 redundancy. The hard disk drives can be configured as RAID1. If one component fails, another component of the same function takes over the tasks assigned to the failed component, ensuring long-term no-fault hardware protection.

- **Fault detection**

  The system monitors the operating status of the entire chassis and key components on security SPUs and interface cards in real time and generates alarms when anomalies occur. Common alarms include fan module alarms, power module alarms, and overheat alarms.

- **Energy-saving and eco-friendly design**

  Dynamic power consumption management: The NIP6000 selects low-power consumption components and highly-efficient power supply module to effectively ensure low power consumption. The NIP6000 software implements dynamic power consumption control based on the chassis loads, enabled functions, interface connections, and device temperature. For example, the system software can be configured to disable unused interfaces and function units and implement independent speed control for the fan module.

  Intelligent heat-dissipation technology: The NIP6000 uses PWM speed control fan modules. The precise level-specific speed control and area-specific heat dissipation technology decreases the power consumption of the fan module by 70% when compared with the legacy heat-dissipation design, which reduces the power consumption and noises of the entire device.

  Environment-friendly manufacturing process: The manufacturing process of the NIP6000 strictly complies with environment laws and regulations, such as RoHS and WEEE and no toxic materials are used. The disassembly and recyclable design of the product ensures that 90% of the materials used in the manufacturing process are recyclable. The packaging design complies with the European directives (94/92/EC) on packaging and packaging waste. Environment-friendly and recyclable materials are used, and the types, quantities, and weights of the materials are under strict control.

- **Robust software system**

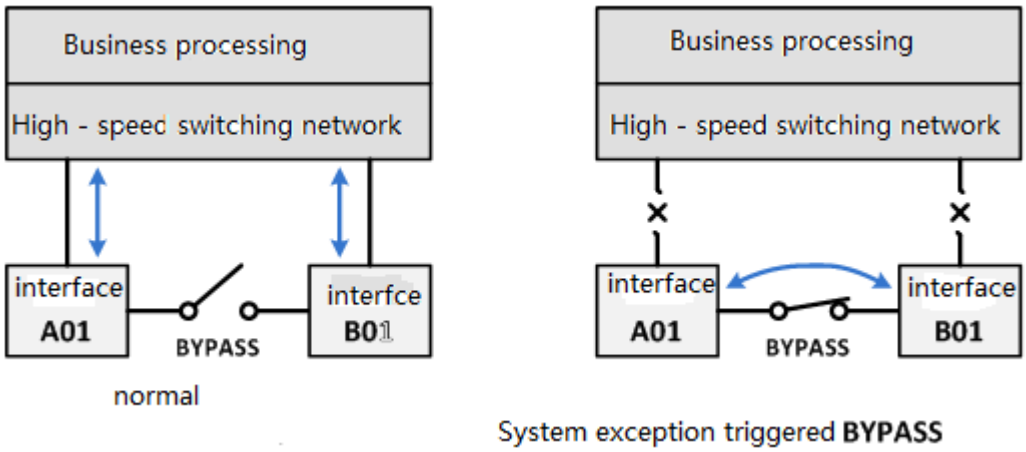
The NIP6000 uses Huawei-developed VRP operating system as the core component. Therefore, the NIP6000 itself can prevent various unreliable elements, such as the security vulnerabilities of universal operating systems and virus attacks.

The VRP operating system is a dedicated platform for data communications. Its software architecture is customized for data communications products and has taken the development of communications technologies into full account. The NIP6000 not only ensures reliable and secure operating, but can also be expanded for the further development of security technologies. All these factors endow the technology advance of the NIP6000 series.

- **Bypass interface card**

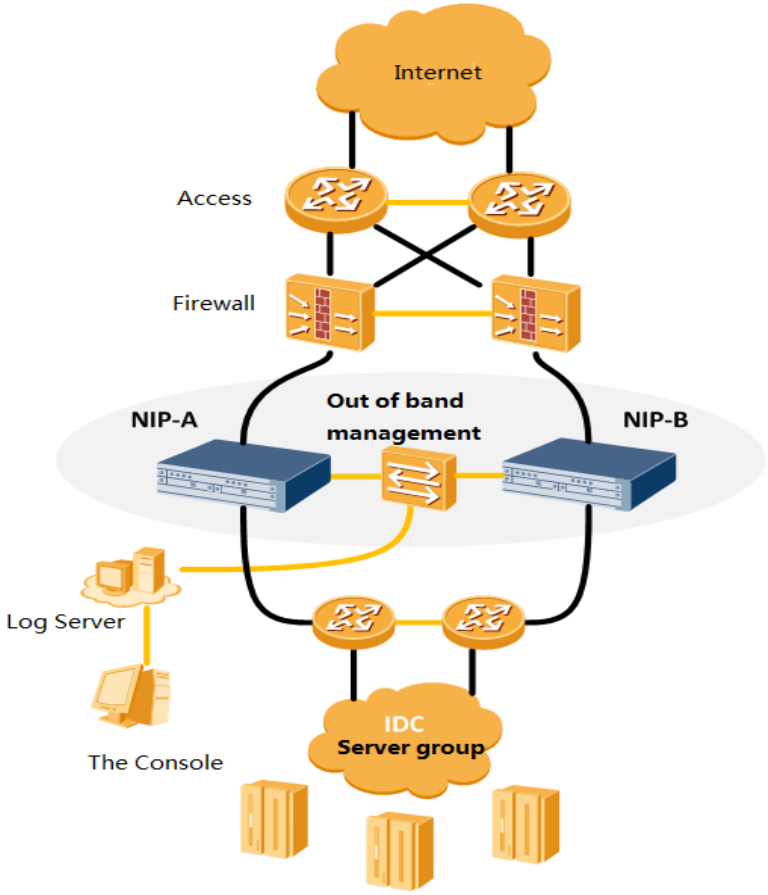
  To prevent service interruption caused by potential software processing anomalies, the NIP provides an electrical bypass card. This card can connect the egress network when the system works improperly (such as software anomaly or system shutdown) so that important services are not interrupted.

  The following figure illustrates the working mechanism of the bypass card. The bypass switch is actually a complex working logic. When an anomaly occurs, the bypass card automatically connects the two interfaces physically. The anomaly might be a software system anomaly, hardware fault, or device power-off.



- **HRP-based HA deployment**

  The NIP provides session- and configuration-based redundancy deployment capability and uses HRP for smooth active/standby switchover when the active device is faulty.



- **High self-security**

  The NIP6000 is highly secure in self-protection.

  Because the NIP6000 uses a dedicated hardware platform, its instruction sets, development tools, and techniques are not common and hard to obtain. Therefore, this system is difficult to be attacked by reverse engineering.

  For a security product, it is very dangerous if the source code is exposed. Therefore, the operating system and middleware module of the NIP uses Huawei-proprietary code instead of open-source code. As a result, the researches into and exploits of open-source code vulnerabilities have no impact on the NIP system.

  The NIP6000 implements security design and penetration test independent from function development during the concept, design, develop, and verification process, providing the highest-level of system security.

  During system running, communications between functional components are encrypted to prevent information leaks or anti-replay and man-in-the-middle attacks.

3.11 Comprehensive Maintenance and Management System

3.11.1 Diversified Management Methods

Huawei NIP6000 supports local and remote maintenance using the following methods:

- Local configuration and maintenance through the console port
- Local or remote operation and maintenance through Telnet
- Maintenance and management through Secure Shell (SSH). It provides information security guarantee and powerful authentication on an insecure network to defend against attacks, such as IP spoofing and plain-text password interception.
- Web- and secure Web-based GUI configuration and maintenance.

3.11.2 SNMP-based Terminal System Management

The NIP6000 supports SNMP (v1, v2c, and v3) and the client/server architecture, and can be managed through the NMS (for example, Huawei eSight).

3.12 Comprehensive Log System

The NIP6000 series collect statistics on the interface traffic and number of sessions during its operating to provide reference for the NMS, generate log information for other modules to make decisions, or deliver the information to customers for debugging use. Statistics collection can be configured flexibly. That is, the customers can define the parameters to collect the statistics that they are interested in.

The log information can be used to view device operating status, analyze network conditions, locate faults, and provide evidence for system diagnosis and maintenance.

System logs enable after-the-event audit. The NIP6000 logs various operations and attacks and provides the log query and filtering means to facilitate log search and analysis.

The generated log information can be displayed through the console port or Telnet. It can be saved in the device or output through the syslog protocol to a log server.

3.12.1 Local Log Storage

Huawei NIP supports plug-in hard disks. Logs generated in the system can be stored on the local hard disks.

When no log server is configured, you can use the local hard disks to store logs. If the hard disks are full, customers can determine whether to discard the latest logs or overwrite earlier logs with the latest ones.

Customers can also export log files on hard disks to prevent log loss.

3.12.2 Log Server

To receive and store the logs of routers, Huawei has launched dedicated log server software. Based on this software, users can conveniently browse, query, and analyze logs. The log server software comprises front-end management and back-end process based on functions. The front-end management supports database configuration, log configuration, log categorization and log query operations, and the back-end process comprises a log collection process and a log monitoring process. The log server software can receive user-defined types of logs and provides log storage, query, export, and backup functions.

3.12.3 Log Export Modes

The NIP6000 outputs syslogs or binary logs. The binary logs are a better choice when traffic load is heavy and massive logs are to be generated. Compared with syslogs, binary logs better suit the scenario in which log contents is massive and a higher network speed is required.

3.12.4 Diversified Reports

Huawei NIP6000 provides diversified reports based on log information for administrators to query. The administrators can customize reports to obtain only the data that they are interested in.

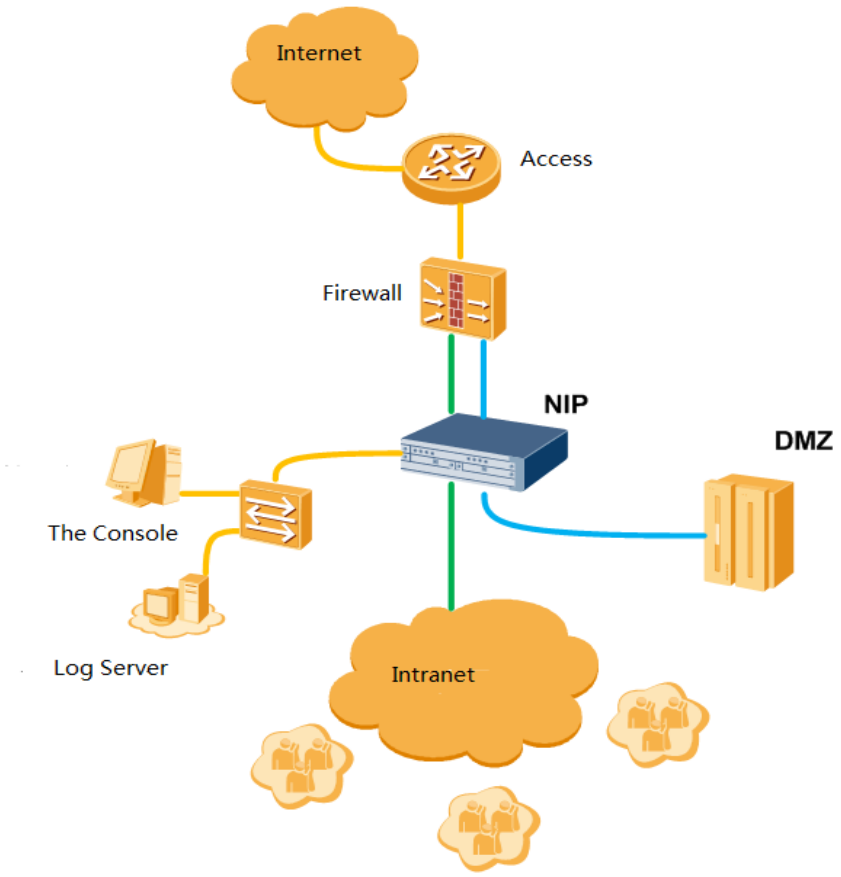
The reports can be sent to administrators in scheduled email.

4 Flexible Deployment

4.1 Comprehensive Border Protection for Enterprise Networks

The NIP6000 is deployed transparently at the Internet ingress of the enterprise network. It directly connects the enterprise network and the Internet access device. If a firewall has been deployed, the NIP6000 should be deployed behind the firewall (on the enterprise network).

The recommended deployment mode is to directly connect the two interface pairs on the NIP6000 to the intranet link and DMZ link to protect the enterprise network from Internet intrusions and the servers from attacks. As shown in the following figure, this access mode maximizes the functions of the NIP6000.



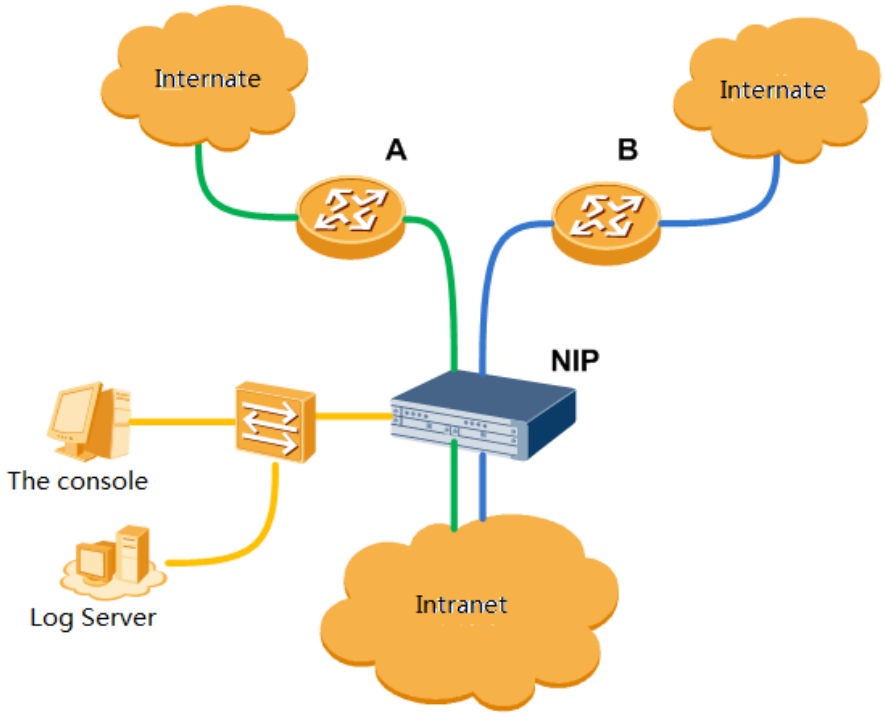
This deployment mode enables the NIP6000 to control the egress traffic and ensure that major services of the enterprise are properly forwarded. Controlled applications include P2P, video, IM, game, and stock applications.

The NIP6000 defends against worm activities and the exploits of browser and plug-in vulnerabilities to ensure the healthy operating of the enterprise network. In recent years, the exploits of browser and plug-in vulnerabilities have become the No.1 threat to office computer security. In about five to eight years ago, most intrusions are targeted on servers. According to the latest Internet security reports, an increasing number of intrusions and attacks directly point to clients, especially the browsers and plug-ins in Windows operating systems. The NIP6000 is capable of defending against such attacks to clients, protecting office computers, and preventing key data loss.

In DMZ protection, the NIP provides powerful virtual patching and anti-DDoS capabilities to improve server defense capability against external threats.

The file virus scanning and prevention function on the NIP6000 can scan email, files downloaded from the Internet, and files to be uploaded to web servers for viruses to prevent intranet servers and PCs from being infected.

Some enterprises have multiple links to connect to the Internet. In such cases, each link should be assigned a group of interface pairs, so that a NIP6000 can protect multiple links, maximizing customer investment. As shown in the following figure, the NIP6000 provides diversified interface pairs to protect each link. Based on the actual condition of the enterprise, each link may need a different security policy. In such cases, the administrator can customize a security policy for each link.

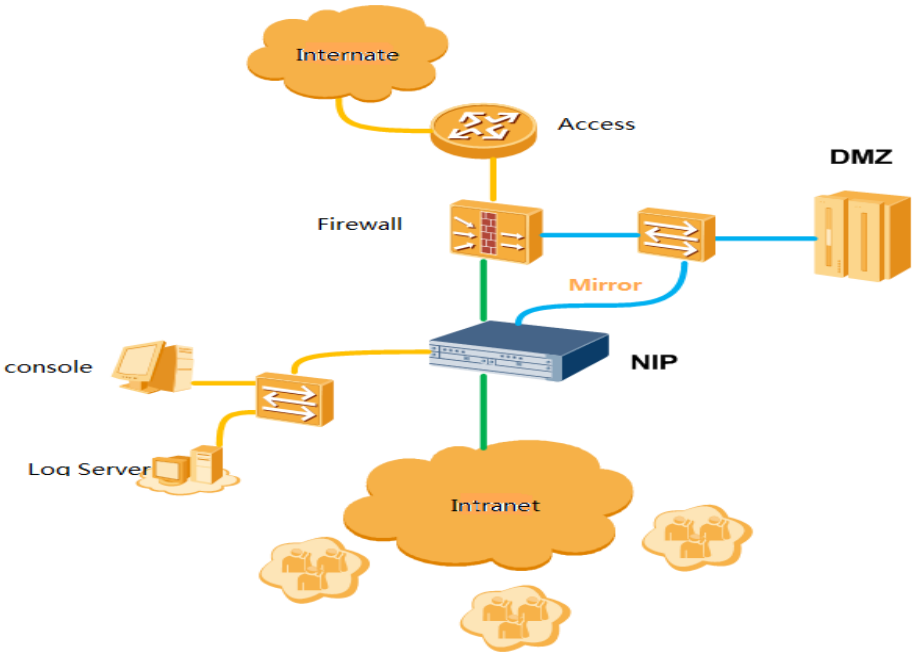


4.2 IDS/IPS Hybrid Deployment

The NIP6000 provides diversified interfaces and flexible working modes, so that one single NIP6000 can provide both IPS and IDS capabilities. Customers do not need to purchase separate IPS and IDS devices.

If customers do not want to deployment IPS in the DMZ, deploy the NIP6000 in IDS mode and use the switch mirroring port to copy the traffic through packet capture or optical splitter to the NIIP6000.

If the NIP6000 works in hybrid mode, the IDS and IPS interfaces are mutually exclusive.



4.3 Deployment for Asymmetric Traffic

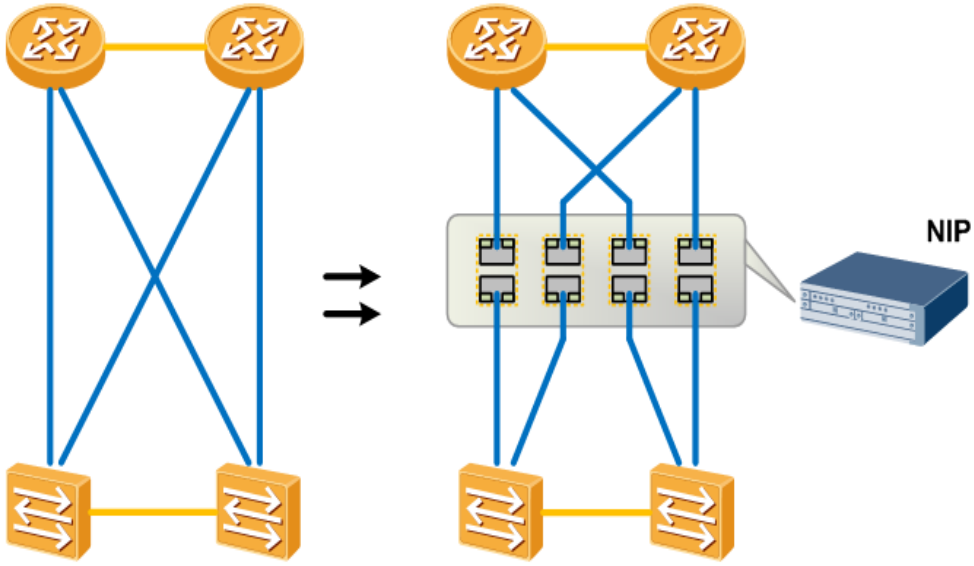
The NIP6000 provides intrusion prevention specific to application-layer protocol status. This is also called the stateful intrusion detection and prevention technology. This technology delivers high detection accuracy, but communication contents on both directions must be available to track protocol status changes for using the correct threat detection method. If only unidirectional traffic or some traffic is available, threat detection and prevention cannot be implemented.

On multiple data center networks, the forward and return traffic paths are different. Two links are provided for data transfer, but each link has only the packets in the forward or return direction. If you connect a common IPS device to one link or both links, the IPS device fails to detect threat and even causes network failures.

The NIP6000 resolves this problem using its interface pairs. You can connect the interface pairs to the links for transparent access and comprehensive detection.

Asymmetric traffic also occurs on high availability networks. The following figure illustrates how the NIP6000 uses its interface pairs for plug-and-play. You do not need to reconfigure the downstream and upstream devices after connecting the NIP6000. The traffic on the redundant

uplink and downlink is not mixed, and most importantly, the NIP6000 is capable of detecting and blocking network threats.



5 Conclusion

The rapid developing network technologies do not reduce network threats. Instead, new security vulnerabilities spring up, attack means become increasingly diversified, and the attacks bring more damages. Enterprise networks and IDCs are faced with unprecedented challenges. In the constantly changing smokeless Internet security war, traditional firewalls and IPS devices cannot effectively protect network security.

Against this background, the NIP6000 is developed. It is a next generation IPS device customized on the basis of the latest network threat posture to ease customers' pain points. The NIP6000 can not only cope with traditional attack means but also identify and block new threats coming along with new technologies and applications. Besides protecting enterprise IT assets from external attacks and intrusions, the NIP6000 helps enterprises maximize bandwidth efficiency, improve enterprise operation efficiency, and reduce network maintenance costs.

With the powerful IPS database, database of botnets, Trojan horses, and worms, antivirus signature database, security vulnerability database, and phishing website database, the NGFW integrates the remote detection capabilities accumulated by Huawei security competence center to enable the cloud security knowledge base update center to provide 24/7 pushing service and guarantee that the device can defend against latest security attacks, securing network users around the globe.