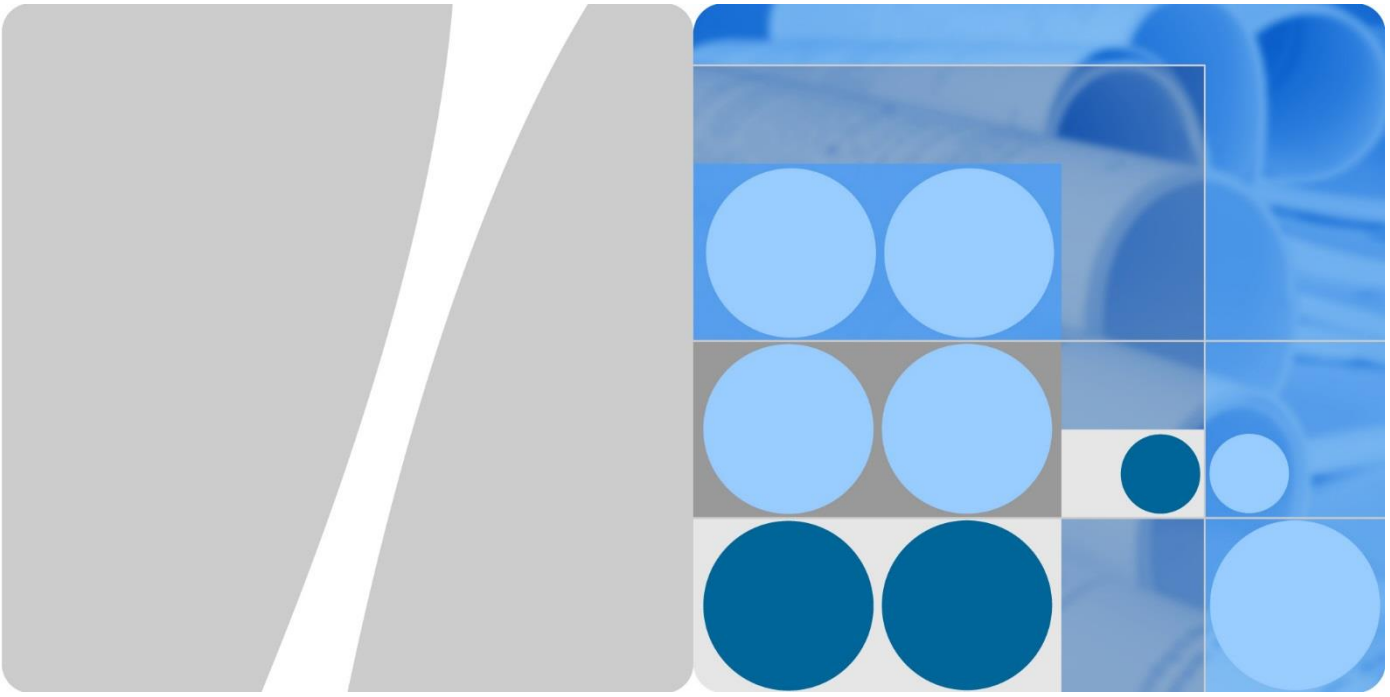


HUAWEI NIP6000 Intrusion Prevention & Detection System Technical Proposal

Issue 02

Date 2017-03-13

HUAWEI TECHNOLOGIES CO., LTD.

HUAWEI

Copyright © Huawei Technologies Co., Ltd. 2017. All rights reserved.

No part of this document may be reproduced or transmitted in any form or by any means without prior written consent of Huawei Technologies Co., Ltd.

Trademarks and Permissions


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

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

Notice

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

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

Huawei Technologies Co., Ltd.

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

Website: http://www.huawei.com

Email: support@huawei.com

About This Document

Change History

Date	Release	Description	Prepared By	Remarks
2014.07.30	V 1.0	First draft	Yan Feng/00381535	
2016.12.31	V 1.1	Updated	Wang Wei/00217251	

Copyright © Huawei Technologies Co., Ltd.

Contents

Copyright © Huawei Technologies Co., Ltd.

Copyright © Huawei Technologies Co., Ltd.

1 Overview

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, tampering, and loss of secret information. Each of these threats would bring significant economic losses 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 large number of vulnerabilities are exposed and exploited by attackers. Therefore, users also become the targets 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.

According to the Websense 2013 Threat Report, you can find the following key points:

Organizations of various kinds experienced a weekly average of 1719 attacks per 1000 users.

The number of malicious sites grew nearly 600% around the globe.

The number of malicious sites grew 720% in North America and 531% in Europe Union.

85% of malicious sites were found on legitimate web hosts.

Over 50% of web-connected malware became significantly bolder, downloading additional malicious executables within the first 60 seconds of infection.

Among all detected malware last year, 7.7% modified system registries to bypass behavior detection systems and anti-virus solutions.

Shortened web links are used across social media platforms to hide malicious content 32% of the time. Cybercriminals typically hide their own malicious pages deep in the directory tree of a legitimate site. This process generates very long and complex web links that might tip off a wary user. To disguise these long and malicious web links, cybercriminals make use of the

Copyright © Huawei Technologies Co., Ltd.

link shortening technologies that are designed for the convenience of information dissemination.

Global spam volume grew to 76% of all email, up from 74% in 2011 and reaching more than a quarter of a million emails sent per hour.

As the Websense's findings indicate, most web threats are gathering on Layer 7, application layer, and some, especially new threats, are even penetrating into the content of information in dissemination.

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

1.1 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.

Anti-evasion

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

Copyright © Huawei Technologies Co., Ltd.

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 anti-evasion.

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 anti-evasion techniques do not function when dealing with these attacks. Attackers may easily evade detection using new methods.

To provide effective anti-evasion, the traditional IPSs have to integrate many new anti-evasion 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 device 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 allow traffic destined to clients to pass 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 a 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.

Copyright © Huawei Technologies Co., Ltd.

1.2 Huawei NIP Overview

1.2.1 Function Overview

Huawei NIP has 10 models in two series as follows: The IPS series includes the NIP6320/6330/6610/6620/6650/6680, and the IDS series includes the NIP6320D /6330D /6620D/6650D.

These models provide the IPS/IDS, application control, anti-DDoS, antivirus, and IPv6 detection modules and meet most of the requirements in the IPS and IDS scenarios.

The NIP implements efficient detection of intrusions and defends against attacks that use worms, Trojan horses, spyware, and protocol exceptions; implements intrusion detection based on vulnerabilities and detects zero-day attacks; detects intrusions in web applications and web servers; provides flexible detection policies and timely updates of signature database; provides flexible response modes and detailed attack reports.

To implement the preceding functions, the NIP provides the following features:

- Virtual patch
- Client protection
- Intruded system monitoring and protection
- Web application protection
- Protocol anomaly detection
- Protocol awareness

Application control enables the identification of over 1000 applications, including P2P, instant messaging, games, and stock trade applications. Users can define their own protocol signatures and configure time-based or category-based application management policies. Furthermore, users can limit the bandwidth allocated to specific applications and restrict the use of certain applications with detailed logs.

Application control enables the NIP to identify and control the following categories of applications:

- P2P
- Instant messaging
- Cyber gaming
- Stock trade
- VoIP
- Video streaming
- Media streaming
- Email
- Data packets originated from mobile terminals
- Remote login

Anti-DDoS employs advanced identification and defense mechanisms to provide the blacklist and whitelist function, defend against DDoS attacks at the network layer, such as TCP and UDP floods, and defend against DDoS attacks at the application layer, such as HTTP- and DNS-based DDoS attacks. In addition, the NIP employs multiple advanced protection techniques to ensure efficient bandwidth use and protect servers from DDoS attacks.

The NIP provides anti-DDoS for the defense against the following types of DDoS attacks:

Copyright © Huawei Technologies Co., Ltd.

- TCP flood attacks
- TCP connection flood attacks
- UDP flood attacks
- ARP flood attacks
- Scanning attacks
- Malformed packet attacks
- ICMP-based DDoS attacks
- Tracert attacks
- Application-layer HTTP- and DNS-based DDoS attacks

Antivirus enables the scanning and removal of common files, compressed files, shell files, and email attachments transmitted over HTTP, SMTP, POP3, and FTP, notifies the concerned of identified viruses through email and web push, and provides regular and manual online update of virus signature database.

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 NIP is also capable of analyzing and processing the traffic within VLAN 802.1Q, MPLS, and GRE tunnels. Specifically, the NIP identifies tunnel traffic and parses the encapsulated packets for security detection, which makes the NIP compatible with complex network situations.

1.2.2 Deployment Mode

IPS series:

The IPS series can be easily deployed in in-line, off-line, and hybrid modes to implement application security and high network availability. These deployment modes are described as follows:

Deploying the NIP in in-line mode requires no change to the existing network topology. Because the NIP supports the interface pair function, the NIP implements security detection and timely response to network threats if the data links to be detected are connected to the NIP.

Deploying the NIP in off-line mode when network availability is critically important or gateway devices cannot be deployed on the existing network in serial mode. To implement intrusion detection when the NIP is deployed in off-line mode, you need to mirror the traffic to be detected to the NIP. In addition, you can configure certain policies so that the NIP can initiate TCP Reset packets through the IPS listening interface to block TCP connections.

Deploying the NIP in the hybrid mode means certain NIP interfaces are connected to the network in serial mode and certain NIP interfaces are connected to the network in parallel mode.

IDS series:

The IDS series can be deployed only in off-line mode. They receive and detect mirrored traffic after being connected to the mirroring ports of switches or routers.

The NIP provides flexible security policies and use different interface pairs to detect intrusions in traffic from different security domains. You can configure a maximum of seven security policies with one privileged policy. Security policies can be flexibly applied to

Copyright © Huawei Technologies Co., Ltd.

detection interfaces. You can create a security policy by making a copy of the default security policy and change certain parameters in the copy.

The NIP of the IDS series provides an independent management interface, whose IP address can be restored to the factory default. You can manage the NIP using the web UI or unified management platform.

1.2.3 Flexible Response Actions

The IPS series supports the following response actions: blocking, traffic control, blacklist, whitelist, interworking with other devices, packet capture, and alarm notification using email, sound, SNMP Trap messages, and logs.

The IDS series supports the following response actions: blocking TCP connection by initiating TCP Reset messages, interworking with other devices, and alarm notification using email, sound, SNMP Trap messages, and logs.

Copyright © Huawei Technologies Co., Ltd.

2 XX Enterprise Network Analysis

[Based on the communication with XX Enterprise, we have a thorough understanding and analysis of its network....]

2.1 Status Quo of XX Enterprise Network

[This section mainly consists of the following parts:

1. *Topology of XX enterprise network: In this section, analyze the improvements that can be made to the network. Check whether IPS/IDS devices are deployed at the ingress and egress of the network. If yes, check whether the capacity of these devices is sufficient and whether an upgrade is in need.*
2. *Services on XX enterprise network: In this section, analyze the necessity of the IPS/IDS devices based on the importance of the intranet services and services available at the network egress.*

2.2 Analysis of the Security Issues on the XX Enterprise Network

[This section mainly includes the following parts (based on analysis and communication with the customer):

1. *No IPS/IDS device is deployed on the network of XX enterprise. Currently, security devices on the network are …*
2. *Currently, attacks exploiting software vulnerabilities and the spread of worms, spyware, and adware are overwhelming on the network of XX enterprise.*
3. *The network of xx enterprise is lacking in effective security assurance measures: No security software is deployed for diversified application software and terminals on the network, no dedicated maintenance engineers, untimely updates of the signature database, …*
4. *Various threats: impact of worms, Trojan horses, and viruses on cyber security APPs…*
5. *The network egress may suffer from DDoS attacks.*
6. *No effective measures are available for the threats to the transition from IPv4 to IPv6.*

Copyright © Huawei Technologies Co., Ltd.

7. *No effective measures are available for the management of diversified network applications, such as P2P software, video streaming applications, online games, and IM software.*
8. *No effective measures are available for the audit of the security of intranet servers and key network segments of users.*

Copyright © Huawei Technologies Co., Ltd.

3 Network Security Design Principles

Based on XX enterprise's requirements and Huawei's experience in network security, the network security design of XX enterprise must comply with the following principles:

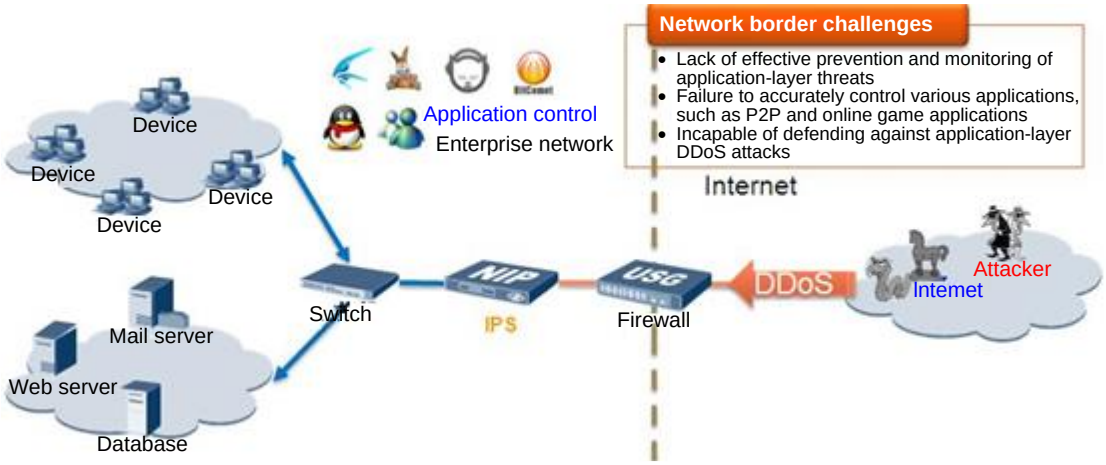
1. Advanced: Security devices on XX enterprise network must use dedicated hardware and secure professional software platforms, be in line with the industry technology development, and be leading in various fields.
2. Highly available: XX enterprise network is the basis for the informatization of the enterprise and therefore is of great vitality. Deployed at key nodes, security devices determine the network stability. The entire network design must take high availability into consideration.
3. Scalable: XX enterprise network continuously develops and expands. The entire network needs to be scalable, especially be able to support the creation and expansion of security zones on the basis of security.
4. Open and compatible: The security product design specifications of XX enterprise must comply with international and industrial standards and support various vendor products to effectively protect investment.
5. Minimal authorization: The security policy management of XX enterprise must comply with the minimal authorization principle. That is, hosts in various security zones can access only corresponding network resources, and network resources must be controlled to prevent unauthorized access and ensure information security.

Copyright © Huawei Technologies Co., Ltd.

4 Huawei Network Security Solutions

4.1 Network Egress Protection

Figure 4-1 NIP solution for enterprise network security

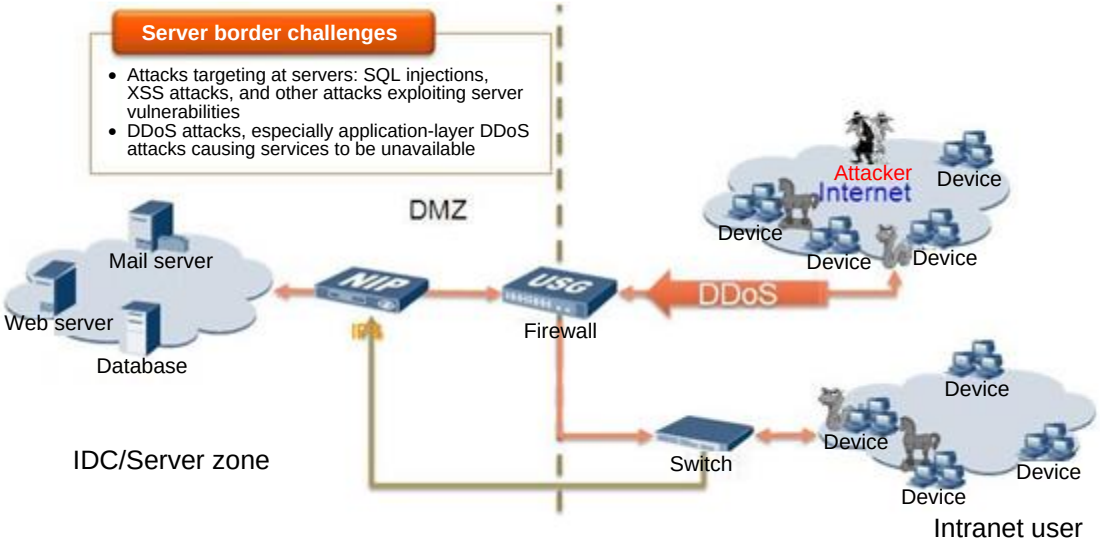


Major functions:

- Comprehensive application-layer attack defense for detecting and defending against the latest attacks
- Flexible application control policies for refined management of diversified applications on the network
- Advanced anti-DDoS capabilities for the protection of application servers from attacks
- Professional antivirus functions for the defense against the spread of viruses on the enterprise network
- Intrusion detection logs with handy query and sorting methods for the generation of detailed reports

Copyright © Huawei Technologies Co., Ltd.

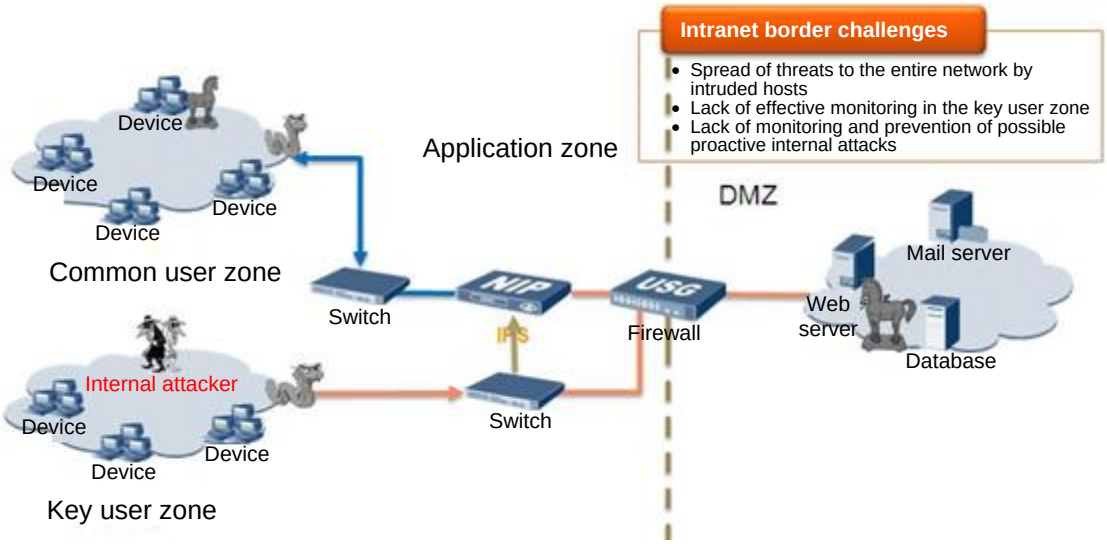
4.2 Server Border Protection



Major functions:

- Effective defense against the attacks exploiting server vulnerabilities
- Effective defense against SQL injections and XSS attacks
- Cleaning of DDoS traffic, especially application-layer DDoS attack traffic, destined for the servers
- Professional antivirus functions for the protection of the server from virus infections

4.3 Intranet Border Protection



Copyright © Huawei Technologies Co., Ltd.

Major functions:

- Automatic blocking of the spread of threats from intruded hosts and attacks initiated by them
- Clear records of the security status of key application zones for the generation of logs and reports
- Defense against DDoS attacks destined for the server zone

4.4 Applicable Security Devices

[State the application NIP models based on the actual network situation.]

Copyright © Huawei Technologies Co., Ltd.

5 Security Solution Features

[Describe the security solution with specific analysis on the security status of the network. If other security devices, such as firewalls and TSMs, are involved, perform the analysis by involving all security devices to be deployed on the network.]

5.1 Advantages of the Security Solution

[Based on the analysis of the existing network service flows and selected solutions, the advantages of XX enterprise network security solution are as follows:

1. *Network scalability: (Provide details based on the actual network situation.)*
2. *High availability: (Provide details based on the actual network situation.)*
3. *High security: (Provide details based on the actual network situation.)*
4. *High performance: (Provide details based on the actual network situation.)*

Copyright © Huawei Technologies Co., Ltd.

6 Huawei NIP Highlights

6.1 Product Features

The NIP is an IPS product 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.

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

Driven by economic benefits, new types of attacks emerge one after another, and threats change quickly. Whenever detecting a new vulnerability, Huawei releases the corresponding signature as soon as possible to defend against known and unknown attacks that exploit this vulnerability, implementing zero-day defense.

6.1.2 Extremely Low False Negatives, Ensuring Service Continuity

False negative is an important metric of IPS products. It represents the accuracy of signatures and the quality of a signature database. A false positive affects normal network services and shall be prevented.

6.1.3 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 policies to provide plug-and-play protection.

6.1.4 Separate Structure, Ensuring Flexibility and Performance

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

6.1.5 Powerful Application-Layer Anti-DDoS Capability for Normal Service Operating

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

Copyright © Huawei Technologies Co., Ltd.

6.1.6 Industry-Leading Application Recognition, Providing Control over Applications

The NIP uses Deep Packet Inspection (DPI) technology to analyze the traffic of different applications and the traffic directions. The DPI 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.

6.1.7 Advanced Virus Scanning Capability and Timely Signature Database Updates

The NIP employs multiple virus scanning and removal techniques to detect and delete traditional, compressed, shelled viruses and variations of PE and non-PE files, such as PDF and DOC files.

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

Driven by economic benefits, new types of attacks emerge one after another, and threats change quickly. Whenever detecting a new vulnerability, Huawei releases the corresponding signature as soon as possible to defend against known and unknown attacks that exploit this vulnerability, implementing zero-day defense.

The professional 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, the worldwide honeypot 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.

6.3 Extremely Low False Negatives, Ensuring Service Continuity

False negative is an important metric of IPS products. It represents the accuracy of signatures and the quality of a signature database. A false positive affects normal network services and shall be prevented.

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 samples, create signatures, and perform false negative tests to achieve near-zero false positive 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 without 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.

Copyright © Huawei Technologies Co., Ltd.

6.4 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 policies to provide plug-and-play protection.

With the growth of network and network devices, easy deployment and configuration are increasingly desired.

The service interfaces of the NIP operate at Layer 2 and the interfaces work in fixed pairs. The NIP can provide protection upon being connected on a network without parameter settings, delivering zero-configuration and plug-and-play protection.

6.5 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 inspection; Intel architecture (IA, or x86)-based devices are efficient in packet inspection, but slow in packet forwarding. IPS products must be efficient in both packet forwarding and inspection. Therefore, both ASIC-based and x86-based devices have performance bottleneck, either in packet inspection 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 inspection. The separate architecture provides both flexibility and performance, ensuring stable performances of the NIP in complex network environments.

6.6 Powerful Application-Layer Anti-DDoS Capability for Normal Service Operating

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

In early days, SYN floods are major traffic attacks. Nowadays, UDP and ICMP floods are most common large-traffic attacks. Another significant characteristic of DDoS attacks is that most DDoS attacks occur at the application layer. The most popular DDoS attacks aim at web and DNS services, especially DNS flood attacks, which lead to damage in a larger scope.

The NIP uses multi-layer cleaning technology to effectively defend against application-layer DDoS attacks, such as the DNS flood, HTTP flood, and HTTPS flood attacks.

Copyright © Huawei Technologies Co., Ltd.

6.7 Industry-Leading Application Recognition, Providing Control over Applications

The NIP uses Deep Packet Inspection (DPI) technology to analyze the traffic of different applications and the traffic directions. The DPI 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 DPI technology to perform in-depth packet inspection, recognize application-layer protocols, and control the traffic of specific types. The DPI knowledge base contains a wide range of protocol features. The NIP analyzes packets and compares the features against the DPI knowledge base to identify traffic of applications, such as games, stock transaction, P2P, IM, and VoIP and implement control policies accordingly.

6.8 Advanced Virus Scanning Capability and Timely Signature Database Updates

The NIP employs multiple virus scanning and removal techniques to detect and delete traditional, compressed, shelled viruses and variations of PE and non-PE files, such as PDF and DOC files.

The intelligent attack defense system of the NIP enables the identification of known and unknown threats based on file protection. The unpacking engine included in the antivirus engine helps unpack executable files and hundreds of shells. For repeatedly packed files, the unpacking engine can remove all the packed shells till the core threat is identified. Advanced hash techniques help scan hundreds and thousands of threats within a millisecond, locate and extract the files that include malicious logic, and generate a one-to-many antivirus library by comparing the hash segments obtained from the extracted files with the signatures in the database. Advanced algorithms enable the scanning of thousands of variations of Trojan horses within a millisecond. Advanced heuristic engine employs CPU simulation techniques to tempt malicious programs to become visible and use fuzzy definitions to identify known and unknown malicious variations. In addition to that, the dynamic proxy technique enables the NIP to forward unidentifiable files, audio and video files, blacklisted or whitelisted files, and oversized files at the adaptation layer for further detection, which ensures virus detection efficiency, reduces network latency, and improves user experience.

Copyright © Huawei Technologies Co., Ltd.

7 Huawei Service

7.1 Service Concepts

1. Customer-oriented services

   Focus on the requirements and experience of the customer, improve the awareness and skills of service, and protect the network running of the customer with superior services to meet the security requirements of the customer.

2. Sophisticated services

   Constantly optimize service contents and provide professional, standard, and diversified services. Attach importance to service initiative and service personalization, build an excellent service brand, and maintain leadership in the industry.

7.2 Description

No.	Service	Supports from Other Parties	Deliverable
1	Preparations	Learn about the network conditions from the customer.	
2	Onsite service	Assistant personnel	Service implementation application Service implementation summary report
3	Test	Assistant personnel	Test reports
4	Onsite training	Training venue and participants	Training summary report

7.3 Service System

Huawei has a three-tier service system for project implementation: the local office, technical support department, and R&D department.

Copyright © Huawei Technologies Co., Ltd.