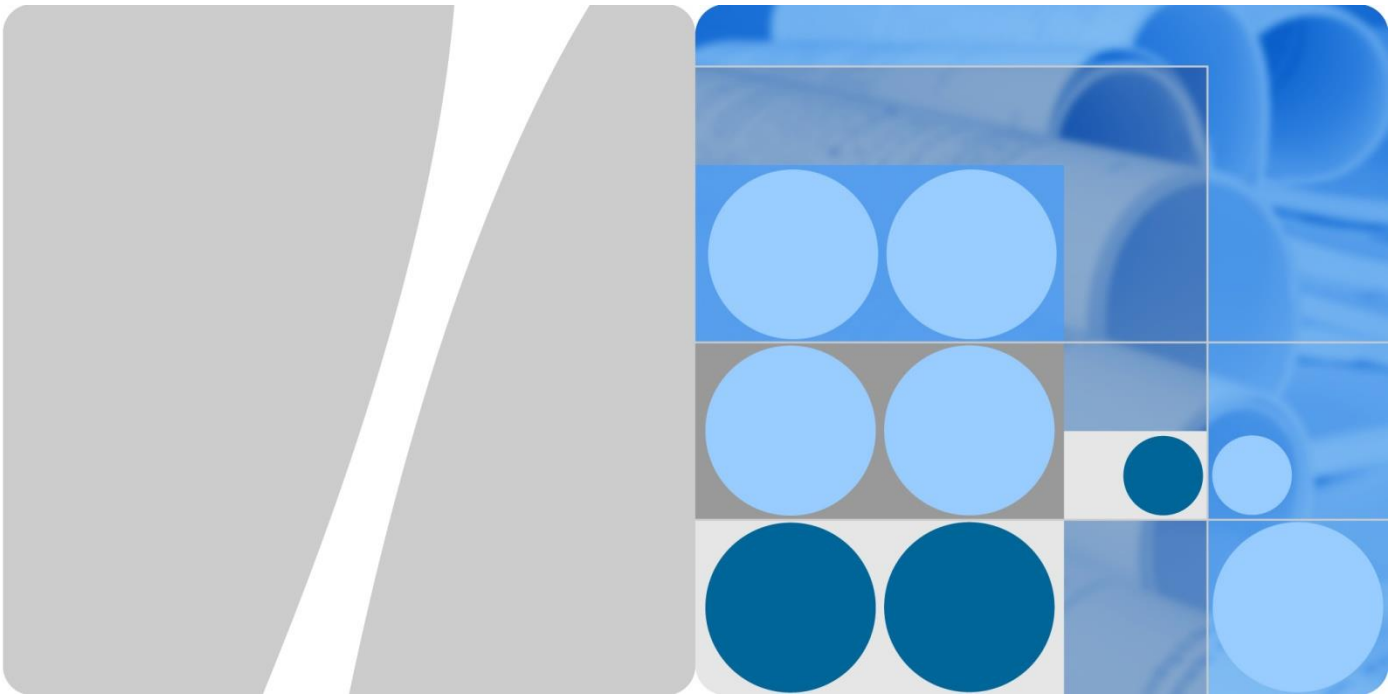


Huawei NIP6000
Feature Description

Issue 1.1

Date 2017-03-03

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

Contents

1 Basic Features 1
1.1 Application-Layer Intrusion Prevention 1
1.2 Application Control 3
1.3 Traffic Security 5
1.4 Network Deployment 14
1.5 System Management 20
1.6 System Security 22
1.7 High Availability 24
1.8 Network Bandwidth Management 27
2 Optional Features 30
2.1 File Virus Scanning 30

1 Basic Features

This document applies to NIP6000 V500R001.

1.1 Application-Layer Intrusion Prevention

Availability

This feature is introduced to the NIP since V500R001.

Summary

Intrusion prevention prevents attacks against application-layer vulnerabilities. Attack defense functions are as follows:

Content identification and parsing: provides content identification irrelevant to ports. The NIP accurately identifies protocols and file types, decodes and processes identified packets in a unified manner, and checks regulation compliance to detect protocol abnormalities.

Vulnerability-based attack detection: provides pre-defined signatures compiled based on vulnerability characteristics to prevent attacks taking advantage of vulnerabilities. In addition, the NIP supports user-defined signatures. Administrators can create user-defined signatures to prevent special attacks and block specific traffic.

Anti-evasive technique: In addition to basic IP fragment and TCP segment reassembly, the NIP provides various application-layer decoding techniques to prevent attacks from escaping detection by using IP fragments, TCP segments, and even advanced application-layer coding and decoding techniques.

Benefits

By detecting attack characteristics, the NIP prevents attacks against application-layer vulnerabilities, such as worms, Trojan horses, SQL injection, script attacks across stations, scanning, spyware, backdoor, and buffer overflow. The NIP brings the following benefits:

Effectively protects intranet servers and clients.

Implements zone-based attack isolation.

Provides flexible configuration. Detection policies vary according to traffic types.

Promptly updates the detecting engine and signature database in online or offline mode to deliver zero-day defense.

Provides attack event reports.

Description

Feature.Threat.01 Application-Layer Intrusion Prevention and Alarm

- Virtual patch

  The NIP provides advanced and vulnerability-based (not attack-based) pre-defined signatures. One vulnerability may develop into different attack means. Only vulnerability-based detection and prevention can detect and prevent attacks taking advantage of that vulnerability. The signatures are created in a generic way because the more generic the signatures, the more likely the NIP prevents future exploits or variants targeting at known vulnerabilities.

  Just as that a key of a specific pattern can unlock a lock of the same pattern, only the worms of specific signatures can attack exploits of the specific vulnerability. The NIP scans the network traffic against the signature to block all packets of the same signature. All attacks that target at the same vulnerability are prevented. Therefore, the signatures function as virtual patches to the system.

- User-defined signatures

  In addition to predefined signatures, the NIP supports user-defined signatures. You can define intrusion behaviors based on network traffic characteristics, such as protocols, severities, directions, and keywords. The keywords can be regular expressions.

  Only advanced users who are familiar with network knowledge are allowed to define signatures.

- Policy configurations

  The NIP provides default policies, which meet the requirements of most application scenarios. In addition, the NIP provides 10 default policy templates. You can select a policy template based on the scenario. If the predefined policies and templates do not meet requirements, you can define policies or modify the existing policies as required. The NIP provides fine-grained policy configuration. You can add signature sets with the same signature feature or add signatures one by one and configure a response mode for each signature.

  You can also associate a policy with a specific source IP address, destination IP address, service port, or VLAN for intrusion detection and prevention.

  The NIP can take the following actions against detected intrusions: prompt on the web page, syslog, log, SNMP trap, SMS alarm, audible alarm, firewall association, IP address isolation, attack packet discarding, and session blocking. You can set an action for a signature set or signature. Only IPS interfaces on IPS devices support IP address

isolation and attack packet discarding. IDS interfaces and devices support only simple session blocking.

The NIP supports log unification to avoid log storms. You can set log unification conditions.

Feature.Threat.02 Intrusion Prevention Signature Database Update

The IPS signature database describes the characters of viruses, worms, Trojan horses, and spyware. The NIP inspects the packets to find out whether they match a signature to prevent intrusions. Signatures are predefined or user-defined. The signature database is a set of predefined signatures. Updating the signature database updates only predefined signatures. Periodical updates enable the NIP to own the latest intrusion prevention capabilities.

The default signature database installation package **ips_update.zip** is in the delivered software package of the NIP. When the NIP starts for the first time, **ips_update.zip** is automatically decompressed from the software package to the CF card and automatically installed to grant the NIP basic intrusion prevention capabilities.

The NIP supports local and online IPS signature database updates. The database can also be rolled back to a previous version or the delivered version upon an abnormality or a request.

Feature.Threat.03 Application-Layer Intrusion Event Report

You can view application-layer intrusion event analysis and reports on the NIP Manager. The analysis of intrusion events as well as rankings and details about attack sources, destinations, events, and types help rapidly understand network attack conditions.

Enhancement

- Models NIP6830, NIP6860 application-layer intrusion prevention and detection capabilities

Dependency

The application-layer intrusion prevention capability relies on the version of the application-layer IPS signature database. You must periodically update the signature database in online or offline mode to enable the NIP to defend against the latest types of intrusions.

The application-layer IPS signature database update requires a knowledge base update license. The NIP can be updated within the validity period of the license. After the license expires, the NIP no longer enjoys the update service.

1.2 Application Control

Availability

This feature is introduced to the NIP since V500R001.

Summary

With the development of technologies, the Internet becomes an integral part of people's life. However, some network applications (such as BT and PPLive) appear and take up a lot of

network bandwidth resources, exhausting network resources and deteriorating user's Internet experience.

Using application identification, the NIP identifies the protocols used by network traffic and takes different actions on the traffic based on protocol types. You can set actions (permit, deny, and rate limit) based on IP addresses and ports, time ranges, and protocol types to manage and control traffic.

Benefits

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

The NIP analyzes packets to identify applications, such as games, stock exchange, P2P, IM, and VoIP, and implement control policies accordingly. In actual applications, multiple control results are available: For example, legitimate web browsing is allowed; the rates of applications (such as P2P) that compete bandwidth with mission-critical applications are limited; undesired applications (such as IM) are blocked.

The NIP provides detailed network traffic protocol statistics and analysis reports.

Description

Feature. AppCtrl.01 Application Traffic Control

Application traffic control is to identify the types of data traffic on the network and implement corresponding control actions, such as traffic blocking, connection number limiting, and rate limiting.

- Protocol classification

  The NIP identifies the application-layer protocols of IPv4 and IPv6 traffic. It can also identify application-layer protocols of MPLS, VLAN, GRE, and IPv4-to-IPv6 tunnel traffic.

  Category: a set of protocols. For example, P2P, IM, VoIP, and Video are protocol categories.

  Protocol: a specific protocol.

- Control mode

  The NIP can apply different control policies to different types of traffic. You can apply a control policy to a protocol category or to a protocol. In most cases, a control policy works for a protocol category. Control modes are as follows:

- Block

  The NIP prevents the traffic of a specified application protocol from passing through. For example, if an enterprise wants to block IM applications, the control mode can be set to block for IM applications.

- Allow

  The NIP allows the traffic of a specified application protocol to pass through. For example, the Web_Browsing category is permitted for normal web browsing services.

- Limit the traffic rate and connection quantity

  You can set a rate or connection limit for packets of a specified application protocol. For example, a rate limit is usually set for the P2P category to ensure the normal running of other services.

IDS devices and IDS interfaces on IPS devices support only network traffic protocol analysis, not traffic blocking or rate limiting.

Feature. AppCtrl.02 Application Control Knowledge Base Update

The application control knowledge base is a collection of feature rules of network packets, including P2P, VoIP, and Video packets. The NIP uses rules in the knowledge base to match network traffic and takes actions, such as permit, block, rate limit, or connection limit on matched traffic. Periodically updating the application control knowledge base enables the NIP to have capabilities of identifying the latest protocol features.

By default, the latest application control knowledge base file is in the delivered software package. When the NIP starts for the first time, the file is automatically decompressed from the software package to grant the NIP basic protocol feature identification capabilities.

The NIP supports local and online application control knowledge base updates. The knowledge base can also be rolled back to a previous version or the delivered version upon an abnormality or a request.

Feature. AppCtrl.03 Application Traffic Statistical Report

You can view application-layer traffic statistical analysis and reports on the NIP Manager. By analyzing application traffic, you can learn about statistics on application category and protocol traffic. In addition, you can query IM audit logs and traffic statistical logs.

Enhancement

Dependency

The application protocol identification capability relies on the knowledge base version. You must periodically update the knowledge base in online or offline mode to enable the NIP to identify the latest protocols.

The application protocol identification knowledge base update requires a knowledge base update license. The NIP can be updated within the validity period of the license. After the license expires, the NIP no longer enjoys the update service.

1.3 Traffic Security

Availability

This feature is introduced to the NIP since V500R001.

The traffic security analysis report function is supported from NIP V500R001C50.

Summary

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

DDoS attacks are DoS attacks launched from distributed sources by multiple attacks or from distributed zombie hosts controlled by attackers. DDoS attacks have become a hazardous social phenomenon in this information society.

Based on multi-layer filtering, the NIP uses static filtering and dynamic filtering based on source validity authentication, behavior analysis, session monitoring, and signature recognition to implement accurate traffic detecting and scrubbing against DoS/DDoS attacks, such as malformed packet attacks, port address scanning, and TCP/UDP/ICMP/HTTP/HTTPS/SIP/DNS Flood attacks.

Benefits

The NIP provides multiple measures to defend servers and network infrastructure against flood and single-packet attacks.

The NIP supports dynamic traffic baseline learning and can automatically learn network traffic models and set attack thresholds.

The NIP provides detailed attack event reports.

Description

The NIP provides the traffic security function to prevent flood, single-packet, and scanning attacks. You can select an attack defense method based on your service type and set appropriate thresholds based on service bandwidth. Diversified attack defense techniques are available for the attacks of the same type. Moreover, the hierarchical attack defense procedure is employed. Based on multi-layer filtering, the NIP uses static filtering and dynamic filtering based on source validity authentication, behavior analysis, session monitoring, and signature recognition to defend against DoS/DDoS attacks.

Feature.DoS.01 Land Attack

An attacker sends SYN packets with the same source address and destination address or with the source address being the loopback address to a target host (same source port and destination port). As a result, the attacker sends SYN-ACK packets to its own address, causing a large number of empty connections. The attacked encounter different problems under Land attacks: UNIX hosts crash and Windows NT hosts run very slowly.

The NIP can check whether an SYN packet has the same source IP address and destination address or whether the source address of the SYN packet is the loopback address. If so, the NIP discards the packet and records a log.

Feature.DoS.02 Smurf Attack

A simple Smurf attack is used to attack a single network. The attacker broadcasts ICMP Echo requests to all hosts on the target network. As a result, all hosts reply to this ICMP Echo request, congesting the network. The traffic volume in this attack is one or two times larger than normal ping packets. An advanced Smurf attack is used to attack a single host. The attacker sends ICMP Echo requests with the source address being set to the address of the victim host to crash it. The volume of the ICMP traffic must be maintained at a significant level for a period of time to become an attack. Theoretically, the more hosts a network contains, the severer the impact will be.

The NIP checks whether the destination address of each ICMP Echo request is an A, B, or C class broadcast address or subnet broadcast address. If so, the NIP discards the packet and records a log.

Feature.DoS.03 Fraggle Attack

When the UDP port (port 19 in most cases) running the Chargen service receives a packet, it generates a string as a reply. When the UDP port (port 7 in most cases) running the Echo service receives a packet, it sends the payload of the packet as a reply. These two types of services may be used by attackers to launch cycling attacks, causing the victim system too busy to respond and congesting links.

An attacker sends UDP packets to the network where the target host resides. The source IP addresses of the UDP packets are the IP address of the target host; the destination IP addresses of the UDP packets are the broadcast address or network address of the subnet where the target host resides; the destination port is port 7 or port 19. On the subnet, every system enabled with this function sends response packets to the attacked host, consuming bandwidth and even congesting the network or crashing the host.

Even though these functions are disabled on the subnet, each system generates an ICMP Unreachable packet, consuming bandwidth. If the attacker changes the source port to port 19 and destination port to port 7 for the UDP packets, a large number of response packets are continuously generated, leading to more severe effects.

The NIP detects UDP packets. If the destination port is port 7 or port 19, the NIP discards the packet and records a log.

Feature.DoS.04 WinNuke Attack

WinNuke attack is also called out-of-band transmission attack. Most WinNuke attackers attack port 139, and the attack packets' URG bit is set to 1, indicating the emergency mode. The WinNuke attack exploits the vulnerabilities of the Windows operating system. The attacker sends certain TCP OOB packets to the port. However, these attack packets are different from normal OOB packets. Their pointer fields are inconsistent with the actual locations of data, causing overlapping. When processing such data, the Windows operating system may crash. Moreover, the attacker sends IGMP fragments that cannot be processed by the operating system and makes the operating system crash.

The NIP checks whether the destination port of a packet is port 139, whether the URG bit is 1, and whether the URG pointer is not null. If the three conditions are met at the same time, the NIP discards the packet and records a log. If an IGMP fragment is detected, the NIP discards it and records a log.

Feature.DoS.05 Ping of Death Attack

The Ping of Death attack uses giant ICMP packets to attack systems. The length field of IP packets has 16 bits, meaning that the maximum length of IP packets is 65535 bytes. If the data length of an ICMP Echo request is more than 65515 bytes, the sum of ICMP data length, IP header length (20 bytes), and ICMP header length (8 bytes) is more than 65535 bytes. After receiving such a packet, certain routers or systems crash, stop responding, or restart due to improper processing. The attacker only needs to use the **ping** command to constantly send packets larger than 65535 bytes to crush the TCP/IP protocol stack of the target host.

The NIP checks whether an ICMP Echo request is longer than 65535 bytes. If so, the NIP discards the packet and records a log.

Feature.DoS.06 Tear Drop Attack

To transmit some large IP data packets and meet the link-layer MTU requirements, network devices need to fragment these IP packets. Each IP packet header has an offset field and a

more fragment (MF) flag. The offset field indicates the position of this fragment in the IP packet. After intercepting IP packets, the attacker sets offset fields to incorrect values. After receiving disassembled packets, the receiver cannot correctly assemble the disassembled packets according to offset fields in the packets. In this case, the receiver attempts to assemble the IP packets continuously, which results in the OS crash for resource exhaustion.

The NIP analyzes the received IP fragments of a packet and checks whether the offset of the packet is incorrect. If so, the NIP discards the packet and records a log.

Feature.DoS.07 Address Scanning

An attacker uses programs such as ICMP packets or TCP/UDP packets to initiate connections to certain IP addresses. By checking whether there are response packets, the attacker can determine which target systems are alive and connected to the target network.

The NIP checks received TCP, UDP, and ICMP packets to determine whether the destination IP address of a packet with a specific source IP address is the same as the destination IP address of the previous packet. If so, the abnormality count increases 1. After the abnormality count exceeds the predefined threshold, the NIP adds the source IP address to the blacklist and discards the packets from this source IP address before the blacklist is aged.

Feature.DoS.08 Port Scanning

An attacker probes the network structure by scanning ports to determine the ports currently enabled on the attacked, specifying the attack mode. In port scanning attacks, the attacker uses the Port Scan software to initiate connections to a series of TCP or UDP ports on a wide range of hosts. According to the response packets, the attacker can determine whether the hosts use these ports to provide services.

The NIP checks received TCP and UDP packets to determine whether the destination port of a packet with a specific source IP address is different from the destination port of the previous packet. If so, the abnormality count increases 1. After the abnormality count exceeds the predefined threshold, the NIP adds the source IP address to the blacklist and discards the packets from this source IP address before the blacklist is aged.

Feature.DoS.09 IP Option Control

- Source route option control

  Usually, routers on IP networks determine the path based on the packet's destination. In contrast, source routing allows a sender of a packet to partially or completely specify the route that the packet takes through the network. This option means allowing the source site to specify a route to the destination instead of the routes specified by intermediate routers. The source route option is usually used for troubleshooting or for special services. The IP source route option may be utilized by attackers to probe the network structure because it neglects the intermediate forwarding processes through various devices along the packet transmission path, regardless of the working status of forwarding interfaces.

  The NIP checks whether the source route option is set for a received packet. If so, the NIP discards the packet and records a log. If not, the NIP forwards the packet.

- IP route record option control

  The IP route record option is used to record the transmission path of an IP packet from the source IP address to the destination IP address. The path is a list of routers that are involved in the handling of this packet. Generally, an IP route record option is used to diagnose faults on network paths but may also be utilized by attackers to probe the network structure.

The NIP checks whether the IP route record option is set for a received packet. If so, the NIP discards the packet and records a log. If not, the NIP forwards the packet.

- IP timestamp option control

  The IP timestamp option in an IP packet is used to record the transmission path of an IP packet from the source IP address to the destination IP address and the time spent in the transmission. The path is a list of routers that are involved in the handling of this packet. An IP timestamp option is used to diagnose faults on network paths but may also be utilized by attackers to probe the network structure.

  The NIP checks whether the IP timestamp option is set for a received packet. If so, the NIP discards the packet and records a log. If not, the NIP forwards the packet.

Feature.DoS.10 IP Fragment Attack

DF and MF flags in the IP header are used for fragment control. A hacker sends illegitimated fragment control packets, resulting in host failures upon receiving such packets.

The NIP checks each received packet. If the control bits in a packet meet one of the following conditions, the NIP discards the packet and records a log:

Both the DF bit and the MF bit are 1.

The DF bit is 1, and the Offset bit is greater than 0.

The DF bit is 0, and the total length of the Offset and Length fields exceeds 65535 bytes.

Feature.DoS.11 TCP Label Validity Check

A TCP packet has the following flag bits: URG, ACK, PSH, RST, SYN, and FIN. The attacker sends a large number of illegitimate packets with the combinations of these flag bits. The attacked hosts are busy identifying these packets, deteriorating system performance. Certain operating systems are unable to process packets, and the hosts may crash.

The NIP checks each received packet. If the TCP flag combination meets one of the following conditions, the NIP discards the packet and records a log:

All flag bits are set to 1.

All flag bits are set to 0.

The SYN bit and the FIN bit are set to 1.

The SYN bit and the RST bit are set to 1.

The FIN bit is set to 1 and the ACK bit to 0.

Feature.DoS.12 Giant ICMP Packet Control

Generally, legitimate ICMP packets are not too large. Oversized ICMP packets are probably used for attacks.

The maximum ICMP packet length can be set on the NIP. When detecting an oversized ICMP packet, the NIP considers that an attack occurs, discards the packet, and records a log. The default ICMP packet length is 4000 bytes.

Feature.DoS.13 ICMP Redirection Packet Control

Network devices can send ICMP redirection packets to a host, requiring the host to change the route. In most cases, devices send ICMP redirect packets only to hosts on the same network. However, an attacker may send forged redirection packets to the hosts on another subnets to change the routing tables of the hosts and interfere with normal IP packet sending on the hosts.

The NIP discards ICMP redirection packets and records logs.

Feature.DoS.14 ICMP Unreachable Packet Control

After receiving an ICMP unreachable packet, a certain system considers the destination network or host unreachable and disconnects from the network or host. Attackers take advantages of this mechanism to forge ICMP unreachable packets to terminate the connection between the victim and destination.

The NIP discards ICMP unreachable packets and records logs.

Feature.DoS.15 Tracert Packet Control

An attacker discovers the path between source and destination hosts by using the replied ICMP timeout packet when TTL is 0 and the ICMP port unreachable packet replied by the destination.

The NIP discards ICMP or UDP timeout packets or ICMP unreachable packets and records logs.

Feature.DoS.16 TCP Flood Attack Defense

- SYN Flood

  An attacker sends a large number of SYN packets with forged source IP addresses to target hosts, consuming host resources by half connections.

  The NIP collects statistics on SYN packet rates based on destination addresses. When the SYN packet rate exceeds the threshold, the NIP enables source authentication to prevent attacks.

  Source authentication is described as follows:

  1. After receiving an SYN packet, the NIP sends an SYN/ACK probe packet to the source address of the SYN packet.
  2. After receiving a response packet, the NIP checks whether the source of the SYN packet is valid to prevent attacks with forged source addresses.

  If the NIP does not receive any response packets, the NIP considers the SYN packet an attack and does not send the packet to the server.

  If the NIP receives a response packet, the NIP checks whether the packet is valid. If the source IP address is legitimate, the NIP whitelists the IP address and directly forwards the subsequent packets. For SYN packets whose source addresses are not in the whitelist, the NIP checks the validity of the source addresses.

- SYN-ACK Flood

  An attacker sends a large number of SYN-ACK packets to a target server, exhausting bandwidth and system resources.

  SYN-ACK Flood attack defense prevents attacks caused by SYN-ACK packets constructed by forged servers. If the rate of SYN-ACK packets destined for the same IP address exceeds the threshold, the NIP records the attack event and enables source

authentication. If the source IP address is legitimate, the NIP whitelists the IP address and directly forwards the subsequent packets. If the source IP address is illegitimate, the NIP discards the packet. For packets whose source addresses are not in the whitelist, the NIP checks the validity of the source addresses.

- SYN-ACK Flood

  An attacker sends a large number of ACK packets to a target server, exhausting bandwidth and system resources.

  If the rate of ACK packets destined for the same IP address exceeds the threshold, the NIP considers that an attack occurs.

- TCP Fragment Flood

  An attacker sends a large number of TCP fragments to a target server, exhausting bandwidth and CPU resources.

  If the rate of TCP fragments destined for the same IP address exceeds the threshold, the NIP considers that an attack occurs. The NIP queries the whitelist. If the source IP address of a packet is whitelisted, the NIP forwards the packet. If not, the NIP discards the packet.

- FIN/RST Flood

  An attacker sends a large number of FIN/RST packets to a target server, exhausting bandwidth and system resources.

  If the rate of FIN/RST packets destined for the same IP address exceeds the threshold, the NIP discards the FIN/RST packets that do not belong to any sessions and forwards the FIN/RST packets that match valid sessions.

Feature.DoS.17 UDP Flood Attack Defense

An attacker sends large numbers of UDP packets or fragments (generally large packets, which are submitted to the upper layer for processing if the application program exists or replied by the host with ICMP unreachable packets if the application program does not exist) to the target server through Botnets. As a result, the server resources are exhausted, and the server cannot respond to normal requests, or even the links are congested.

The NIP limits the UDP traffic rate, performs the consistency check, and learns fingerprints to prevent UDP Flood attacks.

- Traffic limiting

  An overall threshold is set on the NIP. If the UDP traffic rate exceeds the threshold, the NIP discards excess UDP packets or fragments.

- Consistency check

  When the UDP traffic rate exceeds a predefined threshold (different from the overall threshold), the consistency check is triggered. If the payload is the same for every packet, the NIP considers that an attack occurs and discards the packets.

- Fingerprint learning

When the UDP traffic rate exceeds a predefined threshold (different from the overall threshold), the fingerprint learning is triggered. The NIP dynamically generates fingerprints based on the characteristics of attack packets and then discards the packets matching the fingerprints.

Feature.DoS.18 DNS Flood Attack Defense

- DNS Request Flood

An attacker sends a great number of non-existent domain name resolution requests to the DNS server through Botnets, resulting in the severe overload of the DNS server. Hence, the DNS server cannot respond to DNS requests from authorized users. Generally, source IP addresses in such attacks are forged. To achieve overwhelming attack effects, the attacker resets recursive query fields. The current server fails to query required packets and sends requests to its upper-level server. As a result, massive DNS servers fall into the vicious circle.

The NIP collects statistics on DNS request packet rates based on destination IP addresses. If the rate exceeds the threshold, the NIP enables attack defense.

- Passive defense

  The NIP discards the first packet from a specific source IP address and a specific port, so that the source sends a DNS request again. If the subsequent DNS request requires the same domain name as the previous request, the NIP whitelists the source address and forwards the subsequent DNS requests from this source.

- Source detection

  The NIP authenticates the source. If the authentication succeeds, the NIP whitelists the source address and forwards the subsequent DNS requests from this source.

Feature.DoS.19 HTTP Flood Attack Defense

An attacker sends a large number of HTTP packets to the target server through proxies or Botnets. Such requests involve URL access, leading to continuous database reading. As a result, the resources of the server are exhausted, and the server cannot respond to normal requests.

The NIP collects statistics on HTTP packets based on destination IP addresses. If the packet rate exceeds the threshold, the NIP starts attack defense to perform source authentication or fingerprint learning.

Feature.DoS.20 HTTPS Flood Attack Defense

An attacker launches massive connections to the target server directly or through proxies or zombie hosts. As a result, the server resources are exhausted and the server cannot respond to normal requests.

If the rate of HTTPS packets destined for the same IP address exceeds the threshold, the NIP records the attack event and enables source authentication. If the source IP address is legitimate, the NIP whitelists the IP address and directly forwards the subsequent packets.

Feature.DoS.21 TCP Connection Flood Attack Detection

An attacker launches massive TCP connections to a server through Botnets, exhausting the TCP connection resources of the server. Generally, TCP connection flood attacks fall into four types:

- After the three-way handshake is complete, no packet is sent and the TCP connections remain.
- After the three-way handshake is complete, a FIN or RST packet is immediately sent to release the connection at the local end. The attacker quickly initiates a new connection.
- During the connection establishment, the SockStress attack is launched to exhaust the connection resources of the server.
- A large number of TCP retransmission requests, each request with light traffic, congest the upper link.

The NIP collects statistics on the new connection rate and the number of concurrent connections based on destination IP addresses. The source IP addresses that exceed any statistics threshold are blacklisted, and their TCP traffic is cut off.

Feature.DoS.22 SIP Flood Attack Defense

An attacker sends a large number of INVITE messages to a SIP server, causing the SIP server under attack to allocate a large number of resources for recording and tracing sessions until the server becomes unable to respond to the call requests of legitimate users due to resource exhaustion. Alternatively, the attacker constructs and sends the corresponding malformed SIP packets based on the loopholes of the SIP implementation, therefore causing denial of services on the SIP server.

When the system detects that the rates of SIP packets from the destination IP address exceed the threshold, the system enables SIP-based source authentication. Subsequent SIP packets are allowed through after the source IP address is authenticated.

Feature.DoS.23 ICMP Flood Attack Defense

An attacker sends a large number of ICMP packets (such as ping packets) to a target host. The attacked host is busy replying to such packets and cannot provide normal services.

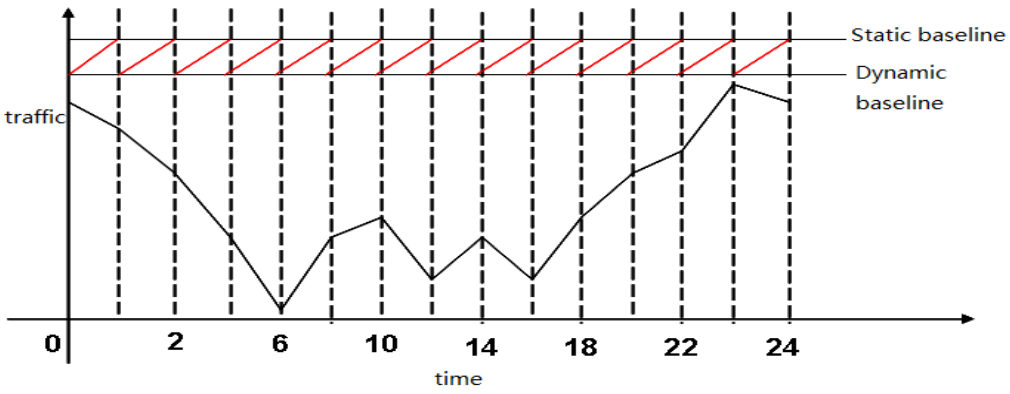
When the ICMP packet rate destined for the same destination address exceeds the threshold, the NIP considers that an attack occurs and discards excess ICMP packets.

Feature.DoS.24 TCP/UDP Rate Limit

The NIP discards excess TCP/UDP packets to prevent TCP/UDP Flood attacks.

NIP V500R001 provides more fine-grained network bandwidth management functions, including TCP/UDP rate limit.

Feature.DoS.25 Traffic Baseline Learning



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.

Feature.DoS.26 Traffic Security Event Analysis Report

You can view traffic security event analysis and reports on the NIP Manager. The analysis of traffic security events helps you understand the traffic changes trends of attack packets of various types, top N IP addresses with the most attack count or the longest attack duration, and top N attack events with the largest number of attack packets or the longest attack duration.

Enhancement

Dependency

None

1.4 Network Deployment

Availability

This feature is introduced to the NIP since V500R001.

Summary

The NIP supports IPS (in-path), IDS (out-of-path), and hybrid (certain interfaces for IPS and certain interfaces for IDS) modes.

The deployment is based on the interface pair or interface pair group. Traffic between different interface pairs or interface pair groups is mutually isolated.

Benefits

The device provides default policies that apply to most scenarios. The interfaces are completely transparent and support plug-and-play and easy deployment.

IPS and IDS deployment scenarios are supported. The IPS mode supports in-path deployment in serial mode and one-armed in-path deployment (attached to a Layer-2 switch).

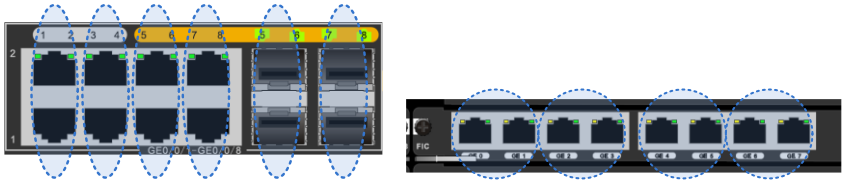
After interface pair aggregation, traffic of multiple interface pairs can be associated to support multiple deployment scenarios, such as inconsistent forward and reverse paths and link binding.

Description

Feature.Deploy.01 In-Path Deployment in Serial Mode as an IPS Through the Interface Pair

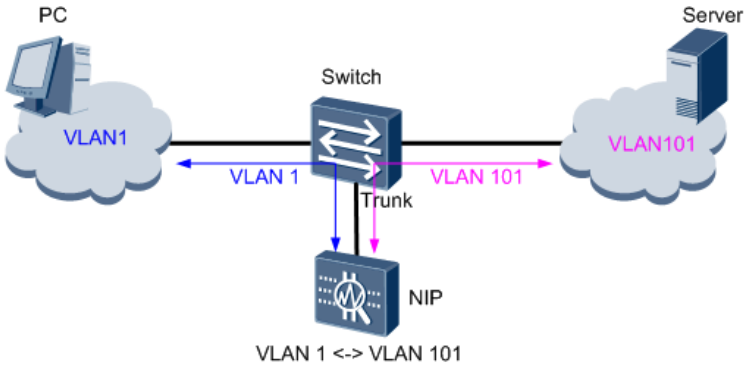
For ease-of-use, the fixed interfaces on the NIP and expansion interface cards are grouped into pairs. By default, interface pairs work in in-path IPS mode. An interface pair is a pair of incoming and outgoing interfaces. Users need only to connect the interface pairs to the links to be protected.

The following figure uses built-in interfaces and 8GE expansion interface cards as an example to describe the grouping of interface pairs.



Feature.Deploy.02 One-Armed Out-of-Path Deployment as an IPS (Attached to a Layer-2 Switch)

One-armed deployment does not require the existing network topology be changed. In this deployment, the NIP serves as an IPS device, with one of its interfaces connected to the Trunk interface on the Layer 2 switch to detect and defend against threats from the traffic between multiple VLANs.

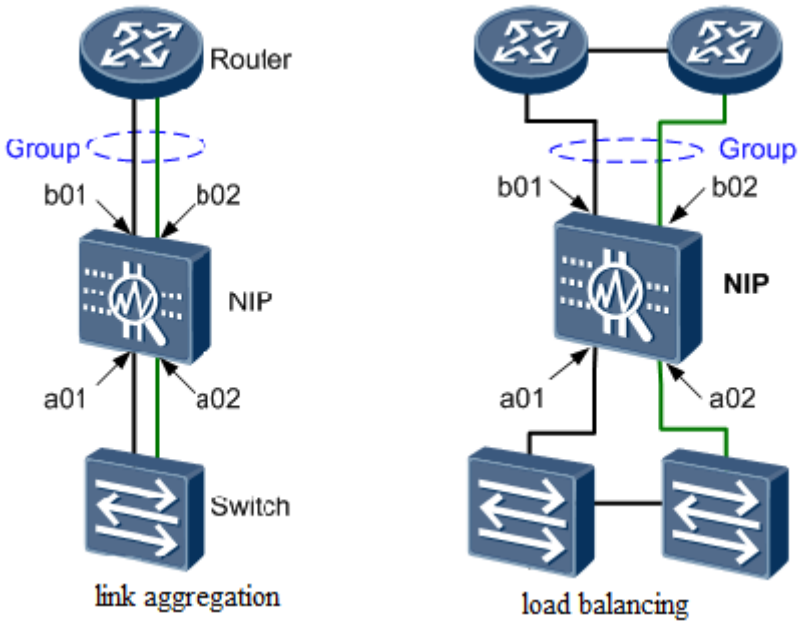


The advantage of one-armed deployment lies in that it does not change the existing network topology and significantly saves NIP physical interfaces.

Feature.Deploy.03 IPS Interface Pair Aggregation

The interface pair group combines multiple interface pairs into a logical group so that traffic of multiple links can be globally monitored and analyzed. The interface pair is used for the asymmetric traffic.

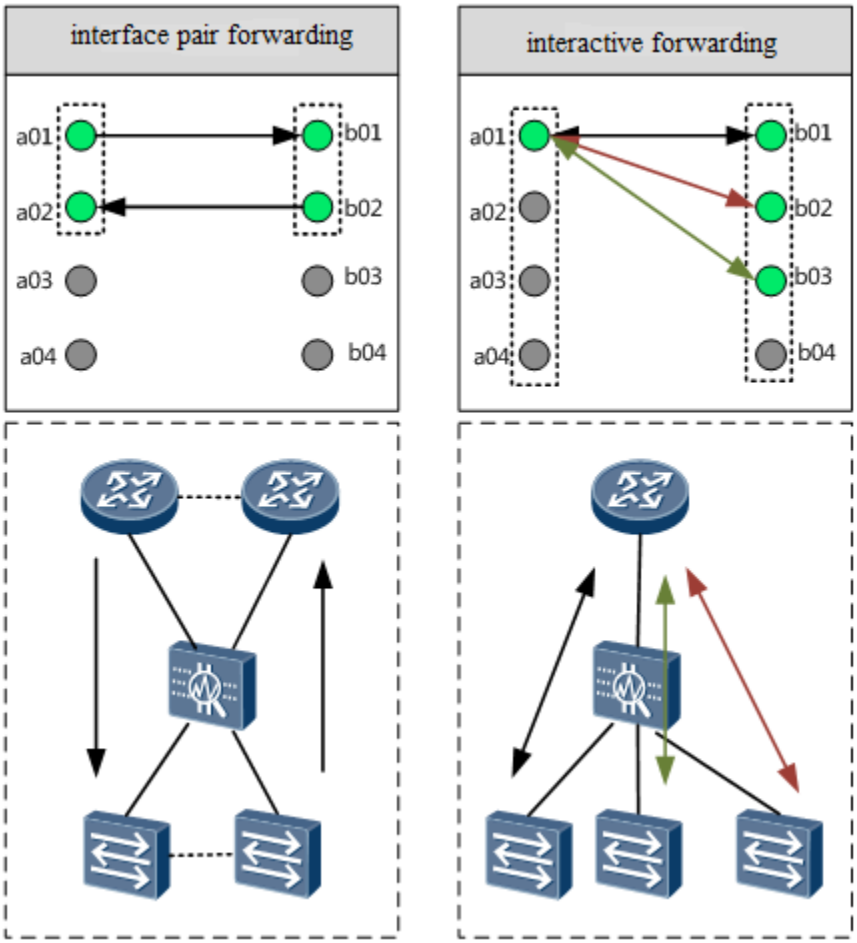
Asymmetric traffic may exist on link aggregation and load balancing networks. In such cases, multiple interface pairs of the NIP are required for access and the interface pair group function must be enabled for the NIP to process packets of multiple links.



After NIP interface pair aggregation, two forwarding modes, namely interface pair forwarding and interactive forwarding, are supported.

In interface pair forwarding mode, packets entering an interface are sent out from the interface that is originally a pair with this interface.

In interactive forwarding mode, packets entering an interface can be sent out from any peer interface of this interface pair. The sending principle is based on the result of learning the mapping between the MAC address and interface. If no mapping relationship is found, packets are broadcast among all peer interfaces. The interactive forwarding mode can transfer the relationships of NIP upstream and downstream links from the original one-to-one to one-to-multiple or even multiple-to-multiple, resulting in more flexible deployment scenarios.

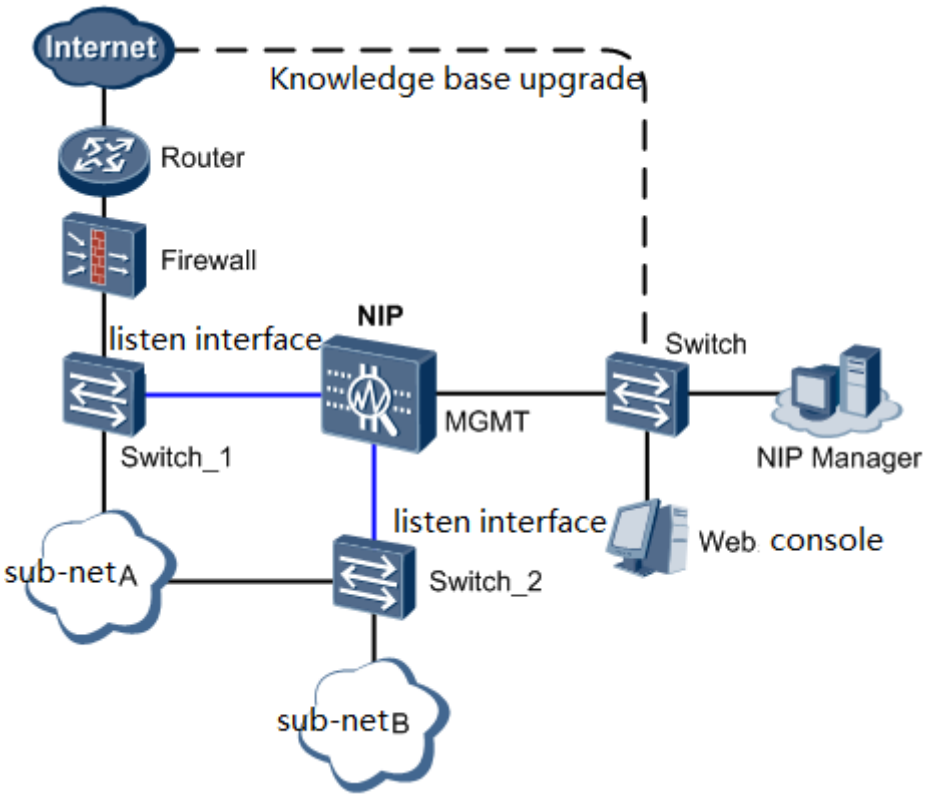


Feature.Deploy.04 Out-of-Path Deployment as an IDS

Out-of-path deployment is used mainly for recording attack events and web application traffic conditions to provide evidence for network security event audit and user behavior analysis. The NIP is not involved in forwarding traffic, and configured security policies specify what threats are detected and recorded.

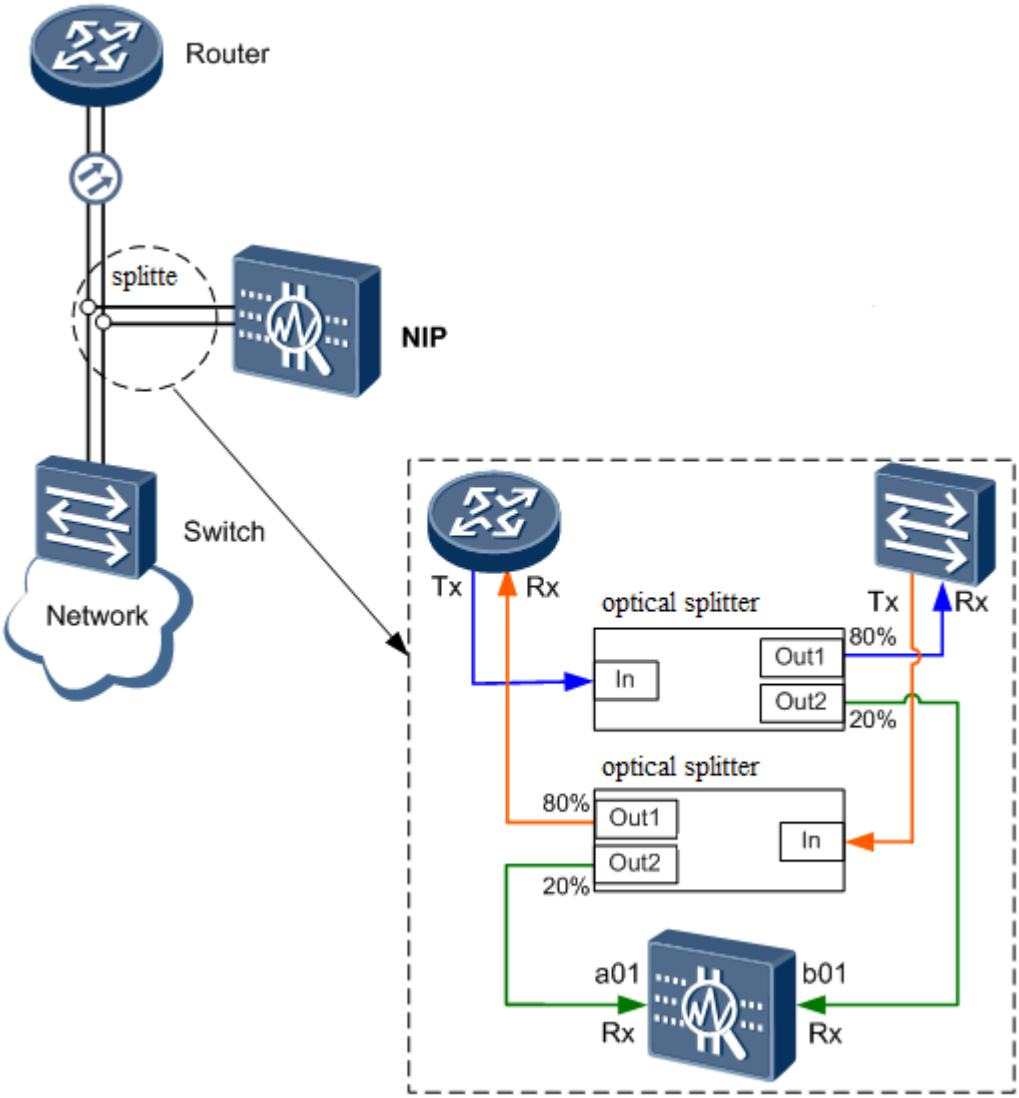
The NIP provides various interfaces and flexible working modes. In addition to NIP IDS models, IPS models support the setting of interfaces to work in IDS mode. Users can use the switch mirroring port to copy the traffic through packet capture or optical splitter to the NIP for traffic intrusion detection and network traffic protocol distribution statistics. The IDS and IPS interfaces are mutually exclusive.

In out-of-path mode, the NIP usually does not implement defense response. For special requirements, the NIP can be configured to block sessions (by sending TCP RST packets). However, the blocking effectiveness is limited due to the deployment mode. Users can also use the function of interworking with the firewall to instruct the firewall to block connections so as to better block subsequent traffic.



When users convert an IPS interface pair to IDS mode, they convert both interfaces to IDS mode. In addition, these interfaces are still a pair. The NIP does not isolate traffic entering these two interfaces. This is because the traffic of these two links needs to be associated for detection in certain scenarios, such as:

- Mirroring through a switch.
- The bandwidth of one interface is inadequate. Therefore, the two interfaces of the same interface pair are used to receive respectively the incoming and outgoing traffic of the same mirroring interface.
- On load balancing networks, traffic of two links must be mirrored for overall analysis. Therefore, the two interfaces of the same interface pair are used to receive the mirrored traffic of the two links respectively.
- Optical splitting through an optical splitter.
- In optical splitting mode, two IDS interfaces of an interface pair need to be used to receive optical splitting traffic of two directions in service links.



After conversion, interfaces paired by default are available for ease-of-use.

In addition, the NIP also supports the aggregation of multiple IDS interfaces into an IDS interface pair group for scenarios in which associated detection is performed on traffic of multiple links.

Enhancement

Dependency

None

1.5 System Management

Availability

This feature is introduced to the NIP since V500R001.

Summary

The NIP employs the web GUI, which enables you to configure all functions of the NIP and query various statistics. Two access modes of HTTP and HTTPS are available.

The NIP supports the built-in web to manage a single device and also supports the usage of the NIP Manager to manage and monitor multiple devices in a centralized manner.

In addition to the NIP system's management platform, the NIP also supports third-party management by connecting to a third-party NMS server or syslog host.

Benefits

Supports GUI-based management.

The centralized management platform facilitates centralized management and monitoring of multiple devices.

Supports third-party platform interfaces to enable users to centrally monitor network devices and summarize events.

Description

Feature.Mgmt.01 Device Clock Configuration

The system time must be set accurately so that the NIP can work together with other devices properly. The NIP supports manual time setting, time synchronization from the local system, and time synchronization from the NTP server. It also supports automatic clock adjustment based on DST.

Feature.Mgmt.02 System Version Upgrade

When the version of the device system software does not satisfy existing working requirements, and the software of a new version is available, you shall upgrade the software. Based on the version, two upgrade modes are usually available. That is, you can directly upgrade the system software or install a patch on the existing system software.

The NIP provides the one-click upgrade service that enables you to complete system software upgrade or patch installation with ease and without having to switch between multiple pages.

Feature.Mgmt.03 Configuration File Management

Configuration files are loaded when the NIP starts. Managing configuration files involves restoring factory settings, exporting configuration files, and configuring configuration files to be loaded during next startup.

After you restore the factory settings, the configurations are restored to the default settings. The current configurations will be lost. Therefore, you need to determine whether you need to back up the configurations before you restore the factory settings.

By exporting existing configurations, you can back up existing configurations on the device to the administrator PC.

To run other configuration files on the device or newly loaded configuration files, set these configuration files to be loaded during next startup. For example, in a scenario where multiple devices of the same type and with similar configurations exist on the network, after one of the devices is configured, you can upload its configuration files to another device and set these configuration files to be used during next startup to reduce workload.

Feature.Mgmt.04 License Management

The update of the intrusion prevention signature database, application control knowledge base, and antivirus signature database requires a license.

You can manage license files used by the NIP on the GUI and view information about obtained licenses.

Feature.Mgmt.05 Device Debugging

- **ping** and **tracert** commands are used to test the network connectivity. When a fault occurs on the network, you can run the **ping** command to check whether the device with the specified IP address is reachable. Then run the **tracert** command to locate the fault and provide evidence for troubleshooting.
- The diagnosis information includes the current operating status of the NIP. Such information includes the system information and interface status. When a fault occurs on the device, the administrator can analyze the cause of the fault and provide help for troubleshooting based on the system operating status of the NIP.
- The log channel test is used to check whether the NIP and the NMS software or log host communicate properly. After configuring the parameters for connecting the NIP and NMS software or log host, you can test the log channel to detect whether the connection is normal.

Feature.Mgmt.06 Device Management

You can perform the individual or centralized configuration and management for the NIP through the built-in web system of the NIP or the NIP Manager. You can configure all features and functions of the NIP and view statistics in the visualized management system.

Both the built-in web system and NIP Manager support two access modes of HTTP and HTTPS.

Feature.Mgmt.07 Management by a Third-Party NMS Server

The NIP provides interactive interfaces for the third-party NMS software and report alarm information to the third-party NMS for analysis and statistics collection. In this way, users can monitor and assess the operating status of the network.

If the user wants to use their own NMS software, but not the NIP Manager of the NIP, parameters for the communication between the NIP and the third-party NMS software can be configured. The NIP uses the standard SNMP to communicate with the NMS, ensuring that the NMS can properly receive the alarm information from the device. SNMP has three versions, namely, SNMPv1, SNMPv2c, and SNMPv3.

Feature.Mgmt.08 Connection to a Third-Party Log Host

The NIP can be connected to a third-party log host already deployed on your own network.

You can configure a third-party log host to output syslogs towards it. You can configure a maximum of three log hosts for one NIP. Each syslog is output by the NIP to different log hosts for backup.

Enhancement

Dependency

None

1.6 System Security

Availability

This feature is introduced to the NIP since V500R001.

Summary

As a network device node, the NIP system itself is exposed to security threats. The NIP protects the security of its own system from secure networking, protocol attack defense, sensitive data protection, and system management and maintenance security.

Benefits

The NIP protects the security of its own system and data.

Description

Feature.Secur.01 Out-of-Band Management

The NIP provides an independent out-of-band management interface to completely isolate management and service. In addition, the NIP employs transparent access mode involving the fixed interface pair and does not have any protocol stack with the access network. Therefore, its IP address is not exposed, and the external world cannot initiate attacks towards its IP address.

Feature.Secur.02 Access Control List

The NIP provides strict access control management. The access control list of the device has strict control over the IP addresses of the connected devices. Only authorized addresses can log in to the device and view configurations and other information. In addition, access control is used together with the identification and authentication mechanisms to prevent unauthorized access.

Feature.Secur.03 Access Control List

The NIP provides strict access control management. The access control list of the device has strict control over the IP addresses of the connected devices. Only authorized addresses can log in to the device and view configurations and other information. In addition, access control is used together with the identification and authentication mechanisms to prevent unauthorized access.

Feature.Secur.04 User Authentication

- Forcing a user out

  The administrator can force a suspicious user out.

- Password complexity

  The password contains at least 8 characters.

  The password must contain:

  - At least one lowercase letter;

  - At least one uppercase letter;

  - At least one digit;

  - At least one special character: `~!@#$%^&*()-_=+\|[{}];:'",<.>/? and a space.

  The password must differ from the reversed account.

- Password lockout

  If the password input attempts (five times by default, and can be configured) exceeds the threshold, the user is locked.

  For the users who are locked for entering incorrect password for N times, you can set the automatic unlock time.

  The user is automatically unlocked when the specified time approaches.

- Passwords cannot be stored in plain text

  Passwords, including the web password, FTP password, operating system account password, database account password, SNMPv2 community name, and SNMPv3 password, are not stored in plain text in the system.

- Password usage rules

  The input password cannot be displayed in plain text or copied.

  Users can change only their own passwords with their old passwords authenticated.

- Verification code

  The NIP Manager application uses the disposable verification code.

Feature.Secur.05 Hierarchical Permission Management

The authorization system is based on roles. Account- and role-based authorization complies with the minimum authorization principle. That is, a role is authorized with only necessary permissions, and an account is authorized to only necessary roles. The system supports data-level role control, which allows users with different roles to perform the same function, but not to query the sensitive information of the function. This ensures separate management, maintenance, and operation.

The NIP system assigns different permissions to different users. In addition to the default system administrator, operator, and auditor, the system also supports user-defined administrator roles. You can define these roles based on the configuration management content and devices to be managed and authorize corresponding permissions to them.

Feature.Secur.06 Device Service Management

The device service can be HTTP service, HTTPS service, Telnet service, or SNMP service.

After the device has the HTTP, HTTPS, or Telnet service enabled, you can log in to the device in the corresponding mode. After the device has the SNMP service enabled, the NMS can properly communicate with the device.

You can disable a non-encrypted transmission channel, such as HTTP and Telnet.

Enhancement

Dependency

None

1.7 High Availability

Availability

This feature is introduced to the NIP since V500R001.

Summary

The NIP guarantees service continuity through high availability means.

- Hot standby

  The NIP supports Huawei Redundancy Protocol (HRP) to implement dual-system hot standby. A backup group includes an active device and a standby device. HRP is in charge of delivering key configuration commands and information about session tables between active and standby devices. In so doing, the standby device can smoothly take over the work of the faulty active one.

- Bypass interface card

  The NIP can house electrical and optical bypass interface cards, which can directly connect upstream and downstream devices when the NIP fails. When the fault is rectified, all traffic is switched back to the NIP to ensure security.

Benefits

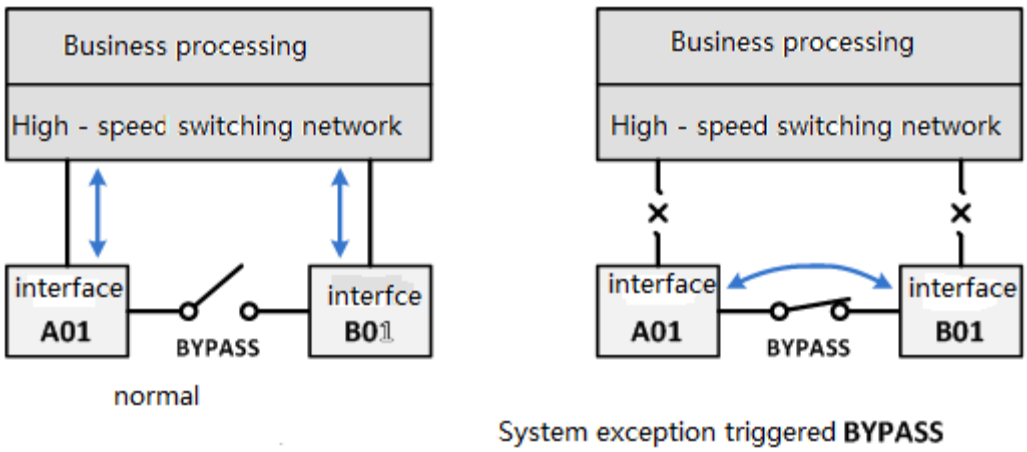
The single point of failure can be removed to guarantee service continuity.

Description

Feature.HA.01 IPS Model Hardware Bypass

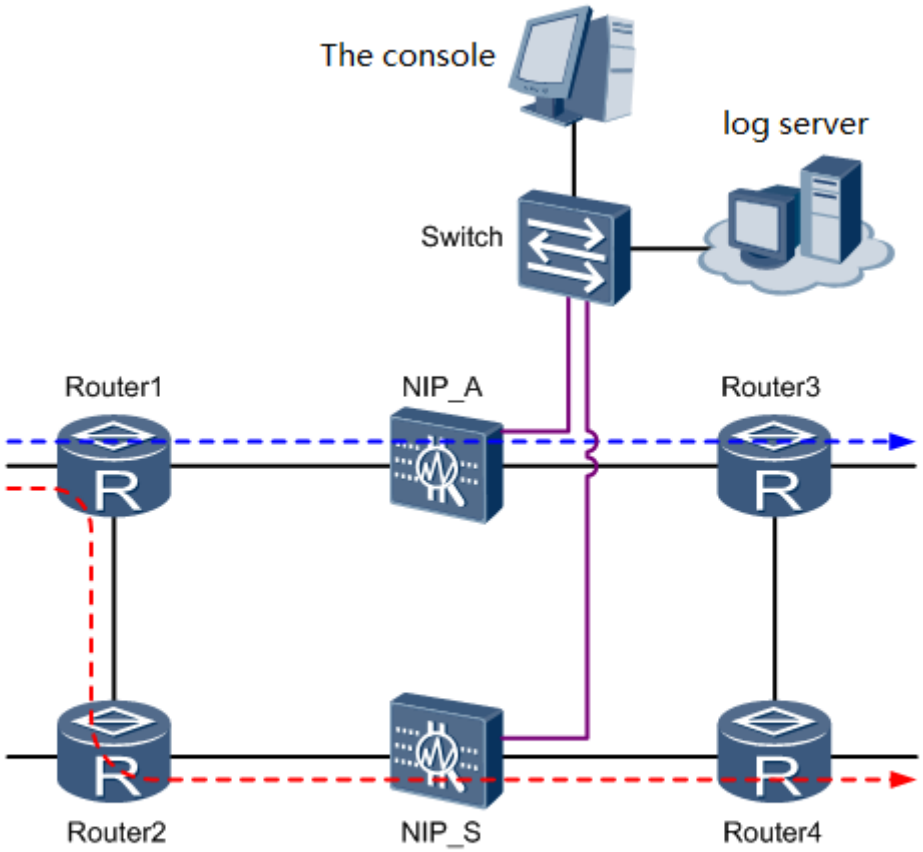
To prevent service interruption caused by potential software processing anomalies, the NIP provides electrical and optical bypass interface cards. These interface cards can connect the ingress network when the system works improperly (such as software anomaly or system shutdown) so that important services 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.



Feature.HA.02 IPS Model Hot Standby Deployment (Active/Active, Active/Standby)

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



There are two working modes in dual-system hot standby deployment.

- Active/Standby mode

  In active/standby mode, the active device processes services, and the standby device stays in standby state. If an error occurs on the interface or link of the active device or the active device is faulty, the standby device becomes active and takes over services.

- Load balancing mode

  Differing from hot standby in active/standby mode, the two devices in load balancing mode share the traffic forwarding load. If one device is faulty, the other device takes over all the services to ensure service continuity.

In load balancing networking, the two devices work in active/active mode. Because of the load balancing nature, the forward and reverse packets may take different paths. In this case, with load balancing configured, the NIP automatically enables asymmetric deployment mode to inspect the traffic in one direction.

In load balancing scenarios, it is possible that the detection rate of application-layer intrusion prevention decreases.

Enhancement

Dependency

The bypass interface card is not standard and must be purchased based on network requirements.

In hot standby deployment of load balancing mode, per-flow load balancing is required. In this deployment, the device can process one-way traffic. However, the detection rate may be compromised.

1.8 Network Bandwidth Management

Availability

This feature is introduced to the NIP since V500R001.

Summary

In bandwidth management, traffic is allocated to different IP addresses for network optimization.

Traffic limiting objects between interface pairs include:

- Limits connections

  Limits the number of connections received or initiated by a specified user, IP address, or network.

  The connections here refer to those established with IP protocols, which can be TCP, UDP, and ICMP connections. A connection is usually uniquely identified by the source IP address, source port, destination IP address, destination port, and protocol (namely, the quintuple). Therefore, an IP address can establish multiple connections with other IP addresses. Connections with different quintuples are considered as different connections. The device collects statistics on the number of connections based on the number of session tables. Therefore, for multi-channel protocols, it is impossible for multiple connections to be established between two network devices.

  In actual applications, multiple connections may be established for certain protocols during one communications process, which consumes massive session resources. The most typical protocol is P2P. Thus, you can limit the connection numbers of the protocols of this type by using the connection number limiting function, thus ensuring the forwarding of other normal services.

- Limits bandwidth

  Limits the bandwidth of a specified user, IP address, or network.

  The bandwidth limit function can optimize network traffic, ensure the normal access rate of users, and indirectly defend against network attacks. In actual applications, you can use bandwidth limiting to allocate network bandwidths and perform differentiated management on users.

Benefits

The connection counts and bandwidths of specified IP addresses and protocols are controlled, and network traffic is optimized to guarantee proper user access.

Network attack defense is implemented.

The allocation of network bandwidth helps implement differentiated management of various users.

Description

Feature.Bandwith.01 Per-IP Traffic Limiting

The per-IP traffic limiting policy implements traffic limiting for an individual IP address (source or destination address). Three functions of maximum bandwidth, guaranteed bandwidth, and maximum number of connections are involved.

- Guaranteed bandwidth: indicates the guaranteed bandwidth of data flows of an individual IP address.
- Maximum bandwidth: indicates the maximum bandwidth of data flows of an individual IP address.
- Maximum number of connections: indicates the limit on the maximum number of connections of data flows of an individual IP address.

If traffic limiting is required for each IP address on a certain network segment, configure a per-IP traffic limiting policy to limit the bandwidths and connections based on source or destination IP addresses.

If multiple per-IP traffic limiting policies are configured at an interface pair, they are matched based on their priorities. If one policy is matched, the matching process ends. By default, the earlier the policy is configured, the higher the priority is. You can use commands to manually modify the priorities of the policies.

Feature.Bandwith.02 Global Traffic Limiting

The global traffic limiting policy performs global management and control over all data flows at an interface pair.

Two functions of maximum bandwidth and maximum number of connections are involved.

- Maximum bandwidth: indicates that the maximum bandwidth of all data flows at an interface pair is limited.
- Maximum number of connections: indicates that the maximum number of connections for all data flows at an interface pair is limited.

To limit the traffic of users or IP addresses on a network segment globally, you are advised to configure the maximum bandwidth and maximum number of connections of the entire network for global traffic limiting.

If multiple global traffic limiting policies are configured at an interface pair, they are matched based on their priorities. If one policy is matched, the matching process ends. By default, the earlier the policy is configured, the higher the priority is. You can use commands to manually modify the priorities of the policies.

Enhancement

Dependency

None

2 Optional Features

2.1 File Virus Scanning

Availability

This feature is introduced to the NIP since V500R001.

Summary

A virus is a type of executable code that infects or attaches to other executable code. Certain viruses can directly result in file deletion or system lockout, whereas certain viruses may result in the generation of a large amount of forged data to exhaust the resources of the infected hosts or networks after they infect other files.

The NIP compares the content of files on which virus scanning is to be performed with the virus signature database for whether information that matches the virus signatures exists. If virus information is detected, the device removes the related content or generates an alarm according to the antivirus policy. If no virus is detected, the device permits the files. Besides virus scanning, you can configure the device to permit or deny oversized files, password-protected files, multi-layer compressed files, and damaged files.

The device can perform virus scanning and corresponding processing on files transferred using the following protocols:

Hypertext Transfer Protocol (HTTP)

Simple Mail Transfer Protocol (SMTP)

Post Office Protocol 3 (POP3)

File Transfer Protocol (FTP)

Various types of virus event analysis reports are supported.

Benefits

File viruses transferred over the network are scanned to protect clients and servers and to prevent virus dissemination.

Description

Feature.AV.01 Antivirus and Alarming

The NIP scans web access, email, and FTP traffic for viruses and forwards the traffic only if no virus is detected. Antivirus enables the comprehensive scanning of compressed files (in various formats), shell files, and email attachments. File viruses are scanned based on real file types, not on file name extensions. In this case, disguised attacks and viruses can be suppressed.

The NIP supports antivirus scanning for files transmitted through HTTP, SMTP, POP3, and FTP. Different virus scanning policies can be flexibly configured for various protocols based on network deployment features, such as response mode configuration, restriction on the size of scanned files, and scanning based on the file type. Users can be notified of the discovered viruses through such means as email and web page pushing. Policies can be applied to specific interface pairs, and scanning can be performed on traffic of specific types to minimize performance consumption of global scanning.

The NIP provides two file scanning modes to satisfy different user needs:

- Intelligent scanning

  Scan files by the actual type. In this mode, the device scans all files.
- Scanning on the basis of file name extension

Scans files based on file name extensions. In this mode, the device scans only files with predefined and user-defined file name extensions but not other files.

Virus scanning cannot be performed on traffic of the IDS device and of the IDS interface on the IPS device.

Feature.AV.02 Virus Signature Database Update

The virus signature database of the NIP records a large number of virus signatures. The NIP compares the content of files on which virus scanning is to be performed with the virus signature database for whether information that matches the virus signatures exists. Periodical updates enable the NIP to provide the latest antivirus capabilities.

By default, the software package delivered with the device does not contain any virus signature database file. Before using the antivirus function, you must update the virus signature database to the latest version. It takes a long time to update the signature database for the first time.

The NIP supports the local and online update of the virus signature database. In addition, it also supports rollback to the source version in cases of anomalies or other requirements.

Feature.AV.03 Virus Event Analysis and Reports

You can view virus event analysis and reports on the NIP Manager. The analysis of virus events as well as rankings and details about attack sources, attack destinations, virus types, and virus event trends help you rapidly understand network security conditions.

Enhancement

Dependency

The antivirus function is supported only by IPS models but not IDS models. Virus scanning cannot be performed on traffic of the IDS interface on the IPS model.

To enable the antivirus function, you must purchase and activate the antivirus update service. Once the antivirus function is enabled, it is not disabled even after the update service expires.

The antivirus capability relies on the version of the virus signature database. You must periodically update the signature database in online or offline mode to enable the NIP to detect the latest viruses.

The virus signature database update requires a database update license. The NIP can be updated within the validity period of the license. After the license expires, the NIP no longer enjoys the update service.

Acronyms and Abbreviations

Table 2-1 Acronyms and Abbreviations

Acronym and Abbreviation	Full Spelling
NIP	Network Intelligent Protection
IP	Internet Protocol
TCP	Transfer Control Protocol
UDP	User Datagram Protocol
ICMP	Internet Control Messages Protocol
IPS	Intrusion Prevention System
IDS	Intrusion Detection System
SNMP	Simple Network Management Protocol
MPLS	Multi-Protocol Label Switching
GRE	Generic Route Encapsulation
VLAN	Virtual Local Area Network
HRP	Huawei Redundancy Protocol
P2P	Peer to Peer
HTTP	Hypertext Transfer Protocol
HTTPS	Hypertext Transfer Protocol over Secure Socket Layer
DNS	Domain Name System
SIP	Session Initiation Protocol
POP3	Post Office Protocol 3
SMTP	Simple Mail Transfer Protocol
FTP	File Transfer Protocol