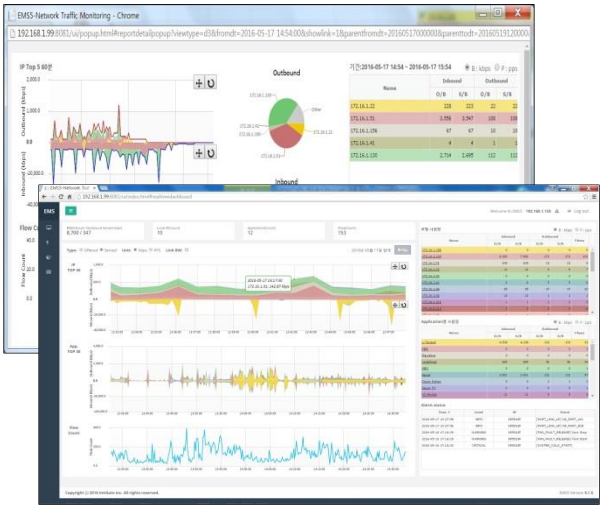
Next Generation L7 QoS Platform

NP5008/NP5016F



NP5016F

Overview

IntiGate's next generation QoS platform, NP5008 / NP5016F is a DPI-based L7 QoS switch which is controlling the application layer of traffic as a role of Internet gateway at last mile.

NP5008 / NP5016F primarily provides traffic management per application for all flows from hosts using DPI engine with L7 signatures. Its powerful traffic classification and management function helps operator to determine exactly which applications are running on each host of their network, and control them. It guarantees the quality of VoIP service and controls P2P traffic automatically and precisely, and it also enhances network security with real-time filtering on undesired URLs and applications based on pre-defined data base which can be easily modified by operator. Unified EMS/NPmon provides dashboard, real-time network monitoring and statistical reporting for multiple NP systems. It has a black-box architecture which accumulates its own analyzing data, so operators can access and monitor it easily using any types of internet browsing devices such as desktops, lab-tops and mobile devices due to its web-based architecture.

NP5008/NP5016F provides high visibility & understandability for the usage of local/remote hosts, services and applications. With an embedded black-box, operator can trace the reason that causes the network collapse with the method of analyzing the traffic history data stored at it.

Key Features

DPI based Traffic Management

- Traffic management based on real-time detection of application
- Precise traffic management combined with IP, service port number and application
- Minimum guaranteed bandwidth & maximum limited bandwidth on more than 8K queues
- Hierarchical QoS on each Application Group Queues
- Egress scheduling with maximum 32 Application Group Queues
- Real-time detection & guarantee of VoIP and IPTV traffic
- Dynamic Fair Sharing for all subscribers with zero-configuration
- Minimum 1K user-defined polices

Security Solution

- Real-time detection of applications using DPI engine with L7 signatures
- Real-time URL matching and filtering for about 1M harmful site DB
- Continuous update on suspicious URL by EMS
- Security policy combined with IP, service port number and application
- Real-time detection, logging and blocking of DDoS attack / abnormal traffic based on traffic behavior model

Network Visibility and Analysis

- Multi-dimensional monitoring focused on application and subscriber with minimum 1 second interval
- Various and efficient analyzing functions based on relational DB
- Real-time management based on system event and logging

Keep Signature Up-to-date

- On-demand & prompt delivery based on 'automatic analysis and extract technology'
- Periodical signature update on new applications

IntiGate

NP5000 Series

Next Generation
L7 QoS Platform

NP5008 / NP5016F

Next Generation L7 QoS Platform

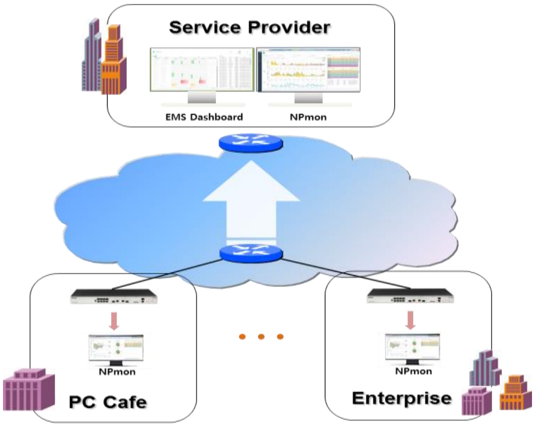
EMS / NPmon

IntiGate provides the centralized traffic monitoring & reporting system as combined EMS with NPmon, which is managing multiple nodes up to several hundreds.

As shown below, EMS provides the dashboard which depicts the current traffic status for all nodes and NPmon linked to each node as for single node, provides a detailed monitoring & reporting information for specific node.

This system architecture collects real-time data stored at SD card device in NP5008/NP5016F as black-box and then provides dashboard & real-time monitoring/reporting function.

NPmon program is distributed to each node operators and boosts them to build up the network policy & the countermeasure to fault by helping to understand the status of event & traffic at node easily.



The dashboard provides the status of traffic for every single node & event for all nodes as a single page, and helps operators to understand a whole status of all nodes and to countermeasure all faults promptly. Not only traffic usage is displayed as a unit of bps, pps and fps, and but also event message shows the occurred time, level and details as table.

Real-time monitoring function shows the detailed traffic status such as traffic summary for link, traffic usage level for IP/application, flow count and event status as both forms of linear graph and table.

Reporting function provides the traffic information of specific date & time per IP & application by the method of search function, and also flow count and event history, as well.

Effect

- Easy tracking & prompt countermeasure for the network failure with black-box structure
- Improvement of network stability through enhanced security function
- Reinforcement of policy for optimal network operation through analyzing reporting data

Specifications

System Capacity

Switching Performance	36G
Packet Queue	8K
User Policy	1K
URL Filter	1M

Hardware

Interface	- LAN . NP5016F: 16 x 1G UTP & FX(SFP) . NP5008 : 8 x 1G UTP - WAN : 2 x 1G UTP or SFP Combo
Dimensions	432mm(W) x 270mm(D) x 43mm(H)
Power Consumption	110 ~ 240V AC, Max. 55Watts
Operational Temperature & Humidity	0 ~ 50°C / 10 ~ 90%

Software

QoS	- L1~L7 Packet Classification - DPI based application recognition by DB - Packet Marking/Remarking - QoS Mode (SPQ, Min/Max BW on 4 Priority Group, Dynamic BW sharing on each IP, Static, Hierarchical BW allocation) - Re-allocation of idle BW Automatically - Traffic Shaping/Limiting - Min/Max rate setting by traffic class - ACL - P2P traffic analysis and control
Security	- DDoS attack defense (IP scan, port scan, TCP/UDP/ICMP flooding) - URL filtering - Application filtering using DPI - Abnormal traffic protection on CPU - ARP inspection - IP spoofing protection - NetBIOS filtering - Max host limitation using MAC count - One IP & One MAC - MAC flood guard
Monitoring / Reporting	- Single/Multi node management - Dashboard (real-time traffic status of each node, event, server performance monitoring) - Real-time monitoring (Link traffic summary, IP top30, Application top30, Flow count, Event, Multi/detail chart) - Reporting (Statistical information of IP top30, Application top30, Flow count, Event, Multi/detail chart) - Traffic monitoring on Inbound/Outbound and Offered/Served
Network	- 802.1D/802.1Q/802.3ad - MAC Address Filtering - Static Routing (Min. 1K Subnet) - Default Gateway (Min. 2) - ECMP routing - Link Load Balancing - Secondary IP / Loopback IP - Hardware based Routing - Routing Loop protection - IPv6 - Packet filtering (IP Flow & L4 Port) - DHCP - VRRP - NTP - Multicast (IGMP proxy, IGMP snooping) - NAT (Static, Dynamic, PAT)
Management	- CLI, EMS, NPmon - SNMP, Syslog - Port Mirroring - Dying Gasp/Auto recovery/Die reason