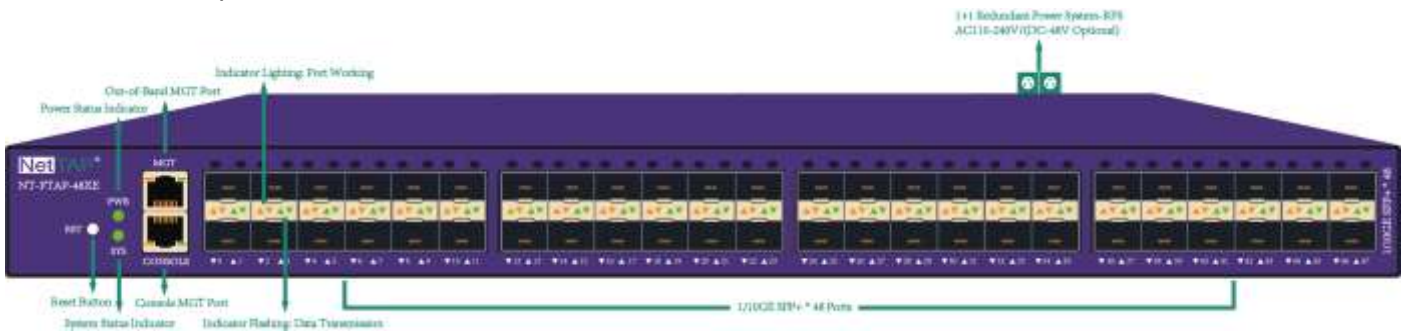
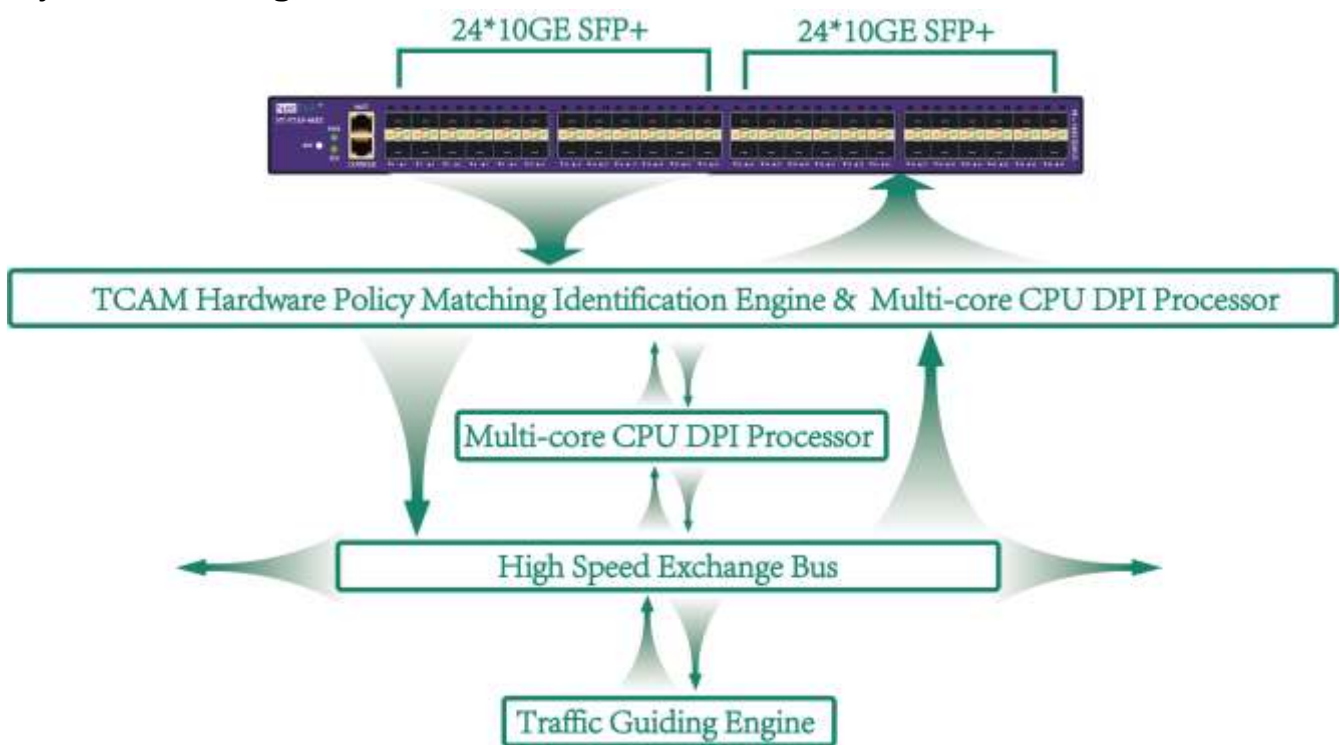


1- Overviews

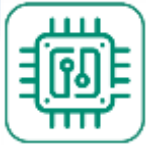
- ☞ A full visual control of Data Acquisition device(48ports \* 10GE SFP+ port)
- ☞ A full Data Scheduling Management device(Max 24\*10GE ports duplex Rx/Tx processing)
- ☞ A full pre-processing and re-distribution device(bidirectional bandwidth 480Gbps)
- ☞ Supported collection & reception of link data from different network element locations
- ☞ Supported collection & reception of link data from different switch routing nodes
- ☞ Supported raw packet collected, identified, analyzed, statistically summarized and marked
- ☞ Supported raw packet output for monitoring equipment of BigData Analysis, Protocol Analysis, Signaling Analysis, Security Analysis, Risk Management and other required traffic.
- ☞ Supported real-time packet capture analysis, data source identification, and real-time/historical network traffic search



2- System Block Diagram



### 3- Intelligent Traffic Processing Abilities



#### ASIC Chip Plus Multicore CPU

*480Gbps intelligent traffic processing capabilities*



#### 10GE Acquisition

*10GE 48 ports, Max 24\*10GE ports Rx/Tx duplex processing, up to 480Gbps Traffic Data Transceiver at same time, for network Data Acquisition, simple Pre-processing*



#### Data Replication

*Packet replicated from 1 port to multiple N ports, or multiple N ports aggregated, then replicated to multiple M ports*



#### Data Aggregation

*Packet replicated from 1 port to multiple N ports, or multiple N ports aggregated, then replicated to multiple M ports*



#### Data Distribution

*Classified the incoming metadata accurately and discarded or forwarded different data services to multiple interface outputs according to user's predefined rules.*



#### Data Filtering

*Supported L2-L7 packet filtering matching, such as SMAC, DMAC, SIP, DIP, Sport, Dport, TTL, SYN, ACK, FIN, Ethernet type field and value, IP protocol number, TOS, etc. also supported flexible combination of up to 2000 filtering rules.*



#### Load Balance

*Supported load balance Hash algorithm and session-based weight sharing algorithm according to L2-L7 layer characteristics to ensure that the port output traffic dynamic of load balancing*



#### UDF Match

*Supported the matching of any key field in the first 128 bytes of a packet. Customized the Offset Value and Key Field Length and Content, and determining the traffic output policy according to the user configuration*



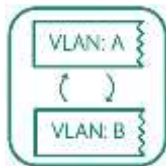
### VLAN Tagged



### VLAN Untagged



### VLAN Replaced



### MAC Address Replacement

Supported the replacement of the destination MAC address in the original data packet, which can be implemented according to the user's configuration



### 3G/4G Mobile Protocol Recognition/Classification

Supported to identify mobile network elements such as (Gb, Gn, IuPS, S1-MME, S1-U, X2-U, S3, S4, S5, S6a, S11, etc. interface). You can implement traffic output policies based on features such as GTPV1-C, GTPV1-U, GTPV2-C, SCTP, and S1-AP based on user configurations.



### IP Datagram Reassembly

Supported IP fragmentation identification and supports reassembly of IP fragmentation so as to implement L4 feature filtering on all IP fragmentation packets. Implement traffic output policy.



### Ports Healthy Detection

Supported real-time detection of the service process health of the back-end monitoring and analysis equipment connected to different output ports. When the service process fails, the faulty device is automatically removed. After the faulty device is recovered, the system automatically returns to the load balancing group to ensure the reliability of multi-port load balancing.



### Time Stamping

Supported to synchronize the NTP server to correct the time and write the message into the packet in the form of a relative time tag with a timestamp mark at the end of the frame, with the accuracy of nanoseconds



### VxLAN, VLAN, MPLS Untagged

Supported the VxLAN, VLAN, MPLS header in the original data packet is stripped and output.



### Data De-duplication

Supported port-based or policy-level statistical granularity to compare multiple collection source data and repeats of same data packet at a specified time. Users can choose different packet identifiers (dst.ip, src.port, dst.port, tcp.seq, tcp.ack)



### Data Slicing

Supported policy-based slicing (64-1518 bytes optional) of the raw data, and the traffic output policy can be implemented based on user configuration



### Classified Data Hidden

Supported policy-based granularity to replace any key field in the raw data in order to achieve the purpose of shielding sensitive information. According to user configuration, the traffic output policy can be implemented.



### Tunneling Protocol Identify

Supported automatically identify various tunneling protocols such as GTP / GRE / PPTP / L2TP / PPPOE. According to the user configuration, the traffic output strategy can be implemented according to the inner or outer layer of the tunnel



### APP Layer Protocol Identify

Supported commonly used application layer protocol identification, such as FTP, HTTP, POP, SMTP, DNS, NTP, BitTorrent, Syslog, MySQL, MsSQL and so on



### Video Traffic Filtering

Supported identify Video Protocol, such as: Youtube, RTSP, MSTP, Youku, etc. According to user configuration, the traffic output policy can be implemented.



### Mail Protocol Identify

Supported identify Email Protocol such as: SMTP, POP3, IMAP, SMTP, etc. According to user configuration, the traffic output policy can be implemented.



### Game Protocol Identify

Supported identify Game Protocol such as: World of Warcraft, Warcraft, Half-life, Battlefield, games on steam platform, etc. According to user configuration, the traffic output policy can be implemented.



### Online Chat Tools Identify

Supported identify Instant Messaging Protocol, such as: Messenger, WhatsApp, Skype, Wechat, QQ, Alitalk, etc. According to user configuration, the traffic output policy can be implemented.



### Packet Capturing

Supported port-level, policy-level packet capture from source physical ports within filter of Five-Tuple field in real time



### Real-time Traffic Trend Monitoring

Supported real-time monitoring and statistics on port-level and policy-level data traffic, to show the RX / TX rate, receive / send bytes, No., RX / TX the number of errors, the maximum income / hair rate and other key indicators.



### Traffic Trend Alarming

Supported port-level, policy-level data traffic monitoring alarms by setting the alarm thresholds for each port and each policy flow overflow.



### Historical Traffic Trend Review

Supported port-level, policy-level nearly 2 months of historical traffic statistics query. According to the days, hours, minutes and other granularity on the TX/RX rate, TX/RX bytes, TX/RX messages, TX/RX error number or other information to query select.



### Packet Analysis

Supported the captured datagram analysis, including abnormal datagram analysis, stream recombination, transmission path analysis, and abnormal stream analysis



**Unified Control Platform**

Supported NetTAP® Matrix-SDN Visual Control Platform Access

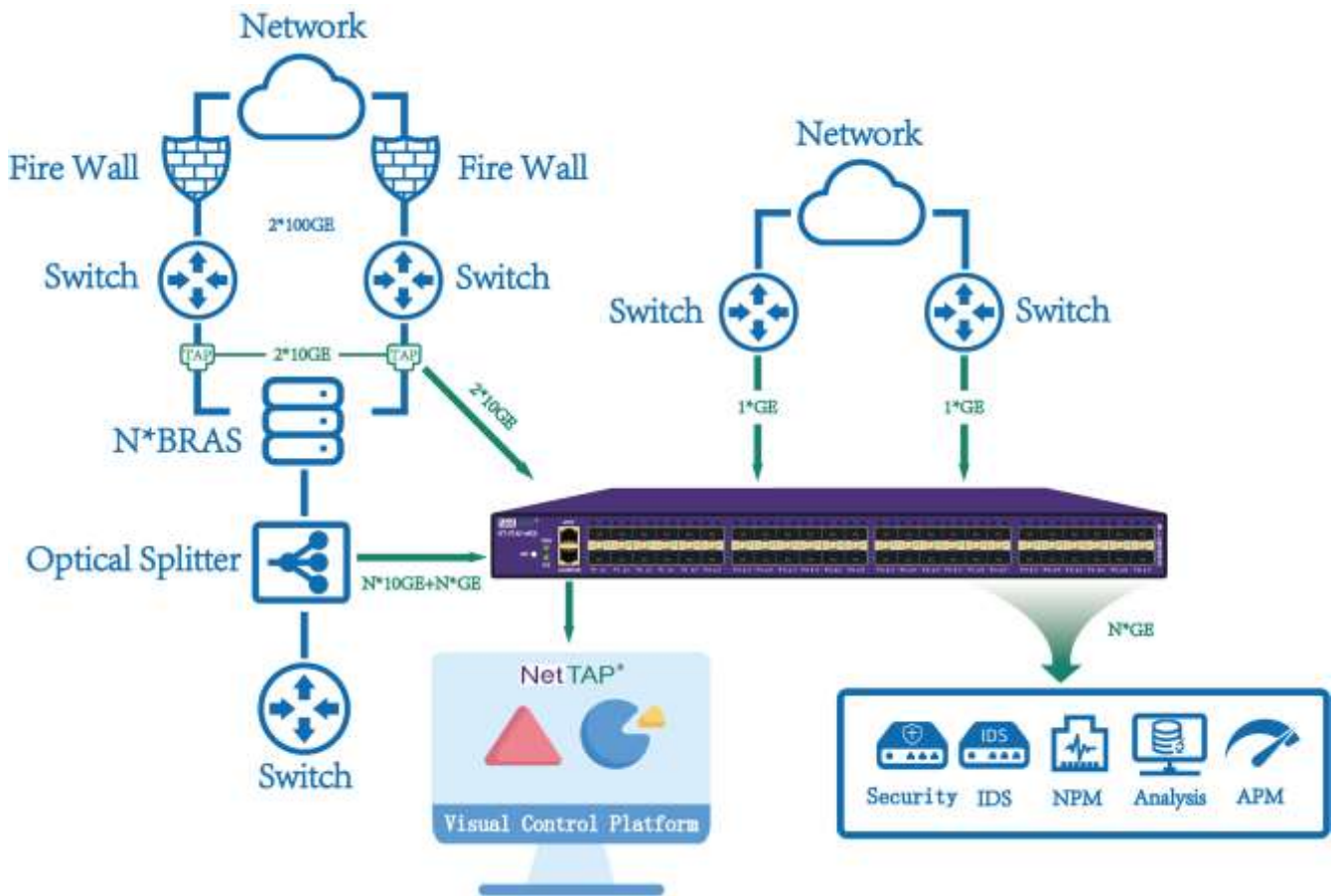


**1+1 Redundant Power System(RPS)**

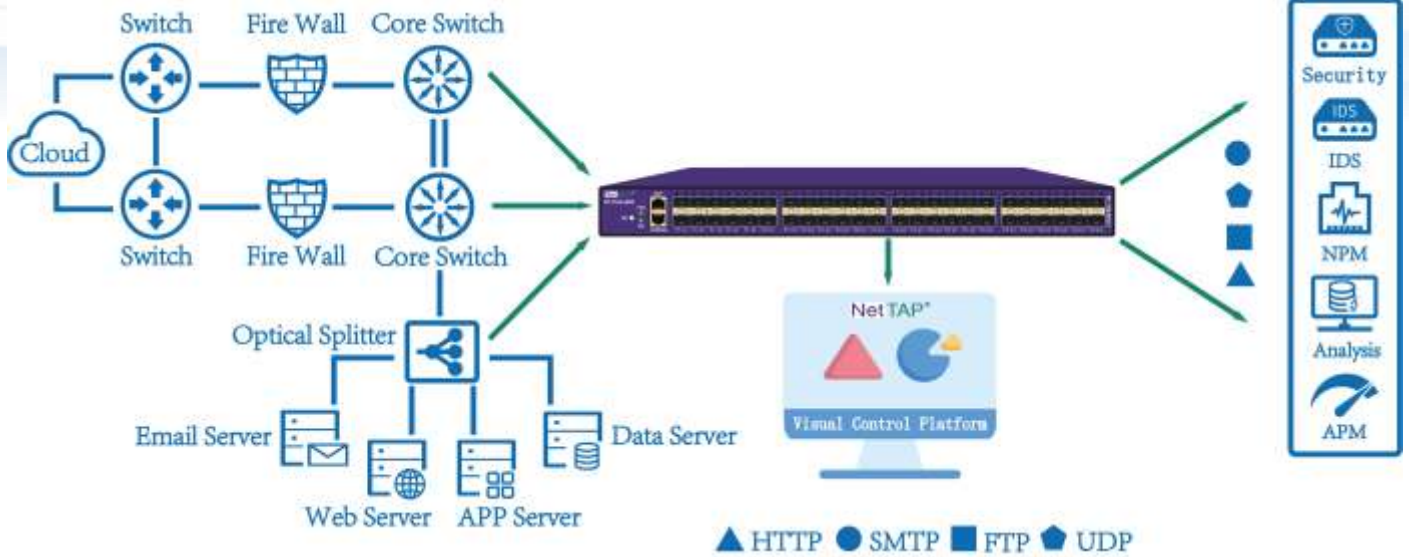
Supported 1+1 Dual Redundant Power System

**4- Typical Application Structures**

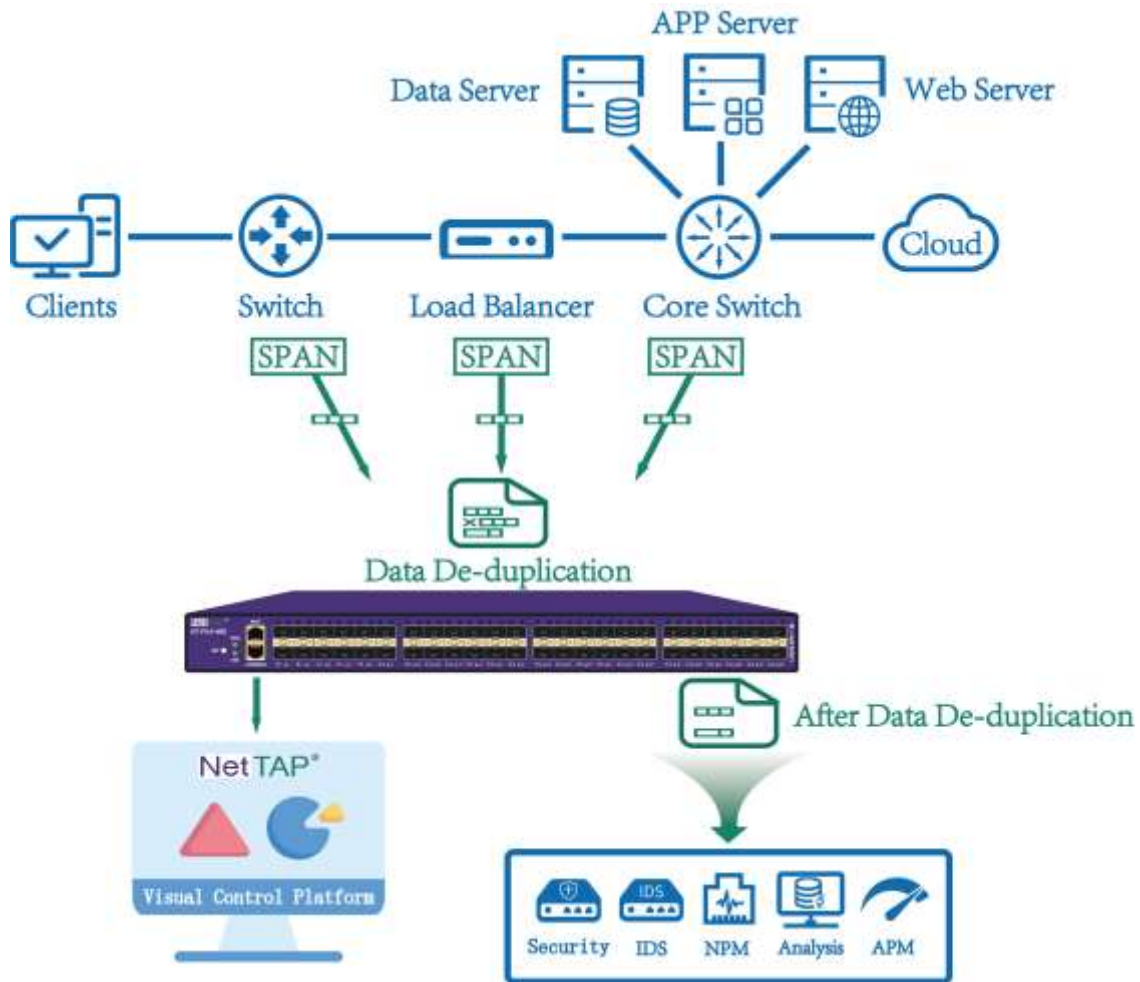
**4.1 Centralized Collection Replication/Aggregation Application(as following)**



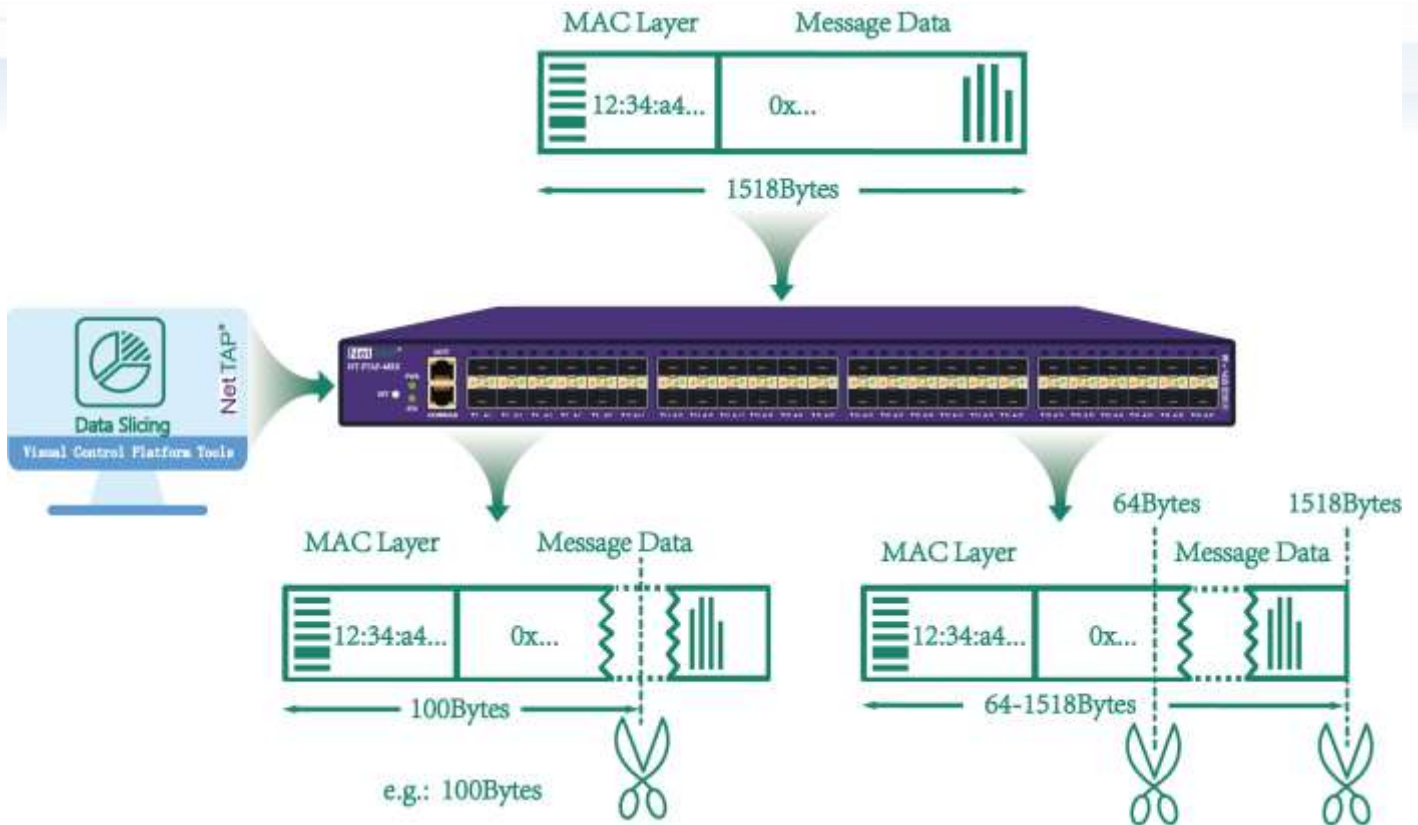
**4.2 Unified Schedule Application for Data Monitoring(as following)**



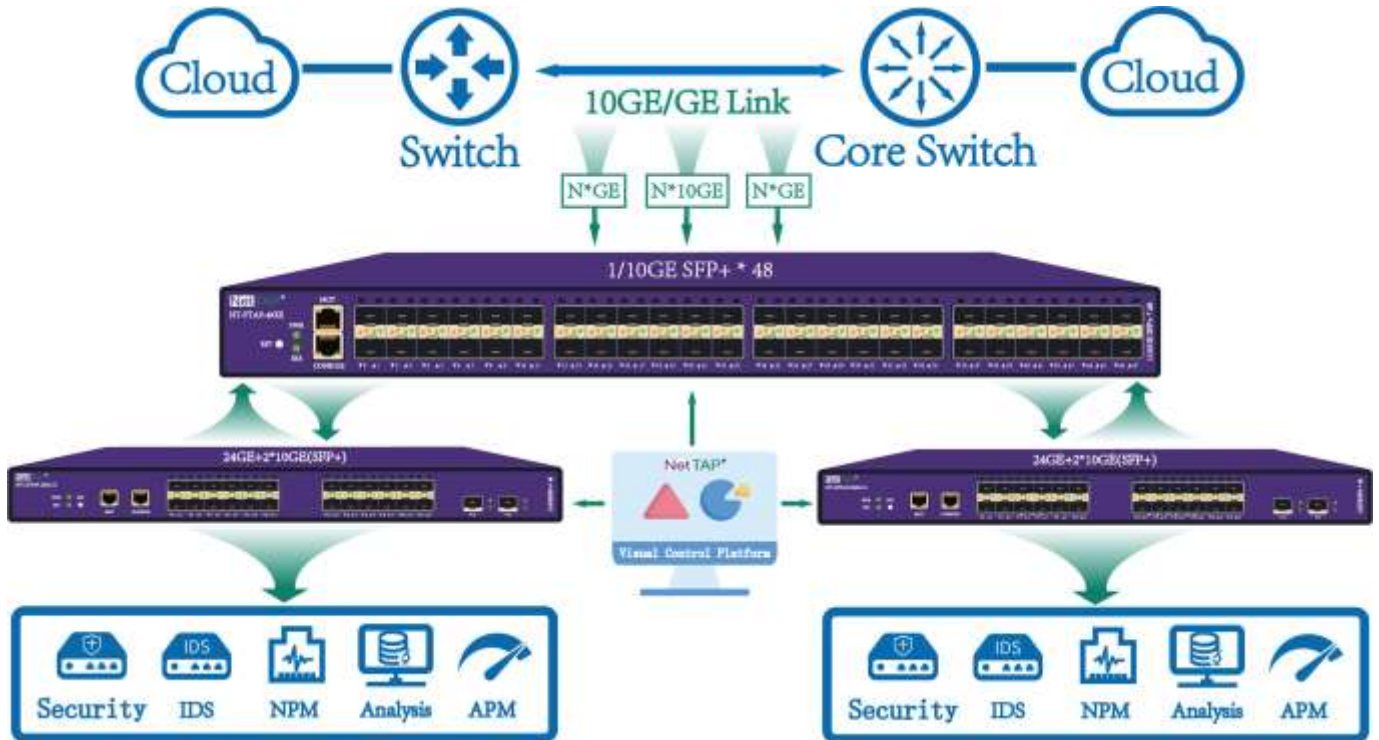
4.3 Data De-duplication Application(as following)



4.4 Data Slicing Application(as following)



4.5 Hybrid Access Application for Data Acquisition/Replication/Aggregation(as following)



4.6 Data Hidden/Mask Application(as following)

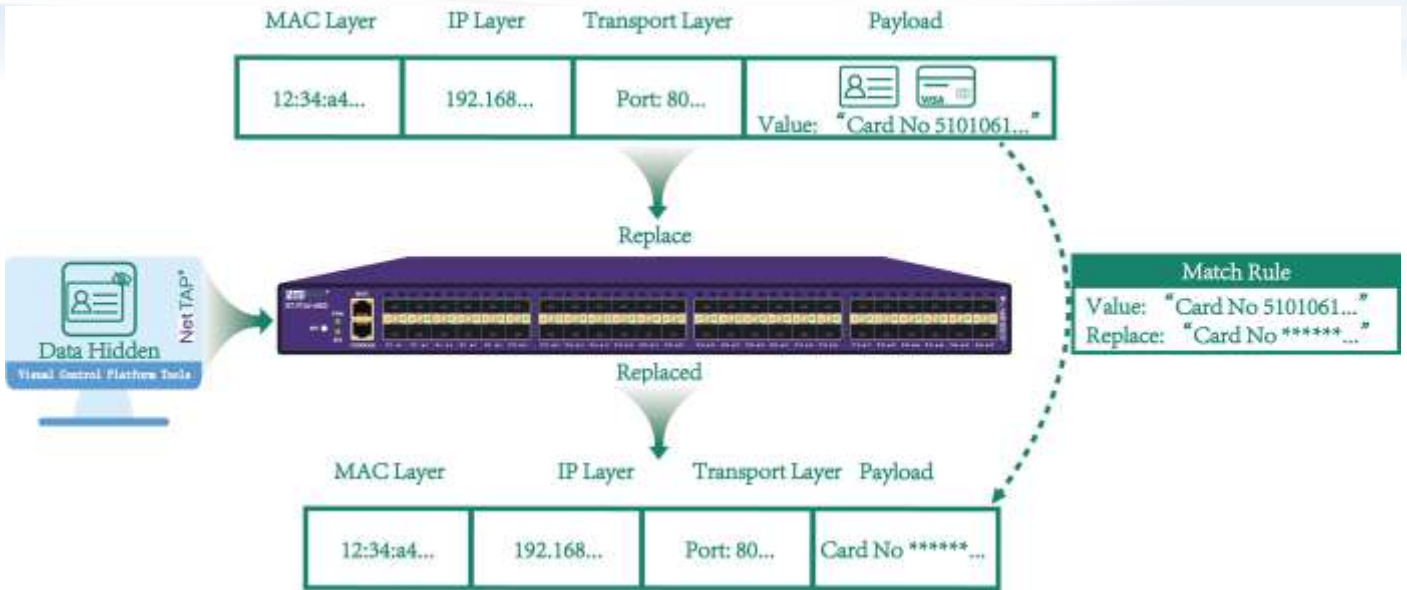
Your Network Traffic Visual Control One-stop Provider

\*Specifications subject to change without notice\*

2F, G4 of TianFu Software Park, Chengdu, China  
 +86-136 7909 3866  
 jerry@nettap.com.cn  
 www.nettap.com.cn







5- Specifications

NT-FTAP-48XE NetTAP® NPB Functional Parameters		
Network Interface	10GE SFP+ ports	48 * SFP+ slots; support 10GE/GE; support for single and multi-mode fiber
	Out of Band management interface	1* 10/100/1000M electrical interface;
Deployment mode	10Gigabit spectral acquisition	Support 24*10GE bidirectional fiber links acquisition
	10Gigabit Mirror span acquisition	Support up to 48 mirror span traffic ingress
	Optical Splitter input	Input port can support single-fiber ingress;
	Port multiplexing	Support input ports simultaneously as output ports;
	Traffic output	Support 48 *10GE ports traffic output;
	Traffic replication / aggregation / distribution	support
	Link QTYs supporting Mirror replication / aggregation	1 -> N link traffic replication (N <48) N-> 1 link traffic aggregation (N <48) G Group(M-> N Link) traffic replication and aggregation [G * (M + N) <48]
Distribution based on traffic identification	support	

NetTAP® Network Packet Broker (NPB)

NT-FTAP-48XE

	Distribution based on IP / protocol / port Five tuple traffic identification	support
	Distribution strategy based on protocol header the key labeled traffic identifies	support
	Ethernet encapsulation independence	support
	CONSOLE network management	support
	IP/WEB network management	support
	SNMP network management	support
	TELNET/SSH network management	support
	SYSLOG protocol	support
	User authentication function	Password authentication based on user name
Electric(1+1 Redundant Power System-RPS)	Rated supply voltage	AC110-240V/DC-48V [Optional]
	Rated power frequency	AC-50HZ
	Rated input current	AC-3A / DC-10A
	Rated power function	200W
Environment	Operating Temperature	0—50°C
	Storage Temperature	-20-70°C
	Operating Humidity	10%-95%, Non-condensing
User Configuration	Console Configuration	RS232 Interface,115200,8,N,1
	Password authentication	support
Rack Height	Rack space (U)	1U 485mm*44.5mm*350mm