Array

Array NTB

Network Traffic Broker

DATASHEET

Array Traffic Brokers offer enhanced visibility, improved security, scalability, performance optimization, simplified management, cost efficiency,and compliance benefits, making them valuable components of modern network infrastructure.

Array Traffic Brokers are designed to improve network security and optimize network traffic. It delivers scalability, performance optimization, simplified management, cost efficiency and compliance benefits, making them valuable components of modern network infrastructure.

Organizations benefit from improved network security, efficient incident response, optimal resource utilization, network performance optimization, regulatory compliance support, simplified management, scalability, and return on investment by deploying network packet brokers within their network infrastructure.

Function Description

Pervasive Inspection

A common data acquisition infrastructure to monitor WAN to LAN, Physical, Virtual, OOB, In-line.

Security Function Offload

Deliver only "packets of interest" for each security device by sophisticated filtering.

Perimeter Defense

Detect, trace and block Internet connection in the frontline according to a massive blacklist of IP and domains.

Function List

Any-to-Any Delivery

- Each interface can be INPUT or OUTPUT
- 1-to-many, many-to-1, many-to-many
- To any selected interface after filtering

Advanced Distribution

- Filter Processor
- Composed of a set of rules with AND/ OR operation
- Session-based filtering and packet-based filtering
- L2-L4 header filtering rule: MAC address, Ethertype, VLAN ID, IP range, TCP/UDP port...
- DPI-enabled Filter Processor
- L4-L7 Pattern-based filtering
- Pattern format: HEX, ASCII strings and Regular Expression
- Tunnel-awareness filter
- Apply all filtering rules on in-tunnel packets where GRE / VxLAN / QinQ / MPLS
- Tunnel ID (ERSPAN/X-tunnel) filtering
- Processor Chain
- User-defined graphs of Filter Processors

Function List

Out-of-band Load balance

- Same Dst IP/ Src IP/ Dst Port/ Src Port sticky to same egress ports
- Same 5-tuple hash sticky to same egress ports
- Delivery HA: Re-distribute to link-up egress ports
- Balance port groups: Max 16 egress ports

Packet Engineering

- Tag removal: MPLS / VLAN / QinQ...
- Unpacking Tunnel (Tag removal and re-encapsulation): GRE / GTP / ERSPAN / NvGRE / VxLAN
- User-defined VLAN tagging for input packets or output packets
- Packet Deduplication

Monitoring Network Virtualization

- GRISM to GRISM tunnel
- Encapsulation: GRE, VxLAN, ERSPAN, X-tunnel

Encapsulation: GRE, VxLAN, ERSPAN, X-tunnel

- Generate Netflow V5/ V9
- Generate HTTP log
- Generate DNS log

Front-line Security

- Massive Blocking
  - IP/ Domain/ URL
  - Max 2,000,000 entries
- 3rd party threat intelligence import

Sensitive Data Protection

- Packet slicing
  - Preserve N bytes Remove TCP/
  - UDP payload
- Data mask
  - Replace sensitive data segment in TCP/ UDP payload
  - Data segment can be defined in regular expression

Function List

In-Line Aggregation and Re-Distribution

- N network links *M monitoring links (N*M)
- In-line session-based load balance with HA strategy
- Intelligent content-based bypass
  - IP address List
  - User-defined pattern in regular expression

PCAP File Processing

- Stream snapshot in PCAP format
- Filter PCAP files with timestamp persistance
- Remote recording agent over L2-L4 switch

Telecom Correlation Processing

- Mobile 3G / LTE data network
  - Filter GTP-C / GTP-U by IMSI/IMEI
  - Subscriber-based load balance
- Fixed ISP network
  - Filter user-plane packets by RADIUS ID
  - Subscriber-based load balance

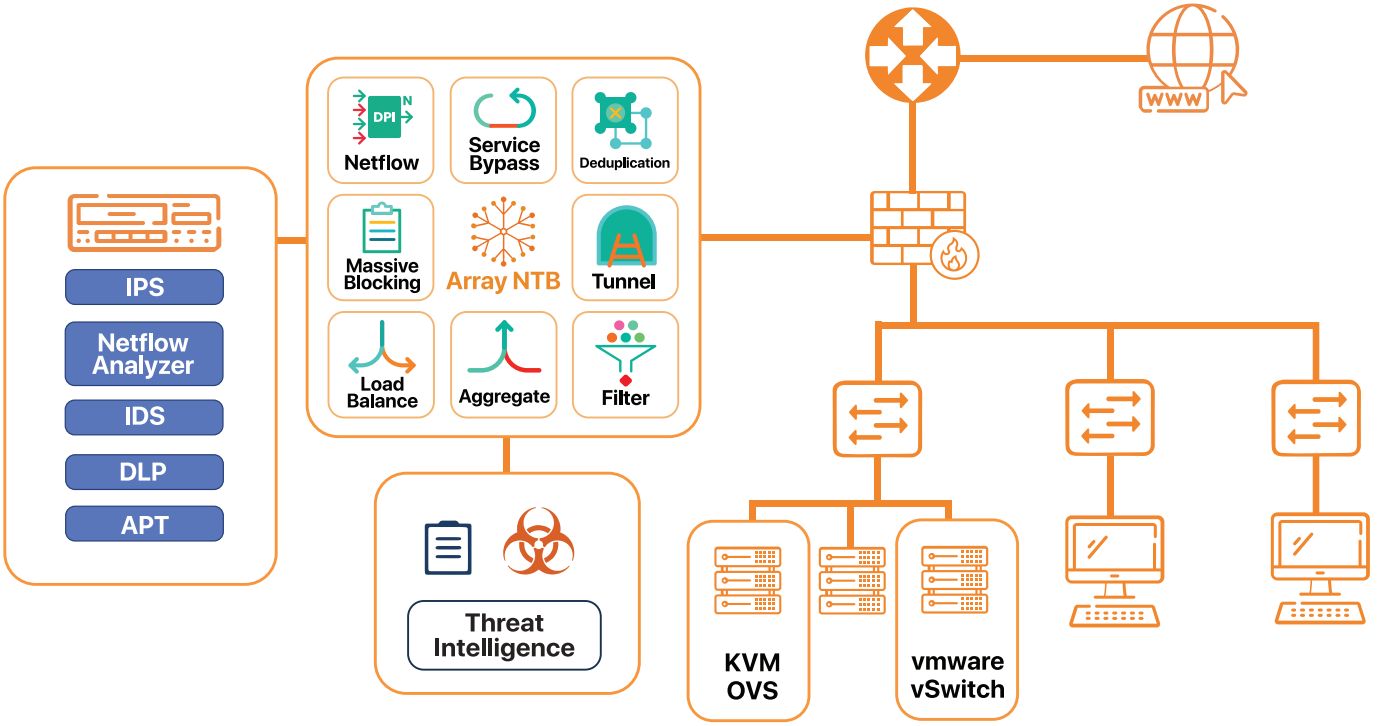
Virtual Machine Traffic

- VM traffic redirection by GRISM-V (as a VM instance)
- Supporting environment
  - KVM
  - VMware ESXi / vSphere

System Control and Operation

- Web GUI agent for authenticated users
- Advanced Control
  - XML script over HTTP
- Management protocol: Telnet, HTTP, SNMP V2

Array Traffic Broker Architecture



Hardware Specs

	NTB G8-BP1	NTB G8-BP2	NTB G8i-BP2	NTB T12s
Basic L2-L4 Throughput	**8Gbps**	**8Gbps**	**8Gbps**	**120Gbps**
Advanced L4-L7 Throughput	**4Gbps**	**4Gbps**	**4Gbps**	**20Gbps**
L2-L4 Filter	eth.addr / eth.src / eth.dst / eth.type, vlan.id / vlan.l2.id / vlan.priority ip / ip.addr / ip.src / ip.dst / ip.proto / ip.fragment / ip.flags.df ip.flags.mf / ip.dsfield / ipv6 / ipv6.addr / ipv6.src / ipv6.dst / ipv6.nxt tcp / tcp.port / tcp.srcport / tcp.dstport / tcp.flags.syn tcp.flags.ack / tcp.flags.fin / tcp.flags.reset udp / udp.port / udp.srcport / udp.dstport, sctp			
L4-L7 Filter	gtp.cp / gtp.data / gtp.imsi gtp.teid, ip.addr.related.gtp.imsi, voip voip.account / voip.from / voip.to dns.a / dns.flags.response / dns.count.add_rr / dns.qry.type dns.qry.name / dns.qry.name_public_suffix / dns.qry.name.resp.ip.addr http/ http.request/ http.request.method / http.request.url, ssl ssl.server_name / ssl.server_name_public_suffix / ssl.handshake.type / ssl.ja3_digest arp / arp.request / arp.reply / arp.request.target.ip arp.request.sender.ip, ftp/ regex / grism.srcport / grism.port.linkdown session.packet.nth/ heartbeat.target.miss.nth heartbeat.target.miss.id, flowtable.matched.fid flowtable.inport / gre / erspan.spanid			
Dimension	1U, 17.3" Wx8.6"Dx1.7"H	1U, 17.3" Wx8.6"Dx1.7"H	1U, 17.3" Wx8.6"Dx1.7"H	1U, 17.3" Wx8.6"Dx1.7"H
Network Interface	1G RJ45x8	1G RJ45x8	1G RJ45x8	10G x12
Hardware Bypass	1Pair GE (include)	2Pair GE (include)	2Pair GE (include)	None
Management Interface	1G RJ45*1			
System Console	HTTPS, CLI, XML over SFTP, RJ45			
Network Management	SNMP V2			
Load Balancing Group	8	8	8	8
Metadata Extraction	1:1 Netflow DNS/SSL syslog			
IoC(IP/Domain/URL) Capacity	1M	1M	1M	3M
Power Supply	Single PowerAC110-220v	Single PowerAC110-220v	Single PowerAC110-220v	Dual PowerAC110-220v

Hardware Specs

	NTB T12s-BP2	NTB T20	NTBAH32	NTBAH64
Basic L2-L4 Throughput	**120Gbps**	**200Gbps**	**3.2T**	**6.4T**
Advanced L4-L7 Throughput	**20Gbps**	**90Gbps**	**NONE**	**NONE**
L2-L4 Filter	eth.addr / eth.src / eth.dst / eth.type, vlan.id / vlan.l2.id / vlan.priority ip / ip.addr / ip.src / ip.dst / ip.proto / ip.fragment / ip.flags.df ip.flags.mf / ip.dsfield / ipv6 / ipv6.addr / ipv6.src / ipv6.dst / ipv6.nxt tcp / tcp.port / tcp.srcport / tcp.dstport / tcp.flags.syn tcp.flags.ack / tcp.flags.fin / tcp.flags.reset udp / udp.port / udp.srcport / udp.dstport, sctp			
L4-L7 Filter	gtp.cp / gtp.data / gtp.imsi gtp.teid, ip.addr.related.gtp.imsi, voip voip.account / voip.from / voip.to dns.a / dns.flags.response / dns.count.add_rr / dns.qry.type dns.qry.name / dns.qry.name_public_suffix / dns.qry.name.resp.ip.addr http/ http.request/ http.request.method / http.request.url, ssl ssl.server_name / ssl.server_name_public_suffix ssl.handshake.type / ssT.ja3_digest arp / arp.request / arp.reply / arp.request.target.ip arp.request.sender.ip, ftp/ regex / grism.srcport / grism.port.linkdown session.packet.nth/ heartbeat.target.miss.nth heartbeat.target.miss.id, flowtable.matched.fid flowtable.inport / gre / erspan.spanid		None	None
Dimension	1U, 17.3" Wx8.6"Dx1.7"H	1U, 17.3" Wx8.6"Dx1.7"H	1U, 17.3" Wx 21"Dx1.7"H	1U, 17.3" Wx 21"Dx1.7"H
Network Interface	10G x16	10G SFP+ x20 40G QSFP x 2+ 10G x12 40G QSFP x 4+ 10G x 4 25G x 4+ 10G x 4	100G GbE x 32 40G GbE x 32 10G GbE x 128	100G GbE x 64 40G GbE x 64 10G GbE x 256
Hardware Bypass	2 Pair 10G (include)	None	None	None
Management Interface	1G RJ45*1			
System Console	HTTPS, CLI, XML over SFTP, RJ45			
Network Management	SNMP V2			
Load Balancing Group	8	20	16	16
Metadata Extraction	1:1 Netflow DNS/SSL syslog		None	None
IoC(IP/Domain/URL) Capacity	3M	6M	None	None
Power Supply	Dual PowerAC110-220v	Dual PowerAC110-220v	Dual PowerAC110-220v	Dual PowerAC110-220v

Hardware Specs

	NTB AH6T48	NTB AH8T48
Basic L2-L4 Throughput	**1.08Tbps**	**2Tbps**
Advanced L4-L7 Throughput	**None**	**None**
L2-L4 Filter	eth.addr / eth.src / eth.dst / eth.type vlan.id / vlan.l2.id / vlan.priority ip / ip.addr / ip.src / ip.dst / ip.proto / ip.fragment / ip.flags.df / ip.flags.mf / ip.dsfield / ipv6 / ipv6.addr / ipv6.src / ipv6.dst / ipv6.nxt tcp / tcp.port / tcp.srcport / tcp.dstport / tcp.flags.syn / tcp.flags.ack / tcp.flags.fin / tcp.flags.reset udp / udp.port / udp.srcport / udp.dstport sctp / sctp.port / sctp.srcport / sctp.dstport 5-tuple	
L4-L7 Filter	None	None
Dimension	1U, 17.3" W x 18.6" D x 1.7" H	1U, 17.3" W x 21" D x 1.7" H
Network Interface	1G SFP/10G SFP+ x 48 100G QSFP28 x 6 / SFP28 x 4	10G SFP+/25G SFP28 x 48 40G QSFP+/100G QSFP28 x 8
Hardware Bypass	None	None
Management Interface	1G RJ45*1	
System Console	HTTPS, CLI, XML over SFTP, RJ45	
Network Management	SNMP V2	
Load Balancing Group	8	8
Metadata Extraction	None	None
IoC(IP/Domain/URL) Capacity	None	None
Power Supply	Dual Power 356W Hot-swappable AC100-240V	Dual Power 550W Hot-swappable AC100-240V

Key Functions

Delivery Accuracy

NTB aggregates several inputs and accurately delivers the packets by not only L2-L4 filtering but also the application-aware patternbased filtering above L4 : filter HTTP connection packets by HTTP URL, filter SIP messages by SIP URI, filter DNS by domain and so on.

NTB's Fair-Distribution mechanism satisfies every analysis device by properly duplicating the packet that belongs to the demand intersection for multiple analysis devices.

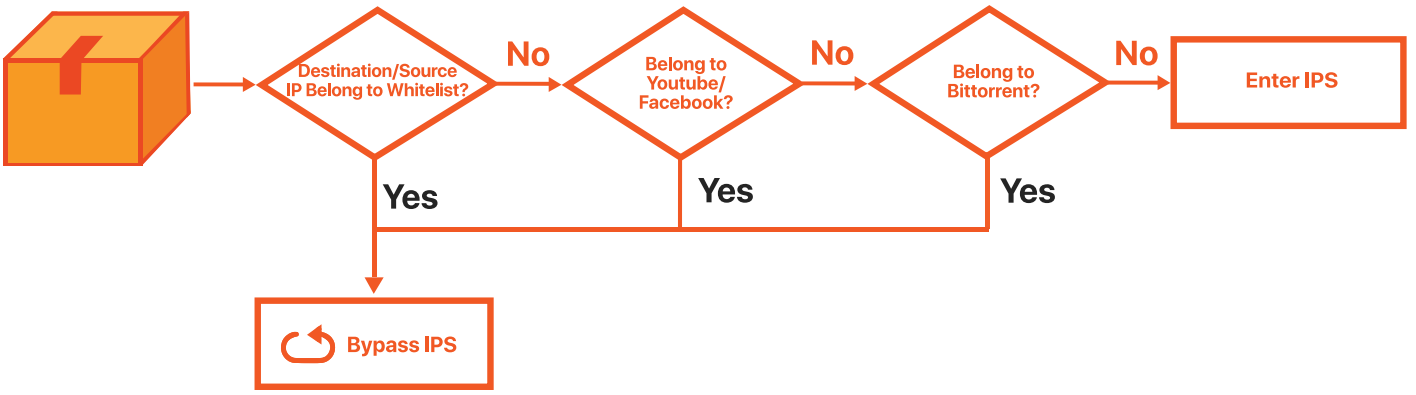
Filtered traffic can be distributed to a group of egress ports with session-based balancing strategy to guarantee "same session to the same destination". When one egress port is disconnected, NTB failovers the stream to the stand-by port or redistribute to the other ports in the group.

Tunnel Handling and Packet Re-engineering

The filtering functions can automatically apply on the tunnel payload if plain Ethernet packets and tunnel packets are mixed in the input traffic. Since most analysis devices can only handle plain packets well, NTB is able to do tag- removal or re-capsulation.

Moreover, slicing packet payload is supported for analysis offload such as removing TCP/UDP payload for the device that works on L2-L4 header only.

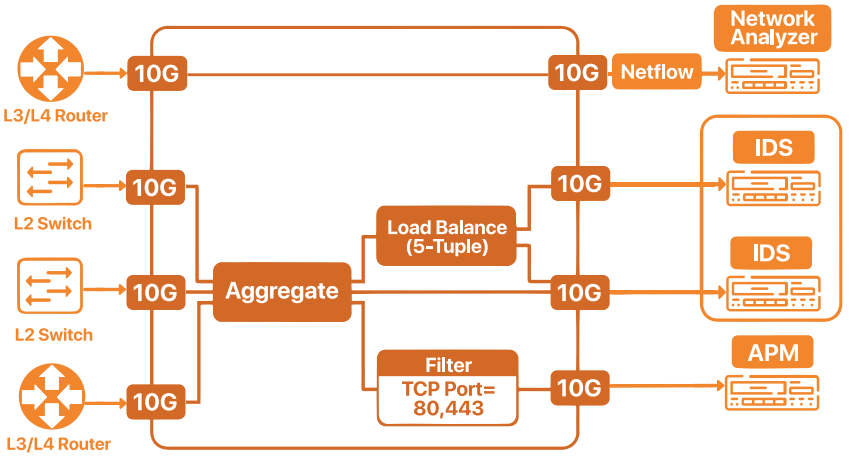
Intelligent Content - based Bypass



NTB supports Intelligent Bypass function to protect production network when in-line analysis devices are deployed. It detects the status of in-line device and immediately enable bypass when that device gets problems. The uniqueness of NTB is to bypass the traffic which is not the packet of interest or with little risk. For example, the enterprise deploys IPS guarded by NTB to avoid YouTube from entering IPS.

Netflow Generation

Some analysis devices also have a lightweight approach: processing Netflow instead of raw packets. Routers or switches are able to generate Netflow but the performance downgrade is inevitable. The better alternative is to let NTB generate Netflow v5/v9 by aggregating and analyzing the span traffic from those routers or switches while span is not a heavy burden. Besides Netflow, NTB is able to generate the application log for HTTP requests.

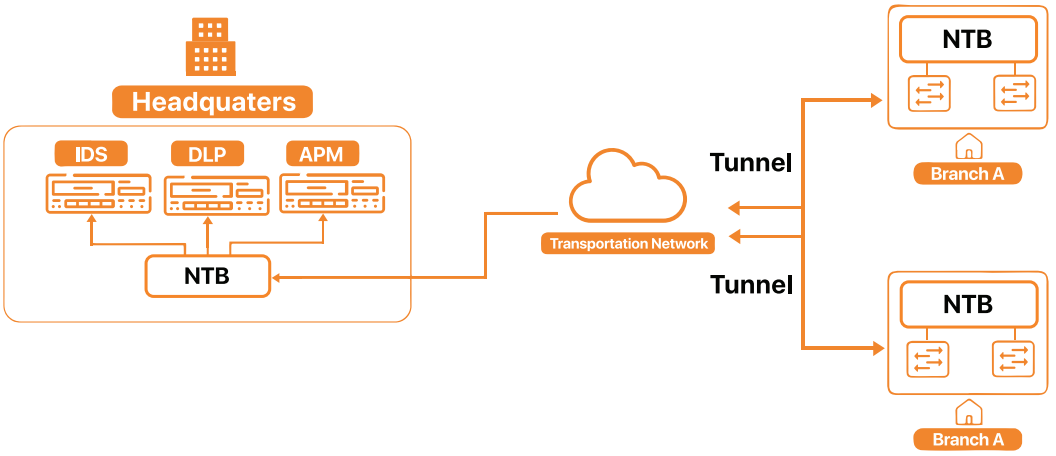


An out-of-band Monitoring Infrastructure

Software-defined Monitoring

NTB xUDN provides a XML script interface to fully control NTB. Comparing to APIs library, XML script is much easier for implementation with little learning overhead.

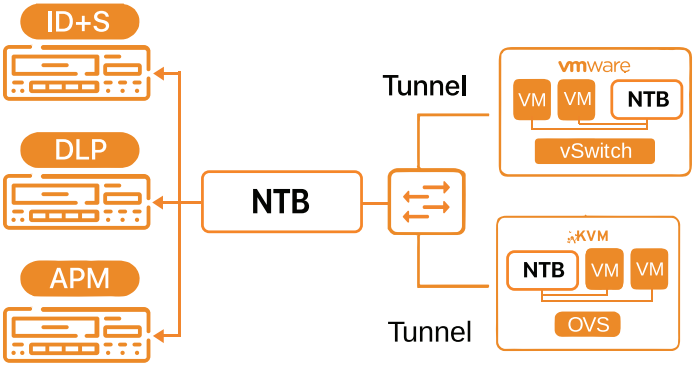
Monitoring Network Virtualization



Centralized Security Analysis Pool

To centralize the analysis resources such as network security devices, we can create the tunnel between two NTBs so that monitoring traffic, mirror span, from different offices can be aggregated to the single site, the tunnel receiver, through IP network. NTB support the proprietary X-tunnel and ERSPAN to carry the span traffic to form a many-to-one topology. The tunnel receiver unwraps the tunnel traffic and distinguish the sender by tunnel ID.

VM Traffic Monitoring



VM Traffic Monitoring

NTB can direct the traffic inside the virtualization environment to those analysis resources which have been in physical networks.

Feature Description

L2~L4 filtering:

NTB is capable of filtering packets by utilizing the protocol headers from Layers 2 to 4 to identify and isolate specific packets. Once these packets are isolated, further modifications or actions can be executed on them.

Traffic aggregation:

NTB's functionality allows for the merging of traffic from various ports into one unified stream. This streamlined process enhances network management, efficiency, and bandwidth utilization, facilitating improved input for security devices and the provision of VPN services.

Packet duplication:

NTB can replicate data streams from an ingress port to multiple egress ports. Combined with filtering and packet modification functionalities, this feature enables the achievement of specific, desired outcomes.

Traffic Redistribute:

NTB enables the redirection of traffic from any ingress port to any egress port. Coupled with additional NTB features, this function streamlines network management and bolsters network flexibility and scalability, particularly in environments with complex network protocols.

Vlan,QinQ Moditication/ Stripping:

NTB can modify VLAN and QinQ tags, facilitating easier network configuration without compromising security. This capability aids in the setup of security devices, allowing packets from multiple VLANs to be combined efficiently.

Threat Blocking:

NTB can block HTTP, SIP, and DNS traffic using specific identifiers like URLs and domain names. This feature allows NTB to efficiently block millions of IOCs, outperforming traditional firewalls in scale and efficiency.

Hardware Bypass:

NTB is equipped with a hardware bypass port. These ports work in pairs, ensuring that, should the NTB become unavailable, the paired bypass ports will maintain a pass-through connection.

Tunneling Support:

NTB can establish tunneling connections with other NTBs, enabling the collection of metadata from offsite networks. This capability facilitates the consolidation of network monitoring into a single environment.

Feature Description

Protocol Header Stripping:

NTB can efficiently removes unnecessary protocol headers like VXLAN, NVGRE, GRE, GENEVE, and ERSPAN from data packets, enhancing monitoring tool performance. It uniquely combines deduplication and header stripping for GRE, NVGRE, and VXLAN at a single point.

Heartbeat Protection:

NTB can send heartbeat packets to assess the health of the network path and intelligently bypass any disabled segments based on the feedback from these heartbeat packets.

Deduplication:

As NTB gathers packets from different network segments, duplications of the same packet can occur, potentially causing traffic congestion and overwhelming security devices. Implementing deduplication can resolve this by removing duplicate copies of packets.

Packet Slicing:

Many network data analyzers do not require access to packet payloads. By eliminating these payloads, there's a reduction in the risk of sensitive data leakage, as well as a decrease in traffic volume. This allows for more packets to be forwarded efficiently.

Deep Packet Inspection:

NTB's Deep Packet Inspection leverages regular expressions to identify and mask sensitive data in compliance with standards like HIPAA and PCI, streamlining setup. It efficiently detects patterns for privacy protection and virus threat identification, enhancing data security.

Netflow, HTTP log , DNA Generation:

NTB not only monitors and consolidates NetFlow records for improved efficiency and cost savings but also simplifies network analysis with 1:1 NetFlow capture and packet filtering. Additionally, it can generate HTTP logs and DNS data, enhancing network performance and monitoring.

Feature Comparison

Feature	NTB G8-BP1	NTB G8-BP2	NTB G8i-BP2	NTB T12s	NTB T12s-BP2	NTB T20	NT AH32	NT AH64	NT AH6T48	NT AH8T48			
L2~L4 filter	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓			
Traffic Aggregation	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓			
Packet Duplication	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓			
Traffic Redistribute	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓			
Vlan, QinQ Modification	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓			
Vlan Stripping	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓			
Threat Blocking	✓	✓	✓	✓	✓	✓							
Hardware Bypass	✓	✓	✓		✓								
Tunneling Support	✓	✓	✓	✓	✓	✓							
Protocol Header Stripping	✓	✓	✓	✓	✓	✓							
Heartbeat Protection	✓	✓	✓	✓	✓	✓							
Deduplication	✓	✓	✓	✓	✓	✓							
Packet Slicing	✓	✓	✓	✓	✓	✓							
Deep Packet Inspection	✓	✓	✓	✓	✓	✓							
Netflow, HTTP log , DNA Generation	✓	✓	✓	✓	✓	✓							

VERSION: JAN-2024-REV-A

1371 McCarthy Blvd.
Milpitas, CA 95035

www.arraynetworks.com

+1-866-MY-ARRAY
+1 408-240-8700