

PROACTIVE VISIBILITY CONSOLIDATES NETWORK SECURITY



Pervasive Inspection



Security Function Offloading



Perimeter Defense



Features

1. Any-to-Any Delivery

- 1.1 Each interface can be INPUT or OUTPUT
- 1.2 1-to-many, many-to-1, many-to-many
- 1.3 To any selected interface after filtering

2. Advanced Distribution

- 2.1 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...
- 2.2 DPI-enabled Filter Processor
 - L4-L7 Pattern-based filtering
 - Pattern format: HEX, ASCII strings and Regular Expression
- 2.3 Tunnel-awareness filter
 - apply all filtering rules on in-tunnel packets where GRE/VxLAN/QinQ/MPLS
 - tunnel ID(ERSPAN/X-tunnel) filtering
- 2.4 Processor Chain
 - User-defined graphs of Filter Processors

3. Out-of-band Load balance

- 3.1 Same Dst IP/Src IP/Dst Port/Src Port sticky to same egress ports
- 3.2 Same 5-tuple hash sticky to same egress ports
- 3.3 Delivery HA: Re-distribute to link-up egress ports
- 3.4 Balance port groups: Max 8 egress ports

4. Packet Engineering

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

5. Monitoring Network Virtualization

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

6. Network Traffic Intelligence Extraction

- 6.1 Generate Netflow V5/V9
- 6.2 Generate HTTP log
- 6.3 Generate DNS log

7. Sensitive Data Protection

- 7.1 Packet slicing
 - preserve N bytes
 - remove TCP/UDP payload
- 7.2 Data mask
 - Replace sensitive data segment in TCP/UDP payload
 - Data segment can be defined in regular expression

8. In-Line Aggregation and Re-Distribution

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

9. PCAP File Processing

- 9.1 Stream snapshot in PCAP format
- 9.2 Filter PCAP files with timestamp persistence
- 9.3 Remote recording agent over L2-L4 switch

10. Telecom Correlation Processing

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

11. Virtual Machine Traffic Monitoring

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

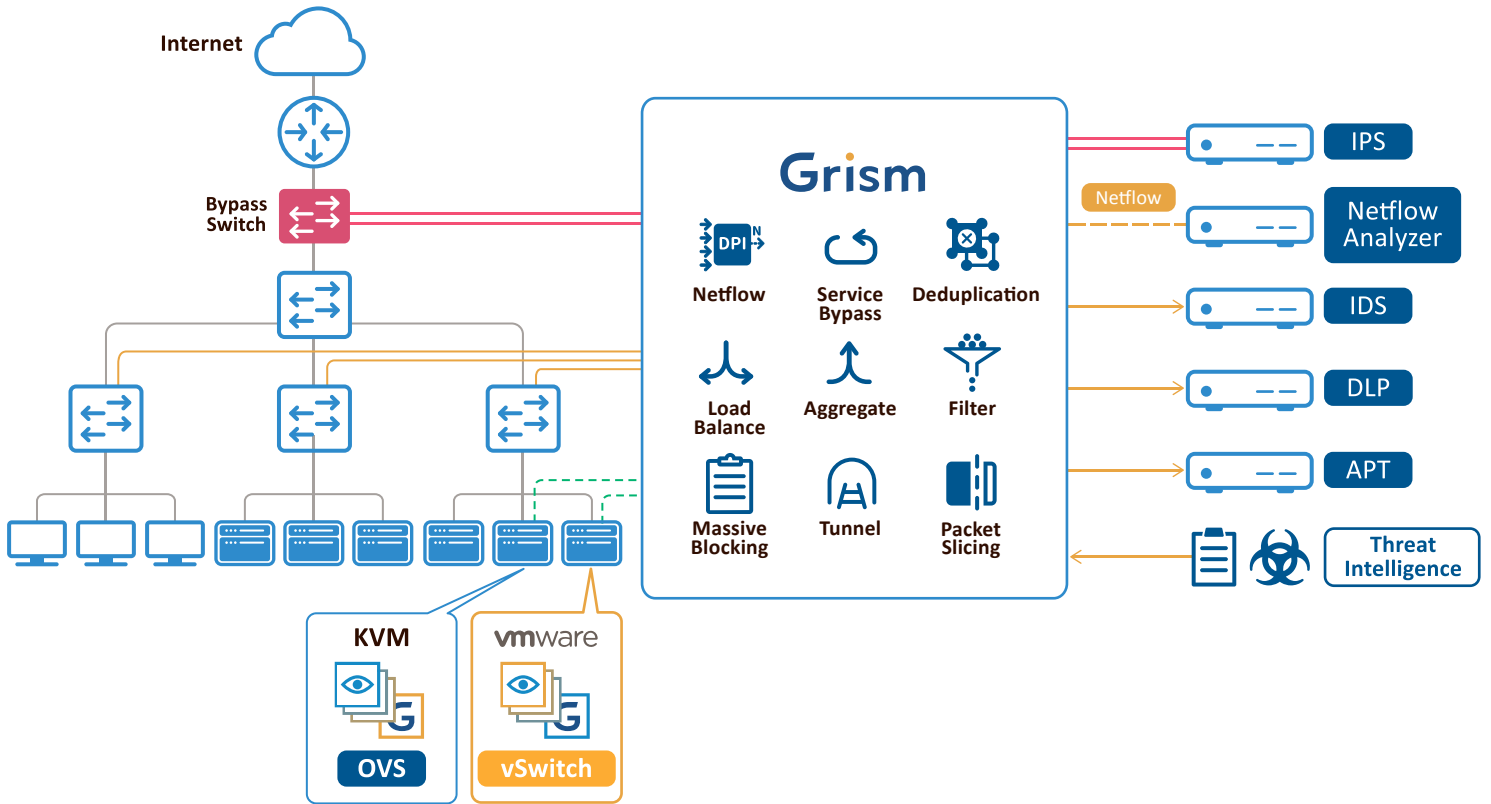
12. System Control and Operation

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

13. Front-line Security

- 13.1 Massive Blocking
 - IP/Domain/URL
 - Max 2,000,000 entries
- 13.2 3rd party threat intelligence import

Architecture diagram



Hardware Spec

	GRISM G8	GRISM T2G8	GRISM T16	GRISM T32
Network Interface	1G RJ45*8	10G SFP+*2 1G RJ45*8	10G/1G SFP+*16	10G/1GSFP+*32
Management Interface	1G RJ45*8	10G SFP+*2 1G RJ45*8	1G SFP*1	1G SFP*1
Data Processing	1.Ethernet 2.PCAP file	1.Ethernet 2.PCAP file	Ethernet	Ethernet
Storage	SATA2*1	SATA2*2	2GB (virtual disk)	2GB (virtual disk)
Forwarding or Replication	8Gbps	28Gbps	160Gbps	320Gbps
NetFlow Processing	3Gbps	10Gbps	30Gbps	60Gbps
Mechanical	Appliance	Appliance	Appliance	ATCA 3U two blade
Power	AC 110V-220V input	AC 110V-220V input	1.Dual DC -48V input 2.Dual AC 110V-220V input (with external PDU)	Dual AC 110-220V input

