IXIA CLOUDLENS PRIVATE

DATA SHEET

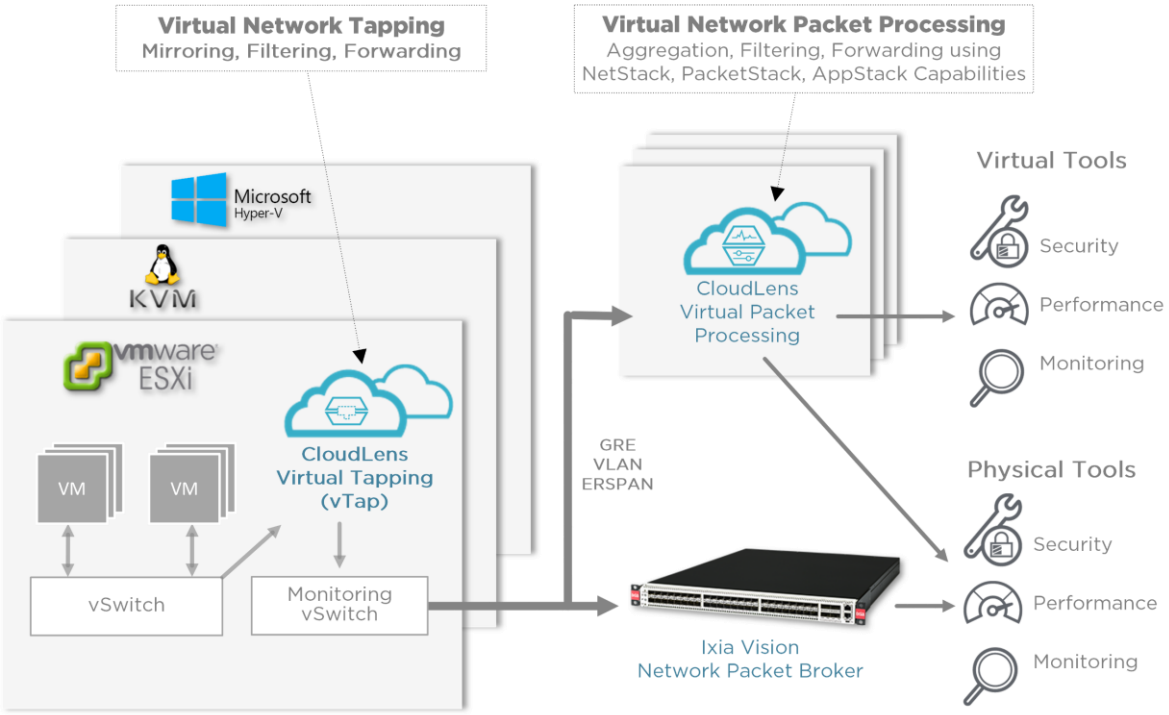
OVERVIEW

Enterprises are adopting cloud technologies in order to leverage the flexibility and power advantages of virtualized environments; they are adopting private cloud technology in order to increase control and reduce costs. However, the limited view of virtualized network traffic creates network blindspots for virtual or physical datacenter security, monitoring and analytics tools.

Ixia CloudLens™ Private, part of the broader CloudLens platform, provides a complete cloud-based visibility solution for virtual network traffic. With CloudLens private you can mirror data, filter and forward traffic between virtual machines and data center tools. It includes two core capabilities. First, an ability to virtually tap (vTap) or capture, filter and forward a copy network traffic to either directly to tools or to a network packet broker. Second, it can operate as a virualized network packet broker, allowing aggregation, filtering and deduplication of virtual network traffic all within a private cloud.

Highlights

- Capture Virtual Machine (VM) network and forward it to physical and/or virtual packet brokers for aggregation, filtering, and deduplication.
- Virtual packet processing and aggregration in your private cloud which traditionally relied on physical packet brokers.
- Aggregrate and deduplicate packet data; originate and terminate tunnels without the need for physical hardware
- Virtual packet processing with AppStack capabilities leverages Ixia's advanced application intelligence with signature based application detection, geolocation, NetFlow and IxFlow (enhanced NetFlow).



PRODUCT FEATURES

FEATURE	BENEFIT
Capture VM traffic (vTap)	Removes blindspots by providing total visibility into all inter-VM traffic. Allows capturing and forwarding traffic of interest to physical or virtual packet brokers, or directly to datacenter monitoring tools. CloudLens virtual tapping capabilities enables complete visibility of east-west, inter-VM, and blade server mid-plane traffic through virtual tapping, filtering and traffic forwarding.
Tap filtering	CloudLens allows optional integrated filtering where data is tapped, which reduces bandwidth consumption. This provides a multi-layer L2-L4 filtering engine that can filter based on IP address, sub-net, protocols, port numbers, and individual VMs
Virtual packet processing	Removes the need for physical packet brokers by allowing users to aggregate, filter, and deduplicate all in a private cloud.
AppStack features	Provides the ability to use Ixia's signature based application (Layer 7) filtering capabilities. This include the following: • Application filtering using a database of application signatures • Geolocation • Application and Device identification • NetFlow and IxFlow generation Also includes the CloudLens Application and Threat Intelligence Dashboard which includes easy-to-use graphs of application, OS and device type characteristics.
Support for vMotion	Guarantees the integrity of visibility as virtual machines are automatically moved due to the dynamic nature of private cloud resourcing.
Hypervisor agnostic	Supports the most private cloud hypervisors including VMware ESXi, Microsoft Hyper-V, KVM, and OpenStack KVM. Integrates with OpenStack orchestration and management to offer multi-tenancy and Tap-as-a-Service (TaaS) support. **(See Specifications section for details below)**
vSwitch agnostic	CloudLens Private is vSwitch agnostic, supporting VMware vSS, vDS, and OpenvSwitch (OVS). **(See Specifications section for details below)**
No agents required	Does not require any services or agents to be installed the virtual machine.
Tool agnostic	Sends traffic to any existing end-point appliance, physical or virtual tool.

THE PRIVATE CLOUD MONITORING CHALLENGE

All networks are inevitably exposed to increasingly complex and advanced security risks and threats. The key is to identify the risks and threats as quickly as possible and take effective action. The goal of a total visibility architecture is to give you access to all the data that crosses your networks, so you can make informed decisions about how to best protect your business and its data, and ultimately deliver an excellent customer experience.

The are two main aspects to every network visibility solution:

1. Capturing all network traffic, and
2. Aggregating, filtering, de-duplicating and modifying the collected network traffic prior to it being forwarded to performance, monitoring and security tools

For collecting the network traffic, traditionally the best method to capture all traffic on a network link is by using a network tap. Taps provide continuous, non-disruptive network access and have these characteristics:

- Receive all traffic on a network link
- Require little to no configuration and can be installed at any time
- Are not IP addressable so they aren't vulnerable to remote attacker access
- Do not introduce delay or alter the content of the data

For aggregating, filtering, de-duplicating and modifying network trafficthe traditional approach is a physical network packet broker (NPB). NPBs are used to process packets and send select packets to specific tools, based on what they are designed to monitor and inspect. NPBs aggregate raw or filtered traffic from multiple monitoring points across your network and fitler and de-duplicate packets so your tools receive only relevant traffic. This reduces data congestion, mimizes false positives, and allows you to handle traffic with with fewer monitoring devices.

However, in today's virtualized deployments, both of these aspects are a challenge:

1. Collecting virtualized network traffic, which can be traffic between virtual machines (inter-VM or east-west), where a traditional physical tap has no visibility
2. Ensuring that the visibility solution scales with the dynamic nature of the private cloud. If virtualized network traffic must be processed by a physical network packet broker, then manual intervention is required to add new resources, and complexities increase.

CloudLens Private addresses both of these problems with two main components, a virtual tapping (vTap) capability which gathers, filters and forwards virtual machine traffic, and a virtual packet processing capability which aggregates, filters, deduplicates and forwards traffic to both virtual and physical datacenter tools. Additionally, CloudLens Private offers the ability to dynamically detect specific applications, not just application types or categories, filtering and forwarding real-time network traffic to appropriate tools for further security, performance or forensic analysis

CLOUDLENS PRIVATE VIRTUAL TAPPING (vTAP)

CloudLens Private provides a vTap service which monitors all inter-VM traffic and forward packets to any end-point of choice, whether virtual or physical security, monitoring or analytics tools, as well as physical network packet brokers, to achieve full visibility and verification across networks.

Capture Virtual Machine Traffic

Remove visibility blindspots by providing total visibility into all inter-VM traffic, capturing and forwarding traffic of interest to physical or virtual packet brokers, or directly to datacenter monitoring tools.

- Enables complete visibility of east-west, inter-VM, and blade server mid-plane traffic through virtual tapping, filtering and traffic forwarding
- Offers a solution with full access to network packets passing between VMs on hypervisor stack
- Sends traffic to any existing end-point, physical or virtual (tool agnostic)
- Follows VMs for continuous visibility throughout migration (VM-level monitoring)
- Supports vMotion and DRS
- Meets SLAs and compliance requirements (SOX, PCI, HIPAA)
- Enables proactive monitoring and security of virtual data centers
- Allows retention of system resources by eliminating any need to install agents or services on the VM or application layer
- Allows control of multiple virtual tapping instances (included software component) for centralized management

Tap Filtering

Integrated filtering reduces vSwitch and LAN bandwidth consumption by filtering at the vTap point, providing a multi-layer L2-L4 filtering engine allowing for filtering based on IP address, sub-net, protocols, port numbers, and individual VMs

- Provides multi-layer L2-L4 filtering engine

CLOUDLENS PRIVATE VIRTUAL PACKET PROCESSING

In addition to tapping capabilities, CloudLens Private supports packet processing within a private cloud environment allowing virtual network traffic aggregation, filtering, deduplication, NetFlow generation, and access to Ixia’s application intelligence capabilities without the need of a physical packet broker.

Ixia's CloudLens virtual packet processing is delivered through a dedicated virtual machine and is an intermediate component in the virtual visibility architecture that “sits” between vTap points and performance and monitoring tools to which can do the following:

- Terminate the GRE and VLAN tunnels
- Aggregate network packets
- Filter and deduplicate traffic
- Duplicate and forward traffic

Such processing traditionally required a physical network packet broker appliance. With CloudLens, these features are available in a cloud format, offering flexibility and simple deployment in dynamic virtual environments.

There are multiple virtual packet processing options available, CloudLens Virtual Packet Processing Standard or Advanced which offers packet manipulation capabilities like header stripping and packet trimming, or CloudLens with AppStack which offers Ixia's best-of-class application and geolocation filtering, NetFlow and IxFlow generation, and data masking (see CloundLens feature table below for more details).

Note: CloudLens Standard or Advanced Virtual Packet Processing must reside in a separate virtual machine than CloudLens Virtual Packet Processing with AppStack.

Aggregation, Replication, Deduplication and Filtering with Virtual Packet Processing

Aggregating, replicating, filtering and deduplication of data within the private cloud allows more effective and effencient use of network bandwidth. Traditionally, all virtual visibility network traffic would be required to leave the private cloud in order to be aggregated and sanitized before forwarded to monitoring tools. With CloudLens™ private, aggregation can occur in the private cloud where it can then be further deduplicated and filtered, allowing much more efficient use of both virtual and physical network capacity.

CLOUDLENS PRIVATE VIRTUAL PACKET PROCESSING WITH APPSTACK

Ixia's CloudLens™ with AppStack includes Application and Threat Intelligence Processing for virtual environments and includes patent-pending capabilities to allow user point-and-click selection of applications, application groups as well as capabilities to dynamically detect new and even unknown applications. It also provides granular application behavior, user geo-location, mobile device identifier, and browser information.

Gathering virtual network traffic data

Private cloud implementations can leverage CloudLens™ packet processing with AppStack for deep packet analysis of the virtual traffic sent from CloudLens™ tapping capabilities.

Application Filtering

CloudLens with AppStack has the ability to identify specific application signatures (hundreds of them!) not just application types, and can identify and segment Netflix and Hulu, Microsoft Outlook and Hotmail, Facebook or Snapchat, SAP and Oracle, to name just a few. Once identified, it applies filters and rules to this traffic to provide IT organizations the ability to dramatically improve the efficiency of their downstream tools. For example, because there is little value in forwarding streaming media traffic to intrusion detection systems (IDS) systems, Appstack capabilities allow an organization to curtail this application traffic from flowing to specific monitors and network appliances. Easily exclude YouTube and Netflix traffic from security inspection - reducing bandwidth to your tools.

Ixia's AppStack detects applications through signatures: static, dynamic or even customized with a patent pending technology. With Ixia doing the heavy lifting of figuring out application signatures and maintaining a database, you or your team don't have to become RegEx experts or track changing applications.

Ixia regularly updates its application database, tracking leading and new applications, as well as developing signatures for unknown applications.

As part of the application signature identification function, AppStack features allow you to identify and flag unknown applications. Rules and filters can then be applied for that traffic to be evaluated for further action. This capability further enhances your security infrastructure, and could indicate the presence of malware, unwanted transmissions, or even hijacked data.

Load Balancing

CloudLens™ Private can be deployed as an inline packet brokering (or processing) VM that can load balance select traffic from the virtual network to virtual tools such as virtual WAN optimization appliances. It operates much like a physical network packet broker. It forwards any workload not selected for optimization, thus bypassing the WAN optimization systems. It forwards the rest of the workload to optimization tools. After optimization, the traffic is sent back to the packet processing VM, which forwards it on the original path.

Real Time Application Dashboard

The CloudLens™ Packet Processing with AppStack Dashboard features easy to use graphical displays and offers an overview of the network traffic map. The administrator can quickly see where the traffic is coming from, what are the most active applications, and countries in a certain period of time. Which operating systems, and devices are active on the network.

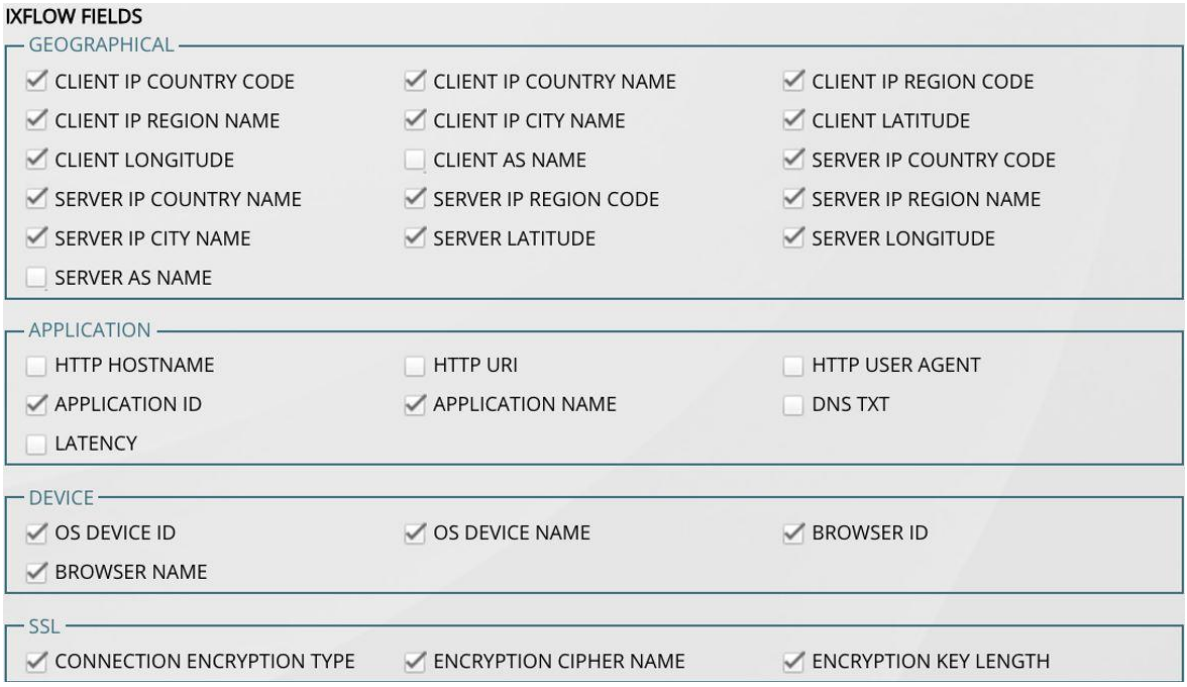
While the Dashboard provides extremely useful information on one screen, CloudLens™ is build to provide third party applications (IPS, IDS, Netflow collectors) the right information at the right time.

The application dashboard shows the following 9 fields:

1. **Traffic**: Real-time traffic volume
2. **App Distribution**: Per-application bandwidth
3. **Latest Dynamic Apps**: Most recently dynamically discovered applications and the generated traffic, in bytes and sessions.

4. **Top Countries**: Countries that generated the largest amount of traffic
5. **World**: A world view, with countries that originate traffic shown highlighted.
6. **Top Devices by OS**: Aggregated per-OS traffic, by bytes and sessions, for the last hour.
7. **Top Filters**: Aggregated per-filter traffic for the last 24 hours.
8. **Top Apps**: Aggregated per-application traffic, by used bandwidth, bytes, and sessions.
9. **Top Browsers**: Per-browser traffic percentage for the last hour.

NetFlow / IxFlow Generation



To expose hidden attacks, CloudLens™ with Appstack capabilities can generate metadata which can be exported as enhanced NetFlow. Additionally, it allows you to enrich NetFlow records with value-add extensions. You can determine what additional information to send to your tools.

- Include geographical information such as region IP, latitude and city name. Application ID or name, device, and even browser type as part of extra information sent to tools.
- Subscriber-aware reporting provides detail on application and handset (device) type for mobile users
- HTTP URL and hostname for web activity tracking
- HTTP and DNS metadata for rapid breach detection
- Transaction Latency for application performance tracking

GeoLocation & Tagging

Separate traffic by location – Pre-defined parameters and signature detection allows for application filtering based on geography so tools can zoom in for close-range visibility. Quickly troubleshoot application issues for a specific remote site by pinpointing a location and application (like VoIP problems from your UK office). If you want to block traffic from specific locations, check out ThreatARMOR. It uses the same information feed and geolocation database as Ixia's ATI Research Center to let you block all traffic to and from untrusted countries, dramatically reducing your attack surface.

- Forward application session traffic based on region, country, city, and in many cases latitude/longitude to the correct tools in your portfolio
- Quickly configure filters, no manual scripting needed
- Support custom locations, such as private IP addresses

Data Masking Plus for Credit Card and Social Security numbers

Achieve Payment Card Industry Data Security Standard (PCI-DSS), HIPAA and other regulatory compliance by leveraging pre-defined data patterns. With personally identifiable information traversing the network, security is key to keeping your consumers and your organization safe.

- Pre-defined patterns to mask – including major credit card, SSN and email addresses
- Reduce false positives with the built-in credit card number validation using the Luhn algorithm
- Leverage in addition to standard data masking at the packet level using a user configurable offset with any number of bytes.

CLOUDLENS				
	Virtual Tapping (vTap)	**Virtual Packet Processing – Standard**	**Virtual Packet Processing – Advanced**	**Virtual Packet Processing with AppStack**
# Virtual network interfaces supported	Not applicable	2	6	8
Max # of filtering rules	Unlimited	20	5000	100
NETSTACK				
L2-L3 Filtering (Eth Type, VLAN, IP)	Yes	Yes	Yes	Yes (IP)
L2-L4 Filtering (Eth type, VLAN, IP, Ports, IP Protocol)	Yes	-	Yes	Yes (IP, IP Protocol)
Aggregation	-	Yes	Yes	Yes

Replication	-	Yes	Yes	Yes (1 GRE Tunnel)
Load Balancing	-	-	Yes	-
PACKETSTACK				
Deduplication	-	-	Yes	Yes
Header Stripping	-	-	Yes MPLS, FabricPath, VXLAN, PPPoE, GRE, ERSPAN, GTP	Yes GRE & ERSPAN
Packet Trimming	-	-	Yes	-
Data Masking	-	-	-	Yes
NetFlow	-	-	-	Yes
Tunnel Origination GRE, ERSPAN	Yes	Yes	Yes	Yes (GRE)
Tunnel Termination GRE, ERSPAN	-	Yes	Yes	Yes (GRE)
APPSTACK				
Application Filtering	-	-	-	Yes
Real-Time Application Dashboard	-	-	-	Yes
Data Masking Plus	-	-	-	Yes
Geolocation & Tagging	-	-	-	Yes

IxFlow	-	-	-	Yes
Available Part Numbers **(See Ordering section for more details)**	*LIC-CL-VTAP-10* *LIC-CL-VTAP-50* *LIC-CL-VTAP-100* *LIC-CL-VTAP-250* *LIC-CL-VTAP-1000* *SUB-CL-VTAP-1000*	LIC-CL-VPP-STD-1 SUB-CL-VPP-STD-1 909-5017	LIC-CL-VPP-AD-1 SUB-CL-VPP-AD-1 909-5016	SUB-CL-AS-1-F 909-5021 LIC-CL-AS-1-F

Table 1: CloudLens™ Private Feature Breakdown

SPECIFICATIONS

TAPPING SPECIFICATIONS – V4.5			
VMware	ESXi 5.0 & 5.1	ESXi 5.5	ESXi 6.0 & 6.5
ESXi - vSwitch (Kernel Module)	Yes	Yes[1]	No
ESXi - vDS	Yes	Yes[2]	Yes[2]
ESXi - vSS	No	Yes[2]	Yes[2]
Microsoft Hyper-V	Windows Server 2012, 2012 R2, and 2016		
KVM	v.2.01 and above with Open vSwitch (OVS) 2.0 and above		
OpenStack KVM	Liberty with KVM OVS (see above)		
OpenStack Tap-as-a-Service (TaaS)	Liberty, Mitaka with v2 authentication (Keystone)		
Network Connectivity	Management Server VM must be accessible via HTTP to access Web UI TCP port 22, 80, 443, and 5989 must be open between Management Server VM and VMware vCenter server		
Disk Storage	Manager: 4 GB - vTap Service (SVM): 2-4GB – TaaS SVM: 5GB		
CPU	Manager: 2 vCPU - vTap Service (SVM): 1-2 Vcpu		
Memory	Manager: 8GB (recommended) – vTap Service (SVM): 512MB to 3GB (Hyper-V), 3GB (ESXi) – Taas: 1GB - KVM (integrated with OVS, no additional resource)		

Web Browser	Google Chrome, Internet Explorer, and Firefox
Licenses	LIC-CL-VTAP-10 LIC-CL-VTAP-50 LIC-CL-VTAP-100 LIC-CL-VTAP-250 LIC-CL-VTAP-1000 SUB-CL-VTAP-1000

[1] For upgrading existing customer or special cases
[2] vCenter required (No standalone ESXi)
[3] Standalone Hyper-V Hosts (No SCVMM)

STANDARD & ADVANCED PACKET PROCESSING SPECIFICATIONS – V1.1	
Supported Hypervisors	VMware ESXi 5.5 & 6.0
CPU	Haswell or later processor, e.g.: E5-26xx 4 vCPU
Disk Storage	8GB – Thin provisioning
Memory	16GB
Network Connectivity	6 predefined interfaces (customizable after installation)
Standard Licenses	LIC-CL-VPP-STD-1 SUB-CL-VPP-STD-1 909-5017
Advanced Licenses	LIC-CL-VPP-AD-1 SUB-CL-VPP-AD-1 909-5016

PACKET PROCESSING WITH APPSTACK SPECIFICATIONS – V1.5.3

Supported Hypervisors	VMware ESXi 5.5 & 6.0
CPU	Intel x86-64 - Westmere or newer processor 6 vCPUs
Disk Storage	30GB – Thin provisioning
Memory	8GB
Network Connectivity	3 predefined interfaces
Licenses	LIC-CL-AS-1-F SUB-CL-AS-1-F 909-5021

ORDERING INFORMATION: VIRTUAL TAPPING

LIC-CL-VTAP-10

Ixia CloudLens vTap 10 License Pack - Perpetual license

This 10 licenses pack includes 10 CloudLens vTap licenses.

LIC-CL-VTAP-50

Ixia CloudLens vTap 50 License Pack - Perpetual license

This 50 licenses pack includes 50 CloudLens vTap licenses.

LIC-CL-VTAP-100

Ixia CloudLens vTap 100 License Pack - Perpetual license

This 100 licenses pack includes 100 CloudLens vTap licenses.

LIC-CL-VTAP-250

Ixia CloudLens vTap 250 License Pack - Perpetual license

This 250 licenses pack includes 250 CloudLens vTap licenses.

LIC-CL-VTAP-1000

Ixia CloudLens vTap 1000 License Pack - Perpetual licenseThis 1000 licenses pack includes 1000 CloudLens vTap licenses.

SUB-CL-VTAP-1000

Ixia CloudLens vTap 1000 License Pack - 1 Year subscription

This license pack includes the right to use 1000 CloudLens vTap SVMs, valid for 1 year.

This license covers the 1st year subscription. Renewals will use 909-5020.

909-5020

Subscription Renewal for SUB-CL-VTAP-1000 (vTap 1000 pack license)

Subscription renewal for vTap 1000 pack - 1 Year extension.

REQUIRES pre-existing purchase and valid subscription of SUB-CL-VTAP-1000, 1st year subscription license.

ORDERING INFORMATION: PACKET PROCESSING - BASIC

LIC-CL-VPP-STD-1

Ixia CloudLens Private Virtual Packet Processing with PacketStack (AFM) - Standard, perpetual license, 1 instance.

Includes: 2 virtual interfaces, NetStack: L2-3 Filtering (Eth type, VLAN, IP), 20 rules ; PacketStack: Multiple GRE tunnel termination, and origination.

Also includes software updates for one (1) year - Access to Customer Web Portal and Technical Support for one (1) year, during normal business hours with best effort

SUB-CL-VPP-STD-1

Ixia CloudLens Private Virtual Packet Processing with PacketStack (AFM) - Standard, perpetual license, 1 instance.

Includes: 2 virtual interfaces, NetStack: L2-3 Filtering (Eth type, VLAN, IP), 20 rules ; PacketStack: Multiple GRE tunnel termination, and origination.

Also includes software updates for one (1) year - Access to Customer Web Portal and Technical Support for one (1) year, during normal business hours with best effort

909-5017

Subscription Renewal for SUB-CL-VPP-STD-1 CloudLens Private Virtual Packet Processing - Standard, 1 instance).

ORDERING INFORMATION: PACKET PROCESSING - ADVANCED

LIC-CL-VPP-AD-1

Ixia CloudLens Private Virtual Packet Processing with PacketStack (AFM) - Advanced, perpetual license, 1 instance.

Includes: 6 virtual interfaces- NetStack: Aggregation, Replication - L2-4 filtering (Eth type, VLAN, IP, Ports, IP Protocol), Up to 9999 rules, Load balancing; PacketStack: Deduplication - 12 GRE originating tunnels, Header stripping.

Also includes software updates for one (1) year - Access to Customer Web Portal and Technical Support for one (1) year, during normal business hours with best effort response time."

SUB-CL-VPP-AD-1

Ixia CloudLens Private Virtual Packet Processing with PacketStack (AFM) - Advanced, perpetual license, 1 instance.

Includes: 6 virtual interfaces- NetStack: Aggregation, Replication - L2-4 filtering (Eth type, VLAN, IP, Ports, IP Protocol), Up to 9999 rules, Load balancing; PacketStack: Deduplication - 12 GRE originating tunnels, Header stripping.

Also includes software updates for one (1) year - Access to Customer Web Portal and Technical Support for one (1) year, during normal business hours with best effort response time.

909-5016

Subscription Renewal for SUB-CL-VPP-AD-1 (CloudLens Private Virtual Packet Processing - Advanced, 1 instance).

ORDERING INFORMATION: PACKET PROCESSING – WITH APPSTACK

SUB-CL-AS-1-F

Ixia CloudLens Private virtual packet processing with AppStack (ATIP). Full Feature pack, 1 instance, perpetual license.

Features included: PacketStack: GRE Termination, Deduplication - AppStack: NetFlow generation - Application Filtering, Geolocation and tagging, Data masking, IxFlow generation.

Also includes software updates for one (1) year - Access to Customer Web Portal and Technical Support for one (1) year, during normal business hours with best effort response time.

909-5021

Subscription renewal for SUB-CL-AS-1-F (CloudLens private virtual packet processing with AppStack). Must have purchased SUB-CL-AS-1-F in year 1 to be able to renew.

LIC-CL-AS-1-F

Ixia CloudLens Private virtual packet processing with AppStack (ATIP). Full Feature pack, 1 instance, perpetual license.

Features included: PacketStack: GRE Termination, Deduplication - AppStack: NetFlow generation - Application Filtering, Geolocation and tagging, Data masking, IxFlow generation.

Also includes software updates for one (1) year - Access to Customer Web Portal and Technical Support for one (1) year, during normal business hours with best effort response time.

IXIA WORLDWIDE
26601 W. AGOURA ROAD
CALABASAS, CA 91302

(TOLL FREE NORTH AMERICA)
1.877.367.4942
(OUTSIDE NORTH AMERICA)
+1.818.871.1800
(FAX) 818.871.1805
www.ixiacom.com

IXIA EUROPE
CLARION HOUSE, NORREYS DRIVE
MAIDENHEAD SL6 4FL
UNITED KINGDOM

SALES +44.1628.408750
(FAX) +44.1628.639916

IXIA ASIA PACIFIC
101 THOMSON ROAD,
#29-04/05 UNITED SQUARE,
SINGAPORE 307591

SALES +65.6332.0125
(FAX) +65.6332.0127