AppStack (ATIP)

CONTEXT-AWARE, SIGNATURE BASED APPLICATION LAYER FILTERING

PROBLEM:

Networks are the most complex and most critical asset to most enterprises today. Organizations urgently need a solution to one of the biggest challenges facing network administrators – complete network visibility that extends past Layer 4 information. For example, many applications today run over HTTP or HTTPS within network or cloud infrastructures, and thus can be obscured. You need application intelligence that serves your monitoring tools the right information at the right time.

SOLUTION:

Relying on both static traffic pattern identification and dynamic application discovery, AppStack provides a comprehensive view of which applications are running within your network, what bandwidth they consume, and where these applications are running geographically. Using AppStack, you can define traffic filters to view or forward specific traffic patterns that you want to monitor, based on application type, operating system, transport protocol, and other criteria. In addition to packet forwarding, NetFlow information, optionally enhanced with application layer data (IxFlow), can be sent to up to tools, enhancing their capability to report granular user and application data.

HIGHLIGHTS

- Improves visibility solutions through highly accurate application identification
- Simple point-and-click management interface allows operators to simply select application traffic types of interest
- Filter application traffic to tools or enhance data provided to tools with enhanced NetFlow
- Greatly improves monitoring platforms by adding a much richer set of geographical, application and device information
- Application signatures are managed and maintained by Ixia, allowing tools to expand awareness automatically as new applications come online
USE CASES:

Deliverables actionable information
1. Monitor application bandwidth explosions
2. Track application failures
3. Identify suspicious activity
4. Track application usage by geography
5. Understand device impacts and user trend behavior
6. Conduct audits for security, policy and infractions

The AppStack Dashboard

1. Real-time traffic volume
2. Application distribution, per-application bandwidth
3. Displays latest dynamic applications, which are applications not known to AppStack, helping you to quickly zoom into potentially malicious applications
4. Top Countries based on the largest amount of traffic generated
5. World view display, with countries that originate traffic highlighted
6. Top Devices by OS displayed by aggregated per-OS traffic, by bytes and sessions, for the last hour
7. Top Filters: displays the aggregated per-filter traffic for the last 24 hours
8. Top Applications by aggregated per-application traffic, by used bandwidth, bytes, and sessions.
9. Top Browsers: This view displays a pie chart showing the per-browser traffic percentage for the last hour

Figure 1 The AppStack dashboard provides comprehensive network traffic information
Each of the nine views can be expanded to show additional information, for instance, clicking the world view shows an enlarged world map, with a list of the top geos that generate server or client traffic session.

Setup application filters within a simple point-and-click interface

Using AppStack filtering, you can define traffic filters to view or forward specific traffic patterns that you want to monitor, based on application type, operating system, transport protocol, and other criteria. Filters can be combined to create detailed data flows that improve monitoring platform accuracy:

- Geographical
- Protocol/Port
- Application Sub-actions
- Application Groups
- IP Address
- Application
- Regular Expression Matching
- SSL Traffic

Figure 2 Enlarged world map shows additional information allowing deeper drill down into data flows

Figure 3 AppStack provides detailed application information, allows filtering by Application Groups, Categories, Provider Type, Transport and more!
For example, you can use the Geographical feature to quickly setup a filter that shows traffic from certain countries.

AppStack allows the combination of any number of filter conditions to devise views important to you and your organization. For example, you could take the same filter and choose to see only specific application data from those countries, for example, just traffic from Android based devices with a simple click of the mouse.

Figure 4 Simple point-and-click interface allows a new filter that identifies all traffic from China, Iran and Saudi Arabia

Figure 5 Selecting all Android based traffic
Application groups allow quick selection of common groups of application traffic

Instead of specifying several different applications, you can specify an entire Application Group to filter by. For example, instead of selecting individual enterprise applications, for instance all the Microsoft office applications, you can simply select the “Enterprise Applications” which will encompass these plus many more.

**Figure 6 Filtering by Application Group allows quick and easy filtering selection, in this case all enterprise application types**

**KEY FEATURES:**

<table>
<thead>
<tr>
<th>FEATURE</th>
<th>FUNCTION</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Application Identification</strong></td>
<td>Ixia’s AppStack detects applications through signatures: static, dynamic or even customized with a patent pending technology.</td>
</tr>
<tr>
<td></td>
<td>• Application identification and filtering based on signature, browser, OS, IP address, and geolocation and forwarding to the right security tools</td>
</tr>
<tr>
<td></td>
<td>• Quickly separate traffic flow by application type – video, email, web or other –device, OS, browser, carrier, BGP AS#</td>
</tr>
<tr>
<td></td>
<td>• Ability to detect unknown applications and add mainstream applications by request</td>
</tr>
<tr>
<td></td>
<td>• Monitor and report top applications’ and countries’ bandwidth consumption</td>
</tr>
<tr>
<td></td>
<td>• Database of &gt;200 applications, that is regularly updated with new applications</td>
</tr>
<tr>
<td></td>
<td>• No regular expression (RegEx) matching required.</td>
</tr>
</tbody>
</table>
### 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.

- 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

### Optional RegEx

Though not required, regular expression matching (RegEx) can be used for additional control and customization. More importantly, it can be used in conjunction with all the other smart filters to offer both ease of use and preciseness of criteria.

- Layer RegEx over the truly intelligent application filtering, geolocation & tagging features.
- Predefined matches for Taxpayer ID, phone numbers, and common credit cards
- Isolate emails from potentially compromised accounts

### IxFlow (NetFlow + meta data)

Ixia 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, browser and even SSL cipher as part of extra information send 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

Let Ixia generate the NetFlow without burdening routers and other network devices.

- Simultaneous NetFlow generation, SSL decryption and Application forwarding
- Rich NetFlow stats including drop counts when the CPU reaches its peak.
- High performing mode – can produce NetFlow records for over 300K TCP sessions/second
- Supports generation of NetFlow v9 and v10/IPFIX data
- Supports up to 10 NetFlow collectors
- Device emulation for router offload, while reporting original device’s ODID and Interface ID
### Packet Capture

Troubleshooting VoIP connections from your office in Germany? Have a repeat issue you need to get to the bottom of? Quickly capture those connection and analyze. With the Packet Capture capability, it is quick and easy to setup a filter and get any slice of traffic you need – from a specific country, application, browser, device, and more – right your fingertips.

- Quickly verify filter configuration by capturing and validating data
- Capture up to 10 samples with 100MB sampling window each
- Easily download to a laptop/workstation for analysis
- Packet capture capability at 30GE line rate

### ATI Subscription

Application and threat intelligence (ATI) subscription provides updates to application signature database, vital for AppStack to stay updated with emerging applications which increases the accuracy of known and unknown application types. This service also includes updates to Geolocation map data, insuring country and city name data are updated with any changes.

Filters that utilize Application Groups will automatically expand to new applications that fall into those groups as they come online.

### Real-time Dashboard

The AppStack Dashboard displays comprehensive network traffic information within nine views that provide real-time network traffic information. It contains nine views that provide real-time network traffic information, such as traffic volume, bandwidth used by the different applications running on the network, the applications that generate most traffic, and more.

### Additional Features

<table>
<thead>
<tr>
<th>Feature</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>FIPS</strong></td>
<td>When the DoD-level security policies are enabled, AppStack restricts a user to a single https session and sessions that exceed a user defined inactivity period are invalidated.</td>
</tr>
<tr>
<td><strong>DOD Compliant Mode</strong></td>
<td></td>
</tr>
</tbody>
</table>
## AVAILABILITY & ORDERING INFORMATION

<table>
<thead>
<tr>
<th>PART NUMBER</th>
<th>DESCRIPTION</th>
</tr>
</thead>
<tbody>
<tr>
<td>SYS-6212-ATP</td>
<td><strong>NTO 6212</strong> - a 1 RU Net Tool Optimizer with integrated Application and Threat Intelligence Processor and 48 SFP+ ports. Port operation requires activation license. ATI Processor Application requires ATIP subscription and port license activation.</td>
</tr>
<tr>
<td>SYS-V-ONE-24x1G-AC</td>
<td><strong>Vision ONE System</strong> with fixed (48) 1G/10G SFP/SFP+ ports, fixed (4) QSFP+ ports, built-in 160G packet processor engine, built-in ATIP engine and (1) blank rear expansion slot. INCLUDES activation license for (24) SFP ports for 1Gbps operation. NOTE: Additional licenses available from Ixia for activation of AFM engine, ATIP engine and remaining ports. Please refer to the Ixia Vision ONE data sheet for more complete details and ordering options.</td>
</tr>
<tr>
<td>MOD-7211-ATP</td>
<td><strong>7300 Series</strong> - Single (1) 48-port Application and Threat Intelligence Processor interface module - supports up to 48 10G SFP/SFP+ ports. Requires activation license for ports and license for ATI Processor application and updates.</td>
</tr>
<tr>
<td>LIC-7300-ATI</td>
<td><strong>Vision ONE / 6000 / NTO 7000 Series</strong> - ATI (Application and Threat Intelligence) Processor one-year Subscription License. Enables application usage and software updates. Does not enable ports. Application will not function without a valid license installed.</td>
</tr>
<tr>
<td>SUB-ATIP-RENEWAL</td>
<td><strong>NTO (Net Tool Optimizer) ATI (Application and Threat Intelligence)</strong> Processor renewal one-year Subscription License. Enables application usage and software updates. Does not enable ports. Application will not function without a valid license installed.</td>
</tr>
</tbody>
</table>
### SPECIFICATIONS FOR 7300 MOD-7211-ATP

#### GENERAL SPECIFICATIONS

<table>
<thead>
<tr>
<th>Performance</th>
<th>Management</th>
</tr>
</thead>
<tbody>
<tr>
<td>• All ports are bidirectional and fully non-blocking</td>
<td>• SNMP v1, v2, v3 support</td>
</tr>
<tr>
<td>• Full line-rate across all ports with filtering enabled</td>
<td>• Local, RADIUS, and TACACS+ support (members and groups)</td>
</tr>
<tr>
<td></td>
<td>• Granular access control features</td>
</tr>
<tr>
<td></td>
<td>• Event monitoring and logging</td>
</tr>
<tr>
<td></td>
<td>• Syslog</td>
</tr>
<tr>
<td></td>
<td>• IT Automation control with web-based API</td>
</tr>
</tbody>
</table>

#### PHYSICAL SPECIFICATIONS

| 1U high interface card for 19” chassis | Operating input voltage: -40 to -60VDC |
| Dimensions: 17.5W x 15L x 1.75H (inches) | Nominal current: 4.15A @ -53VDC, 220W |
| Weight: 17.0lb (7.7 kg) | Maximum operating input current: 5.5A @ 40VDC, 220W max |
| | Heat/power dissipation for module at 100% traffic load: maximum 220W / 751 BTU/hour |

#### OPERATING SPECIFICATIONS

<table>
<thead>
<tr>
<th>Temperature</th>
<th>Humidity</th>
</tr>
</thead>
<tbody>
<tr>
<td>• Operating: 5°C to 40°C</td>
<td>• Operating: 5% to 85%, (non-condensing)</td>
</tr>
<tr>
<td>• Short-term*: -5°C to 55°C (*not to exceed 96 consecutive hours)</td>
<td>• Short-term*: 5% to 90% (non-condensing, *not to exceed 96 hours)</td>
</tr>
<tr>
<td>• Short-term* with fan failure: -5°C to 40°C (*not to exceed 96 consecutive hours)</td>
<td></td>
</tr>
</tbody>
</table>