Application Filtering Intelligence

Classify | Extract | Analyze

It's a constant dilemma for NetOps and SecOps teams: You need insight into the application traffic running on your network so you can better manage and monitor your infrastructure, but getting Layer 7 visibility can be extremely difficult.

Typically, NetOps teams will take an ad hoc approach to gain application visibility and control, such as hardwiring applications to specific ports or writing regex rules that can identify individual applications.

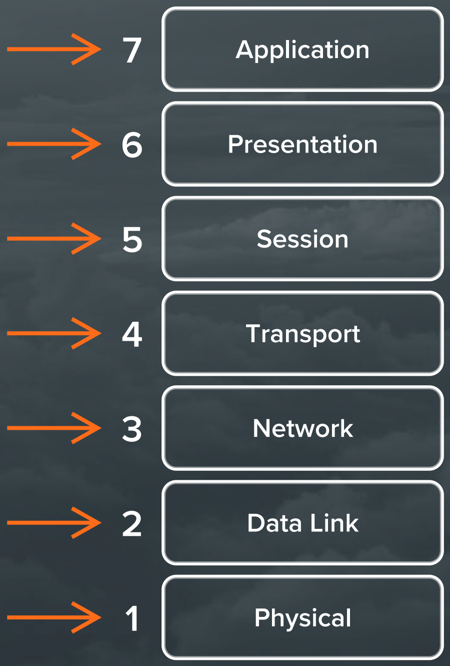


Figure 1: The seven network layers of the OSI model

KEY BENEFITS

- Automatically identifies and classifies more than 3,000 applications, using deep packet inspection
- Significantly boosts efficiency and capacity by sending each application's traffic to the appropriate tools
- Improves security by freeing up existing tools to protect a broader attack surface, including east-west traffic
- Provides bandwidth levels consumed per application for traffic monitoring and throttling excessive use

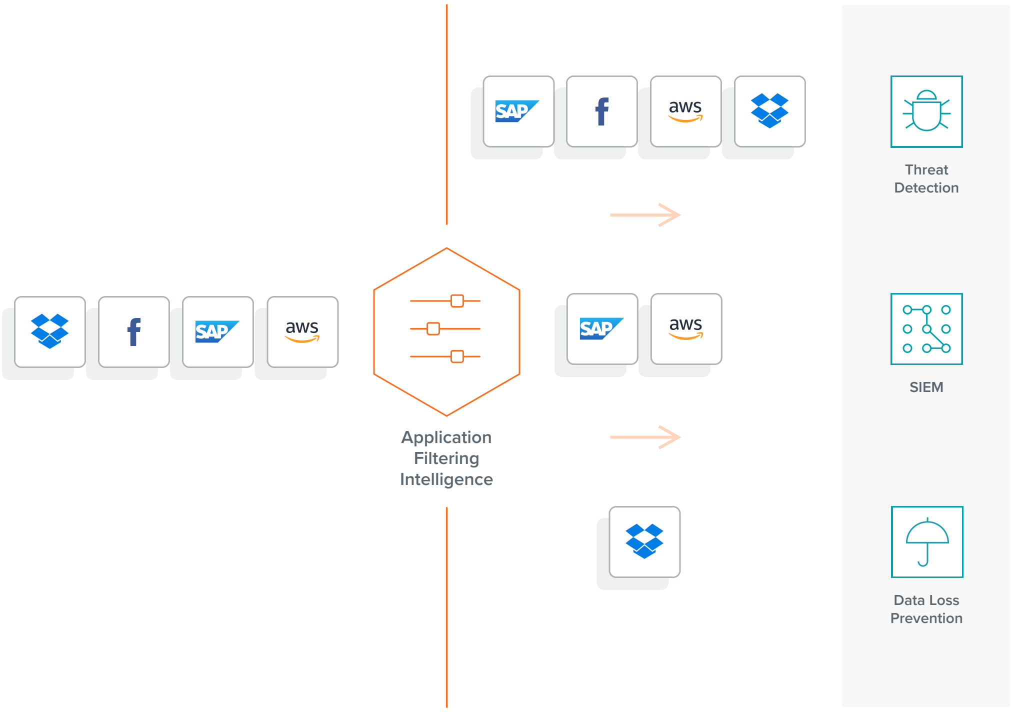


Figure 2: Application Filtering Intelligence helps optimize your tool stack

While these techniques can give you the information you need in the short run, they inevitably make network management a nightmare: Rules have to be constantly updated to keep pace with routinely changing apps and their protocols; the physical network itself needs to be re-segmented; and attackers can elude detection by spoofing port traffic.

If you fail to manage growing application traffic, it can easily overwhelm network and security tools. Security tools can be inundated with high-volume, low-risk traffic, blinding them to the risky applications that do matter. In such an environment, it's difficult to implement zero-trust practices.

Gigamon Provides Unprecedent Insight and Control

Fortunately, Gigamon Application Filtering Intelligence offers visibility into Layer 7 of your network. Part of the Gigamon Visibility Platform, Application Filtering Intelligence automatically identifies application traffic from a growing list of more than 3,000 common business, IT and consumer applications. With individual application traffic extraction, security and network teams can also zero in on performance issues more quickly and make the distinction between high-value apps and ones needing fewer tool coverage.

Then Gigamon Flow Mapping® sends only relevant application traffic to security, performance monitoring or data loss prevention (DLP) tools. For example, threat detection tools would receive all application traffic while DLP tools would receive only email, cloud communication and file transfer data. This increases tool ROI and allows existing tools to better secure your network by analyzing more east-west traffic.

Automatic Identification and Classification Through Deep Packet Inspection

Application Filtering Intelligence doesn't rely on TCP port information, which can be easily spoofed. Instead, it's powered by deep packet inspection. The classification is based on flow pattern matching, bi-direction flow correlation, heuristics and statistical analysis. Packet data is matched against analysis from researchers, which is constantly kept up-to-date.

Of course, a significant portion of traffic on a modern network originates within users' web browsers. So, Application Filtering Intelligence also offers deep insights into HTTP traffic, identifying traffic from thousands of web applications.

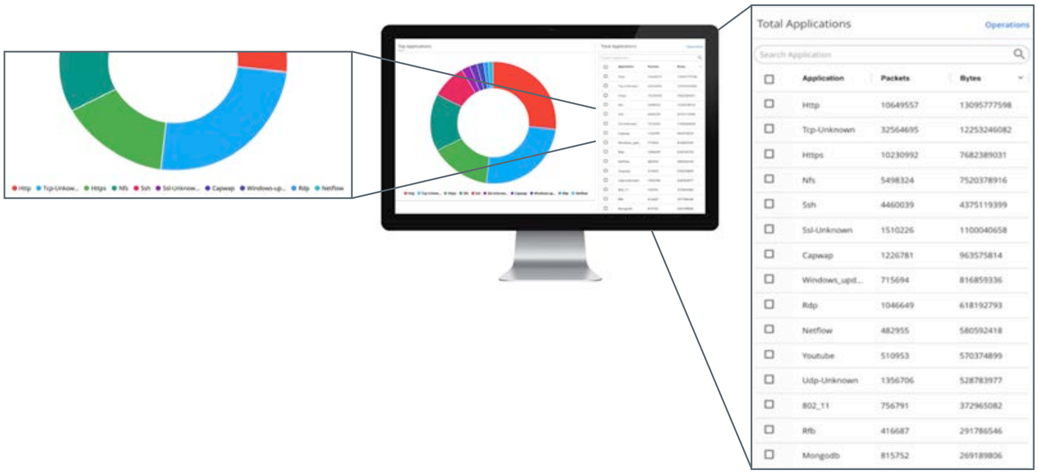
For ease of management, applications are also classified into families to enable you to take Flow Mapping action on families of applications.

A partial list of recognized application families and sample applications includes:

- Tunnels and VPNs
- Streaming media – YouTube, Netflix and Spotify
- Social networking – Facebook (and the apps that run with the Facebook platform), Twitter and Weibo
- Messaging – FaceTime, WebEx and Kaixin
- VoIP services – WeChat and Telegram
- Games – From Candy Crush to Xbox Live
- P2P applications – BitTorrent and Gnutella

Custom Application Support

Custom, in-house applications are often high-value traffic. With Application Filtering Intelligence, you can define signatures for proprietary protocols or extensions, which lets you integrate custom application traffic into your analysis.


● Http ● Tcp-Unkow... ● Https ● Nfs ● Ssh ● Ssl-Unknow... ● Capwap ● Windows-up... ● Rdp ● Netflow

Total Applications Operations

Search Application

□	Application	Packets	Bytes
□	Http	10649557	13095777598
□	Tcp-Unknown	32564695	12253246082
□	Https	10230992	7682389031
□	Nfs	5498324	7520378916
□	Ssh	4460039	4375119399
□	Ssl-Unknown	1510226	1100040658
□	Capwap	1226781	963575814
□	Windows_upd...	715694	816859336
□	Rdp	1046649	618192793
□	Netflow	482955	580592418
□	Youtube	510953	570374899
□	Udp-Unknown	1356706	528783977
□	802_11	756791	372965082
□	Rfb	416687	291786546
□	Mongodb	815752	269189806

Figure 3: Gain visibility to the applications and their bandwidth use on your network

Application Data Presentation

Application Filtering Intelligence data is presented on the Gigamon GigaVUE Fabric Manager UI, as shown in Figure 3. You'll see all the applications running on your network during a specified time period, their traffic volume and their percentage of total traffic.

How You'll Benefit from Application

Filtering Intelligence Application Filtering Intelligence makes the following possible:

- Provides granular insight on the applications running throughout your network
- Reduces the processing and storage resources required by filtering irrelevant traffic before it's processed or stored by security and network tools
- Distributes security tool investment across a larger attack surface by freeing up tool capacity
- Accelerates investigation and analysis of business-critical risks by making it easier to isolate the data needed by SecOps and NetOps teams
- Reduces the time and effort to capture and deliver relevant data for network, network architecture, security, compliance, IT audit and application teams

To see a demonstration and learn what Application Filtering Intelligence can do for you, contact Gigamon for more information at www.gigamon.com/contact-us.

Gigamon®

Worldwide Headquarters
3300 Olcott Street, Santa Clara, CA 95054 USA
+1 (408) 831-4000 | www.gigamon.com