Feature Brief

Application Session Filtering

Challenges with Traffic Complexity in Enterprise and Service Providers

Security and monitoring appliances look at session and application layer data for patterns, also called signatures. They search for these patterns across huge volumes of real world traffic. This process is extremely cumbersome, as every packet would need to be searched for hundreds, and sometimes thousands, of patterns. There is a need for the ability to extract relevant flows of interest that match specific patterns or applications and forward them to tools that need this data. An email security appliance may only be interested in email traffic, and, even more specifically, email traffic with suspicious links and attachments. Likewise, with significant volumes of enterprise traffic being voice or video, it may be prudent to prevent sending them to certain security and monitoring appliances. What is needed is a methodology to extract specific flows belonging to an application or a pattern of interest and forward them to appliances that are looking for that data.

Moreover, it is not enough to send or filter individual packets, but the entire application session. To properly identify and analyze threats, security tools often need visibility into the entire session, from session initialization to session termination. Failing to provide all of the packets in that session will result in errors and uninspected traffic.

Gigamon Solution—Application Session Filtering

With the traffic complexity introduced by today's network applications, Application Session Filtering—an optional extension of GigaSMART® technology—provides a powerful filtering engine that identifies applications based on signatures or patterns that can appear across any part of the packet payload. These patterns can be as simple as a static string at a user-configured offset or as complex as an extremely advanced Perl Compatible Regular Expression (PCRE) at a variable offset. Application Session Filtering builds on top of Adaptive Packet Filtering, another GigaSMART application. While Adaptive Packet Filtering can be used to identify matching content in packets, Application Session Filtering goes a step further to extract entire sessions corresponding to a specific application. Readily available scripts for popular applications can be used by administrators to accelerate implementation of Application Session Filtering.

A session can be any TCP session, UDP session or a subset of fields in a standard IP 5-tuple (IPv4/v6 source address, IPv4/v6 Destination Address, source port, destination port and protocol). Additional fields that can be used for identifying an ASF session include MPLS Labels, VLAN tags and GTP (GPRS Tunneling Protocol) specific identification tags.

Figure 1: Application Session Filtering

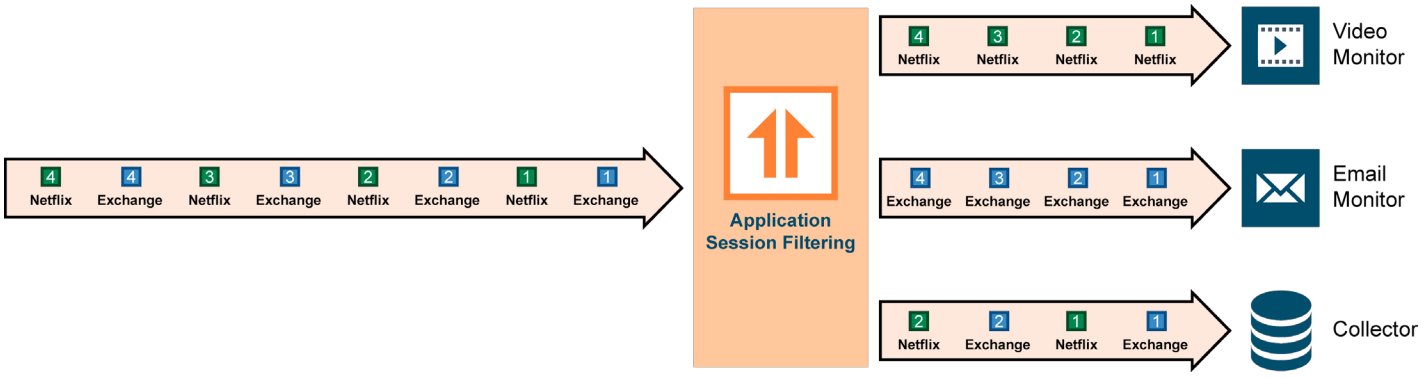
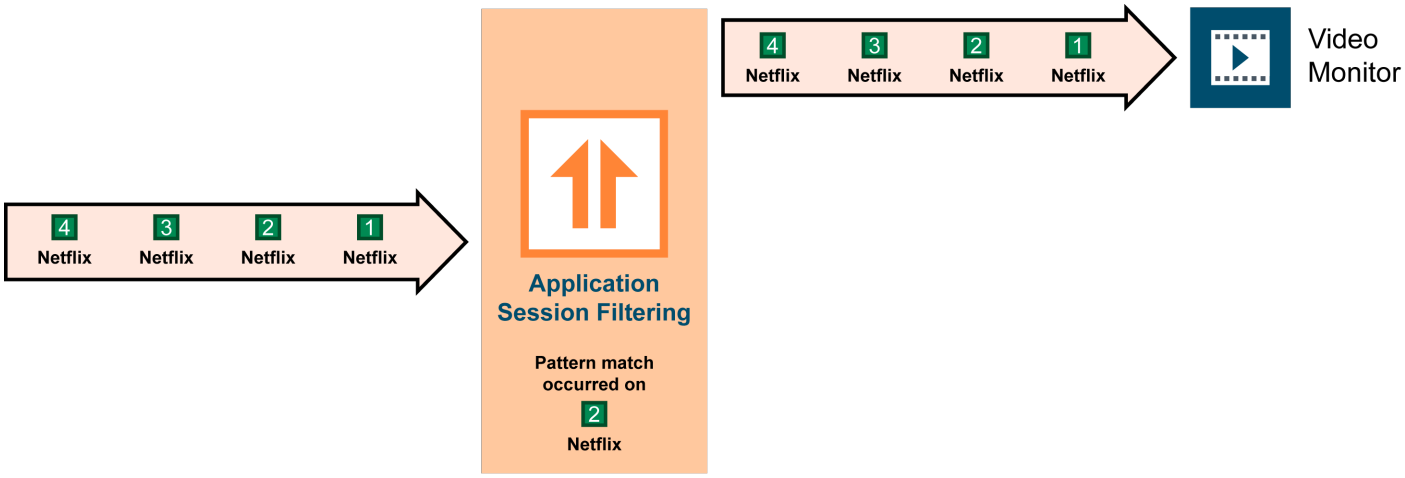


Figure 2: Application Session Filtering with Buffering



Application Session Filtering can be configured with or without buffering. The former ensures that the entire session from start to finish, including the initial TCP handshake for a TCP connection, is filtered or forwarded, whereas the latter provides better performance in instances when the session handshake and initialization packets can be ignored.

Application Session Filtering with Buffering

In this configuration, when the specified pattern is found, the entire session containing that packet is filtered, including those packets in the session that preceded the packet containing the specified pattern. Subsequent actions could be to either send traffic to the desired tool(s) or to drop the traffic, thereby offloading the tool from receiving unnecessary traffic.

Most applications will present the relevant information within the first few packets of a session. The user can specify how many packets of each session to buffer before declaring that no match was found thereby freeing up the memory for other sessions.

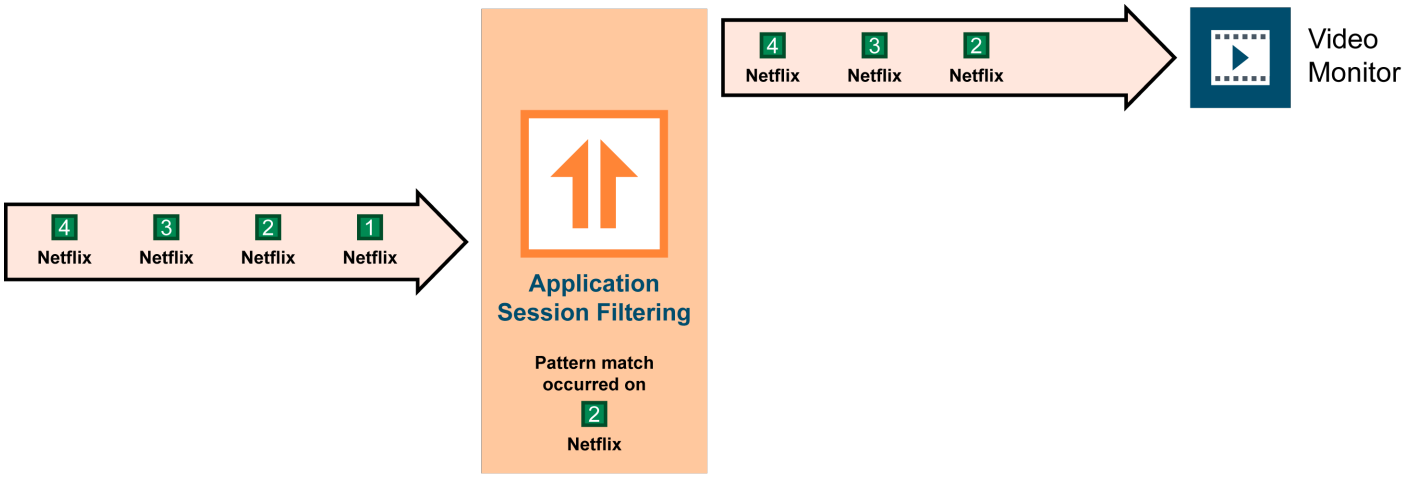
When Application Session Filtering is used with buffering, a session can be specified as some combination of IPv4 or IPv6 flows with UDP or TCP sessions matching any combination of source IP, destination IP, source port, and destination port.

Application Session Filtering without Buffering

In this configuration, when a pattern specified has been matched, that packet and all subsequent packets corresponding to the session are filtered or forwarded as a single session.

If the pattern was matched on packet 2, all further packets belonging to the session will be sent to the destination tool as shown in Figure 3. However, the first packet belonging to the session (packet 1) will not be sent to the tool. In this configuration option, a session can be defined as any combination of IP addresses, ports, protocol, VLAN, GTP identifiers, and MPLS labels.

Figure 3: Application Session Filtering without Buffering



Key Use Cases

With the flexibility offered by Application Session Filtering, administrators can implement many useful use cases such as:

- Filtering all Netflix and YouTube traffic and not forwarding them to monitoring appliances in order to prevent them from being overwhelmed by voluminous traffic.
- Filtering all Windows Update traffic from being forwarded to monitoring and security appliances. This phenomenon is called Patch Tuesday, where Microsoft releases patches on the second Tuesday of every month, and Windows machines worldwide are updated with these patches. This volume of traffic often overwhelms monitoring and security appliances worldwide.
- Allowing https traffic on non-standard ports: SSL traffic (https) uses port 443 but servers can be configured to listen on any port for https traffic. If this packet needs to be sent for inspection or to a decryption device, Application Session Filtering can be configured to look for https traffic on any port.
- Filtering email traffic to only forward emails with links or attachments, as these would be most relevant to email security appliances. Emails containing only text are typically not a vector of infection. However, executing a malicious attachment or a clicking a web link would be more harmful.

Key Benefits

- Optimize Security Tools for Application Inspection
  - Forward traffic corresponding to session of interest to security tools thereby increasing their efficacy
  - Enable selective reduction in traffic to security and monitoring tools
  - Enhance tool performance with reduced traffic loads
- Offload Application Identification to GigaSMART technology
  - Identify applications based on one or more combinations of packet content, ports, URLs, and HTTP content
  - Gain visibility into flows tunneled over HTTP

About Gigamon

Gigamon® solutions have been deployed globally across enterprise, data centers and service providers, including over half of the Fortune 100 and many government and federal agencies. For more information about the Gigamon Unified Visibility Fabric™ visit: **www.gigamon.com**

3169-02 08/15

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