

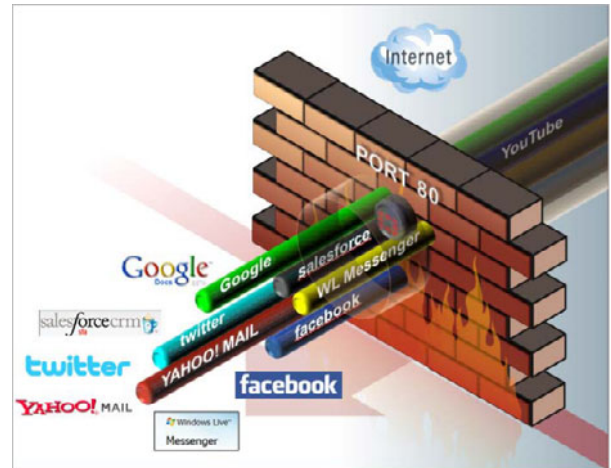


Application Control

FortiOS Application Control enhances content-based security by improving the visibility of applications on the network

Monitoring and Controlling Applications, Not Just Network Ports

Controlling and monitoring applications can seem like a large and, in some ways, daunting task since applications are now running within browsers, or there are applications within applications, and even some applications take advantage of multiple ports. Blocking or allowing TCP and UDP ports that applications use is no longer an option to help control and monitor them. Web filtering can block individual sites but is not useful for complex social networking sites that might have some features of value to an organization. By monitoring and controlling applications in FortiOS, any unwanted applications can be blocked while access to useful applications can be wide open or individually controlled with traffic shaping and authentication.

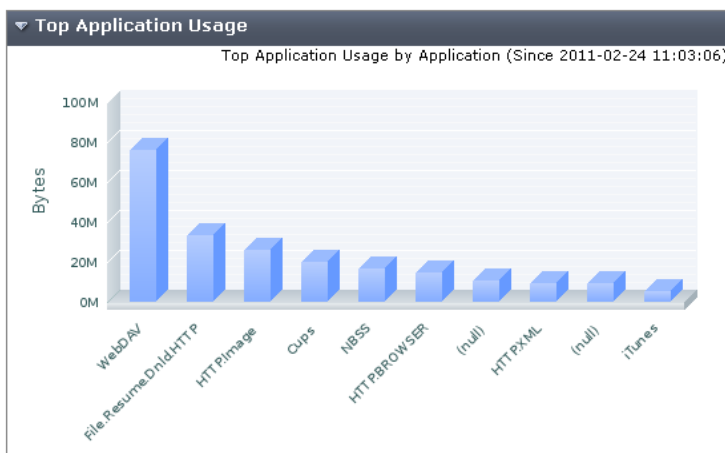


FortiOS provides these two levels of protection when FortiOS application control is combined with content-based FortiOS UTM features such as intrusion prevention, antivirus/antispysware protection, and DLP.

FortiOS Application Control

Application control that complements content-based security has become an essential part of a complete network protection solution. Technologies such as Web 2.0, social media, cloud computing, and virtualization have increased the complexity of network traffic and increased the need to understand what is happening on a network.

FortiOS uses efficient application control techniques to provide a visual picture of the applications that generate traffic on our customer's networks. Application control samples network traffic without affecting network performance. When application traffic is visible, all unwanted applications can be blocked and access control, traffic shaping, antivirus/antispysware protection, intrusion prevention, and other UTM features can be applied to the application traffic that is allowed. After applying control measures, reporting can continue to ensure that the measures are effective and to monitor for unexpected changes in application traffic patterns.



Effective application control starts with configuring application monitoring to get a picture of the application traffic on a network. FortiOS provides periodic and real-time Top Application Usage reports by bandwidth and number of sessions. The reports can also display the source and destination addresses of the application traffic.

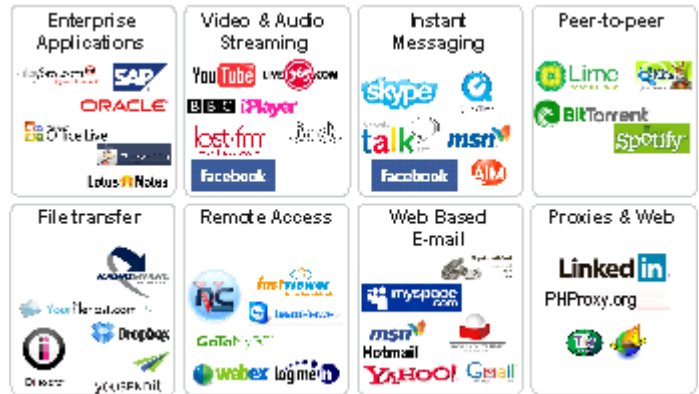
Application control can be applied to regular network traffic and to IPsec and SSL VPN traffic terminated by the FortiGate unit as well as SSL-encrypted traffic including HTTPS, POP3S, SMTPS, and IMAPS passing through the FortiGate unit.

Application Control Sensors

You can create multiple application control sensors, each configured to allow, block, or monitor a unique list of applications. In firewall policies that accept application traffic, you can enable application control and select an application control sensor. Traffic accepted by firewall policies is examined for the applications in the application control sensor, and the configured action is executed.

Application control sensors contain both filters and entries. Filters help to filter through specific application information such as the vendor of the application, the application's behavior, and the type of technology the application is, for example within a web browser. Entries help to monitor or block specific applications, or applications within applications. For example, you need to block Farmville, CuteBear and other non-productive applications within Facebook, but allow chat and playing videos.

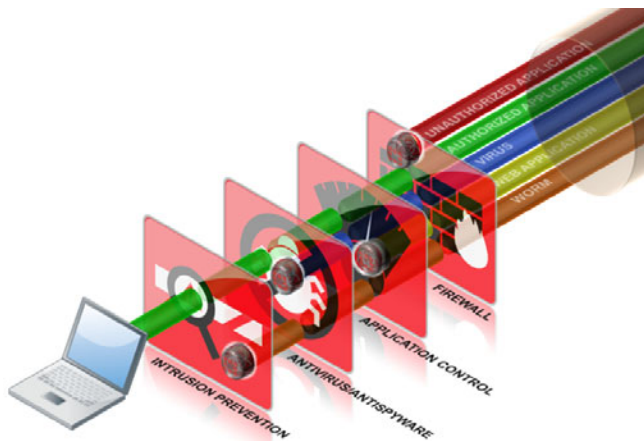
Each application sensor also defines what the action taken with applications not included in the list. Unlisted applications can be blocked so that only traffic from listed applications can pass, effectively creating an application white list. The default behavior allows all unlisted applications, effectively creating an application black list where only the traffic from applications that you explicitly block is not allowed to pass. A locked down high-security network can use an application control list configured as a white list. A more open network that requires blocking of only a few applications can use a black list. You can also mix the white list and black list approach on the same network.



Tagging within an application sensor or application list

Tags are often seen on web sites, such as blogs, and can be very useful for searching and filtering through a lot of information. In FortiOS, tags can be created within an application sensor or within the application in the application control list (also known as the FortiGuard Application Control Database). Tags, whether in an application sensor or application in the application list, provide a means to specify the use of only those tagged objects.

Within application sensors, tags are applied to application control filters and entries. In the application list, tags are applied to each applications that is listed.



The FortiGuard Application Control Database

FortiOS application control detects more than a thousand different web applications, software programs, network services, and traffic protocols. FortiOS uses the FortiGuard Application Control Database, one of the largest application signature databases available. The database is constantly updated to recognize new applications and new versions of existing applications. Application control updates are downloaded to FortiGate units on demand, or as scheduled from the FortiGuard Distribution Network. FortiGuard push updates ensure that FortiGate units have up-to-the minutes application databases.

A complete list and detailed information about all supported applications is available from the online [FortiGuard Application Control List](#). The [FortiGuard Application Control Site](#) lists the top 10 applications that our customers are currently detecting and anyone can request a new application signature or an update to a current signature using our [Application Control Submission Form](#).