



Web Filtering

FortiOS combines sophisticated filtering capabilities together with a powerful policy engine to create a high performance and flexible solution

Cloud Based Model with FortiGuard Web Filtering Service

Fortinet provides an innovative approach to HTTP and HTTPS web filtering technology combining the advantages of a cloud based service offering with a layered response caching option. The multiple FortiGuard data centers around the world hold the entire categorized URL database and receive rating requests from customer FortiGate units typically triggered by browser based URL requests. These rating requests are responded to with the categories stored for specific URLs, the requesting FortiGate unit then uses its own local profile configuration to determine what action is appropriate to the category, such as. blocking, monitoring or permitting the request.

Avoiding Cloud Latency

The question most asked when reviewing this architecture is the latency associated with the rating request. Fortinet has adopted a lightweight query analogous to a DNS lookup. From an end-user perspective the delay introduced by the rating query is similar to the delay introduced by the DNS lookup, unperceivable in the majority of cases.

To maintain this low latency response time FortiGate units are constantly monitoring the performance of the FortiGuard URL rating service ensuring the next query is always sent to the fastest responding FortiGuard server. This latency optimization algorithm uses the geographic location of the FortiGate unit and FortiGuard servers, time zone, server load and real time response data to test queries and guarantee that minimum latency is always achieved.

Rating responses are also cached directly in FortiGate unit memory so that ratings for frequently used sites such as www.google.com can be retrieved directly from the cache, reducing the need for requests to the global FortiGuard network. Caching URLs in memory makes URL lookups almost instantaneous and only use a very small amount of system memory.

Enabling FortiGate Web Filtering

Fortinet's development team has ensured that providing this powerful filtering capability is as simple as possible to enable. All FortiGate units ship with a default web filter profile designed to be useful for most organizations. Assuming the FortiGuard Web Filtering service is active (which can be easily verified from the Web UI) the administrator can enable web filtering by adding the default Web Filter profile to a firewall policy that accepts web traffic.

Customization of URL Categories

With the basic default protection in place administrators can customize Web Filtering by changing the default Web Filtering profile or by adding new custom Web Filtering profiles. This customization allows the selection of specific combinations of allowed, blocked or monitoring categories appropriate to any environment. In addition administrators can create and populate local categories or place specific URLs in existing categories should the FortiGuard rating not be in agreement with an organization's policies and practices.

Web Filtering Overrides

In some environments, especially in the education arena, access is blocked to certain categories but a user with additional authentication credentials may wish to override the block (teacher/student, adult education). The override feature allows a site that is otherwise blocked by the web filter profile to be unblocked after an additional layer of authentication has taken place.

Identity Based Access

Having a single web filtering profile is seldom appropriate for an entire organization. Different groups of users can often require varying levels of access that can change during the day. Typical examples include:

- Restrict access to social networking sites during core business times
- Limit guest users access more than employees
- Limit customer facing employee access

These scenarios require the end user to authenticate with the FortiGate unit to select the correct web profile to apply to each user's traffic. To ensure a completely flexible approach, a number of options are available to achieve end user identification:

- Local User Groups, with optional remote LDAP, RADIUS or TACACS+ databases
- Certificate based with optional two factor authentication
- NTLM Authentication
- Directory Service

Scheduling

Access policies can be further controlled by providing time based controls this would enable particular access to only be possible, or impossible at certain times of the day, week or month.

Image Rating

Where sites contain multiple images, sometimes from different websites it is a feature of FortiOS to allow these images to be separately rated to prevent inappropriate content being displayed. Images from blocked categories will not be displayed in the user's browser.

Safe Search and Search Engine Keyword Enforcement

Popular search engines include the ability to perform image searches, and display thumbnail image results. FortiOS provides a safe search option that enforces the safe mode of popular search engines to limit the displayed results to content considered safe according to the safe search policies of each search engine. In addition search engine keyword filtering can be used to block searches of specific keywords or phrases.

Quota

In addition to a time of day schedule the Quota capability allows a daily time period to be specified to further control access. With quota's enabled it would be possible to, for example, limit access to gaming sites for two hours per day. Quotas can be invoked at various times throughout the day and are reset at the end of each day.

Replacement Pages

When a site is blocked a fully customizable replacement page can be sent in its place. These replacement pages are stored on the FortiGate unit and can be customized to include corporate branding (logos etc), provide details on the category of site blocked, references to any corporate policies, details on how to apply for override privileges or a simple 'site blocked' notification.

Reporting

A FortiGate with an integrated disk storage module can generate reports directly. A default report is included that can be extended and customized as required. Reports at a username level can also be generated and user information can be provided directly from Microsoft Active Directory environments.

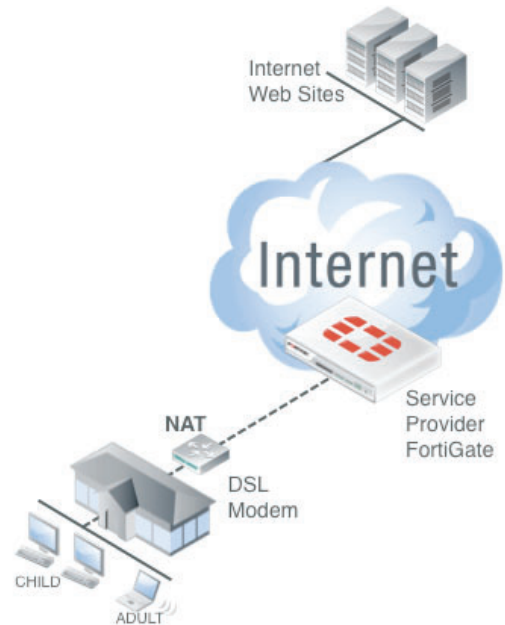
To provide a consolidated report from multiple FortiGate devices a FortiAnalyzer appliance can be added to the solution allow a consolidated report to be produced for groups of FortiGate devices.

Service Provider Dynamic Profile Extensions

For service provider environments an end point identifier, which can range from a username, service, location, or MSISDN (in mobile networks) can be provided to the FortiGate unit. This would occur each time an end point connects to the network as part of a RADIUS authentication event, interim updates could also be permitted to allow for real time changes to the service definitions.

This end point identifier can be used to provide specific filtering controls as part of the dynamic profiles feature that allows per end point web filtering profiles to be created. Each end point can be associated with a filtering profile, logging information will include this identifier.

Consider the scenario where an end point has been identified as a residential customer, it may be desirable to provide differing levels of service to users within the home. This residential parental control can also be provided to users even though they share a common IP address into the service provider network.



Rating Scalability

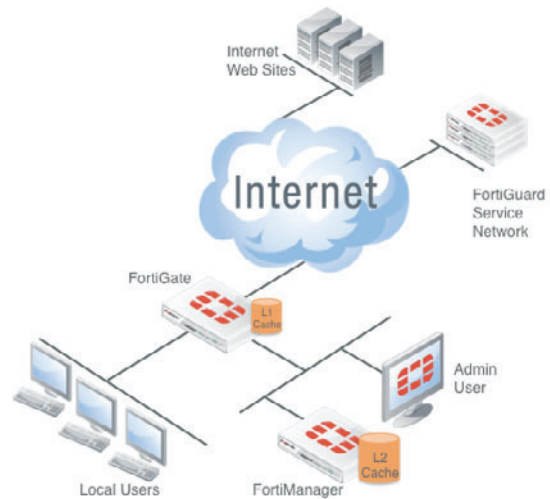
Further performance advantages can be derived by maintaining local rating information. These local details form an integral part of the service and can be provided at two levels:

Level 1: Local FortiGate Rating

Each FortiGate device also provides an advanced cache engine capable of holding in local memory returned rating requests. This active site cache ensures the fastest possible rating response for those parts of the Internet being accessed via a particular FortiGate unit. The local cache returns rating requests independently from any FortiGuard, or FortiManager device.

Level 2: FortiManager FortiGuard Database

An appropriately licensed FortiManager appliance can be synchronized to the FortiGuard network and as such be used in the same way to as the FortiGuard network by a customer but only for their FortiGate devices. This can further reduce any latency associated with the round trip time for individual rating requests whilst at the same time ensuring complete database coverage. Consider the combination of a LAN attached FortiGate cluster and FortiManager combination with the potential to handle tens of thousands of requests per second.



HTTPS Deep Scanning

HTTPS deep scanning provides FortiGuard web filtering of encrypted HTTPS sessions. HTTPS deep scanning performance is enhanced by leveraging FortiASIC HTTPS hardware acceleration. HTTPS deep scanning respects user's privacy by optionally not scanning banking, health care and personal privacy sessions.

FortiGuard Database

The database currently rates more than 50 million sites covering billions of URLs with each site able to be rated in multiple categories and data classes. With support for 70 languages the FortiGuard database provides a truly international service.

For more information of the database, and to perform real time queries on the current database please go to:

<http://www.fortiguard.com/webfiltering/webfiltering.html>