Why FortiGuard Web Filtering Is Better
Version 1

FORTINET™

www.fortinet.com

Why FortiGuard Web Filtering Is Better Technical Note
Version 1
4 July 2006
07-20000-0228-20060704

Trademarks

Contents

Introduction

This chapter introduces you to FortiGuard Web Filtering and to this document. This chapter contains the following topics:

Revision history

Version	Date	Description of changes
First Release	28 December. 2005	First version.
07-20000-0228-20060612		Updated the reliability and scalability information on the first page of “Service Delivery” on page 15.
07-20000-0228-20060704		Corrected and expanded the section “Customized local categories” on page 20.

About FortiGuard Web Filtering

FortiGuard Web Filtering is a managed Web filtering solution provided by Fortinet that sorts billions of webpages into a wide range of categories. System administrators and individual users can configure licensed FortiGate units and FortiClient applications to allow, block, or monitor access to webpages according to FortiGuard categories. FortiGate units and FortiClient applications access the FortiGuard Distribution Network (FDN) to determine the category and class of a requested webpage. Depending on the response from the FDN the FortiGate unit or FortiClient application can allow, block, or monitor access to the webpage.

FortiGuard Web Filtering categorizes over 28 million websites into 76 categories and 7 classes. These 28 million websites include billions of individual webpages. The FortiGuard URL database of categorized websites is continuously updated as the Internet evolves. New websites are discovered, rated, and added to the database. Outdated websites are removed from the database. Also when websites already in the FortiGuard URL database change, ratings for these pages are reviewed and changed as required.

To make configuration simpler, users of FortiGuard services can choose to allow, block, or monitor entire groups of categories. Blocked pages are replaced with a message indicating that the page is not accessible according to your Internet usage policy.

Fortinet categorizes websites and develops the FortiGuard URL database using a combination of proprietary methods that include text analysis, exploitation of the Web structure, as well as a dedicated team of Web analysts. In addition, FortiGuard Web Filtering customers (and indeed anyone else) can go to the FortiGuard Center Web Filtering URL lookup page to submit a URL for rating. As well if you feel that a URL is rated incorrectly in the FortiGuard URL database, you can use this URL lookup page to enter a URL and request a rating change.

The FDN is a world-wide geographically diverse network operated by Fortinet Inc. that provides FortiGuard Antivirus (AV) and FortiGuard Intrusion Prevention System (IPS) updates in addition to FortiGuard Web Filtering and FortiGuard Antispam services to the FortiGate, FortiManager, FortiAnalyzer, FortiClient and FortiMail line of products.

In addition to the URL lookup page mentioned above, the FortiGuard Web Filtering pages of the Fortinet FortiGuard Center include up-to-date descriptions of FortiGuard URL database categories and classes. As well you can access FortiGuard-related documents and articles from the FortiGuard Center page of the Fortinet Knowledge Center.

About this document

This document describes the analysis and comparison of FortiGuard Web Filtering service with three major players in the Web filtering industry:

- Enterprise Information Management system by Websense
- SmartFilter by Secure Computing
- Proventia Web Filtering by ISS

Fortinet's evaluation of FortiGuard Web Filtering against these three major competitors shows that the FortiGuard Web Filtering service rates more webpages more accurately than our competition. The URL coverage of the FortiGuard URL database is superior to our competitors. The accuracy of the FortiGuard URL database is equivalent to the accuracy of the Enterprise Information Management system by Websense; and superior to the accuracy of the SmartFilter and Proventia products. The FortiGuard client-server service delivery model not only offers compelling cost savings over the competition, but also delivers superior user experience and performance.

FortiGuard Web Filtering in combination with FortiGate units and FortiClient also provides a richer feature set than our competition. This rich feature set includes Web content classification, customized local categories, user overrides, and reporting.

Fortinet Knowledge Center

Additional Fortinet technical documentation is available from the Fortinet Knowledge Center. The knowledge center contains troubleshooting and how-to articles, FAQs, technical notes, and more. Visit the Fortinet Knowledge Center at http://kc.forticare.com. See also the FortiGuard Center Knowledge Center page.

Fortinet documentation

The most up-to-date publications and previous releases of Fortinet product documentation are available from the Fortinet Technical Documentation website at http://docs.forticare.com.

Comments on Fortinet technical documentation

Please send information about any errors or omissions in this document, or any Fortinet technical documentation, to techdoc@fortinet.com.

Customer service and technical support

Fortinet Technical Support provides services designed to make sure that your Fortinet systems install quickly, configure easily, and operate reliably in your network.

Please visit the Fortinet Technical Support web site at http://support.fortinet.com to learn about the technical support services that Fortinet provides.

FortiGuard web filtering customer resources

FortiGuard Web Filtering customers can go to the FortiGuard Center Web Filtering URL lookup page to submit a URL for rating. As well if you feel that a URL is rated incorrectly in the FortiGuard URL database, you can use this URL lookup page to enter a URL and request a rating change.

The FortiGuard Web Filtering pages of the Fortinet FortiGuard Center include up-to-date lists of FortiGuard URL Database categories and classes. As well you can access FortiGuard-related documents and articles from the FortiGuard Center page of the Fortinet Knowledge Center.

URL database filtering

All Web filtering solutions take one of these two approaches:

- Dynamic filtering, which analyzes webpage content as the user retrieves it, and categorizes the page using software algorithms.
- Database filtering, which searches out websites and keeps them in a URL database, URL list, or control list.

URL stands for Universal Resource Locator, or the address of a webpage or website. In the URL database, the URLs are categorized generally by a combination of software algorithms and Web analyst reviews. When the user retrieves a webpage, the category of the URL is looked up in the database and used to determine the action to take with the user's request.

There are various pros and cons to the approaches listed above, but many studies have shown that database filtering is the more effective solution. FortiGuard Web Filtering is based on database filtering.

How to evaluate and compare Web filtering services based on database filtering? First and foremost, the quantity and quality of the URL database determines how effective the service is. All companies that provide Web filtering services naturally proclaim the effectiveness of their technology, and especially the accuracy of their URL database or control list. These company claims often list all sorts of database metrics such as number of categorized websites, number of categories, and so on.

Fortinet has determined that the most effective way to compare URL database quality is to test URL databases with real-life traffic. This document looks at two intuitive, and straightforward metrics: coverage and accuracy.

This chapter contains the following sections:

Coverage and accuracy

Coverage is the percentage of URLs in the database relative to the entire World Wide Web. Coverage indicates how many URLs are categorized.

Accuracy is the percentage of URLs correctly categorized relative to all the categorized URLs in the database.

To compare coverage and accuracy, Fortinet uses randomly chosen keywords to search for URLs on Google (http://www.google.com/). Of the hundreds of URLs returned for each keyword, two URLs are randomly picked from each page of 100 URLs. According to Google page ranking, the URLs in the first page of the search results are the most popular websites for the chosen keywords. The URLs in the last page are the least visited websites. The result is a list of URLs that represents random websites in various subjects and various degrees of popularity. Using this methodology, Fortinet samples 300 URLs every week.

A Fortinet Web analyst carefully reviews and categorizes each webpage according to the category description of each Web filtering service. The categorization of webpages can be subjective no matter how well-designed the categorization scheme. To ensure consistency of judgment, the same Web analyst categorizes all of these URLs.

The table below shows the accumulated results over the first half of the year 2005. Note the total number of URLs is reduced from 7800 to 7760 after removing invalid URLs or URLs that cannot be categorized due to lack of contents, or for various other reasons. FortiGuard ranks at the top with 4744 URLs correctly categorized out of 7760 URLs.

Table 1: Statistics or URL database evaluation

Web Filtering Service	Company	Total Number of URLs	Correctly Categorized	Incorrectly Categorized	Not Categorized
FortiGuard	Fortinet	7760	4744	2186	830
Enterprise	Websense	7760	4170	1950	1640
Proventia	ISS	7760	2471	2380	2909
SmartFilter	Secure Computing	7760	2397	2589	2774

Based on the results shown in Table 1, the coverage and accuracy is calculated as shown in Table 2. FortiGuard comes out on the top with coverage at 89%, and tied with Enterprise by Websense with accuracy of 68%. With over 28 million websites categorized, it is no surprise that FortiGuard coverage is way ahead of the competition.

Note: Note that 68% accuracy may seem low. However, this number is based on a very strict standard. As long as a website is categorized not in its designated category, it is considered incorrect even though the difference between the incorrect category and the designated category may not significantly affect most Web filtering policies (to allow or deny the access of the website).

Table 2: Overall coverage and accuracy

Web Filtering Service	Coverage	Accuracy
FortiGuard	89%	68%
Enterprise	79%	68%
Proventia	63%	51%
SmartFilter	64%	48%

Precision and recall

In the theory of information retrieval, the accuracy and efficacy of an information retrieval system is measured by precision and recall. Precision is the percentage of the number of relevant records retrieved compared to the total number of irrelevant and relevant records retrieved. Recall is the percentage of the number of relevant records retrieved compared to the total number of relevant records in the database. There is an inverse relationship between these two metrics that cannot be avoided: Maximizing one minimizes the other and vice versa. Precision and recall must be considered together. A single metric of adding the precision and recall together is a good overall indication of the accuracy and efficacy.

The categorization of websites is an information retrieval process where each URL or webpage can be considered a record. A correctly categorized URL is a relevant record retrieved while an incorrectly categorized URL is an irrelevant record retrieved. The objective of Web filtering is to block webpages that are designated to be blocked and allow webpages that are permitted.

Web filtering precision is a measure of under-blocking. Under-blocking means letting pages through that should be blocked. Higher precision leads to lower under-blocking.

Web filtering recall is a measure of over-blocking. Over-blocking results from false positives and means blocking pages that should not be blocked. High recall leads to fewer false positives and lower over-blocking. A perfect Web filtering system would have 100% precision and 100% recall, or a score of 200% overall.

A customer's Internet access policies dictate the websites to block. In a typical application, all websites that are potentially liable, objectionable or controversial are blocked. Fortinet thus has chosen the 16 categories in these three category groups as blocked categories for our evaluation.

The results are shown in Table 3. The Enterprise Information Management system by Websense achieved 85% of precision and 71% of recall for a total of 156%. FortiGuard is almost on par with 77% of precision and 78% of recall for a total of 155%, or a 1% difference. Both Proventia and SmartFilter are far behind.

Table 3: Precision and recall for a typical policy

Web Filtering Service	# of URLs that should be blocked	Total Blocked	Correctly Blocked	Not Blocked	Precision	Recall	Total of Precision and Recall
Enterprise	510	426	361	113	85%	71%	156%
FortiGuard	510	518	397	149	77%	78%	155%
Proventia	510	488	310	200	64%	61%	125%
SmartFilter	510	539	302	208	56%	59%	115%

The results shown in Table 3 are based on the typical Web filtering policy and show the overall effectiveness of each solution. Precision and recall metrics should be theoretically applied to each Web filtering category. However, the statistics could get quite overwhelming with 76 categories and can only be meaningful with much larger samples of URLs.

Table 4 shows the same precision and recall calculation for the Pornography category, which is a key category for many customers. The calculation of precision and recall for the Pornography category is consistent with the overall results with FortiGuard following closely behind Enterprise Information Management system, by 4% of the precision and recall in total.

Table 4: Precision and recall for blocking pornography websites

Web Filtering Service	# of URLs that should be blocked	Total Blocked	Correctly Blocked	Not Blocked	Precision	Recall	Total of Precision and Recall
Enterprise	257	263	197	60	86%	70%	156%
FortiGuard	257	211	181	76	75%	77%	152%
Proventia	257	334	201	56	60%	78%	138%
SmartFilter	257	345	193	64	56%	75%	131%

Results from live networks

Fortinet regularly analyzes FortiGuard traffic to further verify our sampling and testing results. During a recent week, of all URL queries made by all FortiGuard URL servers around the world, 92% of them were rated, representing a 92% coverage. This coverage is better than the 89% coverage obtained from the sampling test results. The difference occurs because the URLs or websites visited by customers are concentrated in more popular categories.

It is important to note that the coverage experienced by our customer's users is actually higher, over 95% in our estimation. Because URLs and their categorization information are cached on each FortiGate unit, the URL lookups sent to the FortiGuard URL servers might represent a much larger number of actual URL requests. URL caching on local FortiGate units means that repeated requests for the same URLs are answered by the FortiGate unit. These requests are not tracked by the FortiGuard URL servers.

Fortinet believes it is important to categorize as many as URLs as possible, with the objective of categorizing the entire Web. As more URLs or websites are categorized, more potentially liable or likely to be blocked websites are added to the FortiGuard URL Database, and the more effective FortiGuard Web filtering becomes. Better coverage also improves spin off benefits such as FortiGate monitoring and reporting on user Web access trends.

Web Classification

One feature of the FortiGuard URL database that further sets FortiGuard apart from our competitors is Web classification, which will be available with FortiOS v3.0. In addition to categorizing webpage content into one of 76 categories (see FortiGuard URL Database Categories), the FortiGuard Web Filtering service further classifies webpages based on media types or sources. Similar to categorization, classification enables our customers to further refine Web access management. Customers will have the capability to block offensive materials such as pornographic images, by preventing the finding of such materials in the first place.

Classification sorts websites and webpages into one of the classes listed in Table 5 and in FortiGuard URL Database Classes on the FortiGuard Web Filtering webpage.

Table 5: FortiGuard Web classification

Class	Description
Cached Contents	Webpages that are stored or cached in a second website, generally a search engine or translation website.
Image Search	Websites for searching of images or photos, or the results of image or photo searches.
Audio Search	Websites for searching audio clips or the results of audio searches.
Video Search	Websites for searching video clips or the results of video searches.
Multimedia Search	Websites for mixed searching of images, photos, audio and video content or the results of such searches.
Spam URL	Website or webpage URLs that are found in spam email. These webpages often advertise sex sites, singles clubs, and other potentially nuisance or offensive material.
Unclassified	All webpages that do not fall into one of the above classes including regular webpages, Web searches, and others.

What makes the difference

The superiority of FortiGuard URL database is built on a foundation of:

- Fortinet proprietary FortiGuard URL database production system
- The FortiGuard team of 30+ Web analysts
- Integration of third party URL databases and lists
- The Complete FortiGuard Web filtering package

Fortinet proprietary FortiGuard URL database production system

The FortiGuard URL database production system constantly discovers websites from various sources as they become alive. Each website found is then uniquely identified and fingerprinted and its URL stored in our master database. These new websites are then prioritized for processing. New websites are first crawled and profiled and their characteristics for categorization are extracted. Once this first stage is complete, the website is subject to the FortiGuard categorization engine. The FortiGuard categorization engine uses heuristic and AI algorithms to categorize the website.

Websites that are successfully categorized with a high degree of confidence and that pass the FortiGuard QA standard are updated to the live FortiGuard Web Filtering servers around the world. Websites that cannot be categorized with a high degree of confidence are assigned to our team of Web analysts for review.

The FortiGuard aging process constantly verifies URLs and compares the fingerprints of the entire database to detect obsolete URLs and significant changes of contents that require re-categorization. Obsolete URLs are removed from the database and changed websites are subject to the same identification process as new URLs. The aging process keeps existing entries in the master FortiGuard URL database up to date and relevant.

The identification process makes sure that all different addresses of a website are maintained in the FortiGuard URL database including all of the hosting IP addresses.

Our highly accurate categorization engine and prioritization techniques ensure the categorization of as many websites as possible. Fortinet achieves over 90% URL coverage by maintaining all addresses of a website and by using our effective website mining and discovering process. Prioritizing the most popular and sensitive websites for Web analyst review significantly improves accuracy.

The FortiGuard team of 30+ Web analysts

The FortiGuard team of dedicated Web analysts ensures the accuracy of the FortiGuard URL database by manually reviewing high-priority websites. Analysis of live FortiGuard traffic indicates that over 20% of URLs are manually reviewed and categorized. This percentage is continuously increasing as our team of Web analysts categorizes over 18,000 websites per week.

The FortiGuard team of Web analysts is located in three continents. The team brings a wealth of language, cultural diversity and expertise to their work. Fortinet has native speakers or experts in English, French, Simplified Chinese, Traditional Chinese, Japanese, German, Italian, Spanish, Korean, Dutch, Portuguese, and Arabic. Our multilingual Web analysts also use leading edge Web translation technology to help categorize websites in many other languages.

The FortiGuard team of Web analysts are holders of various degrees, diplomas and certificates including: B.Sc. in computer science, B.A. in English Literature, B.A. in French Literature, B.A. in Italian Literature, B.A. in German Literature, B.A. in Spanish Literature, B.A. in Business, B.A. in Education, B.A. in Linguistics, B.A. in International Economics and Trade and many others.

Integration of third party URL databases and lists

Fortinet has purchased and integrated a URL database of mostly Japanese websites, composed and categorized by Neo-Blood in Japan. Fortinet has also integrated the freely available Open Directory and uses its directory hierarchy as inputs for our categorization. Fortinet has also mined various other URL lists on the Web. The integration and cross-referencing of these databases or URL lists also improves the FortiGuard URL database coverage and accuracy.

The Complete FortiGuard Web filtering package

The highly effective FortiGuard URL database production system, combined with the large FortiGuard Web analyst team, and the integration of third party databases results in a superior URL database with 28 million websites categorized. See Table 6 for the comparison of key statistics.

Table 6: Statistics of URL Databases

Web Filtering Service	FortiGuard	Websense	Proventia	SmartFilter
Websites categorized	28 million	10 million[a]	20 million	N/A
Categories	76	90	60	62
Classes	6	Not Supported	Not Supported	Not Supported
Languages	60+	50	N/A	60+
Database update frequency	Continuously	Daily	Daily	Daily

a.As of May, 2005 (latest available information)

Service Delivery

FortiGuard Web Filtering employs a client-server service delivery model. The FortiGuard Distribution Network (FDN) deployed across the world represents the server part of the model. Individual FortiGate units or FortiClient applications act as clients, querying the nearest FDN server to receive URL ratings. Traditional software-based models like Websense and Proventia often use a Web proxy server, where the URL database is downloaded to this proxy server.

The FortiGuard Web Filtering client-server model has the following advantages:

1. Cost saving. The most obvious advantage of the FortiGuard service delivery model is tremendous cost savings for Fortinet customers. There is no need for customers to purchase and maintain a dedicated URL database server.
2. Less management. FortiGuard Web Filtering and the FDN is a fully managed service. The global network of FDN servers is set up, installed, managed and monitored 24/7 by the Fortinet global IT team. It only requires a mouse click on a FortiGate web-based manager interface or FortiClient application page for our customers to enable FortiGuard Web Filtering. There is no extra software to install or server to manage. FortiGuard Web Filtering services are fully integrated with FortiGate units and FortiClient, minimizing the management effort required for superior website access control. Configuration is also relatively simple and can easily be applied to an entire organization.
3. Reliability and scalability. The FDN consists of more than 12 server sites deployed in geographically distributed locations around the world. Each server site consists of redundant high performance Fortinet FDN server hardware deployed in highly secure collocation centers with five-9 availability. The proprietary FDN server selection algorithm implemented in FortiGate units and FortiClient applications is optimized for scalability and reliability. FortiGate units and FortiClient applications choose the optimal server site to query for URL ratings based on the time zone of the server site and on the server site response time. If a server site does fail, FortiGate units or FortiClient applications automatically and promptly switch to a different server site without service interruption or user intervention. Customers can also purchase a FortiManager-3000 unit and host FDN services locally.

   For more information about FDN architecture, reliability, and scalability, see the Fortinet Knowledge Center Article Accessing and Debugging FortiGuard Services.

This chapter contains the following sections:

User experience and performance

One concern with the FortiGuard service delivery model is the overhead of querying the FDN for URL categories and the impact that this overhead has on the user Web browsing experience. The FortiGuard service model appears to require constant queries to the FDN and it is thought that these queries slow down Web access. However, Fortinet testing and analysis shows that FDN queries cause no extra latency in retrieving websites and use negligible bandwidth. The queries have virtually no impact on the user experience in terms of browsing performance. Excellent URL rating performance is achieved by an efficient caching algorithm, and a proprietary protocol between FortiGate units and the FDN and between FortiClient applications and the FDN.

The FortiGuard Cache

Each FortiGate unit contains a cache that holds a small portion of the FortiGuard URL database. The size of this cache varies depending on the FortiGate model. On a typical FortiGate-400, the cache is large enough to store 16,000 URLs. The cache size on high-end FortiGate models is much larger.

FortiGate units store URL ratings in this cache after they are retrieved from the FDN. The cache is then periodically refreshed. Users behind a FortiGate unit often visit a limited number of similar websites, so in practice the most queried URL ratings end up being stored in the cache. As a result, in many cases there is no need to query the FDN and there is no overhead at all. Fortinet tests and analysis have shown that the cache-hit rate in a typical customer site is over 80% for FortiOS v3.0.

Out of cache queries

When a match is not found in the FortiGuard cache, a request is sent to the FDN in parallel with the request sent to the Web server to retrieve the webpages. The time to query the FDN for URL rating is often negligible, and far less than the time to retrieve the webpage because:

- FDN servers are strategically deployed close to the major backbones and the round trip time from a FortiGate unit to the FDN and back is usually less than the round trip time from the FortiGate unit to the website and back.
- The latency of responding to a query is less than 1ms even when an FDN server is operating at its maximum capacity. This compares to generally hundreds of milliseconds to even several seconds to retrieve a webpage because of normal network and Web server latency.
- The average payload of a FortiGuard URL query packet is less than 256 bytes and one round trip is enough to retrieve the rating. The average size of a webpage is 10 Kbytes and usually requires a minimum of 3 round trips.

Performance testing

Testing and measuring FortiGuard Web Filtering performance is a challenge because constantly changing network conditions have the greatest effect on performance. Also, FortiGuard Web Filtering performance may depend on the location of the FortiGate unit on the Internet. Test results and analysis are included in Table 7. Depending on the location and the server queried, it takes from 3ms to 210ms to receive a response from an FDN server. Generally queries from a FortiGate unit in the same continent as the nearest FDN server take less than 100ms, which is the typical application.

In some cases, the FDN round-trip time can be longer than the Web server round-trip time. Even if this happens, a FortiGuard Web Filtering query will not slow down Web browsing unless the FDN round-trip time is 3 times longer than the Web server round-trip time. A difference this great is highly unlikely and would not be permanent, but most likely be a result of a short-term network problem. In summary, regardless of the network conditions, the time of querying FDN servers is negligible and has no impact on the user Web surfing experience.

Bandwidth usage

In terms of bandwidth usage, the overhead created by FortiGuard Web Filtering is again negligible. In most cases, the FortiGuard Web Filtering querying overhead is less than 1% of the bandwidth required to retrieve webpages. Average webpage size (15 Kbytes) is about 20 times of the size of the FDN query request and response (average 256 bytes). Because of the FortiGuard cache, usually only one in every 5 webpages requires a query to the FDN.

Most software-based Web filtering solutions require the daily download of a full URL database, the size of which can range from tens to hundreds of mega bytes. These large daily downloads may cause bursts in bandwidth demand that may negatively impact customer Internet connectivity and response times.

The FortiGuard Web Filtering delivery model only queries and caches URLs that customers need for enforcing their Internet policies and has virtually no impact on customer networks and the browsing experience of their clients.

Fortinet's competitors might claim "less is more" to defend their relatively small URL database size because their service delivery model cannot efficiently handle a larger URL database. With the high performance service delivery of the FDN, our FortiGuard URL database can grow with the Internet and provide the best coverage for Internet access management.

Table 7: Querying the FDN for a URL category and retrieving a webpage

	Retrieving a webpage	Querying a URL category
Average size of payload (bytes)	15K	256
Average number of round trips required	3 (the minimum)	1
Typical round trip time (ms)	150	100
Typical server Latency (ms)	10-300	<=1
Total time required (ms)	450	100
Impact on retrieving the webpage	N/A	None

New Features in FortiGuard v2.0 and FortiOS v3.0

With the release of FortiOS v3.0 and FortiGuard v2.0, Fortinet has added a number of major feature enhancements to FortiGuard Web Filtering. Here are the highlights.

This chapter contains the following sections:

More and finer categories

With the introduction of FortiGuard Web Filtering release 2.0, websites are categorized into finer categories. This provides more control on Web access. For example, websites displaying/selling lingerie and swimsuits are categorized into separate categories from the Nudity category. And sex education material is categorized into the Sex Education category separate from other Adult Materials categories. See FortiGuard URL Database Categories for the up-to-date list of FortiGuard Web Filtering categories.

Web content classification

In addition to categorizing webpage content into 76 categories, FortiGuard Web Filtering further classifies webpages based on media types or sources. Similar to categorization, customers can use classification to further refine Web access management. Customers can block offensive materials such as pornographic images, by preventing the finding of such materials in the first place. See FortiGuard URL Database Classes for the up-to-date list of FortiGuard Web Filtering classes.

Customized local categories

Customers can create their own user-defined local categories and add URLs to these categories. The Local Categories are added to all FortiGate protection profiles. From any protection profile you can allow, block, log and override local categories, just as you can for any FortiGuard category.

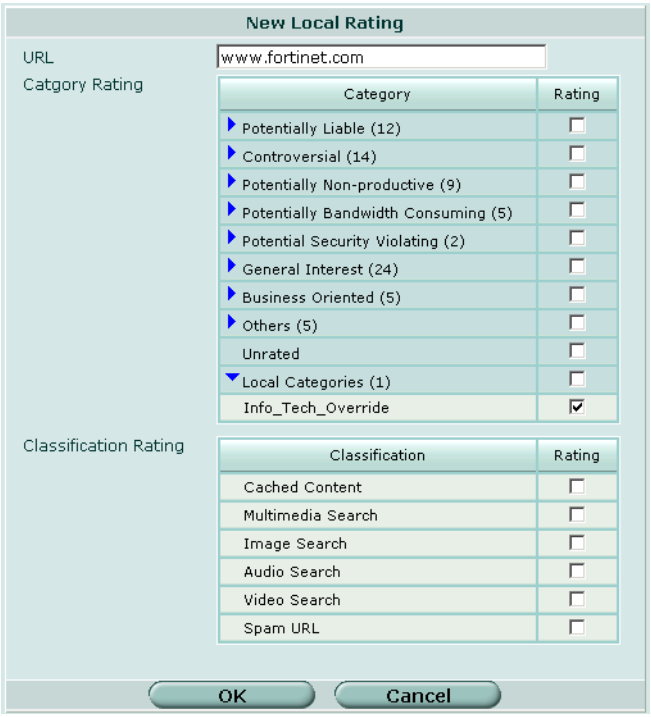
Ratings in local categories override standard FortiGuard category ratings. You can use local categories to create exceptions to the ratings you have configured for the standard FortiGuard categories.

To use a local category to override the action set for a FortiGuard category

If you have created a protection profile that blocks access to Information Technology Web pages (as rated by FortiGuard Web Filtering) your users will not have access to www.fortinet.com. You can use the following steps to add a local category that allows access to www.fortinet.com.

1. Log into the FortiOS v3.0 web-based manager.
2. Go to **Web Filter > FortiGuard - Web Filter > Local Categories**.
3. Add a local category with a name that describes what the category is to be used for. For example: Info_Tech_Override.
4. Go to **Web Filter > FortiGuard - Web Filter > Local Ratings**.
5. Select Create New.
6. Add the URL www.fortinet.com.
7. Open Local Categories and select Info_Tech_Override.
8. Select OK.

Figure 1: Adding a URL to a local category



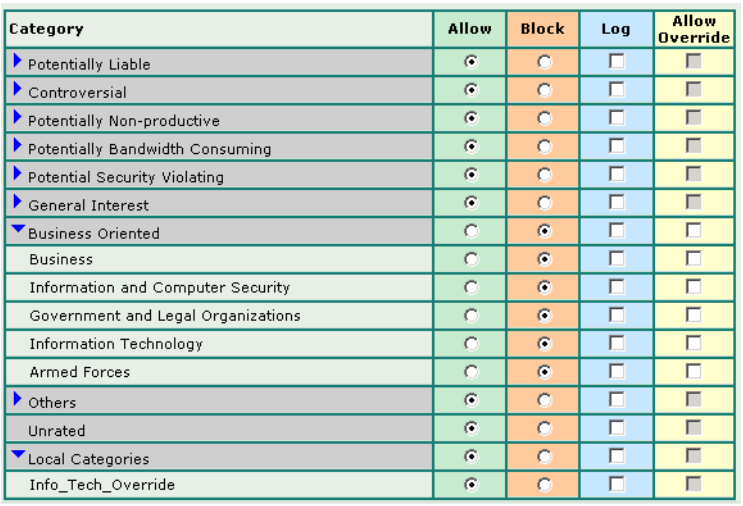
9 Go to **Firewall > Protection Profile** and select the protection profile that includes the FortiGuard Web Filtering configuration that blocks access to Information Technology Web pages.

10 Open FortiGuard Web Filtering.

11 Open Local Categories.

12 Make sure Info_Tech_Override is set to Allow (the default setting) and select OK.

Figure 2: Example **Local category configuration in a protection policy**



Category	Allow	Block	Log	Allow Override
Potentially Liable	●	○	☐	☐
Controversial	●	○	☐	☐
Potentially Non-productive	●	○	☐	☐
Potentially Bandwidth Consuming	●	○	☐	☐
Potential Security Violating	●	○	☐	☐
General Interest	●	○	☐	☐
Business Oriented	○	●	☐	☐
Business	○	●	☐	☐
Information and Computer Security	○	●	☐	☐
Government and Legal Organizations	○	●	☐	☐
Information Technology	○	●	☐	☐
Armed Forces	○	●	☐	☐
Others	●	○	☐	☐
Unrated	●	○	☐	☐
Local Categories	●	○	☐	☐
Info_Tech_Override	●	○	☐	☐

You can add more URLs to the Info_Tech_Override local rating group to allow access to more information technology URLs. You can also add and configure other local categories as required.

Single sign-on

In FortiOS 3.0, user management and Windows Active Directory (AD) authentication are seamlessly integrated. FortiGate administrators no longer need to configure separate policies and configurations to enforce user authentication for Web access. The integration with the Windows AD provides a single sign-on interface for FortiGate clients in a Windows AD environment.

User overrides

Occasionally a user will need access to a website that is usually blocked by FortiGuard. The user override feature allows the FortiGate administrator to provide a username and password to temporarily override the block and allow a user to view the website if allowed by their administrator. If the user enters the wrong password or the administrator does not use the override, the website will still be blocked as normal.

Reporting

FortiGuard Web filtering reports are generated and organized according to category and group. There are per-group statistics in addition to the per-category statistics. Combined with FortiAnalyzer, many reports are supported including:

- Management reports: the most frequently used reports by customers or those of most interest to management. These include Category, Destination, Disposition, Group, Risk, and User.
- Summary reports: Overview of usage with daily and grand totals. Summary Reports are used to view Internet usage trends.
- Detail reports: the most complete picture of Internet usage. Detail Reports can provide an in-depth look at the type of sites your users access.

www.fortinet.com

www.fortinet.com