Data Loss Prevention

Deployment Brief

FORTINET

Data Loss Prevention

Challenge

- Sensitive information, such as personal data, financial records, and intellectual property, can be accidentally or intentionally exposed or shared with unauthorized parties, leading to data breaches.
- Many industries must comply with strict regulations (GDPR, HIPAA, PCI DSS, and so on) that require the protection of personal, financial, and health data. Failure to comply can lead to heavy fines and legal consequences.
- By automatically scanning and blocking such actions, data loss prevention (DLP) solutions help reduce the impact of human error, ensuring that sensitive information remains secure.

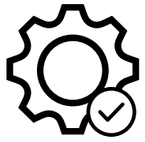
FortiOS Documentation

- Data Loss Prevention
- DLP Techniques
- Basic DLP Settings
- DLP Examples

Key Features of the FortiGate DLP Solution

The FortGate DLP solution is configured based on several components, including the data type, attributes, and file patterns on the content passing through select protocols. A profile can be created and added to a firewall policy based on custom DLP dictionaries and sensors.

Key features of the FortiGate DLP solution include:



CONTEXT BASED DLP

Implement sensitivity labels to emphasize the importance of a file or document based on specific data attributes.

CONTENT BASED DLP

Identifies sensitive and important information by reviewing the content of the file or document.

FORTIGUARD DLP SERVICE

Provides a database of predefined DLP patterns which can be implemented when configuring DLP profiles.

Key Features

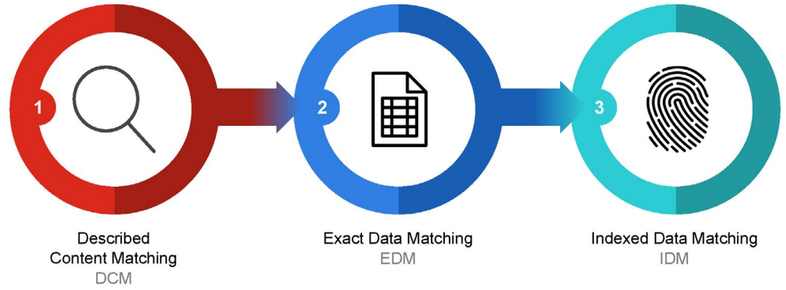
Context Based DLP

Context includes highly useful attributes such as size, file type, header information, metadata, time, format, and so on. It does not include the content of the document itself. Any DLP solution should include contextual analysis as part of the overall solution.

In order to safeguard your organization's data, labels can be employed as markers for sensitive information. Microsoft provides sensitivity labels, which act as identifiers emphasizing the importance of the data they're associated with, thereby enhancing the security measures in place.

See **Sensitivity labels** for more information.

Content Based DLP



Described Content Matching (DCM)

DCM is a content matching method that uses patterns or keywords in the given text or file.

See **Built-in DLP data type**.

Exact Data Matching (EDM)

EDM detects sensitive information by comparing content with a predefined set of structured records.

See **Exact data matching**.

Indexed Data Matching (IDM)

IDM involves creating a unique identifier for specific pieces of sensitive documents.

See **DLP fingerprinting**.

FortiGuard DLP Service

The FortiGuard DLP service offers a database of predefined DLP patterns such as data types, dictionaries, and sensors. Examples include:

- Drivers licenses for various countries, various states in the USA, and various provinces in Canada
- Tax numbers for various countries
- Credit card numbers
- Bank statements
- Source code detection

See **FortiGuard DLP service.**

Deploying DLP

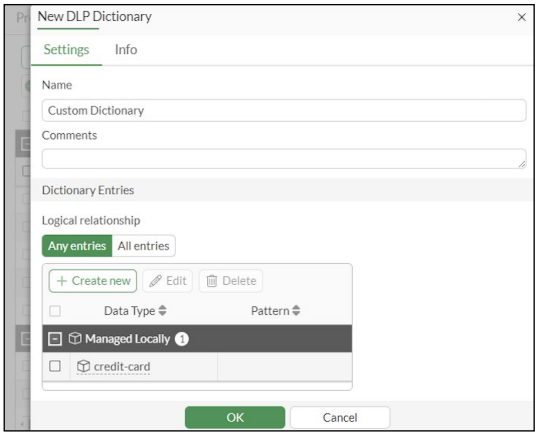
Best Practices

The following best practices should be considered when deploying DLP:

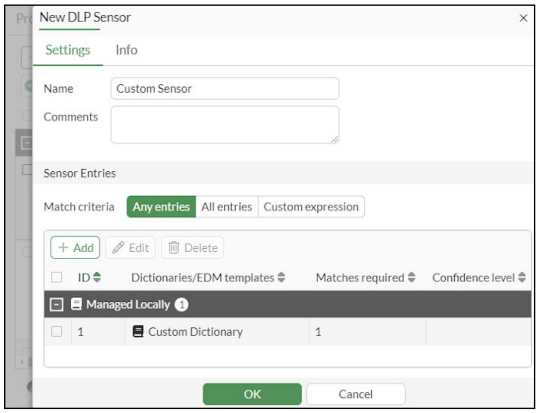
1. It is best practice to protect your data submitted over non encrypted lines. Always have very strict rules for clear text protocols like HTTP, FTP, SMTP, and so on.
2. To increase accuracy of the DLP dictionaries and sensors, consider using proximity search. See **Proximity search**.
3. Using logical expressions will help to create a more tailored sensors for your needs.

The following shows the general process of deploying a firewall policy with a DLP security profile:

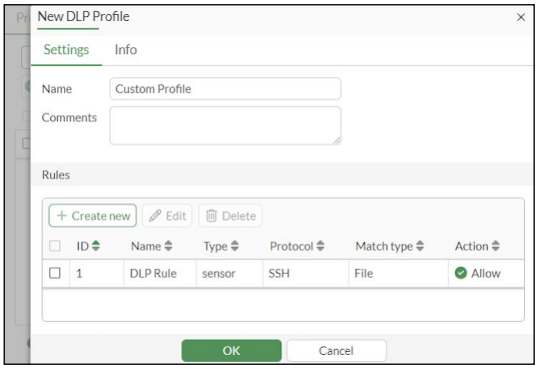
1. Configure a DLP dictionary.



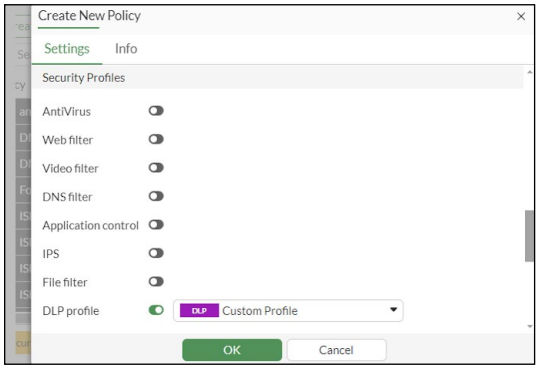
2. Configure a DLP sensor and assign the previously created dictionary.



3. Configure a DLP profile and assign the previously created sensor.



4. Add the DLP profile to a firewall policy.



Deployment Examples

Review comprehensive **DLP examples** for help facilitating your DLP deployment.