Websense Web Security Gateway Anywhere v7.5: Web DLP

Topic 45016/ Updated: 17-June-2010

Applies To:	Websense Web Security Gateway Anywhere 7.5

What is Web DLP?

Registering the proxy with the Data Security module

What's the difference between linking and the Linking Service?

What is Web DLP?

Topic 45017 / Updated: 17-June-2010

Applies To:	Websense Web Security Gateway Anywhere v7.5 Websense Data Security v7.5

Problem description

I'm interested in the Web DLP feature of Web Security Gateway Anywhere, but I'm not fully sure I know how it works.

Do I need Web and data policies for this?

Resolution

Web mail, Instant Messaging and personal networking sites are some of the most common means by which corporate data is leaked. The Web DLP (Data Loss Prevention) functionality included in Web Security Gateway Anywhere is able to detect and block such leaks- even if the connection is encrypted. The Websense PreciseID technology provides accurate fingerprinting of content to support this process.

Web DLP provides all the DLP capabilities of the full Websense Data Security Suite but for the Web channel only. It includes all of the detection capabilities, all of the reporting capabilities, all of the incident management and workflow capabilities of the full Websense Data Security solution the Web, but only for HTTP, encrypted Web (HTTPS), and FTP.

All the DLP analysis capabilities are built into Web Security Gateway Anywhere and performed on the Content Gateway machine, most commonly the V-Series appliance. The only additional requirement to deploy Web DLP is a Data Security Management Server.

Web DLP policies

In order to monitor your vital data, you must set up one or more data security policies in addition to your Web security policies. This is done in the TRITON - Data Security user interface. Most often, you use a policy wizard to create policies from predefined regulatory templates. This is a fast and accurate way to get started. Later, you may choose to create custom policies.

Data security policies typically define the source of the traffic to monitor (for example, the network or IP range), the conditions to watch for (for example, 5 or more 9-digit numbers with the text "SSN"), and the action to take in case of a breach (block or permit). By default, all HTTP, HTTPS, FTP, and FTP-over-HTTP destinations are monitored.

Policy creation is described in detail in the TRITON - Data Security Help.

How data policies differ from Web policies

In the Web security portion of your Websense software, policies govern user Internet access. A Web policy is made up of:

- **Category filters** – Used to apply actions (permit, block) to Web site categories
- **Limited access filters** – Used to permit access to only a restricted list of Web sites
- **Protocol filters** – Used to apply actions to Internet protocols
- **Schedule** – Determines when each category or limited access filter and protocol filter is enforced

In the data security portion of your Websense software, policies govern data usage. Data policies contain:

- **Rules** – Provide the logic for the policy. They are the conditions that govern the behavior of the policy. When should something be blocked? When should managers be notified?
- **Exceptions** – Define the conditions that should be exempt from the rules.
- **Content classifiers** – Describe the data to be governed. You can classify data by file properties, key phrases, dictionaries, natural language processing (NLP), a database record fingerprint, a directory fingerprint, and/or a file fingerprint.

- **Resources** – Describe the source and destination of the data you want to protect, the endpoint device or application that may be in use, and the remediation or action to take when a violation is discovered (such as block or notify).

Websense Web Security Gateway Anywhere includes predefined policies for both Web and data security. You can use these policies or create custom policies as needed.

Registering the proxy with the Data Security module

Topic 45018 / Updated: 17-June-2010

Applies To:	Websense Web Security Gateway Anywhere v7.5 Websense Content Gateway v7.5 Websense Data Security v7.5

Problem description

I am having trouble getting the proxy to register with the Data Security Management Server. Why isn't this working?

Resolution

To enable data loss prevention over Web channels, you must connect the Content Gateway module of your Web security solution to the Data Security Management Server. Follow these steps to establish that connection:

1. Ensure that Content Gateway and Data Security Management Server systems are running and accessible, and that their system clocks are approximately synchronized.
2. Ensure the Content Gateway machine has a fully qualified domain name (FQDN) that is unique in your network. Host name alone is not sufficient.
3. If Content Gateway is deployed as a transparent proxy, ensure that traffic to and from the communication interface ("C" on a V-Series appliance) is not subject to transparent routing. If it is, the registration process will be intercepted by the transparent routing and will not complete properly.
4. Make sure that the IPv4 address of the eth0 NIC on the Content Gateway machine is available (not required if Content Gateway is located on a V-Series appliance). eth0 is the NIC used by the Data Security Management Server during the registration process.

After registration, the IP address can move to another network interface on the same machine; however, that IP address is used for configuration deployment and must be available as long as the 2 modules are registered.

5. From the Content Gateway Manager, select **Configure > Basic > General**.
6. Make sure Data Security is turned on (The **On** radio button and **Integrated on-box** must be selected). Now click the Not Registered link. This opens the **Configure > Security > Data Security** registration screen.
7. Enter the IP address of the Data Security Management Server.
8. Enter a user name and password for a Data Security administrator with Manage System Modules privileges.
9. Click **Register**. You are reminded to synchronize the system time between the proxy machine and the Data Security Management Server.
10. If registration succeeds, a Data Security Configuration page displays. Set the following configuration options:
    a. **Analyze FTP Uploads**: Enable this option to send FTP uploads to Data Security for analysis and policy enforcement.
    b. **Analyze Secure Content**: Enable this option to send decrypted HTTPS posts to Data Security for analysis and policy enforcement.

    These options can be accessed whenever Data Security is registered by going to the **Configure > Security > Data Security > General** page.
11. Click **Apply**.
12. Restart Content Gateway.
13. Deploy the Content Gateway module by clicking Deploy in the TRITON - Data Security user interface.

Troubleshooting the connection

This section contains troubleshooting tips for problems registering the Content Gateway with Data Security.

If you cannot register Websense Content Gateway with the Data Security Management Server?you receive an error in Content Gateway Manager?be sure that you can ping the Data Security Management Server from the proxy machine. (Go to the Linux command line and ping the IP address of the Data Security Management Server.)

If the ping fails, make sure that you have the correct IP address for the Data Security Management Server by going to that machine and running **ipconfig** from the command line.

If the proxy is on a V-Series appliance, try pinging the IPv4 address of the appliance?s C interface from the Data Security Management Server.

If the proxy is not on a Websense appliance, try pinging the IPv4 address of the Content Gateway host system eth0 network interface from the Data Security Management Server. The registration process requires that Content Gateway is reachable on eth0. After registration, the IP address may move to another network interface on the system, but that IP address must remain available while the 2 modules are being registered.

If Content Gateway is deployed as a transparent proxy and the communication interface ("C" on a V-Series appliance) is subject to transparent routing, the registration process was likely intercepted by the transparent routing and prevented from completing. Ensure that traffic to and from the communication interface is not subject to transparent routing.

If registration still fails, make sure that neither the proxy machine or the Data Security Management Server has a machine name with a hyphen in it. This has been known to cause registration problems.

And make sure the Content Gateway machine has a fully qualified domain name (FQDN) that is unique in your network. Host name alone is not sufficient to register the proxy with the Data Security Management Server.

What’s the difference between linking and the Linking Service?

Topic 45019 / Updated: 17-June-2010

Applies To:	Websense Web Security Gateway Anywhere v7.5 Websense Data Security v7.5

Problem description

What's the difference between linking and enabling Websense Linking Service?

Resolution

In Websense Web Security Gateway Anywhere, "linking" is the act of connecting the TRITON - Web Security machine with the Data Security Management Server. You can configure linking in either user interface by providing the IP address of the other manager machine. (See TRITON - Web Security or TRITON - Data Security Help for information.) "Websense Linking Service" is a software component installed with Websense Web Security.

Linking automatically gives data security software access to Websense Linking Service. This:

- Provides access to user and group information gathered by User Service, extending IP address to user name resolution into the Data Security module for DLP Web incidents. This enables TRITON - Data Security to display user names in incident reports rather than IP addresses.

- Gives Data Security software access to Master Database categorization information so data security administrators can add URL categories as resources in their DLP policies.

Linking also enables shared administrative access to the Web Security and Data Security modules of the TRITON Unified Security Center. (Identical administrator credentials must be configured in both managers for this to work.) If you log onto TRITON - Web Security and configure linking there before logging onto TRITON - Data Security for the first time, the password for the WebsenseAdministrator user is automatically applied to this same user in Data Security.

Note that if you manually remove the link between the manager machines, you still have access to the Linking Service. Likewise, if you disable Linking Service manually, the Web and Data Security modules are still linked and you still have shared administration.