MIRACLE
SOFTWARE SYSTEMS

CA API Gateway

Sreevidya Poola
Sumavarsha Padamuthamu
Geetha Madhuri Gadamboyina
APIM Developer
Miracle Software Systems, Inc.

INDEX

Introduction of Gateway

The Gateway is an XML firewall and service gateway that controls how web services are exposed to and accessed by external client applications. The Gateway provides runtime control over service-level authentication, authorization, key management, credentialing, integrity, confidentiality, schema validation, content inspection, data transformation, threat protection (including integration with external virus scanners for SOAP attachment scanning), routing, protocol switching, SLA enforcement, logging, and other functions.

Configured and managed through the GUI-based Policy Manager, the Gateway also acts as an integration point for extending existing PKI, Identity, SSO, federation and MOM infrastructures to web services, ensuring customers can leverage existing security and messaging infrastructure for web services and SOA initiatives.

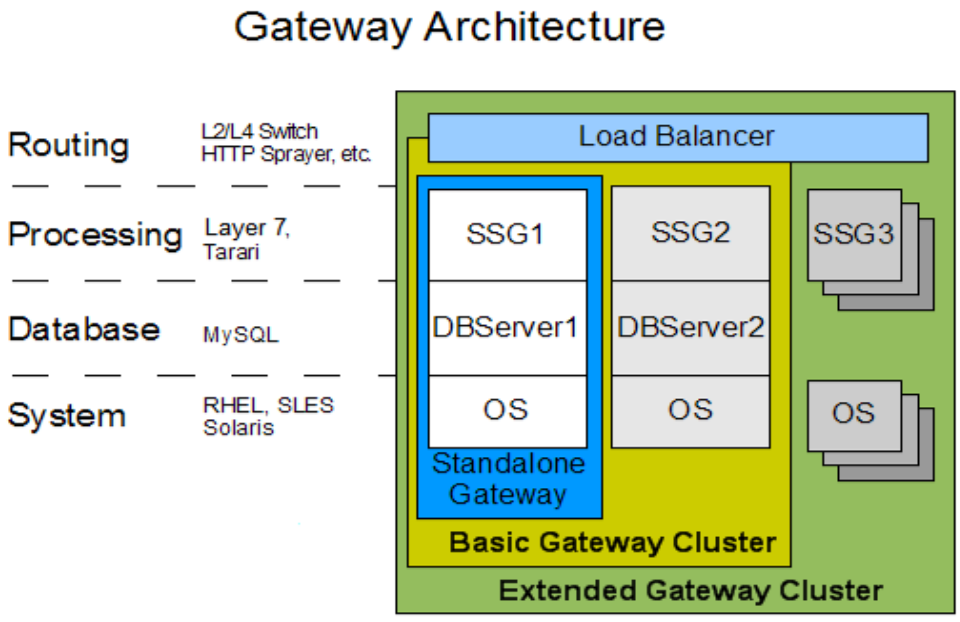
The Gateway is available as a software application running on select operating system and as a preconfigured hardware appliance for optimal performance .

GATEWAY ARCHITECTURE

The working unit of the Gateway is an HTTP, JMS, or FTP-accessible endpoint. Clients access the Gateway via a URL or queue that is compatible with one of the above protocols. The Gateway functions as a reverse proxy for service requests and should be the single web service traffic enforcement point in a network.

Due to the number of subsystems involved, changes made in the Policy Manager may require up to 15 seconds to be reflected in the Gateway.

shielding downstream services as it enforces pre-defined policy assertions on incoming and outgoing messages. In the Gateway, several interdependent layers work together to enable this end-to-end XML firewalling, security, and service protection.



Routing Layer:

The Routing Layer represents an industry-standard load balancer configured to provide TCP-level load balancing and failover. It is not required for a standalone Gateway.

Processing Layer:

The Processing Layer represents the Gateway's core "runtime" component. When a request message is received, the Gateway executes a service resolution process that attempts to identify the targeted destination service. When a published service is resolved, the Gateway executes the Policy Manager-configured policy for the service. If the policy assertions succeed, then the request is routed; if one or more policy assertions fail, then the request is either denied with a SOAP fault or the connection is dropped.

In a Gateway cluster, systems that are installed with this runtime component are referred to as "Processing Nodes".

The Processing Layer may also involve the following components:
Identity Providers, Trust Store, UDDI, Logging and Auditing Functionality and Hardware Acceleration.

Database Layer:

The Gateway stores policies, processing audits, Internal Identity Provider, keystore, configuration details and other information in a MySQL database. In a typical configuration this database will reside on the same physical system as a Processing Node, although in rare circumstances it may reside on a separate system.

In a Gateway cluster, systems that are installed with the database component are referred to as "Database Nodes". There will typically be two replicated Database Nodes in a cluster: Primary and Secondary. The Processing Nodes are configured to communicate with one of the Database

Nodes (normally the Primary) and then fail over to the Secondary Database Node should the Primary become unavailable.

System Layer:

The System Layer represents the Operating System, Java Virtual Machine, and hardware platform. The appliance form factor is based upon a hardened version of Red Hat Enterprise Linux (RHEL) operating system on a Sun Fire server.

Gateway Documentation:

There are three sources of Gateway documentation:

• As the administrative application for the Gateway, the Policy Manager documentation contains in-depth information and instructions for almost all Gateway processes, features, and functions.

• Setup and configuration information for the Gateway is described in the *Layer 7 Installation and Maintenance Manual*.

• Instructions for installing and configuring the custom assertion packages in the Gateway are provided in the *Custom Assertion Installation Manual*.

Configure the Gateway

The Gateway appliance comes pre configured with the most common settings and requires only minimal additional configuration before it can be started.

Note:

It is highly recommended that you review *Appendix I: Network Deployment Guide* first to gain a better understanding of the various network configurations. This knowledge will help you better configure your Gateways.

Accessing the Gateway Configuration Interface

The Gateway configuration interface is a menu driven wizard used to configure networking and application settings. Additionally, it provides access to the privileged (root) shell and other administrative tasks.

1. Is there network connectivity to the Gateway appliance?

- If NO, proceed with step 2.
- If YES, proceed to step 3.

2. At the machine (networking not yet set up):

If networking is not yet set up, you must either be physically at the Gateway appliance or have remote serial console access. You can access the console of the hardware appliance in one of two ways:

- Plug in a USB keyboard and monitor.
- Use a serial connection with the Gateway. For details, see *"Connecting via the Serial Management Port"* .

At the login screen, log in as user ssgconfig using the default password 7layer.

3. Remotely (networking has been set up):

If networking has been set up, you can either log in locally (as described in step 2 above) or remotely connect via SSH to the Gateway as user ssgconfig. For example:

- *Linux:* ssh ssgconfig@*<SSG_host>*
- *Windows:* Use PuTTY or a similar utility.

Configuration menu:

Welcome to the Layer 7 Gateway
This user account allows you to configure the appliance
What would you like to do?
1) Configure system settings
2) Display Layer 7 Gateway configuration menu
3) Use a privileged shell (root)
4) Change the Master Passphrase
5) Display Remote Management configuration menu
6) Manage HSM
7) Display Enterprise Service Manager configuration menu
8) Display Patch Management menu
9) Display Log View menu
R) Reboot the SSG appliance (apply the new configuration)
X) Exit (no reboot)
Please make a selection: 1

Configuring System Settings:

The Configure System Settings option in the Gateway main menu is used to view and edit the essential network settings for the Gateway appliance and to configure other system settings such as the keyboard layout. Network connectivity must be set up before you can configure the Gateway.

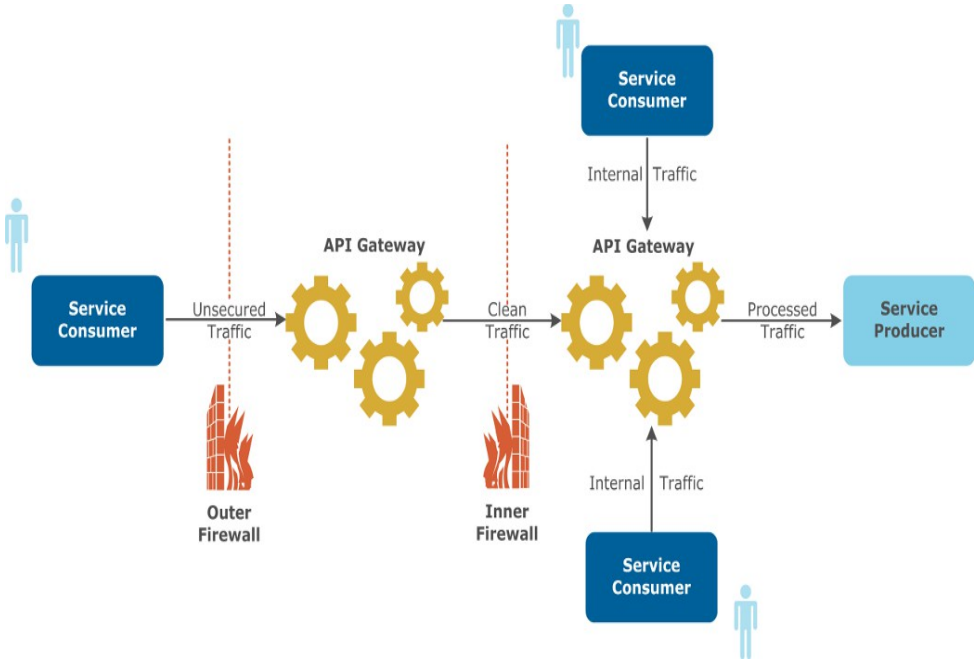
Determining Whether a Default Gateway is Necessary:

A default Gateway is a device that accepts packets that have destinations that do not match anything else in the routing table. Most networks do not require a default Gateway since it is implied by your IP address and the network topology.

During network configuration, you will be given a chance to configure a default Gateway. Whether you choose to define one now or skip over the step depends on several factors:

• Do you have a single network environment? If so, you can most likely skip defining a default Gateway.

• Do you have a multiple network environment? If so, you may want to define a default Gateway. Network environments with more than one interface will usually have more than one network connected to the machine and the most recently configured interface automatically becomes the default. If you do *not* want this interface to be the default, then you will want to specify a default Gateway.



To configure system settings:

1) Configure networking and system time settings
2) Display current network configuration
3) Configure keyboard layout
4) Configure authentication method
4) About system (versions)
6) Exit menu.

Configuring the Gateway for Remote Access:

If the Gateway node will be managed remotely by the Layer 7 Enterprise Service Manager,

Listener Address:

Select this option to enter the IP address of the Internal Management LAN. This is the "eth0" interface shown in the diagrams under "Network Deployment Guide", located in Appendix J.
***Note:** If the IP of eth0 is not readily available or if your deployment contains only a single network interface, enter "*" (asterisk) or "localhost" as the listener IP address.*

Listener Port:

Select this option to change the listening port from the default "8765".
Note: Ensure that the IP address/port number combination is valid and is not used by another process.
Tip: The listen port is stored in the cluster property node. Process ControllerExternalPort. You can update this listen port in the future by modifying the cluster property.

Remote Node Management Enabled:

Select this option to enable or disable remote management for the node:
- *To enable remote management, enter yes.*
- *To disable remote management, enter no.*

By default, remote management is disabled on all nodes.

New Trusted Certificate and Delete Trusted Certificate:

Select this option to enable trust between the node and the Enterprise Service Manager that will be remotely controlling it.
Option 4 will read "New Trusted Certificate" if trust has not yet been established. Once trust is established, it will read "Delete Trusted Certificate".

Configuring the Enterprise Service Manager:

The Enterprise Service Manager is a separate application from Layer 7 Technologies that can remotely manage Gateway clusters located anywhere in the world. To configure the Enterprise Service Manager prior to first use, select option 7 from the Gateway main menu . The following sub options are available:

1) Configure the Enterprise Service Manager
2) Enable/Disable the Enterprise Service Manager
3) Reset password for ESM user account
X) Exit menu

• Select 1 to configure the administrator credentials and listener port for the Enterprise Service Manager. Refer to Table 8 to complete the configurator.

• Select 2 to disable or re-enable the Enterprise Service Manager. This will take effect after the appliance is rebooted.

• Select 3 to reset the password for any Enterprise Service Manager user. Use this option if the password is forgotten. The Enterprise Service Manager must not be currently running. Enter the ESM Username and new ESM Password when prompted, and then press [Enter] again to confirm the change.

Starting and Stopping the Gateway:

The Gateway may need to be stopped and restarted when performing certain maintenance tasks. (Note that as a service, the Gateway does not log messages to the console or screen.)

To stop the Gateway:

1. Log in as *ssgconfig*. The Gateway main menu appears.

1. Choose option 2 (Display Gateway configuration menu). The Gateway configuration menu appears.

2. Choose option 7 (Manage Gateway status). The current status of the Gateway is displayed. Press [Enter] to continue.

3. Select the option to stop the Gateway. It may take a moment for the Gateway to stop completely. Use option 7 to monitor the stoppage ("STOPPING" indicates the node is still stopping; "SDTOPPED" indicates the node has stopped).

Note: You can also run "service ssg stop" from a privileged shell to stop the Gateway node.

To start the Gateway:

1. Log in as *ssgconfig*. The Gateway main menu appears .

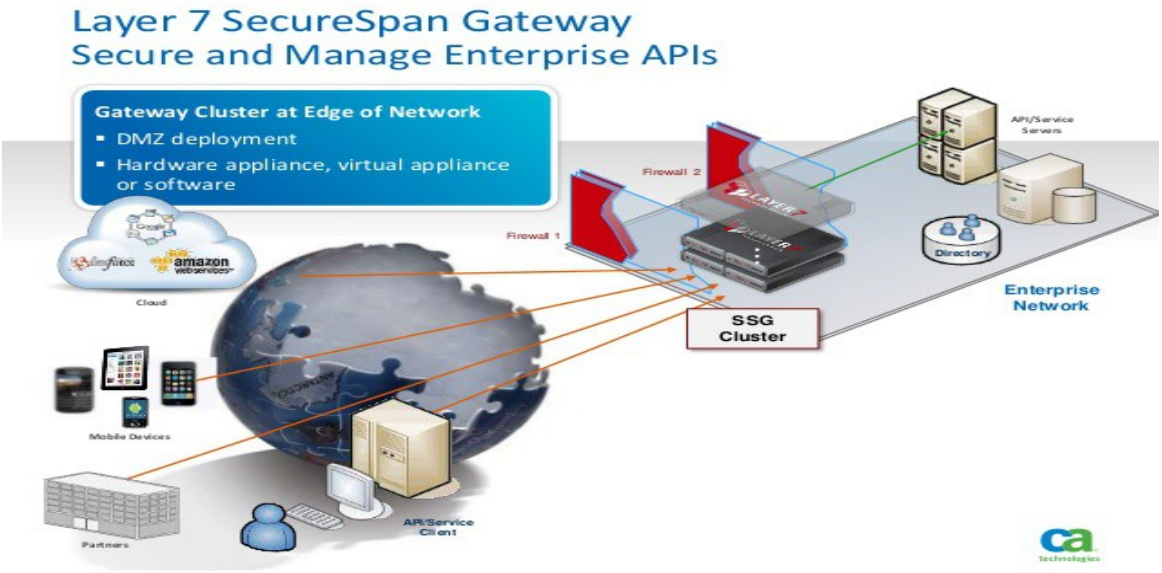
2. Choose option 2 (Display Gateway configuration menu). The Gateway configuration menu appears .

3. Choose option 7 (Manage Gateway status). The current status of the Gateway is displayed. Press [Enter] to continue.

4. Select the option to start the Gateway. It may take a moment for the Gateway to fully start. Use option 7 to monitor the startup ("STARTING" indicates the node is still starting; "RUNNING" indicates the node is up and running normally).
Note: You can also run "service ssg start" from a privileged shell to start the Gateway node.

Configure a Gateway Cluster:

A Gateway cluster consists of multiple Gateway nodes that, through a Load Balancer, present a unified network interface to client systems and software. Loosely-coupled yet synchronized through the replicated database, the Gateway cluster shares the service policies, identity providers, and configuration settings administered in the Policy Manager. This dramatically increases the scalability, processing power, and reliability of the Gateway implementation.



The Gateway cluster is an intelligent information propagation system that distinguishes between time-sensitive data that must be updated synchronously, data that is node-specific, and data that must be commonly available yet updated asynchronously. For example, policy and configuration setting changes are automatically propagated to each cluster node asynchronously within five seconds of the change in the Policy Manager. In contrast, replay attack data and SLA counters require instantaneous synchronized cluster-wide updates for them to be useful.

Tip: Complete the Cluster Configuration Worksheet in Appendix H while preplanning your cluster. This will help you complete the wizard more

quickly when it comes time to configuring the first Gateway processing node.

Note: Gateway clustering is not available if an embedded database is in use. For more information, see “Using the Embedded Database”.

System Requirements:

Gateway cluster node requirements are the same as those for a stand-alone Gateway.

***Configure the Gateway*, a cluster also requires:**

• An industry-standard Load Balancer device installed and configured on the network that can provide TCP-level load balancing and failover

• Each Gateway that will become a node in the cluster must possess its own host name, IP address, and original node address within the Load Balancer. The cluster must also possess a host name and IP address in the Load Balancer.

• Two nodes of the cluster must be installed and configured with the MySQL database with known root user names and root user passwords.

The following is an overview of creating a new Gateway cluster:

1. Install and configure the Load Balancer on the network.
2. Configure database replication on both Gateway database nodes.
3. Configure the first Gateway processing node .
4. Configure subsequent Gateway processing nodes.
5. Start the Gateway cluster.
6. Create a CA key for the cluster if the cluster will be communicating with the XML VPN Client. This applies even if the "cluster" is a single Gateway.

Note: If you need to cluster existing stand-alone Gateways, please contact Layer 7 Technical Support for assistance.

Configuring the First Gateway Processing Node:

Configuring the first node of the cluster will create and initialize the database on both database nodes and establish basic configuration of the Gateway cluster.

Prerequisite:

Before configuring the first processing node, make sure that database replication has been correctly configured (see page 51). This step is very important—failure to do so will require complex steps to enable proper operation of the cluster.

Note: If you completed a Cluster Configuration Worksheet (see Appendix H), use the values from that worksheet.

To configure the first Gateway processing node:

1. Log into DBServer1 as *ssgconfig*. The Gateway main menu appears.

2. Select option 2 (Display Gateway configuration menu). The Configure Gateway menu appears .

3. Select option 2 (Create a new Gateway database). The database configurator starts.

Once this initial node is configured, follow the next section to add subsequent processing nodes.

Maintain and Upgrade the Gateway:

The Gateway and how to upgrade to a newer version of the Gateway:

- Backing up, restoring, migrating the Gateway
- Configuring the Gateway Logging Functionality
- Configuring the Gateway Audit Functionality
- Configuring UDDI Registry Searches