Oracle® Secure Global Desktop

Deployment Guide for Release 5.5

June 2019
F12537-01

Oracle Legal Notices

Table of Contents

Preface

This manual gives an overview of Oracle Secure Global Desktop (SGD) and provides details of how to configure some typical SGD deployments.

Audience

This document is intended for SGD Administrators. It is assumed that readers are familiar with Web technologies and have a general understanding of Windows and UNIX platforms.

Related Documents

The documentation for this product is available at:

https://www.oracle.com/technetwork/documentation/sgd-193668.html

Conventions

The following text conventions are used in this document:

Convention	Meaning
boldface	Boldface type indicates graphical user interface elements associated with an action, or terms defined in text or the glossary.
italic	Italic type indicates book titles, emphasis, or placeholder variables for which you supply particular values.
`monospace`	Monospace type indicates commands within a paragraph, URLs, code in examples, text that appears on the screen, or text that you enter.

Documentation Accessibility

For information about Oracle's commitment to accessibility, visit the Oracle Accessibility Program website at
http://www.oracle.com/pls/topic/lookup?ctx=acc&id=docacc.

Access to Oracle Support

Oracle customers that have purchased support have access to electronic support through My Oracle Support. For information, visit
http://www.oracle.com/pls/topic/lookup?ctx=acc&id=info or visit http://www.oracle.com/pls/topic/lookup?ctx=acc&id=trs if you are hearing impaired.

Document Revision

Document generated on: 2019-06-25 (revision: 6160)

Chapter 1 Overview of Oracle Secure Global Desktop

This chapter presents an overview of Oracle Secure Global Desktop (SGD). Software components and the network architecture model of SGD are described.

1.1 Components of SGD

SGD contains several installable software components:

- **SGD server.** The main SGD component, which installed on *hosts*. The SGD server provides the main functionality of SGD.
- **SGD Enhancement Module.** An optional component installed on *application servers*. The Enhancement Module provides additional functionality for SGD, for example to enable users to access the drives on their client device.
- **SGD Client.** An optional component that can be installed on *client devices*, to enable users to connect to an SGD server.

  As an alternative to installing the SGD Client, users can log in to SGD through an HTML5 web page. In SGD, this is known as using the HTML5 Client.
- **SGD Gateway.** An optional component that is installed on *hosts*. The Gateway provides proxy server and load balancing functionality for an array of SGD servers.

1.2 SGD Network Architecture

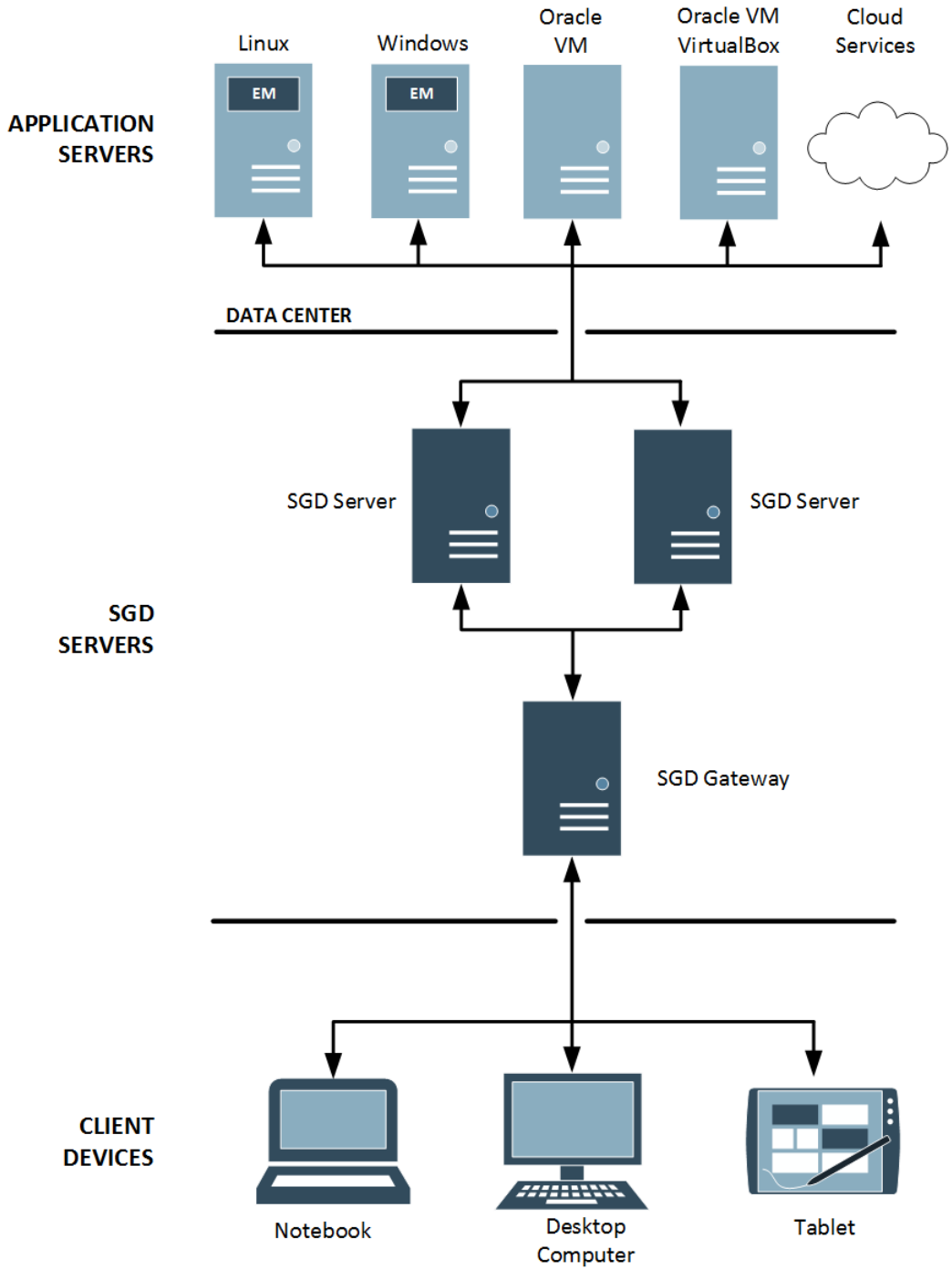
SGD is built around a three-tier network architecture model, consisting of the following tiers:

- Client devices
- SGD servers and Gateways
- Application servers

Different tiers can reside on the same host. For example, a single Linux platform host can act as both an SGD server and an application server.

Figure 1.1, “SGD Network Architecture” shows the three-tier network architecture model used by SGD.

Figure 1.1 SGD Network Architecture



Client Devices

The first tier contains *client devices*. A client device is a computer or tablet that can communicate with SGD using a browser.

The browser on the client device connects to an SGD server on the second tier and displays the SGD workspace to users.

The client device communicates with SGD servers on the second tier and displays the applications that users are running.

If the SGD Client is installed on the client device, the Adaptive Internet Protocol (AIP) ensures optimal network usage between the first and second tiers.

SGD Servers

The second tier contains *SGD servers*, which act as a link between the first and third tiers.

The SGD Servers tier may contain a single SGD server, or several SGD servers configured to form an *array*.

For enhanced security, one or more SGD Gateways may be deployed in front of an SGD array in a demilitarized zone (DMZ).

An SGD server does the following:

- Authenticates users when they log in to SGD
- Negotiates with application servers to authenticate users when they run applications
- Communicates with the client device, to display applications
- Keeps track of running applications even after users have logged out, so that they can resume them later

Application Servers

The third tier contains *application servers* that run the applications and desktop sessions for an SGD user.

When a user clicks a link on their workspace, SGD starts the application on an appropriate application server. Output from the application is redirected by the SGD server from the application server to the client device.

The Application Servers tier can contain conventional UNIX or Linux platform application servers and Windows application servers.

Also supported in this tier are virtual machine hypervisor hosts such as Oracle VM and Oracle VM VirtualBox, and cloud services such as Oracle Cloud Infrastructure Compute Classic.

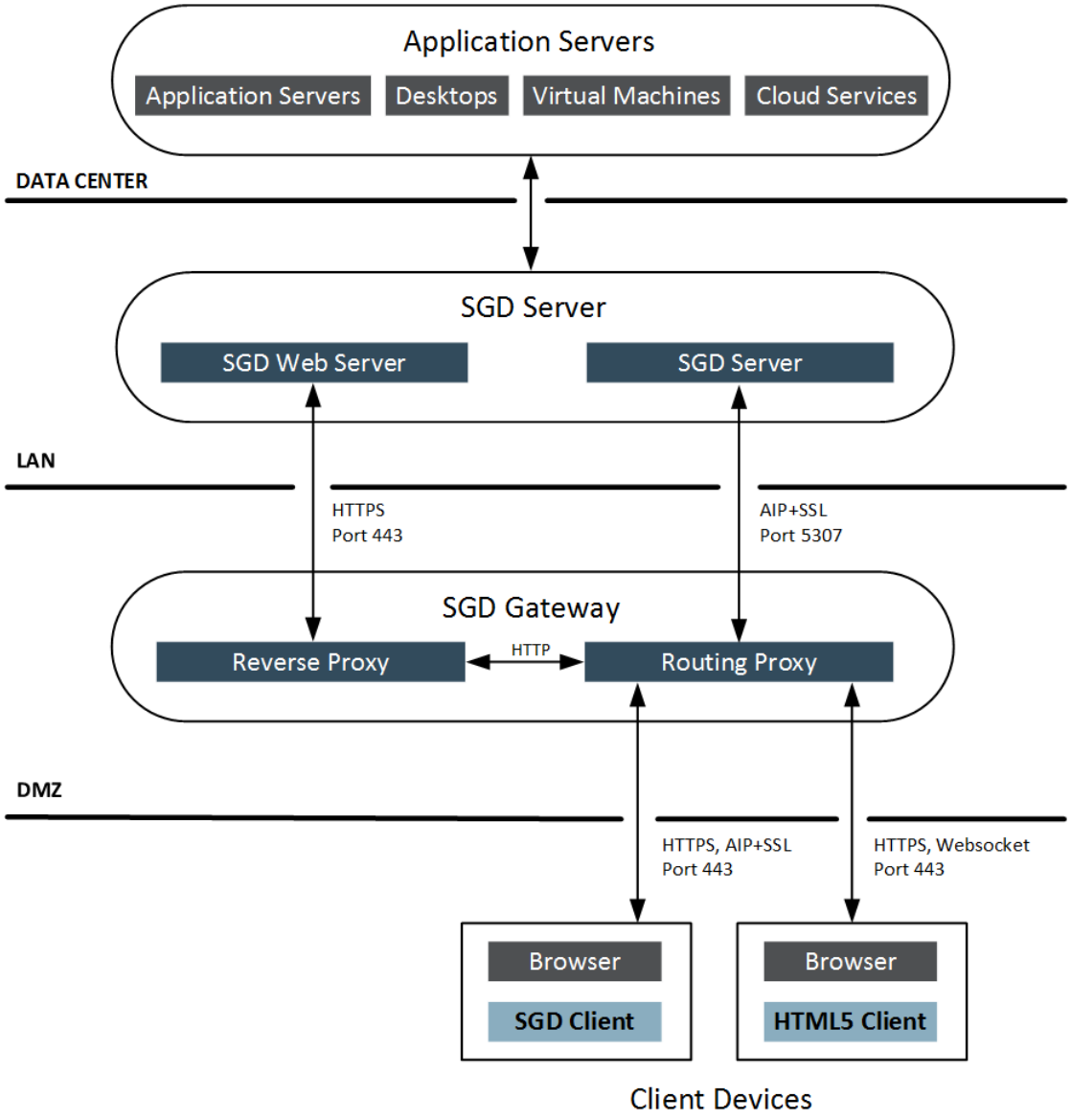
1.3 Connections Used by SGD

An SGD installation is secure by default. Client devices connect to SGD using HTTPS, AIP, and Websocket data connections that are secured using Transport Layer Security (TLS).

Figure 1.2, “SGD Connections and Ports” shows some of the connections and ports used by SGD.

This figure shows how an SGD Client connection uses an AIP data connection and an HTML5 Client connection uses a Websocket data connection.

Figure 1.2 SGD Connections and Ports



Note

See Firewalls in the *Oracle Secure Global Desktop Administration Guide* for more detailed information on the ports used in an SGD deployment.

Chapter 2 Using the Oracle Secure Global Desktop Gateway

The SGD Gateway is a proxy server designed to be deployed in front of an SGD array. The Gateway provides single port access to the SGD array, supports IPv6 connections, and manages load balancing of connections for the SGD servers in the array.

The Gateway can also provide enhanced security when deployed in front of an SGD array in a demilitarized zone (DMZ). This enables the SGD array to be located on the internal network of an organization.

This chapter describes some typical SGD deployments that use the SGD Gateway. The following deployment examples are described:

- **Basic Gateway deployment.** Uses a single SGD Gateway to provide secure access to an SGD array.
- **Single-host Gateway deployment.** A single SGD Gateway and a single SGD server are installed on the same host. This is sometimes called *colocation*.
- **Load-balanced Gateway deployment.** Uses multiple SGD Gateways and a load balancer to provide redundancy and scalability.
- **Secure access to a cloud service.** Uses the enhanced security features of an SGD Gateway deployment to integrate with a cloud service, such as Oracle Cloud Infrastructure.

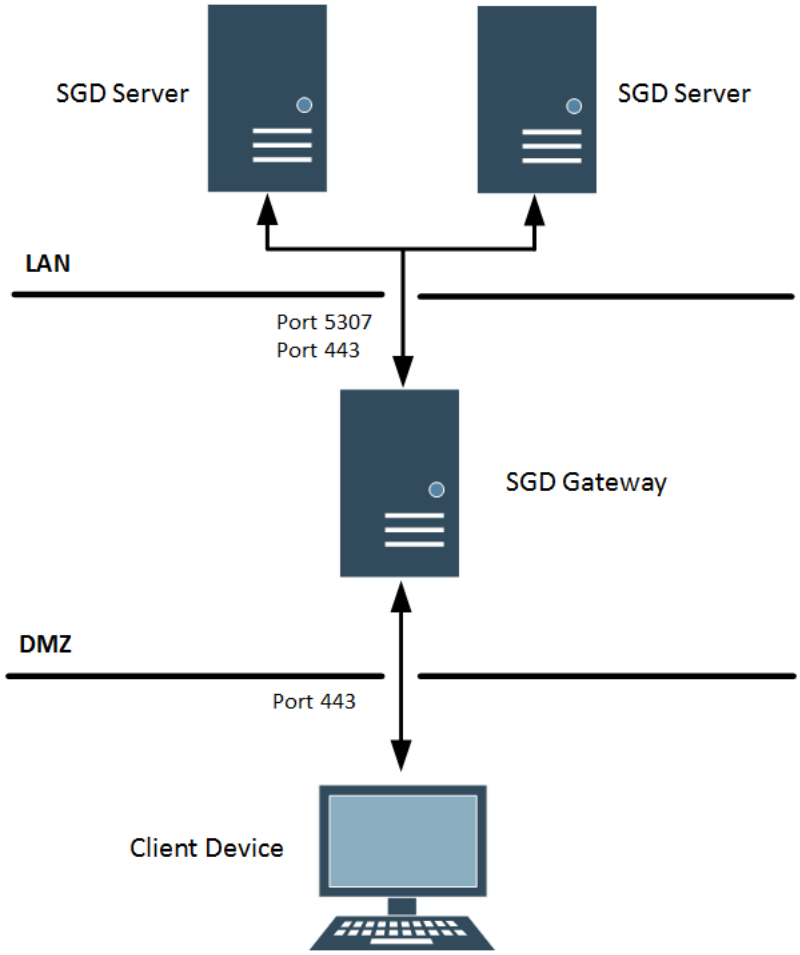
Note

For more information on installing and configuring the SGD Gateway, see the *Oracle Secure Global Desktop Gateway Administration Guide*.

2.1 Basic Gateway Deployment

The basic Gateway deployment uses a single SGD Gateway with an SGD array consisting of one or more SGD servers. See Figure 2.1, “Network Diagram for a Basic Gateway Deployment”.

Figure 2.1 Network Diagram for a Basic Gateway Deployment



The advantages of a basic Gateway deployment are as follows:

- **Secure single port access.** Access is by a single port, TCP port 443. You only need to open this port in your firewall.
- **IPv6 support.** IPv6 support is available by default for this deployment.
- **Load balancing.** The Gateway manages load balancing of HTTP connections for the SGD servers in the array.
- **Enhanced security.** The Gateway is deployed in front of an SGD array in a demilitarized zone (DMZ).
- **Scalability.** You can add extra SGD servers or Gateways to the deployment.

2.1.1 Configuring a Basic Gateway Deployment

Note

The connections between an SGD Gateway and the SGD servers in the array use security certificates for mutual authorization. Configuring these connections involves installation of certificates on Gateway and SGD server hosts.

Use the following steps to configure a basic Gateway deployment.

1. Install the SGD software on the hosts.

   a. Install the main SGD component on SGD server hosts. See Section A.1, “Installing SGD”.

   b. Install the SGD Gateway software on Gateway hosts. See Section A.2, “Installing the SGD Gateway”.

2. Install security certificates for the SGD servers on the SGD Gateway.

   Repeat the following steps for each SGD server in the array.

   a. Copy the following security certificates from the SGD server to the SGD Gateway.

      - **CA certificate.** This certificate is at `/opt/tarantella/var/info/certs/PeerCAcert.pem` on the SGD host.
      - **SSL certificate.** This certificate is at `/opt/tarantella/var/tsp/cert.pem` on the SGD host.

   b. Use the `gateway server add` command to import the certificates into the SGD Gateway keystore. For example:

      ```
      # /opt/SUNWsgdg/bin/gateway server add --server sgd-server1 \
      --certfile /opt/SUNWsgdg/proxy/etc/PeerCAcert.pem --url https://sgd1.example.com \
      --ssl-certfile /opt/SUNWsgdg/proxy/etc/cert.pem
      ```

      See gateway server add in the *Oracle Secure Global Desktop Gateway Administration Guide*.

   c. Restart the SGD Gateway.

      ```
      # /opt/SUNWsgdg/bin/gateway restart
      ```

3. Install the SGD Gateway certificate on the SGD array.

   a. Export the SGD Gateway certificate from the SGD Gateway keystore. For example:

      ```
      # /opt/SUNWsgdg/bin/gateway cert export --certfile gateway1.pem
      ```

   b. Copy the SGD Gateway certificate to the `/opt/tarantella/var/tsp` directory on the primary SGD server in the array.

      After copying, change the file permissions and ownership for the certificate. For example:

      ```
      # chmod 600 /opt/tarantella/var/tsp/gateway1.pem
      # chown ttasys:ttaserv /opt/tarantella/var/tsp/gateway1.pem
      ```

   c. Register the SGD Gateway with the SGD array.

      On the primary SGD server, use the `tarantella gateway add` command to import the SGD Gateway certificate. For example:

      ```
      # tarantella gateway add --name sgd-gateway1 \
      --certfile /opt/tarantella/var/tsp/gateway1.pem
      ```

      See tarantella gateway add in the *Oracle Secure Global Desktop Gateway Administration Guide*.

4. Configure which SGD Client connections can use the SGD Gateway.

   On the primary SGD server, set the `--security-gateway` global attribute.

For example, to specify that all SGD Client connections are routed through TCP port 443 of a single SGD Gateway `gateway1.example.com`:

```
$ tarantella config edit --security-gateway "*:sgdg:gateway1.example.com:443"
```

5. Log in to SGD.

   a. Using a browser, go to the URL for the Gateway. For example, `https://gateway1.example.com`.

      The SGD login page is displayed.

   b. Log in using the default SGD Administrator credentials.

      Enter `Administrator` for the Username and the superuser (root) password for the Password.

      Your SGD workspace is displayed.

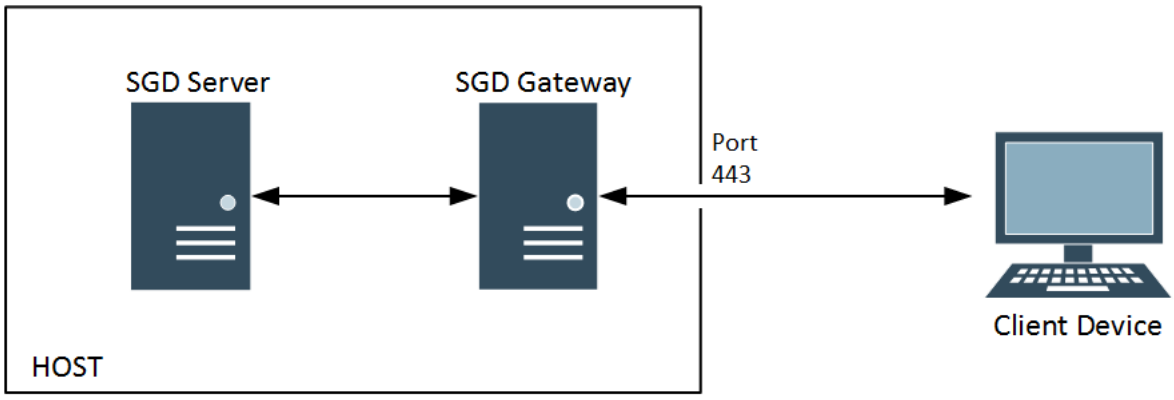
6. Log out of SGD.

   Click the **Logout** button on your workspace and click **OK** when prompted for confirmation.

2.2 Single Host Gateway Deployment

For a single host Gateway deployment, the SGD Gateway and a single SGD server are installed on the same host. See Figure 2.2, “Network Diagram for a Single Host Gateway Deployment”.

Figure 2.2 Network Diagram for a Single Host Gateway Deployment



The advantages of a single host Gateway deployment are as follows:

- **Easy Configuration.** You only need to configure a single host.
- **Secure single port access.** Access is by a single port, TCP port 443. You only need to open this port in your firewall.
- **IPv6 support.** IPv6 support is available by default for this deployment.
- **Gateway discovery.** For this deployment, you can use the *discovery* feature of SGD to automatically discover and configure the Gateway.

Note

In a single host Gateway deployment you cannot use an array with more than one SGD server, or add other Gateways.

2.2.1 Discovering and Configuring a Single Host Gateway Deployment

Use the following steps to discover and configure a single host Gateway deployment automatically.

1. Install and configure the SGD server.

   For more information, see Section A.1, “Installing SGD”.

2. Start the SGD server.

   ```
   # tarantella start
   ```

3. Install the SGD Gateway software.

   For more information, see Section A.2, “Installing the SGD Gateway”.

4. Stop the SGD server.

   ```
   # tarantella stop
   ```

5. Discover and configure the SGD Gateway.

   On the SGD server, use the `tarantella discover gateway` command to discover and configure an SGD Gateway that is installed on the same host as an SGD server.

   ```
   # tarantella discover gateway --local
   ```

6. Start the SGD server.

   ```
   # tarantella start
   ```

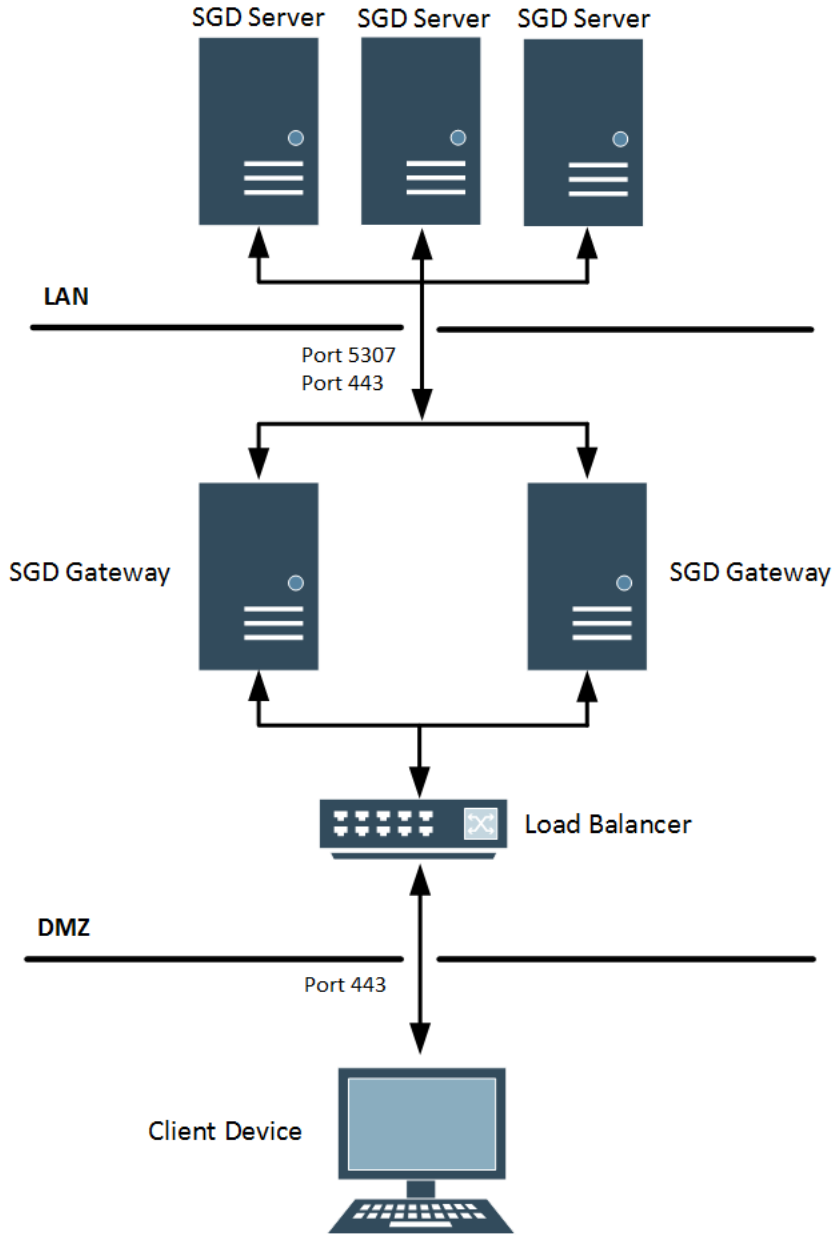
7. Start the SGD Gateway.

   ```
   # /opt/SUNWsgdg/bin/gateway start
   ```

2.3 Load-Balanced Gateway Deployment

The load-balanced Gateway deployment uses multiple SGD Gateways and a load balancer as the network entry point. See Figure 2.3, “Network Diagram for a Load-Balanced Gateway Deployment”.

Figure 2.3 Network Diagram for a Load-Balanced Gateway Deployment



The advantages of a load-balanced Gateway deployment are as follows:

- **Secure single port access.** Access is by a single port, TCP port 443. You only need to open this port in your firewall.
- **IPv6 support.** IPv6 support is available by default for this deployment.
- **Load balancing.** Connections to the Gateways are handled by a dedicated load balancer device.
- **Redundancy.** Unavailability of a Gateway or SGD server is handled automatically.
- **Scalability.** You can add extra SGD servers or Gateways to the deployment.
- **Enhanced security.** The Gateway is deployed in front of an SGD array in a demilitarized zone (DMZ).

2.3.1 Configuring a Load-Balanced Gateway Deployment

Note

The connections between an SGD Gateway and the SGD servers in the array use security certificates for mutual authorization. Configuring these connections involves installation of certificates on Gateway and SGD server hosts.

Use the following steps to configure a load-balanced Gateway deployment.

1. Install the SGD software on the hosts.

   a. Install the main SGD component on SGD server hosts. Follow the steps in Section A.1, “Installing SGD”.

   b. Install the SGD Gateway software on Gateway hosts. Follow the steps in Section A.2, “Installing the SGD Gateway”.

2. Configure your load balancer to forward connections to the SGD Gateways.

   See your load balancer documentation for details of how to do this.

3. Install security certificates for the SGD servers on each SGD Gateway.

   For each Gateway, repeat Step 2 of Section 2.1.1, “Configuring a Basic Gateway Deployment”.

4. Install the SGD Gateway certificates on the SGD array.

   For each Gateway, repeat Step 3 of Section 2.1.1, “Configuring a Basic Gateway Deployment”.

5. Configure which SGD Client connections can use the SGD Gateway.

   On the primary SGD server, set the `--security-gateway` global attribute.

   For example, to specify that all SGD Client connections are routed through TCP port 443 of an external load balancer `lb.example.com`:

   ```
   $ tarantella config edit --security-gateway "*:sgdg:lb.example.com:443/sgd"
   ```

6. Log in to SGD.

   a. Using a browser, go to the URL for the load balamcer. For example, `https://lb.example.com`.

      The SGD login page is displayed.

   b. Log in using the default SGD Administrator credentials.

      Enter `Administrator` for the Username and the superuser (root) password for the Password.

      Your SGD workspace is displayed.

7. Log out of SGD.

   Click the **Logout** button on your workspace and click **OK** when prompted for confirmation.

2.4 Cloud Access and Enhanced Security With an SGD Gateway Deployment

SGD supports the following features, which enable you to enhance the security of an SGD Gateway deployment and integrate with cloud services, such as Oracle Cloud Infrastructure.

- **Client certificate authentication.** Users authenticate to SGD with a security certificate installed on a browser or smart card on the client device.

  With client certificate authentication, users do not need to enter a username or password when they log in to SGD.

  See Using Client Certificates With the SGD Gateway in the *Oracle Secure Global Desktop Gateway Administration Guide*.

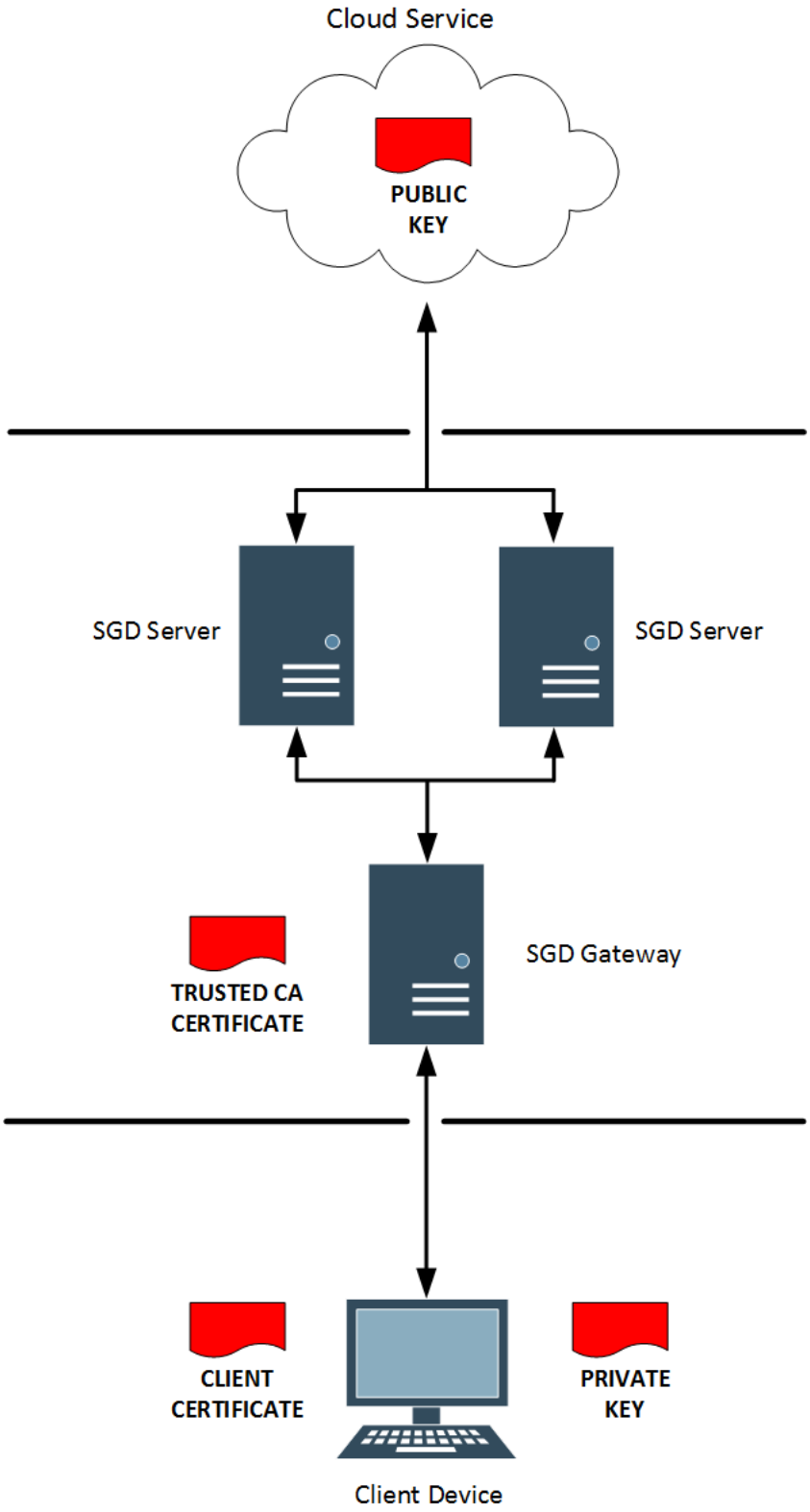
- **Application authentication using SSH keys.** Users authenticate to an application server or cloud service with an SSH key installed on their client device.

  With SSH keys, users do not need to enter a username and password when starting an application on their workspace.

  See Using SSH Keys for Application Authentication in the *Oracle Secure Global Desktop Administration Guide*.

Figure 2.4, “Secure Gateway Deployment, Showing Locations of Client Certificates and SSH Keys” shows a secure Gateway deployment connecting to a cloud service.

Figure 2.4 Secure Gateway Deployment, Showing Locations of Client Certificates and SSH Keys



2.4.1 Configuring a Secure Gateway Deployment

1. Configure a basic Gateway deployment, as described in Section 2.1, “Basic Gateway Deployment”.
2. Configure client certificate authentication.
   a. Generate a client certificate on the client device.
      - Install the client certificate on the browser or smart card on the client device.
      - (Optional) Import the client certificate into the SGD Gateway client keystore.

        You do not need to do this step if the client certificate is signed by a trusted Certificate Authority (CA).

        Use the `gateway clientcert` command to import the certificate. For example:

        ```
        # /opt/SUNWsgdg/bin/gateway clientcert import --certfile mycert.pem --alias mycert
        ```

   b. Configure the SGD Gateway to use client certificate authentication.

      ```
      # /opt/SUNWsgdg/bin/gateway config edit --services-clientcerts required
      ```

      Restart the SGD Gateway.

      ```
      # /opt/SUNWsgdg/bin/gateway restart
      ```

   c. Enable third-party authentication for the SGD array. For example:

      ```
      # tarantella config edit --login-thirdparty 1
      ```

3. Configure SSH keys for application authentication.
   a. Generate an SSH key pair on the client device.
   b. Install the SSH keys.
      - Add the public key of the SSH key pair to the cloud service.

        You can attach the public key to an instance when you create the instance.
      - The private key of the SSH key pair remains on the client device.

        Note

        Private keys never leave the client device and are not sent to the SGD server or cloud service.
4. Configure SGD to enable the cloud administrator to run an application or desktop on a cloud instance.
   a. Create a user profile object for the cloud administrator.
   b. Create an application object to represent the application that you want to run on the cloud service.

      To display a desktop session, you can modify the My Desktop application.
   c. Assign the application to the user profile object for the cloud administrator.
   d. Create an application server object to represent the cloud instance.

- For Oracle VM and Oracle VM VirtualBox services, use a hypervisor host object.
- For other cloud services, use a dynamic application server object, such as a User-defined SGD broker. This broker lists the cloud instances that are assigned to an application object, and also enables users to specify the name of a cloud instance.

e. Assign the application server to the application object.

2.4.2 The User Experience With a Secure Gateway Deployment

The user experience is quicker and more secure, compared to an SGD deployment where usernames and passwords must be entered.

1. Logging in to SGD.

   The user goes to the URL for the SGD server. For example, `https://sgd.example.com/sgd`, where *`sgd.example.com`* is the name of the SGD server.

   - The client certificate in the user's browser is used to authenticate to SGD.
   - The trusted certificate authorities (CAs) in the Gateway's client keystore are used to validate the connection.
   - The user does not have to enter their SGD username and password.
   - The SGD login dialog box is not displayed.

2. Starting an application.

   The user clicks an application link on the workspace.

   - The private key on the client device and the public key on the cloud service are used for application authentication.
   - The user does not have to enter a username and password to start the application.
   - At the first start of the application, the user is prompted for the location of the private key on the client device.
   - User prompts for the private key location are not shown for subsequent instances of the application.

     If the private key is passphrase-protected, a prompt to enter the passphrase is displayed when starting the application.

Appendix A Installing SGD Components

This appendix includes instructions on installing the following SGD components:

- SGD server
- SGD Gateway
- SGD Enhancement Module

A.1 Installing SGD

The following procedure describes how to install the SGD software on an Oracle Linux host. For more detailed instructions, see the *Oracle Secure Global Desktop Installation Guide*.

Note

Before you begin, check the following:

- (Optional) You have access to your SSL certificate and the private key and CA certificate, if needed. The certificates must be in PEM format.
- Ports 80 and 443 are open in your firewall.

  If port 80 and port 443 are in use, you must either shut down the other services using those ports or configure the SGD server to use other ports.

1. Obtain the SGD software.

   The following options are available:

   - Download the software from the Oracle Software Delivery Cloud and save the software package file to a temporary directory on the host.
   - Download the package from the Unbreakable Linux Network (ULN) channel.

   The package file is named `oracle-sgd-server-`*`version`*`.el7.x86_64.rpm`, where *`version`* is the SGD software version number.

2. Log in as superuser (root) on the host.
3. Install SGD.

   If the package file is compressed, you must expand it before installing.

   From a temporary directory:

   ```
   # yum install /tempdir/oracle-sgd-server-5.50.version-1.el7.x86_64.rpm
   ```

   SGD is installed in the `/opt/tarantella` directory on the host.

4. Start the SGD server.

   ```
   # /opt/tarantella/bin/tarantella start
   ```

   The software is installed and configured using the default settings.

A.2 Installing the SGD Gateway

The following procedure describes how to install the SGD Gateway software on an Oracle Linux host.

For more detailed instructions, see the *Oracle Secure Global Desktop Gateway Administration Guide*.

1. a. Obtain the software.

   The following options are available:

   - Download the software from the Oracle Software Delivery Cloud and save the software package file to a temporary directory on the host.
   - Download the package from the Unbreakable Linux Networks (ULN) channel.

   The package file is named `oracle-sgd-gateway-`*`version`*`.el7.x86_64.rpm`, where *`version`* is the SGD Gateway software version number.

   b. Log in as superuser (root) on the host.

   c. Install the SGD Gateway.

   If the package file is compressed, you must expand it before installing.

   From a temporary directory:

   ```
   # yum install /tempdir/oracle-sgd-gateway-version.el7.x86_64.rpm
   ```

   The SGD Gateway is installed in the `/opt/SUNWsgdg` directory.

   After installing the software, you must perform additional configuration of the SGD Gateway. See Configuring the SGD Gateway for details of what you need to do.

A.3 Installing the SGD Enhancement Module

The SGD Enhancement Module is an optional software component that can be installed on application servers.

Instructions for installing the SGD Enhancement Module are in the *Oracle Secure Global Desktop Enhancement Module Administration Guide*.