Oracle® Communications Services Gatekeeper

Security Guide

Release 6.0

E50768-02

November 2015

ORACLE®

Oracle Communications Services Gatekeeper Security Guide, Release 6.0

E50768-02

Contents

3 Deploying Services Gatekeeper in a Demilitarized Zone

4 Implementing Services Gatekeeper Security

5 Security Considerations for Developers

Preface

This guide explains concepts and tasks necessary to securely implement Oracle Communications Services Gatekeeper.

Audience

This document is intended for system administrators and system integrators who secure services in a Services Gatekeeper implementation.

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.

Related Documents

For more information, see the following documents in the Oracle Communications Services Gatekeeper Release 6.0 documentation set:

- *Oracle Communications Services Gatekeeper Concepts*
- *Oracle Communications Services Gatekeeper Multi-tier Installation Guide*
- *Oracle Communications Services Gatekeeper System Administrator's Guide*
- *Oracle Communications Services Gatekeeper OAuth Guide*

Services Gatekeeper is partially based on the Oracle WebLogic Server, and you will find these Oracle Fusion Middleware documents useful:

- *Oracle Fusion Middleware Securing Oracle WebLogic Server*
- *Oracle Fusion Middleware Understanding Security for Oracle WebLogic Server*
- *Oracle Fusion Middleware Securing a Production Environment for Oracle WebLogic Server*

See the Oracle WebLogic Server Product documentation at:

http://www.oracle.com/technetwork/middleware/weblogic/documentation/index.html

1

Services Gatekeeper Security Overview

This chapter provides an overview of the Oracle Communications Services Gatekeeper security features and considerations.

Basic Security Considerations

The following principles are fundamental to using any application securely:

- **Keep software up to date**. This includes the latest product release and any patches that apply to it as well as updates for WebLogic Server, Oracle Coherence and Java.
- **Limit privileges as much as possible**. Users should be given only the access necessary to perform their work. User privileges should be reviewed periodically to determine relevance to current work requirements.
- **Monitor system activity**. Establish who should access which system components, how often, and then monitor those components.
- **Install software securely**. For example, use firewalls, secure protocols such as SSL, and secure passwords. See "Performing a Secure Services Gatekeeper Installation" for more information.
- **Encrypt sensitive data and communications**. For example, use database and network communication encryption tools to ensure Services Gatekeeper data is safe from theft or unauthorized access. See “Securing Services Gatekeeper” in *Services Gatekeeper System Administrator’s Guide* for more information.
- **Learn about and use the Services Gatekeeper run time security features**. See "Implementing Services Gatekeeper Security" for more information.
- **Use secure development practices**. For example, take advantage of existing database security functionality rather than creating your own application security. See "Security Considerations for Developers" for more information.
- **Keep up to date on security information**. Oracle regularly issues security-related patch updates and security alerts. Install all security patches as soon as possible. See the Critical Patch Updates and Security Alerts website:

  `http://www.oracle.com/technetwork/topics/security/alerts-086861.html`

Overview of Services Gatekeeper Security

Services Gatekeeper extends Oracle WebLogic Server, allowing you to offer APIs, and IP-based applications (services). Services Gatekeeper and WebLogic Server include

extensive security features for protecting your Services Gatekeeper implementation, including:

- Authentication
- Authorization
- Single sign-on
- Configurable traffic filters
- Security Assertion Markup Language (SAML) support

When used properly, these capabilities ensure that you can protected your Services Gatekeeper implementation.

Services Gatekeeper requires a database. You use database security features, such as encryption and access control, to ensure that the data and communications used by Services Gatekeeper are protected. Production environments using Oracle Enterprise Database can use Oracle Database Advanced Security to protect data.

Services can support multiple security standards, including:

- Services using SOAP and RESTful-based traffic can use the Service Gatekeeper firewall settings to protect against denial of service (DOS) attacks.
- Services using SOAP-based interfaces can leverage the flexible security framework of WebLogic Server to provide robust system protection. Applications can be authenticated using plaintext or encrypted (digest) passwords, X.509 certificates, or SAML 1.0/1.1 tokens.
- Service requests can use XML encryption based on the W3C standards, for either the whole request message or specific parts of it. To ensure message integrity, requests can be digitally signed by using the W3C XML digital signature standards.
- Services using RESTful interfaces can leverage HTTP basic authentication: user name/password and SSL protection. The use of SAML assertions as authorization grants with OAuth is also supported.

Services Gatekeeper Concepts contains more information about supported security-related standards.

Understanding the Services Gatekeeper Environment

When planning your Services Gatekeeper implementation, consider the following:

- **Which resources must be protected?**

  You must protect resources such as:

  - Subscriber data, for example, credit-card numbers.
  - Partner data, for example, applications, metrics, and contact information
  - Internal data, for example, the MBeans that control Services Gatekeeper.
  - System components from being disabled by external attacks or intentional system overloads.
  - Network nodes that prevent Services Gatekeeper from being disabled by external attacks or intentional system overloads.
  - Communications between network nodes including Services Gatekeeper tiers, databases, and network elements.

- **Who are you protecting data from?**

  For example, you must protect partner data from unauthorized partners, but someone in your organization might need to access that data to manage it. You can analyze your workflows to determine who needs access to the data; for example, a system administrator might manage your system components without needing to access the system data.

- **What will happen if protections on strategic resources fail?**

  In some cases, a fault in your security scheme is nothing more than an inconvenience. In other cases, a fault might cause great damage to you, your partners, or your customers. Understanding the security ramifications of each resource will help you protect it properly.

Recommended Deployment Configurations

This section describes recommended deployment configurations for Services Gatekeeper.

Services Gatekeeper security requirements depend on the deployment type and intended use. Production implementations typically consist of tiered deployments with more features, such as geographic redundancy, that require high security levels to protect subscriber and application data. Test and development implementations usually consist of single-tier deployments with less stringent security requirements.

When deploying Services Gatekeeper, consider the security requirements related to the following deployment types:

- **Tiered** deployments provide multiple security protections, including the possibility of firewalls between tiers, load balancers, separation of the access and network tiers into unique networks, and distribution of system components across machines and geographic locations. For tiered deployments, you should also implement the security capabilities offered by WebLogic Server and your database software.

  See "About Tiered Deployments" in *Services Gatekeeper Multi-tier Installation Guide* for information about medium and large deployments and deployments with service-oriented architecture functionality.

- **Non-tier** deployments provide developers and testers with functional Services Gatekeeper environments in standalone or basic high-availability configurations. Non-tier deployments have limited security. Ensure that these deployments are protected as your business requires. WebLogic Server security features can be implemented if necessary, but the use of database security features is highly recommended.

  See "About Non-tiered Deployments" in *Services Gatekeeper Multi-tier Installation Guide* for information about deployments targeted for smaller groups of developers to develop and test their extension software.

- **Geographically Redundant** deployments protect you from catastrophic failures such as natural disasters. When deploying Services Gatekeeper across multiple geographic locations, you must ensure that communication between sites is secure in addition to securing each location's application components and data.

  See "About Geographically Redundant Deployments" in *Services Gatekeeper Multi-tier Installation Guide* for information about separating Services Gatekeeper geographically to protect your installation against data loss and service failure in the event of a natural disaster or other catastrophic event.

Securing Services Gatekeeper Components

Your Services Gatekeeper environment can include the following components. Configure the security of each component in your environment according to the following recommendations.

Operating System Security

Review the security considerations for your operating system:

- **Oracle Solaris**: See *Oracle Solaris 11 Security Guidelines* on the Oracle Help Center website:

  http://docs.oracle.com/cd/E23824_01/html/819-3195/index.html

- **Oracle Linux**: See *Oracle Linux Security Guide for Release 6* on the Oracle Help Center website:

  http://docs.oracle.com/cd/E37670_01/E36387/html/index.html

- **RedHat**: See *RedHat Enterprise Linux 7 Security Guide* on the RedHat website:

  https://access.redhat.com/documentation/en-US/Red_Hat_Enterprise_Linux/7/html/Security_Guide

Database Security

Consider the security issues related to your database. For a list of supported databases, see "Supported Databases" in *Services Gatekeeper Multi-tier Installation Guide*.

Oracle Databases

Before installing Services Gatekeeper, you install an Oracle database to support Services Gatekeeper.

Oracle strongly recommends that you deploy the Services Gatekeeper Oracle database in its own tier, for both security and performance reasons. For more information about:

- Oracle database security, see *Oracle Database Advanced Security Administrator's Guide*.
- Data security considerations in Oracle Real Application Clusters, see *Oracle Real Application Clusters Administration and Deployment Guide*.

MySQL Databases

MySQL database is an optional database. It is recommended for internal use and is not recommended for your production environment.

For security considerations associated with MySQL Database, see *MySQL 5.6 Reference Manual*.

WebLogic Server Security

See *Oracle Fusion Middleware Securing a Production Environment for Oracle WebLogic Server*.

Security Considerations for Relational Database Authentication Providers

An RDBMS Authentication provider is a user name/password based Authentication provider that uses a relational database (rather than an LDAP directory) as its data store for user, password, and group information.

For security considerations associated with the security store, see *Oracle Fusion Middleware Securing Oracle WebLogic Server*.

Related Applications Security

Consider the security issues related to the following applications:

- **Oracle Communications Converged Application Server**

  For SIP-based services, you access Oracle Communications Converged Application Server (OCCAS) through the Services Gatekeeper console. For information about security implementations in OCCAS, see *Oracle Communications Converged Application Server Security Guide*.

- **Java Messaging Service (JMS) Servers**

  JMS servers are necessary for any additional network tier servers you set up. For more information, see "Creating JMS Servers for Additional Network Tier Servers" in *Services Gatekeeper Multi-tier Installation Guide*.

  For security considerations associated with JMS servers, see *Oracle Fusion Middleware Configuring and Managing JMS for Oracle WebLogic Server*.

- **Oracle Enterprise Manager**

  Oracle Enterprise Manager is purchased, installed, and configured separately. Oracle Enterprise Manager Cloud Control enables you to monitor and manage the complete Oracle IT infrastructure from a single console.

  For information about Enterprise Manager security, see *Oracle Enterprise Manager Administration*.

- **Oracle Business Intelligence Enterprise Edition**

  Oracle Business Intelligence (OBI) is the business intelligence platform that supports Services Gatekeeper Portal applications. It enables you to provide query and analysis tools for your customers (the partner managers and partners) to customize their views of the data seen on the reports pages of their portals.

  Note: You install OBI by using the Oracle Communications Services Gatekeeper extension installer. Before installing Services Gatekeeper reporting and portal support, you must first install OBI.

  For security considerations associated with OBI, see *Oracle Fusion Middleware Security Guide for Oracle Business Intelligence Enterprise Edition*.

- **Oracle Access Manager**

  After you install Services Gatekeeper, set up and configure web services security and Oracle Access Manager (OAM) JMX security.

  For information about:

  – Securing the Oracle Access Manager MBeans, see "Securing the Oracle Access Manager MBeans" in *Services Gatekeeper System Administrator's Guide*.

  – Security considerations associated with Access Manager container framework and MBeans, security keys and the embedded Java keystore, security modes for multi-data centers, and logging for Security Token Service and Identity Federation, see *Oracle Fusion Middleware Administrator's Guide for Oracle Access Management 11g Release 2 (11.1.2.2) for All Platforms*.

External Firewall Security

Firewalls are essential for securing production implementations. Ensure that your firewalls are configured to manage traffic on WebLogic Server SSL listener ports and Oracle Database listener ports.

For information about:

- The location of firewalls in Services Gatekeeper deployment scenarios, see *Services Gatekeeper Multi-tier Installation Guide*.
- Using XML appliances to serve as firewalls in Services Gatekeeper deployment scenarios, see *Services Gatekeeper Multi-tier Installation Guide*.
- Channels, proxy servers, and firewalls, see *Oracle Fusion Middleware Configuring Server Environments for Oracle WebLogic Server*.

Virtual Environments Security

Review the security considerations associated with the following supported virtual environments:

- **Solaris Virtual Environment**

  Services Gatekeeper is deployable and certified on Solaris Zones virtualized environments. For information about securing the Oracle Solaris VM configuration, see *Oracle Enterprise Manager Ops Center User's Guide* on the Oracle Help Center website:

  https://docs.oracle.com/cd/E18440_01/doc.111/e18415/toc.htm

- **Oracle Virtual Machine (VM)**

  Oracle VM enables you to deploy operating systems and application software within a supported virtualization setup.

  For security considerations associated with Oracle VM, see *Oracle VM Security Guide* on the Oracle Help Center website:

  https://docs.oracle.com/cd/E27300_01/E27313/E27313.pdf

2

Performing a Secure Services Gatekeeper Installation

This chapter explains the steps necessary to install Oracle Communications Services Gatekeeper securely.

Pre-Installation Configuration

Before you install Services Gatekeeper, review the following security considerations:

- Ensuring Services Gatekeeper Performance and Security
- Configuring SSL
- Security Considerations Related to User Privileges

Ensuring Services Gatekeeper Performance and Security

To ensure optimal performance by Services Gatekeeper, tune the underlying WebLogic Server to the requirements of your environment. For example, select the appropriate startup mode for your installation.

For information about the default tuning values for WebLogic Server development and production modes, see *Oracle Fusion Middleware Performance and Tuning for Oracle WebLogic Server*.

Configuring SSL

Ensure that you configure the identity and trust store for WebLogic Server securely with SSL. See "Configuring Identity and Trust" in *Oracle Fusion Middleware Understanding Security for Oracle WebLogic Server*.

When you create the WebLogic Server domain for Services Gatekeeper, ensure that SSL ports are used for:

- The WebLogic Server domain for Services Gatekeeper.
- The cluster addresses if you install Services Gatekeeper in a cluster environment

For more information, see “Configuring SSL” in *Oracle Fusion Middleware Securing Oracle WebLogic Server*.

Security Considerations Related to User Privileges

Before you set up roles and user privileges, review the security considerations associated with security policies, users, GPRS, and security roles. Set up secure file system access permissions for the Oracle database.

See “Users, Groups, and Security Roles” in *Oracle Fusion Middleware Securing Resources Using Roles and Policies for Oracle WebLogic Server*.

Set up secure processes associated with the various types of user accounts that you create:

- **Services Gatekeeper Database User**

  After installing the Oracle database during the pre-installation process, you configure the Services Gatekeeper database user. The Services Gatekeeper database user account is configured with an unlimited quota and has privileges to create sessions and tables.

  Safeguard these credentials by recording and protecting them as you would any other administrative password. You reference them during domain configuration. For information, see “Creating the Database and a Database User” in *Services Gatekeeper Multi-tier Installation Guide* for details.

- **Administrator User**

  Every implementation must have a main administrator user. You create this user when you first configure a domain by entering the user name and password. Record and protect these credentials because the main administrator user has the power to grant or deny access for all other users. For information, see “Managing Management Users and User Groups” in *Services Gatekeeper System Administrator’s Guide*.

- **Management Users**

  Management users manage and administer Services Gatekeeper itself. Create as few management users as possible, protect their credentials, and have procedures in place that allow you to quickly remove management users as they are relieved of responsibility.

  For information, see “Managing Management Users and User Groups” in *Services Gatekeeper System Administrator’s Guide*.

- **Traffic Users**

  Traffic users are applications that use application-facing instances to send traffic.

Security Considerations Relating to Passwords

Set up a secure system to control the permissions for access to files and to your data. Use password encryption and store the files containing encrypted passwords in a secure location.

Establish a password policy that protects your system from possible intrusion. For information about:

- Managing security, see “Managing Security for Oracle Database Users” in *Oracle Database Security Guide*.
- Authentication security providers in WebLogic Server, see "Configuring Authentication Providers" in *Oracle Fusion Middleware Securing Oracle WebLogic Server*.

Installing Services Gatekeeper Securely

Follow the steps in *Services Gatekeeper Multi-tier Installation Guide* to install Services Gatekeeper. However, the port numbers, user name, password, and database SID should be changed from the default values.

You can perform a custom installation or a typical installation. Perform a custom installation to avoid installing options and products you do not need. If you perform a typical installation, remove or disable features that you do not need after the installation.

Configuring a Secure Domain for Services Gatekeeper

Your Services Gatekeeper domain is based on Oracle WebLogic Server. For information about:

- Possible domain configurations, see “Configuring the Services Gatekeeper Domain” in *Services Gatekeeper Multi-tier Installation Guide*.
- High availability considerations with respect to WebLogic Server, Oracle database access, and Oracle ASAOA suite, see *Oracle Fusion Middleware High Availability Guide*.
- Clustering, see “Clustering Best Practices” in *Oracle Fusion Middleware Using Clusters for Oracle WebLogic Server*.
- Setting security configuration options for the domain, see “Configuring Security for a WebLogic Domain” in *Oracle Fusion Middleware Securing Oracle WebLogic Server*.

Post-Installation Configuration

This section explains security-related tasks that you perform during and immediately after installing Services Gatekeeper, but before you put it into production.

- Securing Partner Relationship Management Portals
- Securing Web Services
- Adding Custom Password Validators
- Adding Custom Password Validators

Securing Partner Relationship Management Portals

Secure the Services Gatekeeper Partner Relationship Management portals by securing the administrative users. See "Administering Partners".

For more information, see “Security” in *Services Gatekeeper Portal Developer’s Guide*.

Securing Web Services

Web services security determines the level of protection that Services Gatekeeper requires for the web messages it sends and receives. The default level of security requires authentication tokens (user name and password) for all messages. The choices are:

- User name/password authentication (user name token)
- XML digital signatures (X.509 certificate token)
- Encryption (SSL or TLS SAML tokens)

You set the authentication level by web service by using the Services Gatekeeper Administration Console, and, if more security is required, by using WebLogic Server tools.

For information about securing web services and MBeans, see “About Services Gatekeeper Communication Security” in *Services Gatekeeper System Administrator’s Guide*.

Adding Custom Password Validators

A password validator is not required to run Services Gatekeeper. However, it does ensure that your partners and their subscribers adhere to a consistent level of password security. See "(Optional) Adding a Custom Password Validator" in *Services Gatekeeper Multi-tier Installation Guide* for information about adding custom password validators.

Installing Java Cryptography Extension (JCE)

Java Cryptography Extension (JCE) is not required for Services Gatekeeper to run. However, it does relieve web servers from the burden imposed by SSL security. See “(Optional) Adding Java Cryptography Extensions” in *Services Gatekeeper Multi-tier Installation Guide* for information about adding JCE.

3

Deploying Services Gatekeeper in a Demilitarized Zone

This chapter explains how to deploy Oracle Communications Services Gatekeeper in an unsecure environment. This chapter refers to this type of deployment as a *demilitarized zone* (DMZ) *deployment*.

Overview and Recommended Configurations

A Services Gatekeeper DMZ deployment should include multiple networks configured for access on separate networks cards. Access points on each host shield back-end systems such as administration servers and database servers from DMZ/Internet traffic. In particular, host Services Gatekeeper administration servers on a separate network to isolate administration traffic from application traffic.

If your Services Gatekeeper installation must be deployed in the DMZ, Oracle recommends that you use one of the multi-tier Services Gatekeeper implementations shown in Figure 3–1, Figure 3–2, or Figure 3–3 to protect its components. These implementations take advantage of these technologies that Services Gatekeeper uses to protect itself:

- A design that incorporates network layer access control so you can give individual Services Gatekeeper components the level of protection they require. This modular design enables you to restrict access to Services Gatekeeper from the Internet using firewalls, and restrict access within Services Gatekeeper using WebLogic connection filters.
- The ability to require Secure Socket Layer (SSL) communication between Services Gatekeeper components.
- Using operating system hardening to protect specific sensitive files and programs.

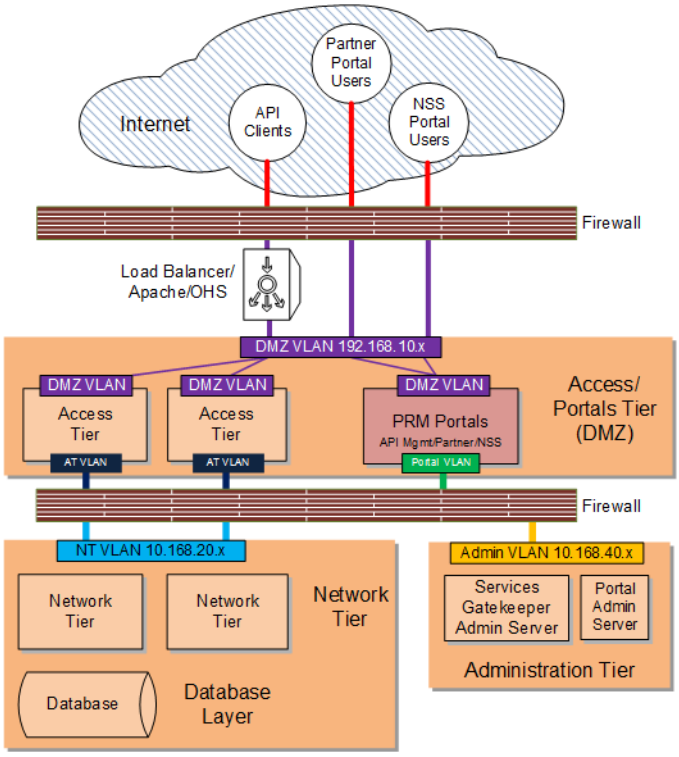
Note: Figure 3–1, Figure 3–2, and Figure 3–3 are only intended to show a high level overview of possible Gatekeeper networking configurations. For explicit routing details between Gatekeeper components, see the following sections:

- Securing Traffic Between the Internet and the Access Tier
- Securing Traffic Between the Access and Portal Tiers
- Securing Traffic between the Access Tier and the Network Tier
- Securing the Services Gatekeeper Administration Server
- Securing the Database

Figure 3–1 shows the most exposed Services Gatekeeper components, API clients and Partner Portal Users, outside firewall protection in the Internet, with the traffic being filtered by the firewall before being passed through to the access tier and the PRM portals. The Services Gatekeeper access and portal tiers are deployed in the DMZ behind a firewall as well as a suitable load balancing device. Suitable load balancing devices include the Apache Software Foundation HTTP web server using **mod_wl**, the F5 Networks 5 load balancer, or the Oracle HTTP Web Server using **mod_wl_ohs**. Oracle recommends that you obtain and install a component with proxy capability to limit traffic between the firewall and the Services Gatekeeper Access Tier/Portal Tier.

See "Securing Services Gatekeeper Components in the DMZ" for the list of tasks required to implement this deployment.

Figure 3–1 Services Gatekeeper DMZ Deployment



If your deployment requires an additional layer of protection, Figure 3–2 shows the administration server isolated in its own network behind the firewall.

See "Securing Services Gatekeeper Components in the DMZ" for the list of tasks required to implement this deployment.

Figure 3–1 shows the network tier behind both firewalls, and freely accessing the database through a JDBC connection. Figure 3–2 shows an additional layer of protection the database layer can be located behind its own firewall.

Figure 3–2 Services Gatekeeper DMZ Deployment with Isolated Administration Server

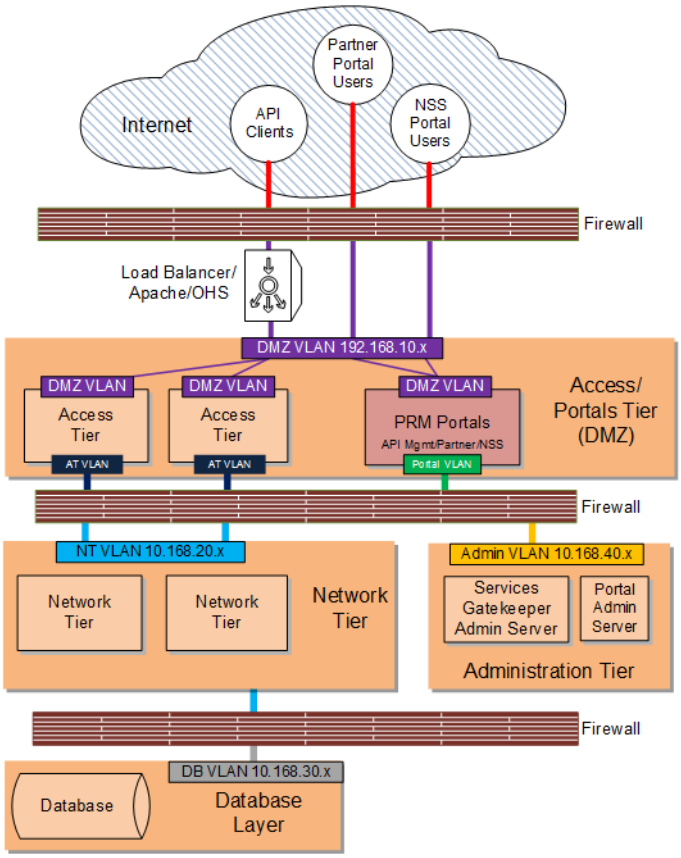
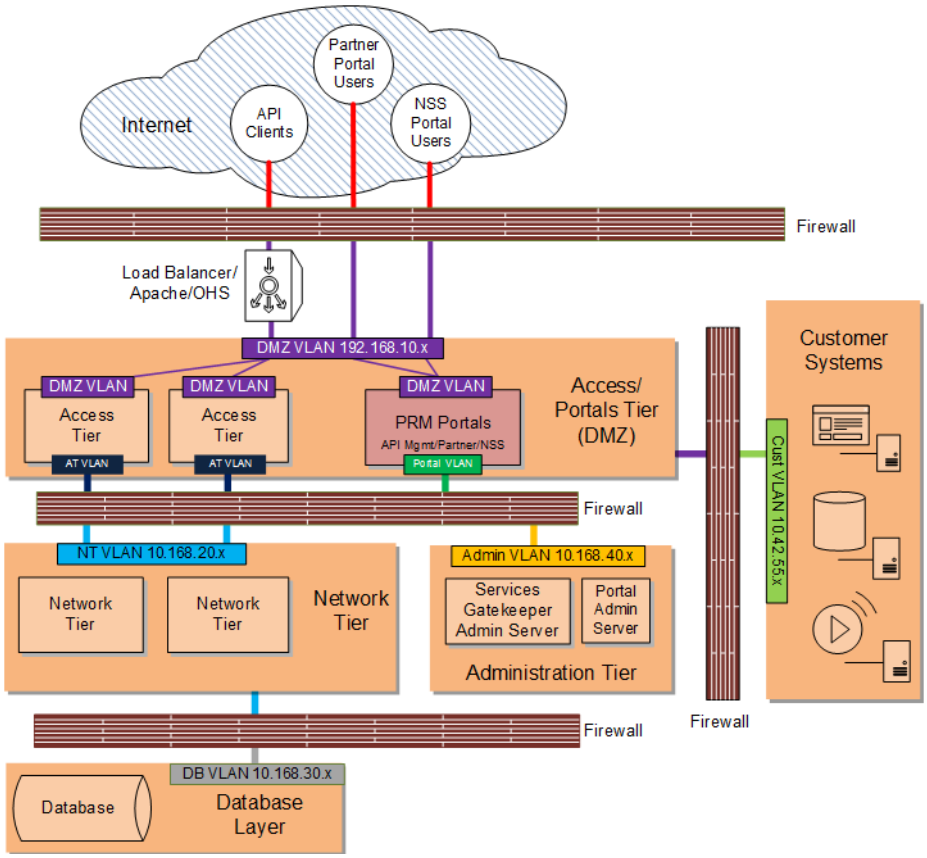


Figure 3–3 shows a Services Gatekeeper DMZ deployment with an isolated administration server, a fire-walled database layer, and an additional firewall separating customer systems such as database servers, media servers, and others. In this deployment, the customer systems are on a separate private sub net behind a firewall which can only connect to the Services Gatekeeper access tier. For an additional layer of protection, use a VPN tunnel as an access gateway to the customer systems as well (not pictured).

See "Securing Services Gatekeeper Components in the DMZ" for the list of tasks required to implement this deployment.

Figure 3–3 Services Gatekeeper Interfaced with Customer Systems



Securing Services Gatekeeper Components in the DMZ

This section includes instructions for configuring specific Services Gatekeeper components for a DMZ configuration:

Complete these tasks to implement a DMZ deployment as shown in Figure 3–1 and Figure 3–2:

- Securing Traffic Between the Internet and the Access Tier
- Securing Traffic Between the Access and Portal Tiers
- Securing Traffic between the Access Tier and the Network Tier
- Securing the Services Gatekeeper Administration Server
- Securing the Database

Complete all of the tasks in this section and add a firewall between your customer systems and the Services Gatekeeper to implement a DMZ deployment as shown in Figure 3–3.

Securing Traffic Between the Internet and the Access Tier

You secure traffic between the Internet and access tier by:

- Configuring servers in your access/portal tiers to use non-default ports as well as HTTPS, and certificates if required. See "Encrypting RMI Traffic Between the Access Tier and the Network Tier" for details.

- Hardening the underlying operating system components as explained in this section.

The following sections have details.

Encrypting RMI Traffic Between the Access Tier and the Network Tier

To encrypt RMI traffic between the access tier and the network tier for each server in each tier:

1. Open the Administration Console for your domain.
2. Click the **Lock & Edit** button.
3. Expand the **Environments** node in the Domain Structure pane and click the **Servers** node.
4. Click the **Configuration** tab in the Summary of Servers pane and click the name of the server in the Servers table that you want to configure.
5. Check **SSL Listen Port Enabled**.

> **Note:** Weblogic server uses the default JKS file store (Demo Identity and Demo Trust) for SSL configuration. However, you could specify a custom trust Keystore. See the *Oracle WebLogic Server 12c: Configuring Managed Servers* document for details.

6. Enter a numeric port number in the **SSL Listen Port** edit box.
7. Click **Save** to save your configuration changes.
8. Expand the **Environments** node in the Domain Structure pane if it is not already expanded and click **Clusters**.
9. Click the AT cluster and then click the **General** tab.
10. Replace the port in the **Cluster Address** edit box with the SSL port you configured in step 6.
11. Click the **Configuration** tab, then the **Replication** tab.
12. Check **Secure Replication Enabled**.
13. Repeat steps 9 through 12 for the remaining AT and NT servers.
14. Click **Save** to save your configuration changes.
15. Click **Activate Changes** to apply your changes to the engine servers.
16. To enable a secure channel for Java Message Service (JMS) add the **-Dweblogic.DefaultProtocol=t3s** flag to **JAVA_OPTIONS** in the *middleware_home*/**bin/setDomainEnv.sh** script:

```
JAVA_OPTIONS="${JAVA_OPTIONS} -Dweblogic.DefaultProtocol=t3s"
export JAVA_OPTIONS
```

17. Change the **ADMIN_URL** item in the *domain_home*/**bin/startManagedWeblogic.sh** script to **https://***IP_address*:*port_number*
18. Restart each AT and NT servers with this command:

```
startManagedManaged.sh server_name https://IP_address:port_number
```

> **Note:** Make sure you enable SSL on your administration server as well to ensure that SSL is used throughout the cluster. For more information, see "Securing Services Gatekeeper" in *Oracle Communications Services Gatekeeper System Administrator's Guide*.

Network traffic between the access tier and network tier is now encrypted.

> **Note:** Keep the following points in mind:
>
> - Services Gatekeeper multiplexes RMI and HTTP through the same port. If you set that port to require encryption, the browser either encrypts the traffic automatically, or returns an error if this is not possible.
> - While it is possible to have both SSL and non-SSL ports configured at the same time, it is recommended that you disable the non-SSL ports.
> - Once RMI encryption is enabled you can no longer use the Platform Test Environment (PTE) to manage Services Gatekeeper. You can, however, use the PTE to test APIs.

Hardening the Operating System

Keep these operating system level security considerations in mind:

- Confirm that the Services Gatekeeper binaries are owned by the Services Gatekeeper installation user.

  > **Note:** File permissions and ownership are set correctly by the Services Gatekeeper installer, but you should verify that they have not been modified before deployment.

- Lock down access to everything except:
  - Read/write access to the file system below the WebLogic domain directory
  - Access to the Java Virtual Machine (JVM)
  - Access to the RMI, and HTTP/HTTPS ports (the default SSL ports are 8002 for the access and network tiers, and 7002 for the administration tier).
- Periodically audit the operating system file system file to notify administrators of unauthorized system binary changes.

File system hardening and auditing procedures will differ depending upon your operating system. See the following sections for information on popular Services Gatekeeper options.

Hardening Oracle Linux 6

For detailed hardening instructions pertinent to Oracle Linux 6, see the following sections in the *Oracle Linux Security Guide*:

- *Pre-Installation Tasks* which includes information on physical security, BIOS passwords and other system level considerations.

- *Installing Oracle Linux* which includes information on configuring shadow passwords and hashing, disk partition encryption, software selection and network time services.
- *Implementing Oracle Linux Security* which includes information on topics including:
  - *Configuring and Using Data Encryption*
  - *Configuring and Using Access Control Lists*
  - *Configuring and Using SELinux*
  - *Configuring and Using Auditing*
  - *Configuring and Using System Logging*
  - *Configuring and Using Process Accounting*
  - *Configuring Access to Network Services*
  - *Configuring and Using Chroot Jails*

Hardening Oracle Solaris 11

For detailed hardening instructions pertinent to Oracle Solaris 11, see the following sections in the *Oracle Solaris 11 Security Guidelines*:

- *Securing the System*
- *Securing Users*
- *Securing the Kernel*
- *Configuring the Network*
- *Protecting File Systems and Files*
- *Securing Applications and Services*

Securing Traffic Between the Access and Portal Tiers

You secure the Access and Portal tiers by configuring a firewall between the Internet and the Access and Portal Tiers. See "Configuring a Firewall to Protect the Access and Portal Tiers" for details. The API and Partner Management Portal is not connected to the public Internet, so you do not need to configure traffic through the Internet load balancer/firewall for it. Configuring this firewall protects the Partner Portal and Network Service Supplier Portal traffic.

Configuring a Firewall to Protect the Access and Portal Tiers

Configure a firewall as explained in the example in Table 3–1. This example uses the sample components and IP addresses/ports shown in Figure 3–2. Yours will be different.

Table 3–1 Configuring a Firewall Between the Internet and the Access/Portals Tiers

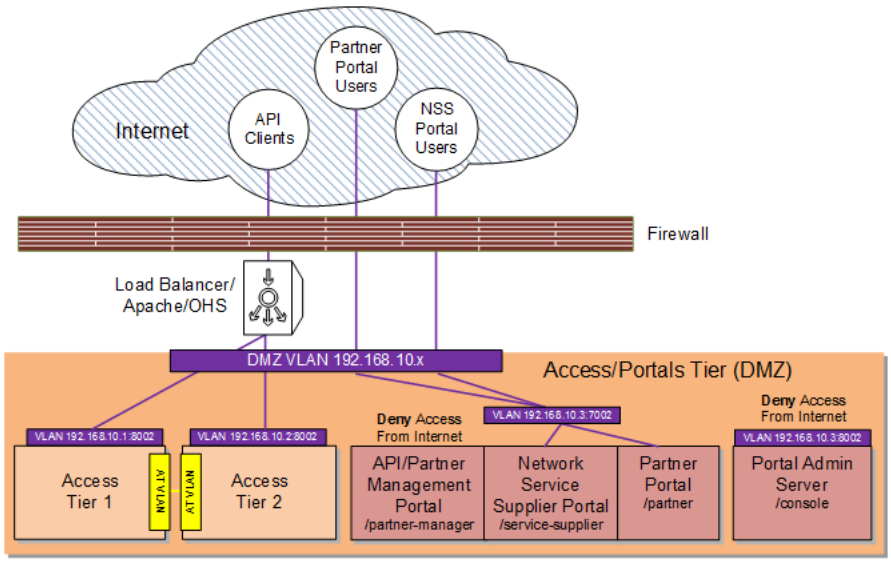
Specifically Allow Traffic From:	To The Component/IP Address:Port	Notes
API Clients	AT1 (192.168.10.1:8002)	Allow Internet API call traffic to the Access Tier.
API Clients	AT2 (192.168.10.2:8002)	Allow Internet API call traffic to the Access Tier.
Portal Admin Server	N/A	*Disallow* Internet traffic to the Portal Admin Server (**https://192.168.10.3:8002/console**).

Table 3–1 (Cont.) Configuring a Firewall Between the Internet and the Access/Portals Tiers

Specifically Allow Traffic From:	To The Component/IP Address:Port	Notes
API/Partner Management Portal	N/A	*Disallow* Internet traffic to the API/Partner Management Portal (**https://192.168.10.3:7002/partner-manager**).
Partner Portal Users	PRM Portals/Portal Administration Server (192.168.10.3:8002)	Allow Internet traffic to the Partner Portal **(https://192.168.10.3:8002/partner).**
Network Service Supplier Portal Users	PRM Portals/Portal Administration Server (192.168.10.3:8002)	Allow Internet traffic to the Network Service Supplier Portal (**https://192.168.10.3:8002/service-supplier**).

Figure 3–4 illustrates the configuration in Table 3–1.

Figure 3–4 Firewall Configuration: Internet to Access Tier/Portals



Securing Traffic between the Access Tier and the Network Tier

To secure traffic between the access tier and the network tier:

- Obtain and configure a firewall between the access tier and network tier so that it allows only:
  - RMI traffic between the ATs and NTs (you control the NT using RMI)
  - (As Needed) JMS traffic between the ATs and NTs (for creating and communicating EDRs)
  - HTTP/HTTPS traffic from the Partner Portal

  See Table 3–2 for an example based the example components shown in Figure 3–2, and your firewall documentation for installation and configuration instructions.
- Specifying that traffic between the NTs and ATs in your implementation required SSL communication. You did by following the instructions in "Encrypting RMI Traffic Between the Access Tier and the Network Tier".

Configuring a Firewall Between the ATs/Portals and the NTs

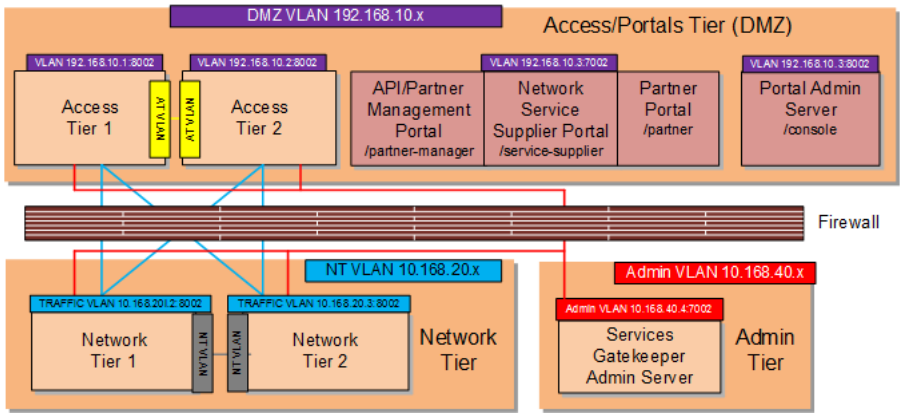
This example uses the sample components and IP addresses/ports shown in Figure 3–2. Yours will be different.

Table 3–2 Configuring a Firewall Between the Internet and the Access/Portals Tiers

Specifically Allow Traffic From:	To The Component/IP Address:Port
Access Tier1	Network Tier1 (10.168.20.2:8002)
Access Tier1	Network Tier2 (10.168.20.3:8002)
Access Tier2	Network Tier1 (10.168.20.2:8002)
Access Tier2	Network Tier2 (10.168.20.3:8002)
Access Tier1	Services Gatekeeper Administration Server (10.168.40.4:7002)
Access Tier2	Services Gatekeeper Administration Server (10.168.40.4:7002)
Network Tier1	Services Gatekeeper Administration Server (10.168.40.4:7002)
Network Tier2	Services Gatekeeper Administration Server (10.168.40.4:7002)

Figure 3–5 illustrates the configuration in Table 3–3.

Figure 3–5 Firewall Configuration: Access Tier to Network Tier



Securing the Services Gatekeeper Administration Server

Securing the administration server involves these tasks:

- Configuring the Services Gatekeeper administration server to use a nonstandard port so that you can use customized firewall rules as well as encryption (HTTPS, IIOPS, or T3S)
- Changing the administration server context path from the default of **/console** to something else. For example: **/adminportal**.
- Configuring Services Gatekeeper to only allow SSL traffic to the administration server. See "Restricting Administration Server to SSL" for details.

Restricting Administration Server to SSL

To configure administration server to only allow SSL:

1. Open the Administration Console for your domain.
2. Click **Lock & Edit**.

3. Expand the **Environments** node in the **Domain Structure** pane and click the **Servers** node.
4. Click **AdminServer(Admin)**.
5. Click **Configuration** in the **Summary of Servers** pane and click the name of the server in the Servers table to configure.
6. Click **General**.
7. Check **SSL Listen Port Enabled**.

> **Note:** Weblogic server uses the default JKS file store (Demo Identity and Demo Trust) for SSL configuration. However, you should specify a custom trust Keystore. See the *Oracle WebLogic Server 12c: Configuring Managed Servers* document for details.

8. Enter a numeric port number in the **SSL Listen Port** edit box.
9. Uncheck the **Listen Port Enabled** box.
10. Click **Save**.
11. Click **Activate Changes** to apply your changes to the engine servers.

Securing the Database

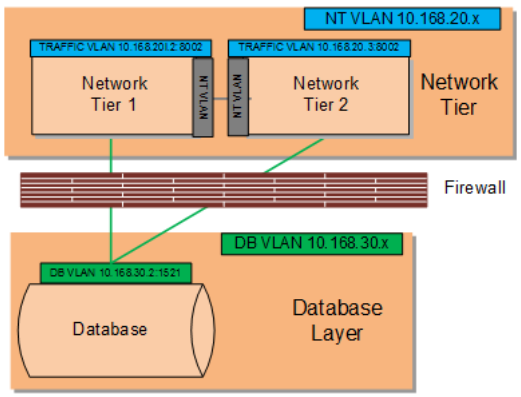
Configure a database between your Network Tier/Administration Server. See your firewall documentation for details. Table 3–3 has example instructions based on the sample components and their IP *addresses:ports* shown in Figure 3–2. Your components and IP addresses will be different.

Table 3–3 Configuring a Firewall Between NTs and the Database

Specifically Allow Traffic From:	To The Component/IP Address:Port
Network Tier1	Database (10.168.30.2:1521)
Network Tier2	Database (10.168.30.2:1521)

Figure 3–6 illustrates the configuration in Table 3–3.

Figure 3–6 Firewall Configuration: Network Tier to Database Layer



Securing OBIEE in Services Gatekeeper

Services Gatekeeper uses Oracle Business Intelligence Enterprise Edition (OBIEE) to generate statistics and to create reports about API usage. The OBIEE components deployed in Services Gatekeeper are located in the network tier and are subject to the same protections from firewalls and operating system hardening.

Partner statistics and reports are protected by username/passwords, so partners only have access to their own statistics and reports.

For general information on securing OBIEE, see *Fusion Middleware Security Guide for Oracle Business Intelligence Enterprise Edition* at the Oracle documentation website:

http://docs.oracle.com/cd/E14571_01/bi.1111/e10543/toc.htm

Securing Node Manager Access to Services Gatekeeper

You can control Services Gatekeeper by using Oracle WebLogic Node Manager (Node Manager) features. Node Manager relies on a one-way SSL connection for security. See "Configuring Java-based Node Manager Security" and "Using SSL with Java-Based Node Manager" in *Fusion Middleware Node Manager Administrator's Guide for Oracle WebLogic Server 12c* for details.

Configuring Connection Filters Instead of a Firewalls

In cases where Services Gatekeeper components are not separated by firewalls, for instance between the network tier and the database layer, you can use WebLogic connection filters to provide network layer access control and block unwanted intrusions.

To configure a WebLogic connection filter:

1. Set your Services Gatekeeper environment:

   ```
   cd ~/domain_home/bin
   . ./setDomainEnv.sh
   ```

   where *domain_home* is the path to the domain's home directory.

2. Start WLST:

   ```
   java weblogic.WLST
   ```

3. Connect to the server using the *username* and *password* you configured during installation:

   ```
   connect('username','password','t3://myserver:port_number')
   ```

4. Switch to the domain security MBean:

   ```
   cd('/SecurityConfiguration/'+domainName)
   ```

5. Enable a connection filter:

   ```
   cmo.setConnectionLoggerEnabled(true)
   ```

6. Define the connection filter implementation:

   ```
   cmo.setConnectionFilter('weblogic.security.net.ConnectionFilterImpl')
   ```

Note: The example above uses the default connection filter implementation. For information on creating custom connection filters see "Developing Custom Filters" in *Fusion Middleware Programming Security for Oracle WebLogic Server*.

7. Configure the rules as a string array:

```
set('ConnectionFilterRules',jarray.array
([String('myserver ip_address port allow t3s https'),
String('ip_address/subnet_mask ip_address port allow'),
String('ip_address ip_address port deny t3 http')],
String))
```

4

Implementing Services Gatekeeper Security

This chapter explains the tasks required to implement Oracle Communications Services Gatekeeper securely.

Securing Communication Services

The communication services that your partners provide generally require both authentication and authorization services to remain secure. You can provide this security in several ways:

- The Services Gatekeeper security provider authenticates subscribers by verifying their application's IDs and passwords.
- The Services Gatekeeper service-level agreements (SLAs) provide authorization. You secure communication services by authorizing service requests with SLAs, and by authenticating users making the requests with web services security. This is true for services created by you or your partners. SLAs can define the API and TPS that the application can use. For more information, see:
  - Authenticating Service User Requests for Communication Services
  - Authorizing Access to Services with SLAs
- OAuth provides both authorization and SSO authentication for third-party resources. See "Authenticating and Authorizing Resources with OAuth" for more information.

Authorizing Access to Services with Single Sign-On

You can use Security Assertion Markup Language (SAML) credentials to gain access to resources protected by OAuth 2.0 in Services Gatekeeper. Services. This enables you to create single sign on (SSO) features that provide your subscribers with one authorized SAML token (federated identity) for use in accessing multiple third-party resources. See “Support for SAML Assertions” in *Services Gatekeeper OAuth Guide*.

Authenticating Service User Requests for Communication Services

Communication services do not have security enabled by default because Services Gatekeeper has no way of knowing what kind of security they allow. Ensure that you add or take advantage of the communication service’s security measures before allowing subscribers to use them.

Services Gatekeeper supports these types of communication services:

- SOAP-based

- RESTful
- Native

For information about securing these communication services, see "About Services Gatekeeper Communication Security" in *Services Gatekeeper System Administrator's Guide*.

Securing SOAP-Based Communication Services

The first step in protecting your SOAP communication services is to ensure that all communication with Services Gatekeeper happens within a session. You set this in the Services Gatekeeper Session Manager Web Service, and it automatically requires applications to provide authorization.

Applications communicating with Services Gatekeeper that use a SOAP interface have these options for authentication:

- User name/password authentication (user name token)
- Digital signatures (X.509 certificate token)
- Encryption (SAML token)
- Session IDs

For information about creating and securing a SOAP-based communication service, see the following in *Services Gatekeeper Application Developer's Guide*:

- About Creating Applications that Interact with Services Gatekeeper
- Managing Communication Sessions

Securing RESTful Communication Services

The RESTful service interfaces use HTTP basic authentication and session IDs for security.

For information about:

- Implementing HTTP security, see "About Services Gatekeeper Communication Security" in *Services Gatekeeper System Administrator's Guide*.
- Creating and securing RESTful communication services, see "Using the RESTful Interfaces" in *Services Gatekeeper Application Developer's Guide*.
- Requiring sessions for all RESTful communication, see "Managing Communication Sessions" in *Services Gatekeeper Application Developer's Guide*.

Securing Native Communication Services

Services Gatekeeper supports communication services using the MM7, SMPP, and UCP protocols. The following shows security considerations for each protocol:

- **Native MM7 Communication Services**

  Services Gatekeeper uses HTTP basic authentication to secure native MM7 communication services. For more information, see "Native MM7" in *Services Gatekeeper Communication Service Reference Guide*.

- **Native SMPP Communication Services**

  Services Gatekeeper uses authentication credentials to secure native SMPP communication services. For information about creating a native SMPP communications service, see "Native SMPP" in *Services Gatekeeper Communication Service Reference Guide*.

- **Native UCP Communication Services**

  Services Gatekeeper uses a credential store to secure native UCP communication services. For information about configuring connection information and the credential map, see "Managing and Configuring Native UCP Connections" in *Services Gatekeeper System Administrator's Guide*.

Authorizing Access to Services with SLAs

Your partners create Service Level Agreements (SLAs) to define who is authorized to use their services. Every communication service must have an SLA that specifies access privileges to Services Gatekeeper and the network nodes it communicates with.

For more information, see *Services Gatekeeper Portal Developer's Guide*.

Authenticating and Authorizing Resources with OAuth

OAuth provides both authorization and authentication services and replaces more traditional SSO mechanisms. For information about using the OAuth protocol to grant access to resources (such as photos, video, and so on) without compromising the resource owner's security, see:

- *Services Gatekeeper OAuth Guide*
- *Services Gatekeeper System Administrator's Guide*

Monitoring Your Services Gatekeeper Implementation

Services Gatekeeper includes tools that monitor the number of transactions that Services Gatekeeper is processing. You use these tools to calculate usage and group reports, but they can also be valuable tools for alerting you of denial of service (DOS) attacks. For more information, see "Managing and Configuring Statistics and Transaction Licenses" in *Services Gatekeeper System Administrator's Guide*.

Services Gatekeeper provides a mechanism that alerts you to impending system overload using the Oracle WebLogic Overload Alarms feature.

Backing Up and Restoring Services Gatekeeper Configuration Data

Regular backups are an essential part of a secure Services Gatekeeper implementation. You must configure secure ways to handle the following:

- Redundancy and failover for clustered services
- Automatic restart for managed servers
- Managed server independence mode
- Automatic migration of failed managed servers
- Backing up the domain configuration
- Restarting a failed administration server
- Restarting failed access and network tier servers
- Moving an access or network tier server to a different system.

For more information, see "Managing, Backing Up, and Restoring Services Gatekeeper" in *Services Gatekeeper System Administrator's Guide*.

Security Considerations for Services Gatekeeper System Administrators

If you are the system administrator for Services Gatekeeper, consider the security associated with configuring and managing the following:

- Filtering Tunneled Parameters
- Securing SOAP-Based Web Services with Web Services Security (WS-Security)
- Securing RESTful Web Services with SSL
- Securing Network-Facing Servers With Keystores
- Securing the Oracle Access Manager MBeans

For more information, see "Securing Services Gatekeeper" in *Services Gatekeeper System Administrator's Guide*.

Securing Communication with Service Interceptors

Configuring tunneling for a communication service can serve as a "white list" or "black list" that filters parameters. A while list limits communication service messages to only the parameters that you specify (nothing is limited by default). A black list is a list of just the prohibited messages. White lists especially can be quite restrictive and impractical for most communication, but may fit into your security needs. For information about implementing tunneling, see "Using Parameter Tunneling" in *Services Gatekeeper Extension Developer's Guide*.

Administering Partners

Your partners use the Partner Manager Portal application to add their services to Services Gatekeeper and to include the network service interfaces created by their network service suppliers. Network service suppliers use the Network Service Supplier application to create the network services interfaces. Partner managers publish or expose these services as APIs. Your partners use the Partner Portal application to create applications with these APIs.

All three roles require secure access control. When partners and network service suppliers log in, the application asks them security questions to obtain the access privilege and authentication with secure passwords. For example, partners are assigned one of the service provider interfaces created for them. These interfaces are administrative user types and must be managed like other administrative users and only granted the access privileges they require.

Configure the required security setup to monitor the accounts being created to ensure that they are legitimate and allowed access to the Partner Portal, Network Services Supplier, and Partner Manager Portal applications. Ensure that the granting, monitoring, and revoking service access is a secure process and takes into account whether the users are internal or external to your organization. For more information, see "Service Provider Interfaces" in *Services Gatekeeper Portal Developer's Guide*.

Setting Up the Partner Relationship Management Portals

Your service providers use Partner Portal to administer their partner accounts, including granting and revoking service access. The service providers may be internal or external to your organization. Set up Partner Portal and Partner Manager Portal with the security appropriate for your implementation.

Make sure you educate your service providers to:

- Enable security for communication services.
- Use the secure interfaces supplied with Services Gatekeeper to communicate with Services Gatekeeper.
- Use OAuth to manage access to secured resources (such as pictures or secured URLs).
- Record their Partner Portal credentials somewhere safe.
- Change their automatically generated application IDs as soon as possible because they are predictable.

For more information, see *Services Gatekeeper Portal Developer's Guide*.

5

Security Considerations for Developers

This chapter provides information for developers about how to secure applications for Oracle Communications Services Gatekeeper.

Securing Applications Against Malicious Traffic

Your network implementation can be vulnerable to denial of service (DOS) attacks, which generally try to interfere with legitimate communication inside the Services Gatekeeper Access Tier. To prevent these messages from reaching your network, Services Gatekeeper offers configurable SOAP and RESTful message filtering. You configure this filtering behavior by using the **ApiFirewall** configuration MBean. **ApiFirewall** determines how Services Gatekeeper filters messages attempting to enter the Services Gatekeeper application tier.

Table 5–1 lists network attacks that Services Gatekeeper protects against, and lists where you can find information about configuring those protections.

Table 5–1 Message-Based Attacks and How to Protect Against Them

Attack Strategy	Protection Strategy	Default Result
Malicious Content Attack, including: SOAP message attacks: ■ Oversize payloads. ■ Oversize element, attribute, comment, or namespace. ■ Oversize attributes per element. ■ Messages with an inordinately large number of nested elements. ■ Oversize processing instructions, comments, CDATA items, or attribute values. RESTful message attacks: ■ Oversize message layouts. ■ Oversize JSON or element values. ■ Oversize JSON array elements. ■ Messages with an inordinately large number of nested elements.	The **ApiFirewall** MBean settings (application tier) limit the acceptance of oversize message entities. See the "All Classes" section of *Services Gatekeeper OAM Java API Reference* for details.	Rejects the message and returns the error message specified with the **ErrorStatus** attribute of **ApiFirewallMBean**.
Continuous wrong password attack.	The default WebLogic Security Provider setting (application tier) locks a subscriber out for 30 minutes after 5 wrong password attempts. This behavior is configurable. See the section on protecting user accounts in *Administering Security for Oracle WebLogic Server* for more information.	Rejects the message and returns a **500 Internal Server Error** message.
Malformed SOAP Message (does not match the SOAP schema), including: ■ Messages that deliberately do not match the schema. ■ Messages that include a custom entity extension (XML bomb) or circular reference. ■ Messages that include a recursive entity expansion. ■ Messages that attempt to change the DTD definition.	You can direct the WebLogic SOAP message processor (application tier) to validate the SOAP schema and reject malformed messages. See "Validating the XML Schema" in *Oracle Fusion Middleware Getting Started with JAX-WS Web Services for Oracle Weblogic Server* for more information. Also, the WebLogic Server SOAP engine ignores any attempt to change the DTD definition in a SOAP message.	Rejects the message and returns a **500 Internal Server Error** message.
Malformed RESTful messages (do not match the REST schema).	The Jersey parsing engine (network tier) rejects these types of messages.	Rejects the message and returns a **500 Internal Server Error** message.
External Entity Reference	The Services Gatekeeper **ApiFirewall** (application tier) prohibits any references to external entities. This behavior is not configurable.	Rejects the message and returns a **500 Internal Server Error** message.

Configuring Network Traffic Security

You configure network security traffic by performing the following general tasks:

- Deciding which error message to return when a SOAP or REST message is rejected. The default error message is **400 Bad Request**, which is the most descriptive. You set the error message by using the **getErrorStatus** attribute of **ApiFirewallMBean**. See the "All Classes" section of *Services Gatekeeper OAM Java API Reference* for details.
- Setting the maximum limits for error messages, including:
  - The maximum total size of a single message entity, such as a comment, by using the **MaxItemValueLength** attribute of **ApiFirewallMBean**.
  - The maximum total size of an error message by using the **getMaxMessageSize** attribute of **ApiFirewallMBean**.
  - The maximum number of nested message elements by using the **getMaxChildElementDepth** attribute of **ApiFirewallMBean**.
  - The maximum number of unbounded elements by using the **getMaxUnboundedItems** attribute of **ApiFirewallMBean**.
- (Optional) Creating a list of trusted APIs. Most of the **ApiFirewall** MBean security attributes filter messages that are potential security risks. This filtering process degrades performance slightly. To avoid this performance penalty, create a list of trusted APIs that are exempt from the filtering process by using the **setApiConfigXml** attribute of **ApiFirewallMBean**.

For a description of the attributes and operations of the **ApiFirewallMBean** MBean, see the "All Classes" section of *Services Gatekeeper OAM Java API Reference*.