

Firewall and Virtual Private Network Communication for Oracle Enterprise Manager 9.2.0.1.0

Firewalls protect a company's IT infrastructure by providing the ability to restrict network traffic by examining each network packet and determining the appropriate course of action. Firewall configuration typically involves restricting the ports that are available to one side of the firewall; for example, a company will commonly place a firewall to protect their business systems from being accessed from the Internet. It can also be set up to restrict the type of traffic that can pass through a particular port such as HTTP. If a client attempts to connect to a restricted port (a port not covered by a security 'rule') or uses a protocol that is incorrect, then the client will be disconnected immediately by the firewall. Firewalls can also be used within a company Intranet to restrict user access to specific servers.

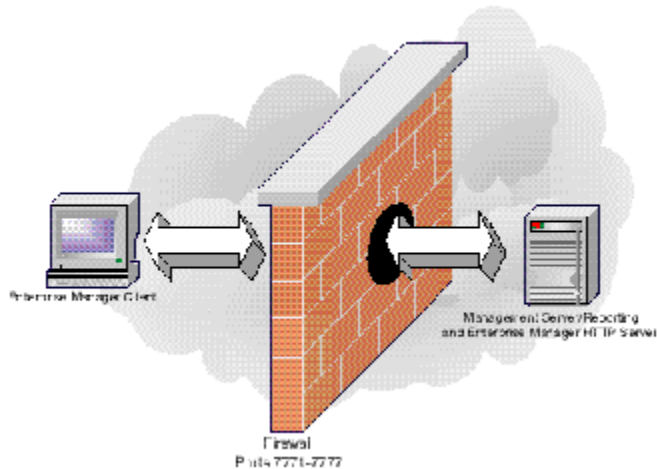
The various components of Enterprise Manager 9i (Console, Oracle Management Server, and Intelligent Agents) can be deployed on different nodes, which in turn can be separated by firewalls. This paper describes how firewalls and Virtual Private Networks (VPN) can be configured to allow communication between the different components of Enterprise Manager. The most common deployments are covered:

- [Firewall Between the Console and Management Server](#)
- [Firewall Between the Management Server and Agent\(s\) on Monitored Nodes](#)
- [Firewall Between the Management Server and the SMTP Mail Server](#)
- [Firewalls and Network Address Translation \(NAT\)](#)
- [Virtual Private Network Configuration for Enterprise Manager](#)
- [VPN Connections Between the Enterprise Manager Client and Management Server](#)
- [VPN Connections Between the Management Server and Intelligent Agents](#)
- [Running the Console in Standalone Mode](#)
- [Performance Manager, Capacity Planner, and Firewalls](#)

Firewall Between the Console and Management Server

In this configuration, the Enterprise Manager Console and Management Server are separated by a firewall.

Console and Management Server on Opposite Sides of a Firewall



To enable network communication between the Enterprise Manager Console and Management Server, several network ports must be opened in the firewall to allow TCP traffic. The port range of 7771-7777 covers all these. If the Console is running in a browser, then the firewall needs to allow HTTP traffic over port 3339 from the Enterprise Manager Website HTTP server to any browser client. Functional assignments for these ports are shown in the following table.

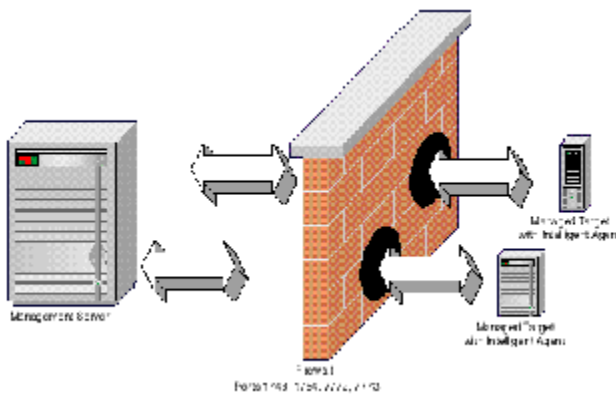
Port Usage	
Port Number	Usage
3339	Communication between the Enterprise Manger HTTP server and the Enterprise Manager client.
7771, 7773, 7776	Communication between the Enterprise Manager Console and the Management Server.
7774	Communication between the Oracle Applications Manager and the Management Server.
7775, 7777	Communication between the paging server and the Management Server.

Special configuration is not required for either the Console or the Management Server in this case.

Firewall Between the Management Server and Agent(s) on Monitored Nodes

In this configuration, the Intelligent Agent that runs on the managed node and the Management Server are on opposite sides of the firewall, as shown in the following illustration.

Firewall Between the Management Server and Agent



To enable network communication between the Management Server and Intelligent Agents on managed targets, several network ports must be opened in the firewall to allow TCP traffic. Functional assignments for these ports are shown in the following table.

Port Usage	
Port Number	Usage
1748, 1754	Management Server communicating with the Agent to discover new targets.
7772	Agent communicating with the Management Server.
7773	Agent communicating with the Management Server via SSL.

No special setup and configuration is required for the Management Server or Intelligent Agents in this situation.

If the Management Server and administered database (or other managed target) are separated by a firewall, then the Management Server acts as a proxy for the Enterprise Manager Console, resulting in the remote database viewing the Management Server as the client. For this reason, there must be a SQL*Net proxy between the Management Server and the administered database. If the Console is launched in Standalone Mode, there must be a SQL*Net proxy between the Console and the Management Server, and between the Management Server and ALL collections services (Data Gatherer) connections.

Firewall Between the Management Server and SMTP Mail Server

If a firewall exists between the Management server and SMTP Mail server, one-way communication is possible via TCP from the Management Server to the SMTP Mail Server using Port 25.

Port Usage	
Port Number	Usage
25	Management Server communicating one-way to the SMTP Mail Server

Firewalls and Network Address Translation (NAT)

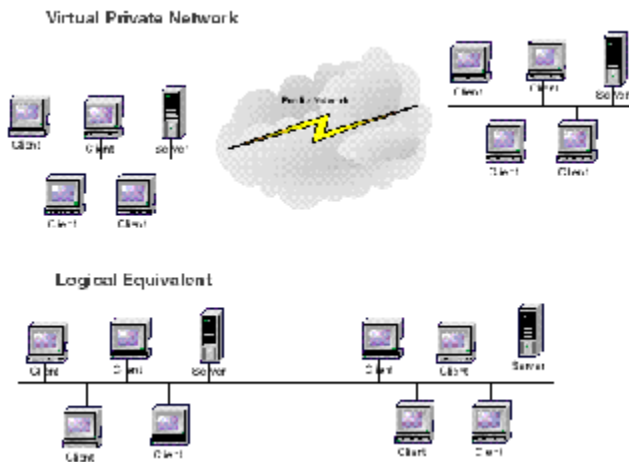
Some firewalls use a feature called Network Address Translation (NAT). This feature masks the true IP address of a client by translating it to a different IP address. The server will know packets sent from a remote client to a server through the firewall by this translated address. As the client and server communicate, the NAT software handles the mapping of the true IP address to its translated address. Of the two Enterprise Manager configurations previously discussed, only an Enterprise Manager Console and Management Server can be separated by firewalls using NAT. No changes are required for Enterprise Manager to support NAT in this configuration.

The Management Server and Intelligent Agent cannot be separated by firewalls using NAT because the Management Server and Agent communication includes the other's host address information, which is stored in the data packet rather than in the IP header. Since NAT only looks for (and translates) addresses in the IP header, NAT will not work with Management Server/Agent communication.

Virtual Private Network Configuration for Enterprise Manager

Virtual Private Networks (VPNs) allow remote employees to connect in a secure fashion to a corporate server located in the corporate Local Area Network (LAN) using the routing infrastructure provided by a public network (such as the Internet). From the user's perspective, the VPN is a point-to-point connection between the user's computer and a corporate server. The nature of the intermediate network is irrelevant to the user because it appears as if the data is being sent over a dedicated private link.

Virtual Private Network



In order to provide a secure point-to-point channel of communication, VPN software includes services such as user authentication and data encryption. It also implements security standards defined by the IP Security (IPSEC) protocol. IPSEC is a series of guidelines for the protection of Internet Protocol (IP) communications. It specifies standardized ways for securing private information transmitted over public networks. Communication between security systems developed by different vendors is possible if they comply with the IPSEC standards.

To create secure VPNs, VPN software typically operates in IPSEC Tunnel Mode. In this mode, data sent from a client is first encrypted and then encapsulated before being transmitted over an insecure, public network such as the Internet. Upon arriving at its destination, VPN software unpacks, decrypts and authenticates the data received, then forwards it on to its final destination.

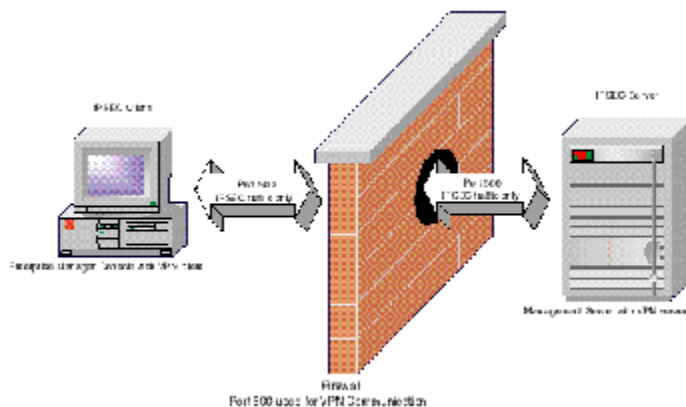
Many e-businesses use both VPNs and firewalls as part of their security infrastructure. In these configurations, the firewall must allow IPSEC-compliant traffic to pass through (port 500 is used by default). Application data that is sent via VPN is first encapsulated and tunnelled through port 500 in the firewall, unpacked, and sent to its final destination.

Targets that have been set up to use VPN thus avoid having to open up additional ports in the firewall. Applications that run on VPN-enabled nodes can also communicate safely and securely across the firewall.

VPN Connections Between the Enterprise Manager Client and Management Server

As previously discussed, VPNs that comply with IPSEC standards allow the secure transfer of information over the internet: Remote clients can connect to a secure server with minimum configuration and maximum security. It is also possible to use VPNs in conjunction with firewalls. The following example shows a VPN environment with the Enterprise Manager Console and the Management Server on opposite sides of the firewall.

Firewall Configuration In a VPN Environment



In this example, both the Console and Management Server machines have VPN software configured to provide a secure communication channel between the two. Specifically, the machine running Enterprise Manager client must have the VPN client software installed. The machine running the Management Server must have the VPN gateway software installed. Additionally, the firewall must be configured to allow only IPSEC traffic (IPSEC by default uses port 500). In this configuration, all the network traffic between the Console and the Management Server will be tunneled automatically through port 500 by the VPN software.

No additional configuration is required for Enterprise Manager components since the VPN software handles communication tasks automatically.

When the Enterprise Manager Console is launched, the user may be prompted by a VPN client software dialog to enter user security information. Once a valid username and password are provided to the VPN client, subsequent communication between the Console and Management Server across the virtual network will appear seamless.

No additional changes are required for the firewall configuration if IPSEC traffic is already allowed.

VPN Connections Between the Management Server and Intelligent Agents

Some VPN providers may allow server processes on different nodes to communicate. In these configurations, it is possible to deploy the Management Server on one VPN-enabled node and the Agent on another VPN-enabled node. The same principles as described in the previous section apply. It is important to note that communication between the Management Server node and Agent node is bi-directional, so each would need to function as both a VPN client and VPN server. Hence, both the VPN client and server software must be installed on each node.

NOTE: Sun Solaris version 8 supports VPN server process communication. Refer to the Solaris System Administrator's Guide for more details.

Running the Console in Standalone Mode

If the Enterprise Manager Console is launched in Standalone mode, the Console connects directly to a managed target (e.g. database) in the traditional client-server mode, using SQL*Net to communicate. If a firewall separates the Console and its target, several options are available. These include using VPN software on the Enterprise Manager Console node and target node, and using Oracle Net features that support firewall configurations. These options are described below.

Use VPN software on the Enterprise Manager Console node and target node

In this case, the setup will be similar to the Console - Management Server using VPN setup as described in the previous section.

Use Oracle Net features that support firewall configurations. These include:

Oracle Net Firewall Proxy

Several firewall vendors (e.g. CheckPoint) include an Oracle Net proxy capability which allows SQL*Net traffic to pass through its firewalls. This functionality is primarily available from the firewall vendors.

Oracle Net's Connection Manager

Oracle Net's Connection Manager provides database connection pooling capabilities. Client applications connect to Connection Manager which in turn redirects the connection to the database. In this case, firewalls need to allow connections from the client to Connection Manager.

Refer to the Oracle Net documentation for more details.

Performance Manager, Capacity Planner, and Firewalls

The Performance Manager or Capacity Planner applications can be launched separately in order to connect directly to the Intelligent Agent (which incorporates the data collection services) on a target node. If a firewall separates Performance Manager and the Agent, or Capacity Planner and the Agent, then the firewall needs to be configured as follows:

- Port 1808 over TCP: Used for communication between Performance Manager and Agent; or Capacity Planner and the Agent.
- Port 1809 over TCP: Used for communication between the Performance Manager and the Agent over SSL or for Capacity Planner and the Agent over SSL

No additional configuration is required for Performance Manager, Capacity Planner or the Intelligent Agent.