Transparent Management Proxy Service using ZoneRanger's Gateway Virtual Interface

Jim Doble, CISSP
Tavve Software Co.

Tavve Software Co.
One Copley Plaza
Suite 480
Morrisville, NC 27560
+1 919-460-1789
http://www.tavve.com

Transparent Management Proxy Service using ZoneRanger’s Gateway Virtual Interface

Executive Summary

Network partitioning via firewalls is a well-established strategy for improving security. A common embodiment of this strategy is the use of DMZ’s to create a degree of separation between network and computing assets that are exposed to external network traffic and the company’s internal network. The proliferation of DMZ’s has created a problem for network managers who need to manage DMZ devices using their existing network management applications, because essential management protocols such as ICMP, SNMP, SSH, or HTTPS may be blocked by the firewall. The same problem applies to systems management, security management, and configuration management applications that also depend on these protocols.

Some management application vendors have addressed this problem by providing remote probes or agents that can be deployed within the DMZ. However, these probes or agents are typically limited to a single vendor’s applications. As a result, an enterprise that utilizes management applications provided by different vendors is faced with the prospect of deploying multiple probes or agents in their DMZs, along with the additional firewall configuration required to allow each application to communicate with its associated probe or agent.

As an alternative to purchasing and deploying multiple application-specific probes and agents, Tavve’s ZoneRanger can provide a single, common proxy service for the management protocols utilized by various management applications. Because the ZoneRanger is not tied to a specific management application, the proxy services provided by ZoneRanger can be shared by multiple management applications, eliminating the need for application-specific probes or agents, and reducing the number of firewall rules required to allow management applications to communicate with DMZ devices.

Many management applications do not currently provide any built-in support for the use of a proxy service. As a result, in order to be able to use a proxy service with these applications, it is necessary to ensure that the applications can effectively remain unaware that a proxy service is being used. This ability is referred to as *transparent proxy*. ZoneRanger is able to provide transparent proxy for management protocols through the use of the Gateway Virtual Interface (GVI) service, which enables the ZoneRanger to intercept management traffic destined for DMZ devices, allowing ZoneRanger to integrate with a wide variety of management applications.

Introduction

The basic concept of a management proxy service is illustrated in Figure 1.

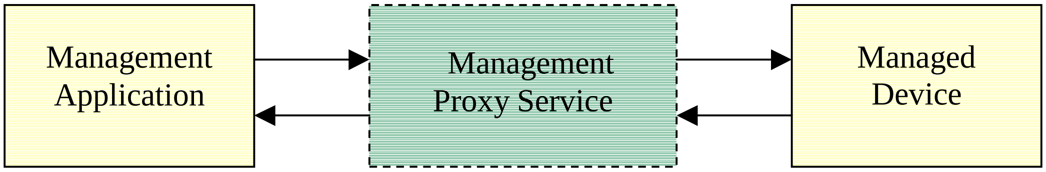


Figure 1. Management Proxy Service

The goal of a management proxy service is to act as a relay point for network traffic between management applications (e.g. OpenView NNM, Tivoli NetView, CA Unicenter, InfoVista Server, NetScout nGenius, Concord eHealth, Micromuse NetCool, CiscoWorks, Cisco Security MARS, etc.) and a set of managed devices (e.g. routers, switches, servers, load balancers, etc.). Benefits associated with the use of a management proxy service include the following:

- Firewall rule simplification/reduction.
- Traffic filtering.
- Traffic validation[1].

Management proxy services can be helpful in a variety of scenarios. A typical example is the case where the flow of management traffic is restricted or prevented, due to a firewall installed between the management application and the managed devices[2].

A management proxy service is considered to be *transparent*, if the management applications are able to remain essentially unaware of its presence, not needing to be configured in a special or non-standard way in order to use the proxy.

The basic ZoneRanger management proxy service architecture consists of two parts:

1. The Tavve **Ranger Gateway** software, which typically is installed on a shared server along with one or more management applications, but may also be installed on its own dedicated server.
2. The Tavve **ZoneRanger** appliance, which is installed in a network location from which it is able to communicate with the managed devices.

[1] A proxy service that provides traffic validation is also called a *proxy firewall*.

[2] A traffic-restricted VPN (e.g. a VPN to an extranet) is another case where management traffic may be restricted or prevented.

This architecture is illustrated in Figure 2.

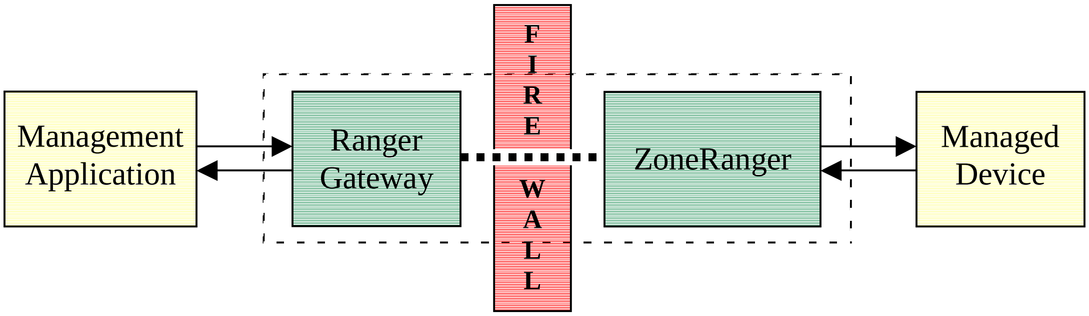


Figure 2. Typical ZoneRanger Architecture

In the typical case where there is a firewall between the Ranger Gateway and the ZoneRanger (e.g. the ZoneRanger is installed in a DMZ), the firewall must be configured to permit a single TCP connection on a single port between the Ranger Gateway and the ZoneRanger. Note that this approach requires a minimum of one ZoneRanger to be installed within each DMZ where there are devices to be managed. When high availability is required, it is recommended that an additional “redundant” ZoneRanger also be installed in each DMZ.

When the Gateway Virtual Interface (GVI) service on the Ranger Gateway is configured and enabled, traffic originated by management applications and destined for managed devices is intercepted by the Ranger Gateway, effectively hiding the existence of the proxy from the management application. As a result, the combination of a Ranger Gateway and a ZoneRanger can effectively provide a transparent management proxy service. The sequence of steps for processing a typical management transaction (e.g. ICMP echo request, SNMP get/set request) using this approach is illustrated in Figure 3.

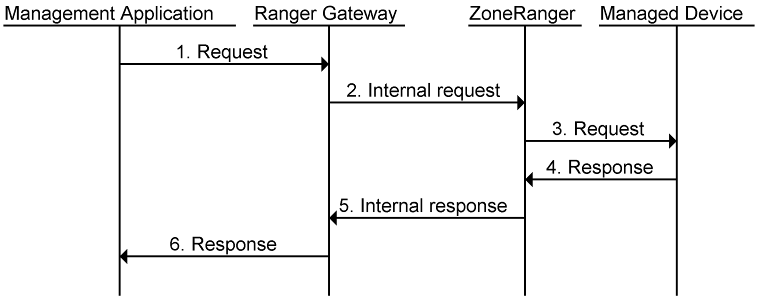


Figure 3. Management Transaction using ZoneRanger Proxy

Notes:

1. The management application generates a request, addressed to a specific managed device. The operating system on the server where the management application is installed (i.e. the *management application server*) routes this request to the GVI service on the Ranger Gateway, based on pre-configured static routing rules.

2. The Ranger Gateway inspects the request, identifies a ZoneRanger that is managing the managed device, and sends the request to that ZoneRanger in an internal format via an encrypted SSL/TCP connection.
3. The ZoneRanger forwards the request to the managed device.
4. The managed device responds to the request.
5. The ZoneRanger receives the response, verifies that the response is valid, and that it corresponds to an outstanding request, and forwards the response in an internal format to the Ranger Gateway.
6. The Ranger Gateway relays the response to the management application.

Two services within the Ranger Gateway play a vital role in the implementation of transparent proxy services:

- The Gateway Virtual Interface (GVI) service.
- The Proxy Map service.

The operation and configuration of these services are described in further detail in the following sections.

The Gateway Virtual Interface (GVI) Service

The Gateway Virtual Interface (GVI) service on the Ranger Gateway is responsible for intercepting network traffic originated by management applications and intended for managed devices, so that this traffic can be handled by the proxy services implemented within the Ranger Gateway and ZoneRanger. When the GVI service is enabled, it configures a virtual point-to-point interface on the management application server. In addition, the GVI service can be configured to add one or more static routes to the management application server so that traffic intended for DMZ devices is routed to this virtual interface. The Ranger Gateway, as the creator/owner of the virtual interface, receives all traffic that is routed to the virtual interface. The basic architecture and operation of the GVI service are illustrated in Figure 4.

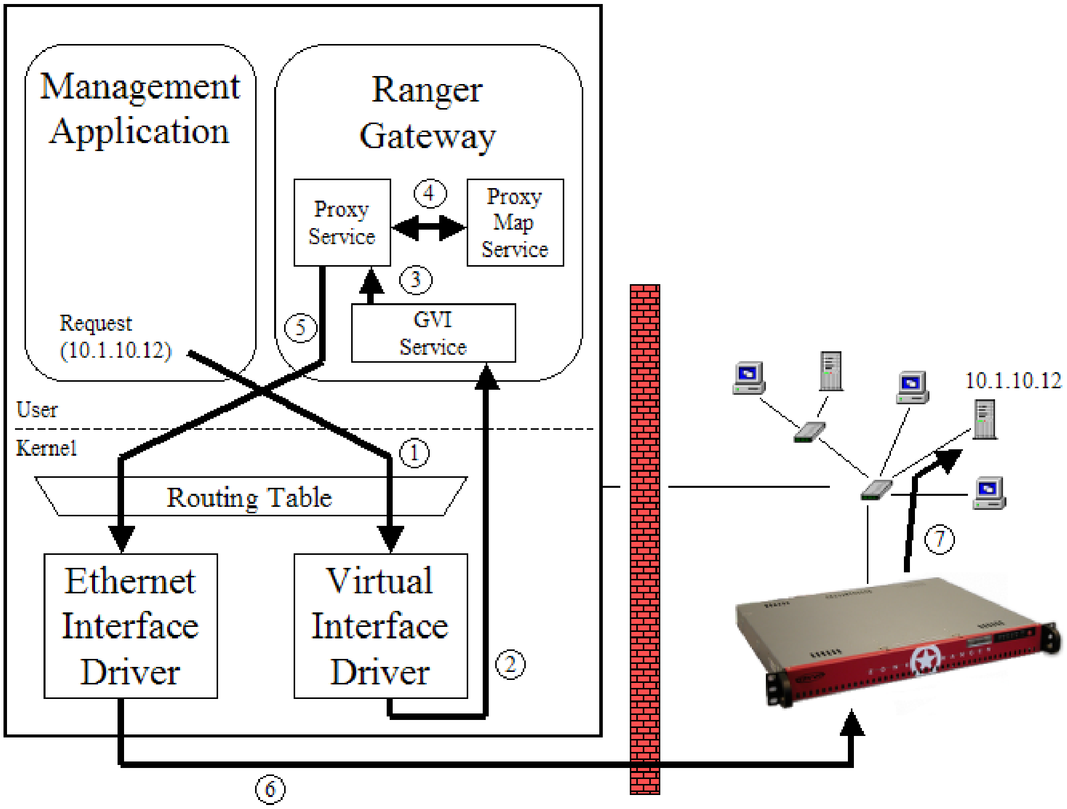


Figure 4. GVI Architecture and Operation

Notes:

1. The management application generates a request, addressed to a specific managed device. The operating system on the server where the management application is installed (i.e. the *management application server*) routes this request to virtual interface driver, based on pre-configured static routing rules.
2. The virtual interface driver forwards the request to the GVI service within the Ranger Gateway.
3. The GVI service forwards the request to the appropriate proxy service within the Ranger Gateway (e.g. ICMP Proxy, SNMP Proxy, TCP Proxy).
4. The selected proxy service validates the request, then consults with the Proxy Map service in order to select a ZoneRanger that is able to relay the request to the target device.
5. The selected proxy service forwards the request to the selected ZoneRanger.
6. The request is routed to the selected ZoneRanger.
7. The selected ZoneRanger forwards the request to the target device.

The target device will typically reply back to the ZoneRanger, which will validate the reply, then forward the reply to the Ranger Gateway, which forwards the reply to the management application via the GVI.

The primary advantage of GVI is that the existence of the proxy service is completely transparent to the management application. GVI uses common routing mechanisms within the underlying operating system to intercept traffic bound for managed devices, so there is no need to modify or reconfigure the management application in any way. Another advantage is that the same mechanism can be used for a variety of proxy services (e.g. ICMP proxy, SNMP proxy, TCP proxy).

GVI is currently supported on Solaris, Windows, and Linux operating systems. In cases where a management application server uses an operating system for which GVI is not supported, it is possible to install the Ranger Gateway software in a separate server, and to configure the management application server to route traffic intended for DMZ devices to the server where the Ranger Gateway has been installed. Note that the Ranger Gateway server must reside in the same subnet as the management application server, and must have IP forwarding enabled.

The Proxy Map Service

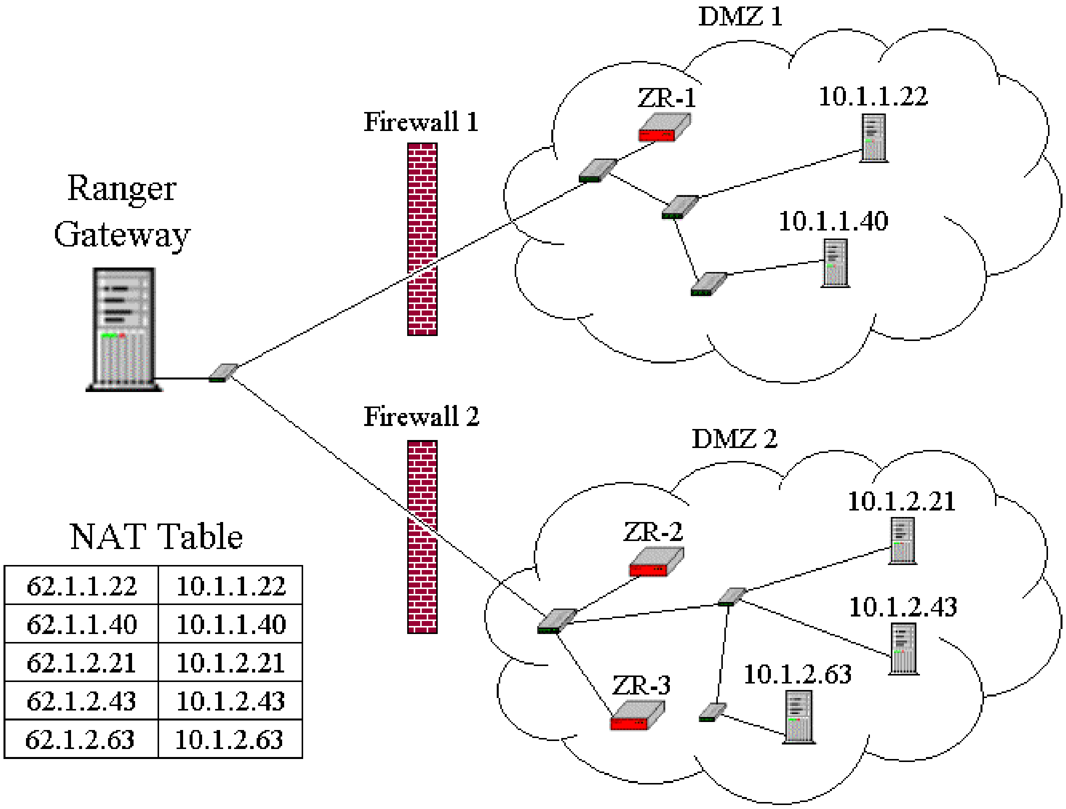
The Proxy Map service within the Ranger Gateway is responsible for identifying the set of ZoneRanger candidates that are able to relay a given proxy request to the indicated target device, and selecting one of these candidates for each request. The Proxy Map service makes these decisions based on the content of an internal configuration file referred to as the *active proxy map*. The active proxy map can be viewed as a table, where each row consists of a the following fields:

rg-address: The host name or IP address of the target device for a proxy transaction as indicated to the Ranger Gateway by the management application.

zoneranger: The host name or IP address of a ZoneRanger which may be selected to relay a proxy transaction.

zr-address: The actual host name or IP address that the ZoneRanger should use to access the target device. Note that where NAT is not in effect, this field can be omitted.

For example, consider the network shown in Figure 5.



NAT Table

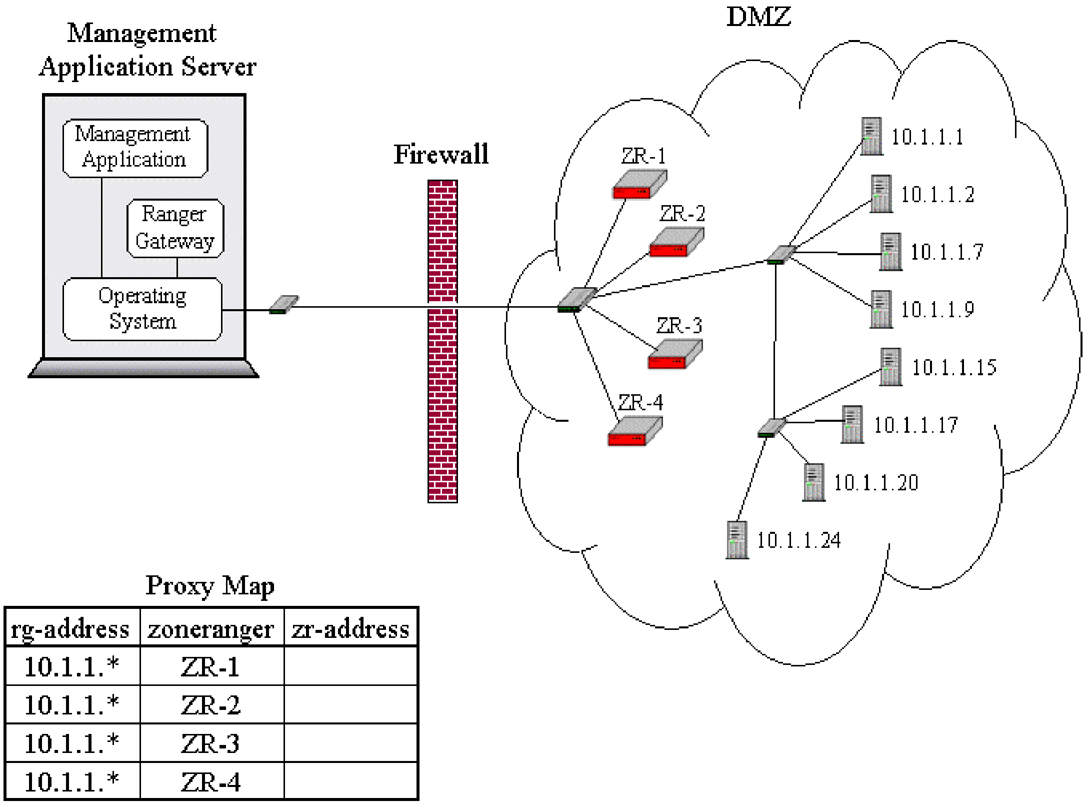
62.1.1.22	10.1.1.22
62.1.1.40	10.1.1.40
62.1.2.21	10.1.2.21
62.1.2.43	10.1.2.43
62.1.2.63	10.1.2.63

Figure 5. Network Example

Assuming that the firewalls are configured to perform NAT as indicated by the NAT Table shown in the figure, the active proxy map configuration corresponding to this network would be as follows:

rg-address	**zoneranger**	**zr-address**
62.1.1.*	ZR-1	10.1.1.*
62.1.2.*	ZR-2	10.1.2.*
62.1.2.*	ZR-3	10.1.2.*

The Proxy Map service also supports the ability to deploy ZoneRangers in pools in order to handle cases where there is a high volume of proxy traffic. For example, consider the network shown in Figure 6.



Proxy Map

rg-address	zoneranger	zr-address
10.1.1.*	ZR-1	
10.1.1.*	ZR-2	
10.1.1.*	ZR-3	
10.1.1.*	ZR-4	

Figure 6. Network Example with a ZoneRanger Pool

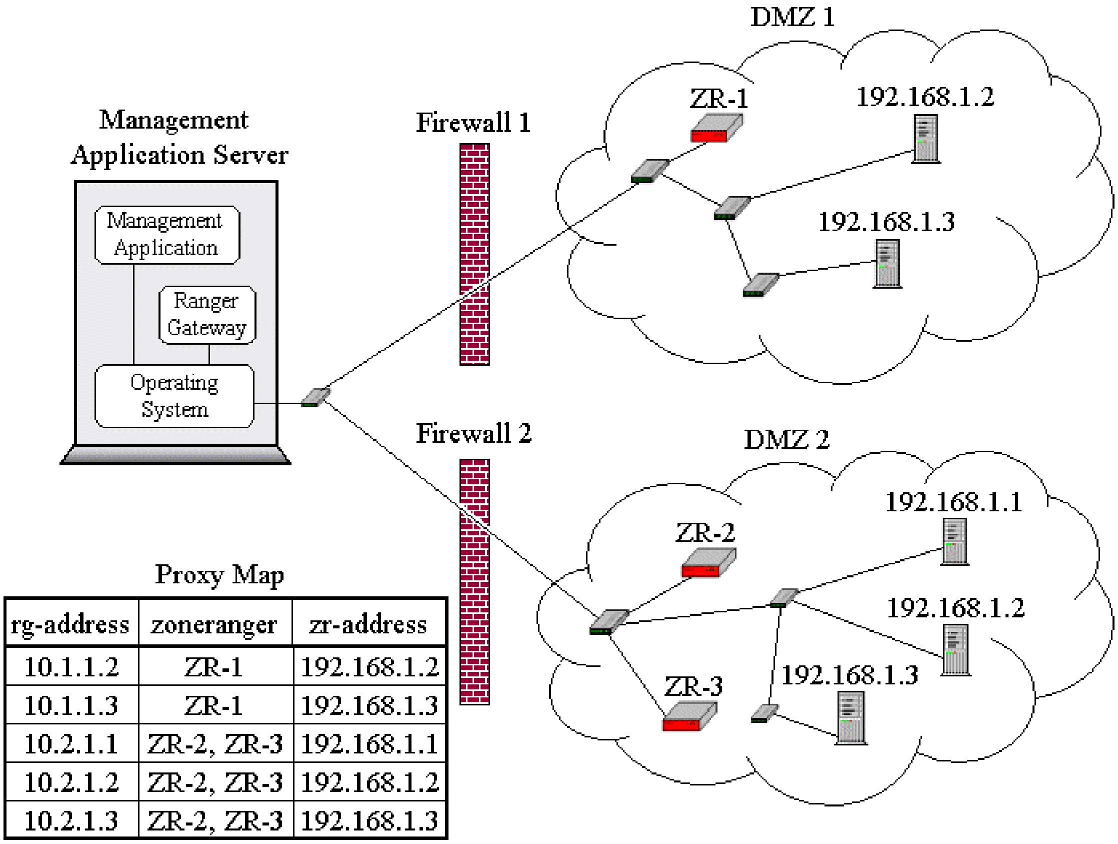
In this example, a pool of four ZoneRangers has been deployed to proxy management traffic across a single set of devices. The Proxy Map service configuration indicates that any of these ZoneRangers can be chosen to relay proxy traffic destined for devices with addresses in the 10.1.1.0/255.255.255.0 subnet. The algorithm whereby the Proxy Map service chooses a ZoneRanger for a given proxy request can be configured in one of two modes:

- *Load Balancing Mode*: The algorithm looks at recent selection statistics and ZoneRanger status and selects the least frequently selected ZoneRanger from the pool of eligible healthy ZoneRangers.
- *High Reliability Mode*: The algorithm looks at ZoneRanger status and selects the eligible ZoneRanger that has most recently demonstrated evidence of good health.

Note that in both modes, the selection algorithm attempts to bypass ZoneRangers that are unavailable (e.g. disconnected, rebooting, failed). As such, the use of a ZoneRanger pool will increase the availability of the proxy services, regardless of the configured selection mode. The difference between the algorithms is that in load balancing mode, any healthy, eligible ZoneRanger may be selected, whereas in high-reliability mode, the algorithm will always select the eligible ZoneRanger that appears most likely to be healthy. In most cases where there is a high volume of traffic, load balancing mode is recommended, because the traffic load will be spread across the available ZoneRangers. When the Ranger Gateway detects that one or more ZoneRangers in the pool are unavailable, the Ranger Gateway will automatically adjust to spread the load across the remaining healthy ZoneRangers.

The Proxy Map service can also be helpful in situations where an organization needs to manage a network where IP address ranges are reused across multiple network zones. For example, this situation can arise whenever companies that have been using private internet addresses are merged. In the absence of NAT, the recommended solution is to define unique virtual addresses that are mapped to real device addresses by the Proxy Map service.

For example, consider the network shown in Figure 7.



rg-address	zoneranger	zr-address
10.1.1.2	ZR-1	192.168.1.2
10.1.1.3	ZR-1	192.168.1.3
10.2.1.1	ZR-2, ZR-3	192.168.1.1
10.2.1.2	ZR-2, ZR-3	192.168.1.2
10.2.1.3	ZR-2, ZR-3	192.168.1.3

Figure 7. Network with Overlapping IP Addresses

Note that addresses 192.168.1.2 and 192.168.1.3 are defined in both DMZ 1 and DMZ 2, and that virtual addresses 10.1.1.2-3 and 10.2.1.1-3 have been configured to map to the devices in the two DMZ’s.

Even though this approach requires some amount of effort to manage and configure virtual addresses, it should be noted that in most cases, the scope of these addresses is confined to the management application server. As such, routers, firewalls, and other applications would have no awareness or visibility of these addresses, resulting in much simpler configuration and maintenance effort than alternatives such as static NAT.

Configuring Transparent Proxy Services

The following steps are required to configure transparent proxy services:

1. The active proxy map in the Proxy Map service must be configured with a set of (*rg-address*, *zoneranger*) and/or (*rg-address*, *zoneranger*, *zr-address*) rules. In the simplest case, each rule maps a single device address or range of device addresses to a ZoneRanger that are able to access the corresponding devices. Where address translation is required (e.g. NAT or virtual addresses are being used) each rule will additionally specify the address or address translation rule (i.e. the *zr-address*) used to derive the address that the ZoneRanger should use to access the device.

2. The GVI service must be configured with the set of routes that it will need to create, in order to ensure that network traffic from management applications to managed devices is routed through the GVI. A route can be specified in the form of a single device address or a subnet.

3. The GVI service must be enabled.

The ProxyMap and GVI services are configured on the Ranger Gateway using the `proxyMapTool` and `gvi` commands, respectively. As an example, for the network shown in Figure 5, the following commands would be required to configure and test the GVI service:

1. Add proxy map rules indicating the subnets being managed by each ZoneRanger:

   ```
   proxyMapTool add 10.1.1.* ZR-1
   proxyMapTool add 10.1.2.* ZR-2
   proxyMapTool add 10.1.2.* ZR-3
   ```

2. Add routes for the `10.1.1.0/255.255.255.0` and `10.1.2.0/255.255.255.0` subnets to the GVI route list:

   ```
   gvi add-route 10.1.1.*
   gvi add-route 10.1.2.*
   ```

   Note that in this case, the two subnets could be optionally combined into a single route:

   ```
   gvi add-route 10.1.0.0/255.255.252.0
   ```

3. Enable the GVI service:

```
gvi enable
```

4. Test the configuration, specifying the address of a few managed devices:

```
gvi test 10.1.1.40
gvi test 10.1.2.63
```

Conclusion

Proxy services can provide an effective way to securely extend management functionality into regions of the network where management protocols are constrained or are not allowed to travel. Given that many management applications do not currently provide any built-in support for the use of a proxy service, the ability to provide proxy services without requiring special or non-standard configuration management applications, also known as *transparent proxy*, is essential. Tavve's ZoneRanger provides transparent proxy services for management protocols through the use of the Gateway Virtual Interface (GVI) service, which enables the ZoneRanger to intercept management traffic destined for DMZ devices, allowing ZoneRanger to integrate with a wide variety of management applications.