SNMP Proxy into DMZ with ZoneRanger

Jim Doble, CISSP
Tavve Software Co.

Anthony V. Edwards, CISSP
Tavve Software Co.
SNMP Proxy into DMZ with ZoneRanger

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 SNMP may be blocked by the firewall. The same problem applies to systems management, security management, and configuration management applications, which may also rely on SNMP. This paper describes how SNMP proxy, as provided by Tavve’s ZoneRanger product, can be used to address this problem. Though the paper focuses on DMZ’s, the concepts described are equally applicable to management of any partitioned network architecture.

Introduction

The basic concept of SNMP proxy is illustrated in Figure 1.

![Figure 1. SNMP Proxy through Firewall](image)

The goal of SNMP proxy is to enable a management application (e.g. OpenView NNM, Tivoli NetView, CA Unicenter, InfoVista Server, NetScout nGenius, Concord eHealth, Micromuse NetCool, CiscoWorks, Cisco Security MARS) to be able to perform SNMP operations (e.g. SNMP GetRequest, SNMP SetRequest), on SNMP agents residing on managed DMZ devices (e.g. routers, switches, servers, load balancers). SNMP proxy is required whenever the flow of SNMP traffic is restricted or prevented, due to a firewall (e.g. Cisco, Nokia, CheckPoint) installed between the management application and the managed devices.

---

1 A traffic-restricted VPN (e.g. a VPN to an extranet) is another case where SNMP traffic may be restricted or prevented.
The basic ZoneRanger SNMP proxy 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 the DMZ, along with the managed devices.

This architecture is illustrated in Figure 2.

![Figure 2. ZoneRanger SNMP Proxy](image)

The message flow for an SNMP proxy request is illustrated in Figure 3.

![Figure 3. SNMP Proxy Message Flow](image)

Each SNMP proxy request originates in the management application and is forwarded to the Ranger Gateway [1]. 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 [2]. The ZoneRanger forwards the request to the managed device [3], which processes the request and sends a reply back to the ZoneRanger [4]. The ZoneRanger inspects the reply then forwards it to the Ranger Gateway [5], which in turn forwards the reply to the management application [6].

Note that the firewall must be configured to permit the TCP connection between the Ranger Gateway and the ZoneRanger. Also 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.

The interaction between the ZoneRanger and the managed device is relatively straightforward. A ZoneRanger sends an SNMP request to the managed device, and the managed device simply replies back to the address from which the request appears to have originated (i.e. the ZoneRanger’s address).

The interaction between the management application and the Ranger Gateway is more involved, because the SNMP request from the management application must initially be delivered to the Ranger Gateway, as opposed to the managed device for which it is actually intended (i.e. the target device). In addition, on receiving the request, the Ranger Gateway must be able to identify the target device, and any ZoneRanger(s) that are managing the target device. Due to the wide variety of management applications that must be supported, differences between the various operating system platforms on which these applications run, and varying network configurations and customer requirements, there is no single best approach to address these issues. As a result, Tavve has developed a variety of mechanisms that can be used to provide SNMP proxy, so that customers can choose the mechanism that best suits their requirements:

- **Gateway Virtual Interface (GVI)**: The management application sends SNMP requests intended for a DMZ device to the actual address of the target device, or an address that can be uniquely mapped to the target device. The management application server is configured with static routing rules, so that traffic destined for DMZ devices is routed to a virtual point-to-point interface which forwards the traffic to the Ranger Gateway.

- **SOCKS**: The management application sends SNMP requests intended for a DMZ device to the actual address of the target device, or an address that can be uniquely mapped to the target device. If the management application provides built-in support for SOCKS, or if a compatible SOCKS shim is installed on the management application server, the client or shim can be configured to forward SNMP traffic destined for DMZ devices to a SOCKS server integrated within the Ranger Gateway.

- **IP Address Aliasing**: The management application sends SNMP requests intended for a DMZ device to the actual address of the target device, or an address that can be uniquely mapped to the target device. The management application server is configured with a set of IP address aliases, corresponding to the set of DMZ devices to which management traffic may be directed. The SNMP Proxy service on the Ranger Gateway listens on the configured SNMP proxy port for SNMP requests destined for any IP addresses that have been defined on the management

---

2 SOCKS is an Internet standards-track protocol for generic TCP and UDP proxy services, defined in RFC 1928.

3 The default is port 4852.
application server. As a result, any SNMP proxy traffic destined for DMZ devices will be received by the Ranger Gateway.

- **Community String Conventions**: The management application sends SNMP requests intended for a DMZ device to the configured SNMP proxy port on the Ranger Gateway. The management application must also be configured to include the actual target device address, and optionally the address of the ZoneRanger that should be used to relay the request, within the request’s community string, according to specified conventions. The SNMP Proxy service on the Ranger Gateway listens for SNMP requests on the SNMP proxy port and uses the additional information in the community string to determine how the request should be routed. The additional information in the community string is removed before the request is relayed to the target device.

Further detail regarding these mechanisms is provided in the following four sections.

**Gateway Virtual Interface (GVI)**

When the **Gateway Virtual Interface (GVI)** service on the Ranger Gateway 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 SNMP traffic that is routed to the virtual interface, and forwards this traffic to the SNMP Proxy service within the Ranger Gateway. The SNMP Proxy service validates the request, consults the Proxy Map service in the Ranger Gateway in order to identify a ZoneRanger that is able to relay the request to the target device, and then forwards the request to the selected ZoneRanger, which in turn, forwards the request to the target DMZ 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.

Consider the network example in Figure 4. Two DMZ’s are shown. The first DMZ has one ZoneRanger (ZR-1) and the second one has two (ZR-2, ZR-3). The IP addresses in the two DMZ’s do not overlap.

---

4 The same approach can be used for ICMP Proxy and TCP Proxy services.

5 The Proxy Map service is part of the Ranger Gateway software, and uses configured rules to map target device addresses, as specified by management applications, to the set of ZoneRangers that are able to proxy requests to the corresponding devices, and the actual addresses that those ZoneRangers would use to forward management traffic to the target devices. The Proxy Map service is also responsible for selecting the ZoneRanger to be used for each proxy request from the available candidates. The Proxy Map service is described in detail in the ZoneRanger User’s Guide.
Figure 4. Network Example with GVI

The messaging flow for an SNMP proxy request using GVI is illustrated in Figure 5.

Note the following from this example:

- The management application requests that a UDP datagram containing the SNMP GetRequest message be sent to the address of the target device (10.4.1.2) [1].
- The routing table in the management application server is preconfigured to route traffic destined for the 10.4.1.2 address to the GVI driver. Note that the GVI...
service in the Ranger Gateway includes a *route manager* that simplifies creation and management of the static routes that are needed to ensure that management traffic is routed to the GVI.

- The GVI driver forwards the request to the SNMP Proxy service in the Ranger Gateway [2].
- The SNMP Proxy service consults the Proxy Map service in the Ranger Gateway to determine the list of ZoneRangers that manage the target device (ZR-2, and ZR-3). One of the ZoneRangers (ZR-2) is selected, and the request is forwarded to the selected ZoneRanger [3].
- The selected ZoneRanger forwards the request to the target device [4].
- The target device replies back to the ZoneRanger [5], which relays the response to the Ranger Gateway [6]. The SNMP Proxy service relays the response to the GVI driver [7].
- The GVI driver forwards the response to the management application [8].

The primary advantage of GVI is that the existence of the SNMP proxy is completely transparent to the management application. GVI uses common routing mechanisms within the underlying operating system to intercept traffic bound for DMZ 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 other proxy services, such as ICMP proxy, or 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.

**SOCKS**

SOCKS is an Internet standards-track protocol for generic TCP and UDP proxy services, defined in RFC 1928. SOCKS can be used to redirect management traffic from the management application to a SOCKS server integrated within the Ranger Gateway. In order to use SOCKS, either the management application must built-in support for SOCKS, or generic SOCKS “shim” software must be installed on the management application server. The shim software inserts itself between the management application and the server’s TCP/IP stack, and redirects traffic for specified IP addresses and ports to a SOCKS server, based on configuration information.
Figure 6 shows a SOCKS shim inserted between the management application and the operating system.

The messaging flow for an SNMP proxy request using a SOCKS shim is illustrated in Figure 7.

Figure 6. Network Example with SOCKS Shim

Figure 7. SNMP Proxy Message Flow using SOCKS
Note the following from this example:

- The management application requests that a UDP datagram containing the SNMP GetRequest message be sent to the address of the target device (10.4.1.2) [1].
- The SOCKS shim intercepts the request, performs a SOCKS protocol handshake with the SOCKS server in the Ranger Gateway, to establish a “UDP association” [2, 3], then forwards the SNMP request, to the SOCKS server, along with a header indicating that the datagram is intended for address 10.4.1.2 [4].
- The SOCKS server in the Ranger Gateway forwards the request to the SNMP Proxy service in the Ranger Gateway.
- The SNMP Proxy service consults the Proxy Map service in the Ranger Gateway to determine the list of ZoneRangers that manage the target device (ZR-2, and ZR-3). One of the ZoneRangers (ZR-2) is selected, and the request is forwarded to the selected ZoneRanger [5].
- The selected ZoneRanger forwards the request to the target device [6].
- The target device replies back to the ZoneRanger [7], which relays the response to the Ranger Gateway [8]. The SNMP Proxy service relays the response to the SOCKS server, which forwards the response to the SOCKS shim along with a header indicating that the response was received from 10.4.1.2 [9].
- The SOCKS shim forwards the response to the management application [10].

If a management application has built-in support for SOCKS, or is compatible with a SOCKS shim, the SOCKS mechanism can be a very effective alternative. One advantage of SOCKS over GVI is that it is typically possible to configure the SOCKS client to route traffic for certain ports to the Ranger Gateway, while traffic destined for other ports is routed normally. In addition, some SOCKS clients can be configured to only intercept traffic sent from specified applications. While it is still necessary to specify the ranges of IP addresses to be intercepted, this is done in the SOCKS client configuration, instead of the management application server routing table, which keeps these rules separate from static routing rules that may be required for other purposes.

One disadvantage of SOCKS is that the SOCKS protocol only supports TCP and UDP. As a result, SOCKS cannot be used for ICMP proxy. In addition, many management applications do not provide built-in support for SOCKS and reliable SOCKS shims may not be available for the operating system being used. In these cases, an alternative SNMP proxy mechanism will need to be selected.

**IP Address Aliasing**

Operating systems typically provide a means to associate multiple IP addresses with each network interface (i.e. a primary address, and one or more “aliases”). If IP address aliases corresponding to the managed DMZ devices are defined on the management application server, all traffic generated by the management application and destined for these devices will be routed as local traffic to the interface where the IP address aliases have been
defined. The SNMP Proxy service on the Ranger Gateway will listen on the SNMP proxy port for requests destined for any of these IP addresses, and will consult with the Proxy Map service to select a ZoneRanger to which the request should be forwarded.

If the management application and the Ranger Gateway software have been installed on the same server, the IP address aliases can usually be added to the server’s loopback interface. If they have been installed on different servers, the IP address aliases must be added to an appropriate network interface on the Ranger Gateway server, and static routes will need to be defined on the management application server to ensure that SNMP requests are routed to the Ranger Gateway server.

Consider the network example in Figure 8. In this example, the management application and the Ranger Gateway have been installed on the same server. Two DMZ’s are shown. The first DMZ has one ZoneRanger (ZR-1) and the second one has two (ZR-2, ZR-3). The IP addresses in the two DMZ’s do not overlap.

![Figure 8. Network Example with IP Address Aliasing](image)

In order to manage this network, addresses 10.2.1.1, 10.2.1.2, 10.4.1.1, 10.4.1.2, and 10.4.1.3 would be configured as IP address aliases on the management application server, corresponding to the five managed devices, and the Proxy Map service in the Ranger Gateway would be configured as shown in the figure. An example of the messaging flow for an SNMP proxy request is shown in Figure 9.
Figure 9. SNMP Proxy Message Flow using IP Address Aliasing

Note the following from this example:

- The management application requests that a UDP datagram containing the SNMP GetRequest message be sent to the address of the target device (10.4.1.2), using the SNMP proxy port [1]. Assuming that the specified destination IP address has been defined as an IP address alias on the management application server, the request will be delivered to the SNMP Proxy service within the Ranger Gateway.

- The SNMP Proxy service in the Ranger Gateway consults the Proxy Map service in the Ranger Gateway to determine the list of ZoneRangers that manage the target device (ZR-2, and ZR-3). One of the ZoneRangers (ZR-2) is selected, and the request is forwarded to the selected ZoneRanger [2].

- The selected ZoneRanger forwards the request to the target device [3].

- The target device replies back to the ZoneRanger [4], which relays the response to the Ranger Gateway [5].

- The Ranger Gateway forwards the response to the management application [6].

By default, the SNMP Proxy service on the Ranger Gateway listens for SNMP requests on a special port (i.e. 4852) so as to avoid conflict with an SNMP agent on the server where the Ranger Gateway is installed that may be listening on port 161, and the ZoneRanger forwards requests to managed devices on port 161. The SNMP proxy port on the Ranger Gateway can be configured as required to avoid conflicts with other applications or to allow integration with management applications. For example, some management applications assume that all SNMP requests should be directed to port 161 and do not allow this to be configured or changed. In such cases, the SNMP Proxy service would need to be configured to listen on port 161.

The port to which the ZoneRanger sends SNMP requests can be configured on a per-device basis. This allows different managed devices in the same DMZ to listen for SNMP requests on different ports.

IP address aliasing can be used on all operating systems where the Ranger Gateway software is supported. The main disadvantage of the IP address aliasing technique is the
administrative effort required to add and maintain IP address aliases for all managed
devices on the Ranger Gateway server. Another concern is that operating systems may
limit the number of IP address aliases that can be defined. As a result, this technique may
not be able to support the required number of managed devices for some applications.

Community String Conventions

In all of the previously described mechanisms, the Ranger Gateway determines the
address of the target device for each SNMP request based on the address to which the
management application sent the request. An alternative is to configure the management
application to send the SNMP request to an arbitrary interface on the server where the
Ranger Gateway is installed, and for the SNMP Proxy service within the Ranger Gateway
to determine the target device address based on additional information embedded into the
SNMP request’s community string, according to specified conventions. For example, the
following community string format can be used:

    community@ZoneRanger@device

where community is the actual community string that the target device is expecting (e.g.
public), ZoneRanger is the name or IP address of a ZoneRanger that is managing the
target device, and device is the name or IP address of the target device. In this case, the
Ranger Gateway would extract the ZoneRanger and device values from the community
string, and would forward the request to the specified ZoneRanger. The ZoneRanger
would then send the request to the target device. Note that the ZoneRanger and device
values are removed before the request is forwarded to the target device, so the target
device only sees the community value that it is expecting.

Consider the network example in Figure 10. In this example, the management application
and the Ranger Gateway have been installed on different servers\(^6\). Two DMZ’s are
shown. The first DMZ has one ZoneRanger (ZR-1) and the second one has two (ZR-2,
ZR-3). The IP addresses in the two DMZ’s do not overlap. The IP address of the Ranger
Gateway Server is 10.254.1.1.

\(^6\) The community string conventions mechanism can also be used in cases where the Ranger Gateway is
installed on the management application server. In such cases, the management application would need to
send SNMP requests to an address on the management application server.
An example of the messaging flow for an SNMP proxy request is shown in Figure 11.

Note the following from this example:

- The management application directs the SNMP request to the Ranger Gateway’s IP address (10.254.1.1), using the SNMP proxy port [1]. The ZoneRanger to which the request should be forwarded (ZR-2), and the target device’s actual IP
address (192.168.1.2) are embedded in the community string, along with the community string value that the target device expects (i.e. public).

- The SNMP Proxy service in the Ranger Gateway receives the request, parses the community string, and forwards the request to the specified ZoneRanger [2].
- The ZoneRanger forwards the request to the target device [3], with the ZoneRanger and device portions of the community string removed.
- The target device replies back to the ZoneRanger [4], which relays the response to the Ranger Gateway [5].
- The Ranger Gateway forwards the response to the management application [6].

The SNMP Proxy service can be configured for different community string formats. The following formats are supported:

1. community@ZoneRanger@device
2. device@ZoneRanger@community
3. community@device
4. device@community
5. community

Formats 1 and 2 require management applications to specify the ZoneRanger (or ZoneRanger group) that will relay the SNMP request to the target device. When using redundancy or grouping, the ZoneRanger field in the community string can be replaced with a group name that identifies a group of ZoneRangers, and the SNMP Proxy service in the Ranger Gateway will automatically select a ZoneRanger from this group to relay the request. The only difference between formats 1 and 2 is the order of the fields. The ability to configure the SNMP Proxy service to use different field orders has been provided in order to handle situations where management applications and managed devices are using their own community string prefix or suffix conventions.

Formats 3 and 4 do not require the management application to specify a ZoneRanger. Instead, the SNMP Proxy service consults the Proxy Map service, in order to identify a ZoneRanger that is able to relay traffic to the target device, and then forwards the SNMP request to the selected ZoneRanger. The only difference between formats 3 and 4 is the order of the fields. The ability to use different field orders has been provided in case management applications and managed devices are using their own community string prefix or suffix conventions.

When the Proxy Map service is used, the responsibility for identifying the ZoneRanger to relay each request is essentially moved from the management application to the Ranger Gateway. The advantages of this approach are:

- Associations between ZoneRangers and DMZ devices, and any required address translations for DMZ devices (e.g. if NAT is in effect) are configured in one place,
and can be shared by multiple proxy services across multiple management applications.

- The Proxy Map service can be configured to balance proxy requests across a set of ZoneRanger candidates, resulting in a more even distribution of proxy traffic in situations where DMZ devices are being managed by multiple ZoneRangers.

Figure 12 shows a message flow example, based on the sample network from Figure 10, using the `community@device` convention.

![Figure 12. SNMP Proxy Message Flow using Community String Conventions (2)](image)

Note the following from this example:

- The management application directs the SNMP request to the Ranger Gateway’s IP address (10.254.1.1), using the SNMP proxy port [1]. The target device’s actual IP address (10.4.1.2) is embedded in the community string, along with the community string value that the target device expects (i.e. public).

- The SNMP Proxy service consults the Proxy Map service in the Ranger Gateway to determine the list of ZoneRangers that manage the target device (ZR-2, and ZR-3). One of the ZoneRangers (ZR-2) is selected, and the request is forwarded to the selected ZoneRanger [2].

- The selected ZoneRanger uses the actual IP address of the target device (192.168.1.2) to forward the request to the target device [3], with the `device` portion of the community string removed.

- The target device replies back to the ZoneRanger [4], which relays the response to the Ranger Gateway [5].

- The Ranger Gateway forwards the response to the management application [6].

Format 5 implies that no special information is embedded in the community string, and is used in conjunction with the IP address aliasing mechanism.

By default, the SNMP Proxy service on the Ranger Gateway listens for SNMP requests on a special port (i.e. 4852) so as to avoid conflict with an SNMP agent on the server where the Ranger Gateway is installed that may be listening on port 161, and the
ZoneRanger forwards requests to managed devices on port 161. The SNMP proxy port on the Ranger Gateway can be configured as required to avoid conflicts with other applications or to allow integration with management applications. For example, some management applications assume that all SNMP requests should be directed to port 161 and do not allow this to be configured or changed. In such cases, the SNMP Proxy service would need to be configured to listen on port 161.

The port to which the ZoneRanger sends SNMP requests can be configured on a per-device basis. This allows different managed devices in the same DMZ to listen for SNMP requests on different ports. In addition, when community string conventions are being used, the management application can override the configured port for a given device, by adding “:port” to the device part of the community string, where port is the desired port number.

Community string conventions are best suited for management applications that can be configured to send SNMP requests for all managed devices to a single address. The primary advantage of community string conventions is that there is no need to install a GVI driver, or a SOCKS shim on the management application server. The three-part community string format (e.g. community@ZoneRanger@device) is also useful when managing DMZ’s with overlapping addresses. The primary disadvantage is that the management application must be configured in an atypical way in order to use the proxy. Some management applications require unique addresses for each managed device, and do not support the concept of a common proxy address. In these cases, an alternative SNMP proxy mechanism will need to be selected.

Choosing an SNMP Proxy Mechanism

A number of factors need to be considered in order to identify the best SNMP proxy mechanism for each situation:

- If the Ranger Gateway is installed on a management application server that supports the GVI service, then GVI is likely to be the preferred alternative, especially if there is a need to proxy other management protocols in addition to SNMP. Note that if ICMP proxy is also a requirement, GVI is the really the only alternative. The advantages of GVI are that it is largely transparent to the management applications, and that it does not require configuration of IP address aliases or special community strings.

- If ICMP proxy is not required, and if the management application has built-in support for SOCKS, or if the management application is compatible with an available SOCKS shim on the management application server’s operating system, then SOCKS may be a good alternative. SOCKS is comparable to GVI in that it does not require configuration of IP address aliases or special community strings.

Community string conventions can also be used when the management application uses different addresses for different target devices. However, the GVI, SOCKS, or IP address aliasing mechanisms are likely to be preferred in such cases, because the need to configure special community strings for each device is eliminated.
strings. Additionally, SOCKS clients can be configured to only intercept traffic destined for specified TCP and UDP ports, allowing other traffic to be routed in the normal manner.

- If neither GVI nor SOCKS are viable, but the number of managed devices is small, then IP address aliasing may be the best solution. The constraint, in this case, is that the number of managed devices must be less than the maximum number of IP address aliases that the operating system on the Ranger Gateway server will allow.

- If neither GVI nor SOCKS are viable, and the number of managed devices is large, then community string conventions may be the best technique, provided that the management application can be configured to send SNMP requests for all devices to a single address. This technique avoids the need to configure IP address aliases on the Ranger Gateway server, but does require the management application to be configured with special community strings.

Another alternative to consider, if neither GVI nor SOCKS are viable on the management application server, is to install the Ranger Gateway, with GVI enabled, on a dedicated Solaris, Linux, or Windows 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.

**Handling Overlapping IP Addresses**

It is not uncommon for an organization to need 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.

The resulting overlap of IP addresses can create a challenge for management applications, which need to be able to uniquely identify and communicate with different managed devices that share the same IP address. One solution is to deploy multiple instances of each management application to manage the different network zones, but that can be expensive, and largely defeats of purpose of centralized management. Another way to address the problem is to configure static NAT at the network boundaries where overlapping address ranges are encountered, but that can be both expensive and complicated.

An alternative that may be simpler and less expensive is to use ZoneRangers to proxy management traffic into network zones with overlapping addresses. In the specific case of SNMP, each of the proxy mechanisms described previously can be used to help address the problem of overlapping IP addresses.

In the case of the GVI, SOCKS, and IP address aliasing mechanisms, where the management application directs SNMP requests to device addresses, the solution is to define unique virtual addresses that are mapped to real device addresses by the Proxy Map service in the Ranger Gateway.
For example, consider the network example in Figure 13.

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. An example of the messaging flow for an SNMP proxy request, using the GVI mechanism, is shown in Figure 14.
Note the following from this example:

- The management application requests that a UDP datagram containing the SNMP GetRequest message be sent to the virtual address associated with the target device (10.2.1.2) [1].

- The routing table in the management application server is preconfigured to route the request to the GVI driver, which forwards the request to the SNMP Proxy service in the Ranger Gateway [2].

- The SNMP Proxy service in the Ranger Gateway consults the Proxy Map service in the Ranger Gateway to determine the list of ZoneRangers that manage the target device (ZR-2, and ZR-3), as well as the actual IP address of the target device (192.168.1.2). One of the ZoneRangers (ZR-2) is selected, and the request is forwarded to the selected ZoneRanger [3].

- The selected ZoneRanger uses the actual IP address of the target device (192.168.1.2) to forward the request to the target device [4].

- The target device replies back to the ZoneRanger [5], which relays the response to the Ranger Gateway [6]. The SNMP Proxy service relays the response to the GVI driver [7].

- The GVI driver passes the response to the management application [8].

The message flows for the SOCKS and IP address aliasing mechanisms are similar to those shown in Figures 7 and 9, except that the management application uses virtual IP addresses, and the Proxy Map service maps these addresses to real device addresses. In each of these cases, the interaction between the SNMP Proxy service and the Proxy Map service in the Ranger Gateway is as illustrated in Figure 15.

The Proxy Map service can be configured with rules for mapping individual addresses, or rules for mapping entire address ranges. For example, the Proxy Map configuration for the network in Figure 13, can be simplified to the following:

<table>
<thead>
<tr>
<th>Virtual Address</th>
<th>ZoneRangers</th>
<th>Real Address</th>
</tr>
</thead>
<tbody>
<tr>
<td>10.1.<em>.</em></td>
<td>ZR-1</td>
<td>192.168.<em>.</em></td>
</tr>
<tr>
<td>10.2.<em>.</em></td>
<td>ZR-2, ZR-3</td>
<td>192.168.<em>.</em></td>
</tr>
</tbody>
</table>
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.

The community string conventions mechanism can also be employed to address the problem of overlapping IP addresses, while avoiding the need to define virtual addresses, because SNMP requests are directed to the Ranger Gateway’s IP address, and the target device can be identified by specifying the ZoneRanger that is managing the target device and target device’s actual IP address. An example of the messaging flow using this approach, based on the network in Figure 13, is shown in Figure 16.

Note the following from this example:

- The management application directs the SNMP request to the Ranger Gateway’s IP address (10.254.1.1), using the SNMP proxy port [1]. The ZoneRanger to which the request should be forwarded (ZR-2), and the target device’s actual IP address (192.168.1.2) are embedded in the community string, along with the community string value that the target device expects (i.e. public).
- The SNMP Proxy service in the Ranger Gateway receives the request, parses the community string, and forwards the request to the specified ZoneRanger [2].
- The ZoneRanger forwards the request to the target device [3], with the ZoneRanger and device portions of the community string removed.
- The target device replies back to the ZoneRanger [4], which relays the response to the Ranger Gateway [5].
- The Ranger Gateway forwards the response to the management application [6].
Load Balancing

ZoneRangers can be deployed in pools in order to handle cases where there is a high volume of SNMP proxy traffic. For example, consider the network example in Figure 17.

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 SNMP proxy 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.

It should be noted that a pool of ZoneRangers can be deployed with or without the use of the ZoneRanger redundancy feature. The redundancy feature establishes a relationship between a pair of ZoneRangers so that if the configuration of one of the paired ZoneRangers is modified, the change is automatically propagated to its redundant peer. When deploying a pool with two ZoneRangers, the redundancy feature can be used to help reduce configuration effort, and ensure that the configurations of the two ZoneRangers remain synchronized. If there are more than two ZoneRangers in a pool, there is currently no automated means to propagate and synchronize configuration changes across the pool. However, manual saving and loading of configuration profiles should provide a reasonable acceptable alternative.

Load balancing can be used with all of the previously described SNMP proxy mechanisms, except in the case where community string conventions are used to designate a specific ZoneRanger to handle a request.

**SNMPv3 Conversion**

The ZoneRanger SNMP Proxy service can be used to proxy SNMPv1 and SNMPv2c requests to managed devices. In addition, ZoneRanger can be configured to translate SNMPv1 or SNMPv2c requests to SNMPv3 requests, as illustrated in Figure 18.

This feature enables authentication and encryption of SNMP messages in the DMZ, where enhanced security is arguably most needed, while avoiding the need to configure or upgrade existing management applications to support SNMPv3. SNMPv3 conversion can be configured on a per-device basis, so that the additional administrative effort required for SNMPv3 can be limited only to those devices where security is most needed.
Conclusion

SNMP proxy is an effective way to extend management functionality into regions of the network where management protocols are not allowed to travel. ZoneRanger supports a variety of SNMP proxy mechanisms, in order to be able to deal with the wide variety of management applications, operating systems, and network configurations where SNMP proxy is needed. SNMP proxy can also facilitate SNMP-based management in situations where duplicate IP addresses have been used in various network partitions. ZoneRanger’s SNMPv3 conversion feature can be used to increase management protocol security for sensitive devices, without impacting existing management applications.