Proxy SNMP Trap Reception from DMZ

Anthony V. Edwards
Tavve Software Co.
Proxy SNMP Trap Reception from DMZ

Anthony V. Edwards
Tavve Software Co.

Executive Summary

With the proliferation of DMZ’s (so-called De-Militarized Zones or firewall protected areas) and extranets today, network managers are increasingly faced with the problem of receiving SNMP traps from servers and networking equipment when security policy prevents SNMP traps from crossing the firewall from these segregated areas. This paper discusses three solutions for SNMP trap reception from the DMZ: 1) add a trap receiver into DMZ, 2) use a separate network management network, or 3) add a proxy trap receiver into DMZ. This paper discusses the problem the security policy creates and three solutions for this problem.

The SNMP trap Receiver

Network managers have embraced receiving SNMP traps to monitor network activities and troubles for a long time. Network managers trust and rely upon those SNMP traps. Many sites configure their equipment to forward all SNMP traps to a single trap receiver (or Network Management System (NMS)), which processes them to raise alerts or warnings.

A variety of applications are available today to process SNMP traps. NMS platforms include Hewlett Packard’s OpenView Network Node Manager, IBM Tivoli’s NetView, Computer Associates’ Unicenter, Concord Communication’s Aprisma, BMC Software Visualis, Open Service NerveCenter, and others. For point solutions, products include Concord Communication’s TrapExploder, Micromuse NetCool SNMP Trap Probe, and others. Shareware products include Net-SNMP’s snmptrapd.

When Security Becomes an Obstacle

SNMP traps can be received as long as the network path allows it. Increasingly, security policies are prohibiting the passing of trap traffic. The firewall becomes an obstacle, preventing these messages from reaching the trap receiver. For example, see Figure 1 depicting an agent failing to transmit SNMP traps to its Aprisma receiver.

Clearly, if the firewall blocks SNMP traps from the receiver, it is time to re-architect this part of the network management design. In the remainder of this paper, we will look at three possible solutions: (1) add a trap receiver on the DMZ side, (2) use a separate network management network, or (3) use a proxy trap receiver.
Solution 1: Add a Trap Receiver

A solution to the security policy issue of no SNMP traps through the firewall is to deploy a trap receiver in the DMZ (such as DNNM). Instead of the SNMP traps going through the firewall, it instead goes to the DMZ trap receiver server. The receiver then requires an instance of trap processing (or NMS) software. Some applications use TCP through the firewall (such as a web browser) that interfaces with the NMS software. This requires at least one firewall rule per trap receiver to allow the central server enterprise-side application to interface with the DMZ trap receiver. See Figure 2 below.

Figure 1. Security Policy Means the Firewall Blocks SNMP traps.

Figure 2. A Trap Receiver (DNNM) per DMZ Design
To implement this solution, you will need a trap receiver (DNMM) in every isolated DMZ that contains equipment to monitor, even if that DMZ only contains a few devices. For each trap receiver, you need to

1. Acquire and install a computer as the hardware for the receiver
2. Purchase and install the trap processing software
3. Add a firewall rule (or likely more) so the trap receiver can communicate with the enterprise-side NMS; perhaps this is just user web access from the enterprise, but more than likely it is more involved, depending upon your NMS.
4. Configure the servers to forward SNMP traps to new trap processing software

The advantage of this solution is:
1. It requires no more expertise to setup/configure trap receivers in a DMZ than ordinarily needed in the enterprise.

The disadvantages of this solution are:
1. The extra cost required for each instance of NMS software per DMZ
2. The additional hardware cost involved with those new NMS instances
3. The added labor cost involved with OS and NMS software setup
4. The delays or justifications with security to negotiate all those new firewall rules
5. The ongoing labor cost involved with OS and software maintenance/upgrades

Solution 2: Use Separate Network Management Network

Another solution to the security policy issue of no SNMP traps through the firewall is to deploy a parallel network management network. All devices generating SNMP traps need an interface dedicated to a network management traffic only subnet. The trap receiver is deployed as dual-homed with one interface on the corporate network and one interface on the network management network. SNMP traps are carried over the network management network to the trap receiver. The trap receiver communicates to the NMS over the corporate network (or it may be the same server).

To implement this solution, you will need a dedicated interface per device:
1. Dedicate an Ethernet interface on each server to the network management network
2. Dedicate an Ethernet interface on each router to the network management network
3. Connect your switch’s network management LAN port to the network management network. If your switch does not have a dedicated management port, then it cannot be part of this solution.
4. Add an extra network interface to the NMS
5. Configure all these dedicated interfaces to be on the same subnet

The advantages of this solution are:
1. This is a very low cost approach, presuming the dedicated interface cost is low.
2. There is no need for a dedicated NMS per DMZ
3. No proxy software or appliance is needed

The disadvantages of this solution are:

1. It may be difficult to get approval from your security group. Security groups consider the scenario where a DMZ device becomes compromised. In such a scenario, security may be concerned that attacking traffic may infiltrate the network management network. In turn, the attacking traffic could infiltrate the NMS before ultimately attacking the corporate network. Such an attack would circumvent the protection of the firewall, which is undesired.

2. Some network equipment (such as switches) do not have a dedicated network management interface, rendering this solution incomplete.

**Solution 3: Add a Proxy Trap Receiver**

Another solution to the security policy issue of no SNMP traps through the firewall is to deploy proxy receivers in the DMZ. Instead of the SNMP trap traffic going through the firewall, it instead goes to the proxy receiver. The proxy receiver in the DMZ then communicates to proxy software in the enterprise, which can be co-located with the enterprise-side trap receiver. The proxy software generates the SNMP traps for the trap receiver. The trap receiver conveys the messages to the application server, even if the

![Diagram Showing Solution 3: A separate network management subnet bypasses firewall]
trap processing software is located on a different server. This requires only one firewall rule to allow the proxy receiver to forward the messages.

One such proxy trap receiver is Tavve’s ZoneRanger system/network management appliance. It fits into the solution as shown in Figure 5 below.

![Diagram of proxy trap receivers sharing one central trap receiver design]

To implement this solution, you will need a proxy trap receiver in every isolated DMZ that contains devices generating SNMP traps. Several proxy trap receivers can report their messages to the same central trap receiver. For each proxy trap receiver, you need to

1. Acquire and install a proxy trap receiver appliance (ZoneRanger)
2. Add one firewall rule so the proxy trap receiver can communicate with the proxy software on the NMS
3. Configure the devices generating SNMP traps to send them to the new trap receiver.
If the proxy trap receiver is an appliance, such as ZoneRanger, you do not need to configure rules for system administrator or software maintenance access through the firewall to it. The one firewall rule that allows the ZoneRanger to communicate with the complementary Ranger Gateway software also allows configuration by web browsing to a Ranger Gateway port.

The advantages of this solution are:

1. The ZoneRanger appliance does not require system or software maintenance to setup or maintain – the system/network management support team configures it
2. No more additional trap receiver servers required than usual
3. Only one firewall rule (per proxy trap receiver) needed in firewall (easier to negotiate with security)
4. It can proxy all SNMP traps or it can selectively proxy some SNMP traps based on filtering criteria. Criteria are setup in named groups. Each group is a list of traps.
5. Aside from proxying SNMP traps, it proxies other network management traffic (SNMP, syslog messages, NetFlow, sFlow)

The disadvantage of this solution is:

1. It is a new tool, so some learning is required

Figure 5. Sample ZoneRanger Screenshot.
Conclusion

When the security policy of your enterprise prevents you from sending your SNMP traps to your enterprise-side central trap receiver, you can choose one of three solutions: (a) add a trap receiver into each isolated DMZ, (b) use a separate network management network, or (c) add a proxy trap receiver into each isolated DMZ. Depending upon product and ongoing administration costs, one solution may be more favorable than the other for your enterprise.

Product References