Remote OPNSense Monitoring with Zabbix

We had a request to monitor remote opnSense routers with Zabbix, and we wanted to do this as securely as possible. opnSense is an Open Source router firmware based on FreeBSD that can turn many devices into highly secure router/firewalls. As an Open Source project, there are many additional modules to work with such as Zabbix Agent and SNMP.

We modified the built in templates *FreeBSD by Zabbix Agent* and *OPNsense by SNMP* by cloning them and appending - *Daily Data* to the end of the name for some light customization we wanted.

Collect Information

1. From Router
    1. Get interface name of WAN network port (normally vtnet0 on virtuals)
        1. Interfaces | WAN | Device
    2. Get Host Name
        1. Lobby | System Information | Name
    3. Get public IP address
        1. Lobby | Interfaces | WAN
2. From Zabbix
    1. Get public Interface IP Address
        1. use something like whatsmyip.org from the LAN the Zabbix server is on, or just look at public IP of router Zabbix server is behind
3. Also create an SNMP Community name containing alphanumerics and underscores/dashes (no spaces, please)

Set up opnSense router

Note: most of the time, to add a plugin, your router firmware needs to be up to date. If you get a message about not being able to install a plugin, you may need to update your firmware.

1. Add Zabbix Agent and SNMP Daemon
    1. System | Firmware | Plugin
        1. os-zabbix6-agent
        2. os-net-snmp
2. Configure Zabbix Agent
    1. Services | Zabbix Agent | Settings
        1. Main Settings tab
            1. Enabled: check
            2. Hostname: name of router from *Host Name* above
            3. Listen Port: 10050
            4. Listen IP's: Public IP of the router
            5. Zabbix Server: Public IP of Zabbix Server
        2. Zabbix Features Tab
            1. Enable Active Checks: uncheck
    2. Configure SNMP Daemon

1. Services | Net-SNMP
    1. General Tab
        1. Enable SNMP Service: check
        2. SNMP Community: SNMP Community Name you created
        3. SNMP Location: Some string about where this is
        4. SNMP Contact: Some responsible party information
        5. Listen IPs: Public IP of the router
3. Set up firewall access
    1. Create an alias for the ports you need (161 for SNMP, 10050 for Zabbix)
        1. Firewall | Aliases | Add (plus sign)
            1. Enabled: check
            2. Name: monitoring
            3. Type: Ports
            4. Content: 161, 10050 (note, press comma or enter after each)
            5. Description: Ports needed for monitoring Zabbix and SNMP
        2. Click Apply Button
    2. Create rule to allow access only from the Zabbix server
        1. Firewall | Rules | WAN | Add (Plus sign)
            1. Action: Pass
            2. Quick: Check
            3. Interface: WAN
            4. TCP/IP Version: IPv4
            5. Protocol: TCP/UDP (Zabbix uses TCP, SNMP uses UDP)
            6. Source: Single Host or Network
                1. ip.of.zabbix.server/32
            7. Destination: WAN Address
            8. Destination Port Range:
                1. From: monitoring
                2. To: monitoring
            9. Category: Monitoring
            10. Description: Monitoring network traffic from Zabbix
    3. Save
    4. Apply Changes

Test from Zabbix Server

Log into your Zabbix server. This assumes you have snmpwalk and zabbix_get installed. If not, install them and test. It will save a lot of time. The first command returns several screens of data, the second command returns a single value (uptime, in seconds)

Test SNMP

```
snmpwalk -c SNMP_Community_Name -v 1 Public.IP.Of.Router
```

Test Zabbix Agent

```
zabbix_get -s Public.IP.Of.Router -p 10050 -k system.uptime
```

Set up Zabbix

Log into the webui of your Zabix server.

1. Configuration | Hosts | Create host
    1. Hostname: name of router that you created under Zabbix Agent
        1. Templates:
            1. FreeBSD by Zabbix agent
            2. OPNsense by SNMP
        2. Groups (these, or whatever you want)
            1. Remote
            2. Network Devices
        3. Interfaces | Add | Agent
            1. DNS Name: Resolvable DNS name of monitored router
            2. Connect To: DNS
            3. Port: 10050
        4. Interfaces | Add | SNMP
            1. DNS Name: Resolvable DNS name of monitored router
            2. Connect To: DNS
            3. Port: 161
            4. SNMP Version: SNMPv1
            5. SNMP community: SNMP community you created
            6. Use bulk requests: checked
            7. Description: free form to describe this server
            8. Enabled: checked
2. Click Add button

NOTE: I used DNS name for the SNMP and Agent addresses, but you can use IP address instead. Just choose IP instead of DNS in *Connect To*

The host will take about an hour to fully populate. It has to Discover all of the network interfaces, which only happens once an hour. But, you should see some data populated within 10-15 minutes. Wait for host to fully populate. In Monitoring | Hosts, you will see the number of graphs jump to 10-15, indicating it has found all of the network interfaces.

Create Dashboard (optional)

We created a Dashboard for the client named Remote, and we added all of the external traffic graphs to that, so I'll describe how that is done here.

1. Monitoring | Dashboard | Remote
2. Edit Dashboard
3. Add
    1. Type: Classic
    2. Source: Graph
    3. Graph: Find graph for Interface Name on router (from Discovery)

4. Show Legend: checked