Monitoring Servers And Services Behind a Firewall

Contents

Overview

Uptime Infrastructure Monitor can monitor services and servers globally from a single monitoring station. Communicating with servers across global networks can be complex and it can be difficult to monitor servers and services that are behind firewalls so you may need to apply special settings to address common security policies within your network.

This article provides a brief description of how to configure your firewall and Uptime Infrastructure Monitor to allow full monitoring of protected servers and services.

Monitoring Publicly Available Services and Servers Behind the Firewall

If a service or server is publicly available to the general network but is behind a firewall, you should not experience problems adding that service or server to Uptime Infrastructure Monitor for monitoring. To ensure that you are able to monitor all services and servers, follow these rules:

- Use the same hostname to add your system into Uptime Infrastructure Monitor as you would to normally access the system.
- Ensure that a port is open to accept incoming connections from the monitoring station. The default port is 9998; however, you can configure a different port for each agent.
- Ensure that the common port for any services that you want to monitor is open to accept incoming connections from the monitoring station. For example, to monitor an SMTP service behind your firewall, open port 25 for incoming connections on the firewall.
- All connections made to agent systems must originate from the monitoring station server.

Monitoring NAT Servers and Services Behind the Firewall

Monitoring Network Address Translation (NAT) addressed servers behind a firewall is slightly more complex. NAT addressed servers are available only to the private network behind the firewall, so you must adjust the firewall settings to allow additional access.

To allow monitoring of privately addressed servers:

1. Enable port forwarding on your firewall.
   Each server that you wish to monitor from outside the firewall must have a distinct port assigned to forward incoming connections to the correct NAT address. The exact procedure to enable port forwarding will depend on your firewall manufacturer (please contact your firewall vendor for assistance).
2. Create hostname alias addresses on the monitoring station for each NAT address behind the firewall that you want to monitor.
   For example, if your firewall address is fw with an IP address of 192.168.19.200 and you want to monitor the servers named mailbox and filestore, you must add the two named aliases to the firewall IP address.

   Creating and editing aliases for each server you would like to monitor is done on the monitoring station system by editing a local system file to recognize these aliases. The alias file can be found in the following locations on most common platforms:

   ```
   Linux and Solaris: /etc/hosts
   Windows: C:\WINDOWS\system32\DRIVERS\ETC\HOSTS
   ```

   The format for this file is the same across all platforms. The following is an example of the line you would add (or update) in this file to create aliases for the two NAT servers behind the firewall.

   ```
   192.168.19.200fw mailbox filestore
   ```

   > ⚠ **Note**
   >
   > Choose alias names that do not already exist on your network

   Ping all three addresses from the monitoring station to verify that the aliases have been properly created. If they have, you should receive a reply.

3. Add your servers into Uptime Infrastructure Monitor using the web interface.
   When adding each server, enter the alias that you have created in the Host Name field of the Uptime Infrastructure Monitor Add System window. Set the communications port to the port that you have assigned to be forwarded to the correct server through your firewall.