ESET Tech Center

Network Configuration Requirements for allowing clients to connect to ESET Security Management Center remotely

Anish | ESET Nederland - 2018-09-12 - Comments (0) - ESET Security Management Center

Issue

- Allow both internal and external (remote) clients to check in to a central ESET Security Management Center (ESMC) server

Solution

Requirements

- External clients must be able to communicate with the ESMC server on port 2222
- Internal and external DNS servers must be configured to point to the correct IP address of the ESMC server based on where the client is located

---

Network configuration steps

1. Create a NAT rule on your firewall/router that points traffic received on port 2222 TCP to the internal IP address of your ESMC server.

2. Add a new DNS record on your internal DNS server that points to the ESMC server (in the example below, a record would be created pointing avserver.example.com to 192.168.0.123).

3. Add a new DNS record via your domain name registrar that will allow clients outside of your internal network to locate the external IP of your ESMC server.

4. Make sure that all necessary ports are open on servers and client workstations.

Example scenario

In the example below, the external IP of the Corporate Firewall / Router is 89.202.157.256. The corporate edge device is set to forward traffic on port 2222 to the ESMC server. Therefore, example.com will point avserver.example.com to 89.202.157.256 so that clients external to the corporate network can communicate with the ESMC server.

Figure 1-1

KB Solution ID: KB6870 |Document ID: 25848|Last Revised: August 20, 2018