Configure Proxy Ports for Non-Standard Port Traffic on WSA 1000V

Contents

Issue

A WSA 1000V proxy hosted on VMware was processing client traffic correctly on ports 80 and 443, but was not processing traffic on non-standard ports such as port 8890. When access to a destination using a non-standard port was initially blocked by policy, the WSA correctly logged the blocked request. However, after adding the IP address and URL to an allow policy, the traffic still failed and no corresponding logs were generated on the proxy. This behavior suggested that the traffic was not reaching or being processed by the WSA after the allow policy was created, impacting client access to applications using non-standard ports.

Environment

- Cisco WSA 1000V proxy hosted on VMware
- Software version 15.0.0
- Traffic on ports 80 and 443 processing normally.
- Non-standard port traffic (for example, port 8890) not being processed by the proxy.
- Allow policies configured for affected destinations.

Resolution

The issue was resolved by configuring the WSA to support non-standard ports in the Identification Profile settings. The proxy ports configuration needed to be updated to include the required non-standard port numbers.

Configuration Steps

Step 1: Access the Web Security Manager interface.

Step 2: Navigate to the **Identification Profiles** configuration.

Navigate to **Web Security Manager > Identification Profiles**.

Step 3: Select the desired **identification profile** that requires non-standard port support.

Step 4: Expand the **Advanced configuration** options.

On the identification profile page, expand the **Advanced** tab.

Step 5: Configure the **Proxy Ports** setting.

Select the **link** next to **Proxy Ports** to access the port configuration.

Step 6: Add the required non-standard **port numbers**.

Add the specific **port numbers** that clients use for non-standard port connections (for example, 8890).

Step 7: **Save** and **commit** the configuration changes.

After implementing these configuration changes, the WSA is able to process and inspect traffic on the specified non-standard ports, allowing the proxy to properly handle client connections and apply policies to traffic using these ports.

Cause

The WSA 1000V was configured with default proxy port settings that only included standard HTTP (port 80) and HTTPS (port 443) ports. The identification profile proxy ports configuration did not include the non-standard ports required by the client applications. Without these ports being explicitly configured in the Identification Profile Advanced settings, the WSA was unable to intercept, process, or apply policies to traffic using non-standard ports, even when allow policies were configured for the destinations.

Related Content

- Cisco Technical Support & Downloads