### Subnet Groups

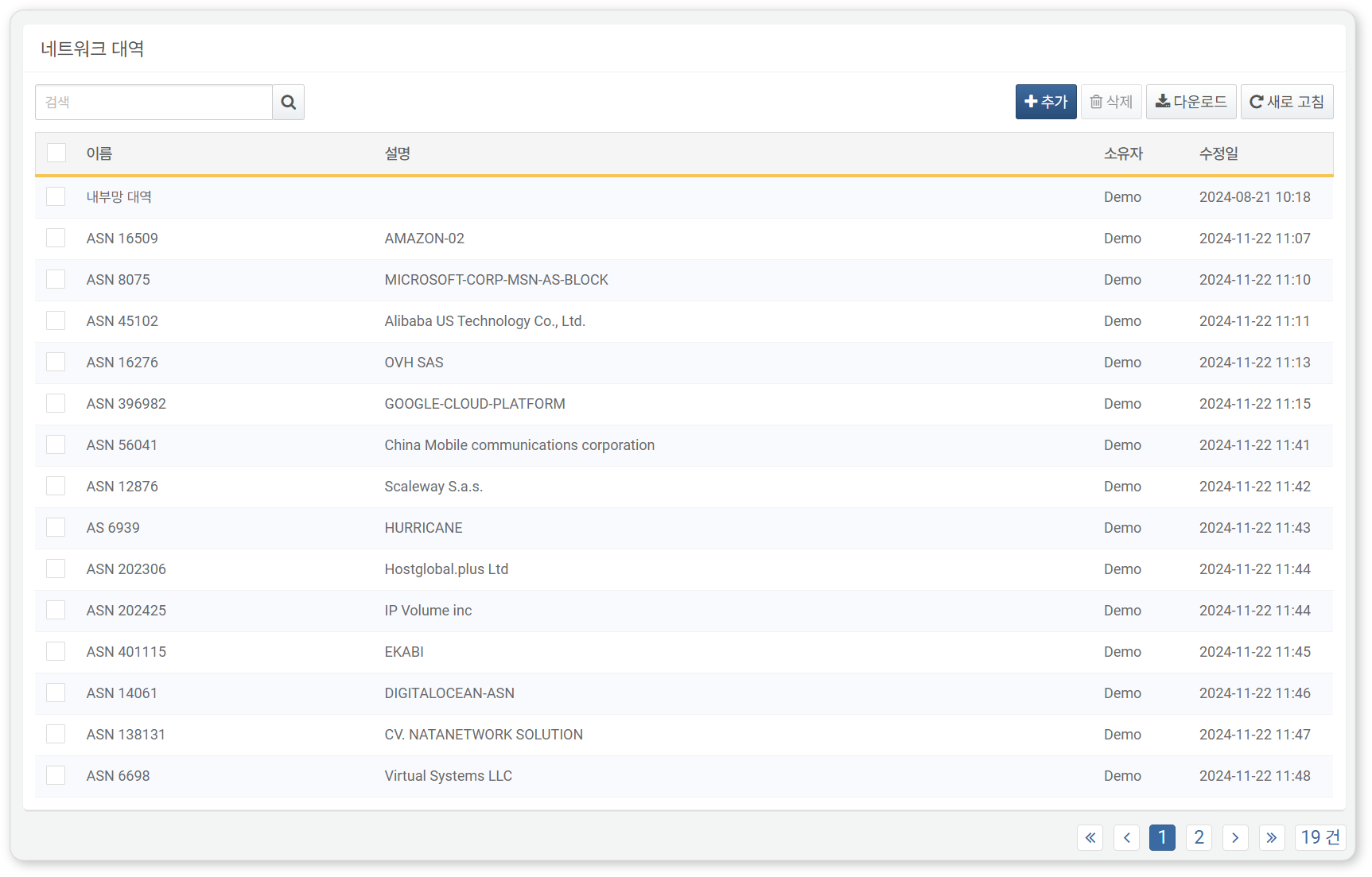
#### Overview

Subnet Groups support the management of IP address ranges by groups and enable their reflection in detection policies. They are typically used to define internal networks by groups and to monitor activities at network boundaries or to handle policy exceptions.

This feature only supports IPv4 addresses.

#### Viewing the Subnet Group List

You can view the list of subnet groups under **Policies > Subnet Groups**.



* **Name**: The unique name of the subnet group
* **Description**: A description of the subnet group
* **Owner**: The user account that added the subnet group
* **Modified Date**: The date the subnet group was created or last modified

Downloading the List

To download the subnet group list as a file to your local PC, click **Download** in the toolbar.

Refreshing the List

To refresh the list of subnet groups with the latest information, click **Refresh** in the toolbar.

#### Searching for Subnet Groups

To find a specific subnet group in the list, use the search tool in the toolbar. You can search by combining a single IP address, whitespace characters, and keywords, with the following behaviors based on the presence of whitespace:

If the search keyword does not contain whitespace, the search behaves as follows:

* **Inputting only an IP address**: Displays only the subnet groups that include the entered IP address.
* **Inputting only a keyword**: Displays only the subnet groups that include the keyword in their **Name** or **Description**.

If the search keyword contains one or more whitespace characters, the search behaves as follows:

* **Inputting both an IP address and a keyword**: Only one IP address can be entered as a keyword. Displays subnet groups that include the IP address and have the keyword in their **Name** or **Description**.
* **Inputting two or more keywords**: Displays only the subnet groups that include all keywords in their **Name** or **Description**.

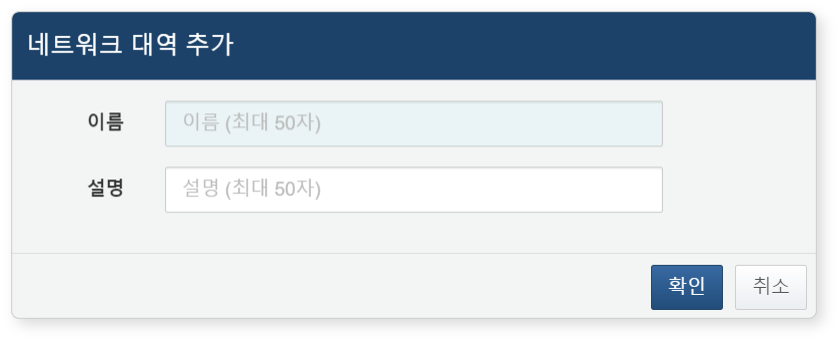
The search tool is case-insensitive.

#### Adding a Subnet Group

To add a subnet group:

Click **Add** in the toolbar on the [Subnet Group List](https://docs.logpresso.comnull).

In the **Add Subnet Group** dialog, enter or select the required values, then click **OK**.



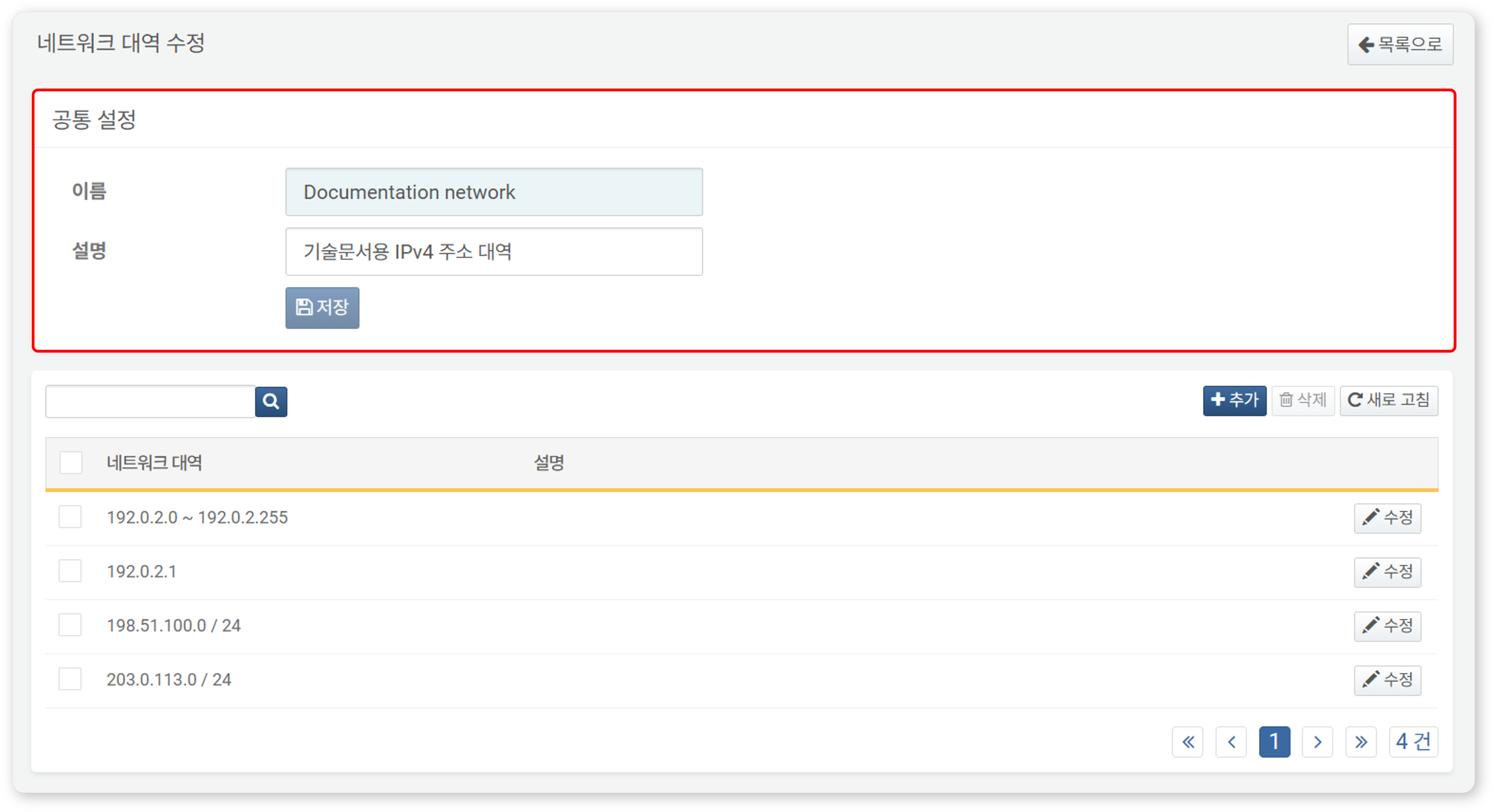
* **Name**: The unique name of the subnet group (up to 50 characters)
* **Description**: A description of the subnet group (up to 50 characters)

#### Modifying a Subnet Group

To modify a subnet group:

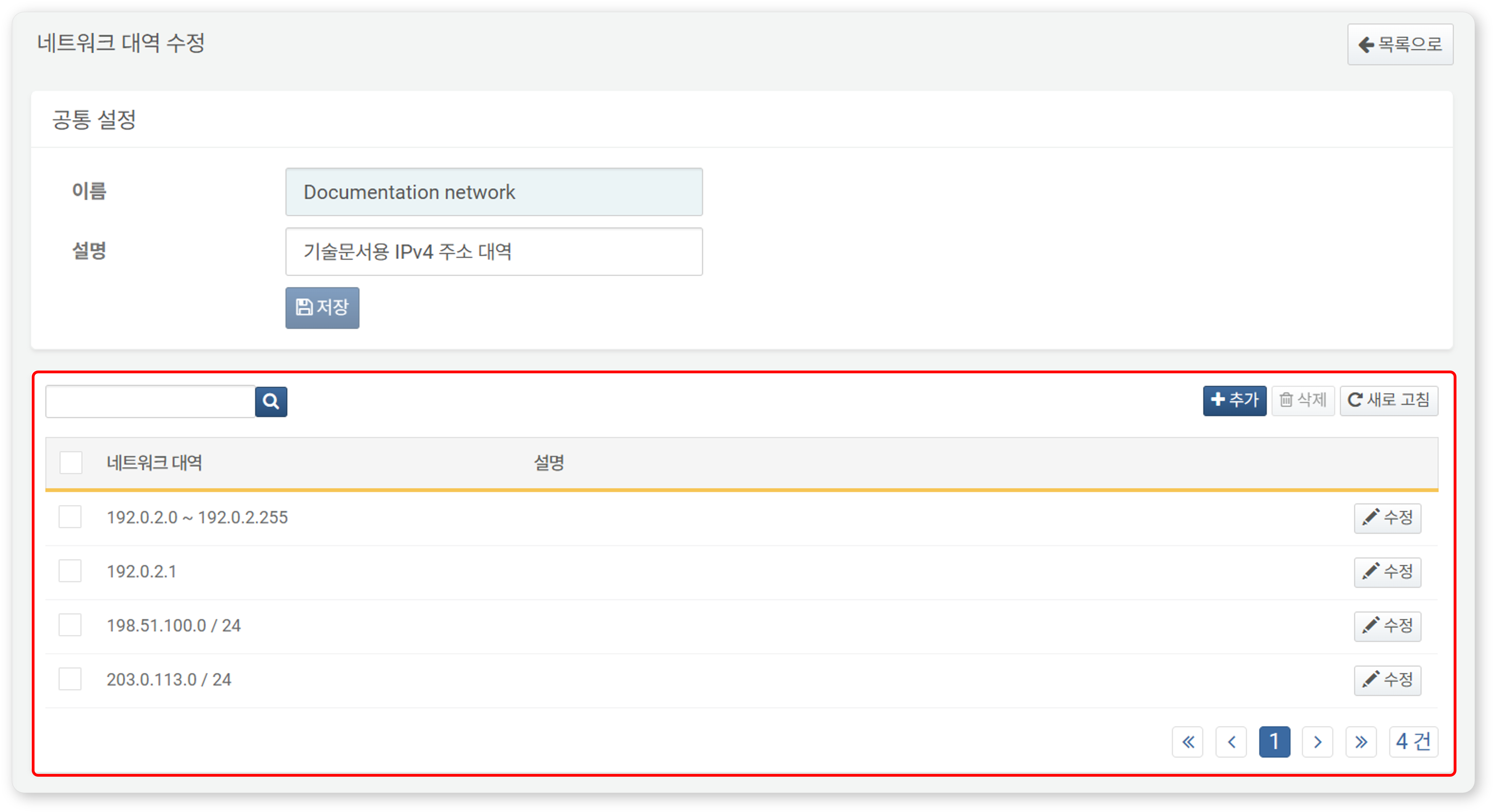
Click the **Name** of the subnet group you wish to modify in the [Subnet Group List](https://docs.logpresso.comnull).

In the **Modify Subnet Group** screen, update the information and click **Save**.



Viewing/Search Networks

You can view registered subnet groups in the **[Modify Subnet Group](section-subnet-group#outline8)** screen.



* **Subnet Group**: Information about the subnet group. The input format for the subnet group is displayed as a single IP address (e.g., 192.0.2.1), an IP address range (e.g., 192.0.2.1 ~ 192.0.2.254), or a CIDR network (e.g., 192.0.2.0/24).
* **Description**: Detailed description of the IP address.

The **Modify Subnet Group** screen also supports searching. This search function operates the same as described in [Searching for Subnet Groups](https://docs.logpresso.comnull), with the following differences:

* Searching for IP addresses within the subnet group in the **[Modify Subnet Group](section-subnet-group#outline8)** screen.
* Networks do not have assigned **Names**, so only those with the keyword in the **Description** will be displayed.

Adding Networks

To add a network to a subnet group:

Click **Add** in the toolbar on the **[Modify Subnet Group](section-subnet-group#outline8)** screen.

In the **Add Network** dialog, enter the network information to be added and click **OK**. The fields to be filled vary based on the selected **Type** (**IP Address Range**, **Single IP Address**, **CIDR**).

* When the **Type** is **IP Address Range**:
* **Start**: The first IPv4 address of the subnet group
* **End**: The last IPv4 address of the subnet group
* When the **Type** is **Single IP Address**:
* **IP Address**: The IPv4 address
* When the **Type** is **CIDR**:
* **Network Address**: The network address excluding the host part from the IPv4 address
* **Bits**: The subnet mask bits for the network address (1 to 32)
* **Description**: Detailed description of the network (up to 255 characters)

Modifying Networks

To modify a registered network in a subnet group:

Click **Modify** on the row of the network you wish to edit in the **[Modify Subnet Group](section-subnet-group#outline8)** screen.

In the **Modify Network** dialog, update the information and click **OK**.

Deleting Networks

To delete a registered network from a subnet group:

Select the checkbox for the network row you wish to modify in the **[Modify Subnet Group](section-subnet-group#outline8)** screen.

Click **Delete** in the toolbar.

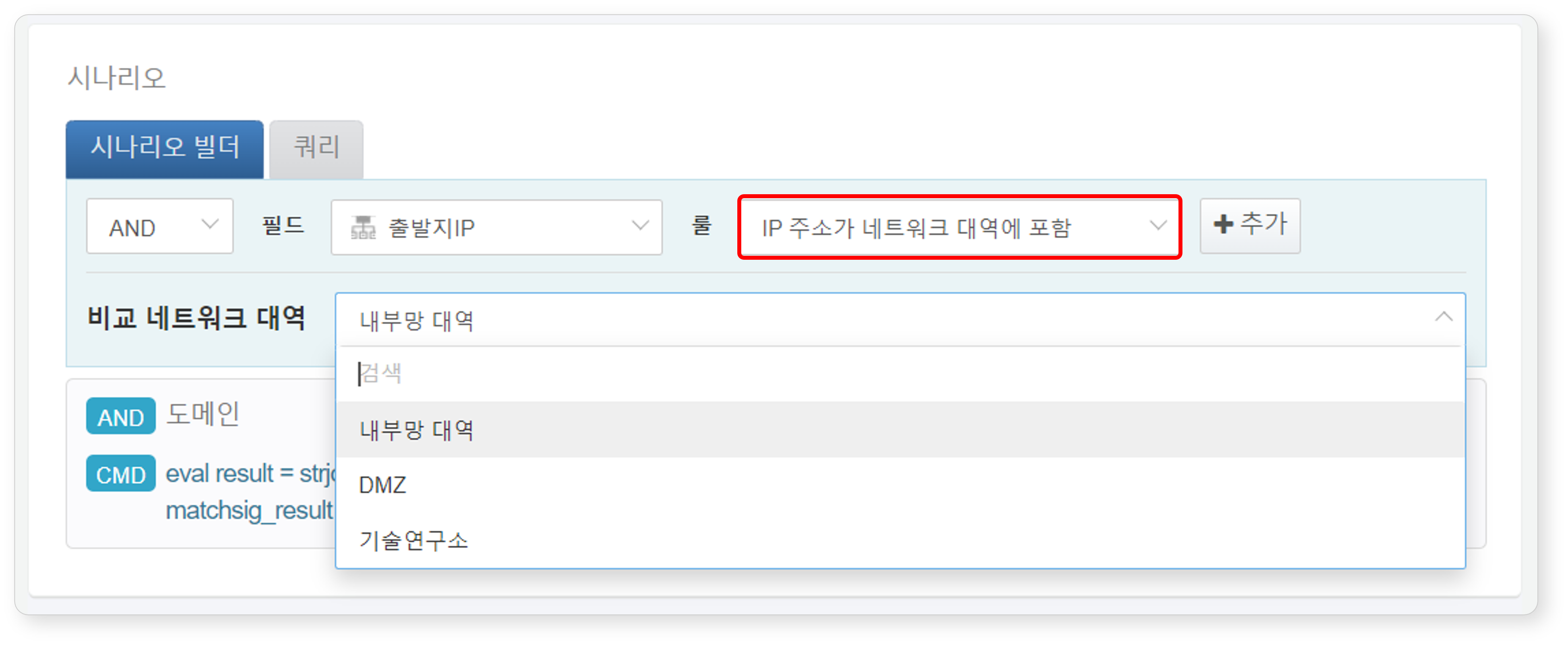
In the **Delete Network** dialog, review the list of networks to be deleted and click **Delete**. Click **Cancel** if you do not wish to delete.

#### Utilizing Subnet Groups

Subnet groups can be used in the following ways:

Scenario Builder

In **Policies > Real-Time Detection**, you can configure scenarios using the Scenario Builder to check if an IP address suspected of being a threat is already registered in an address group.



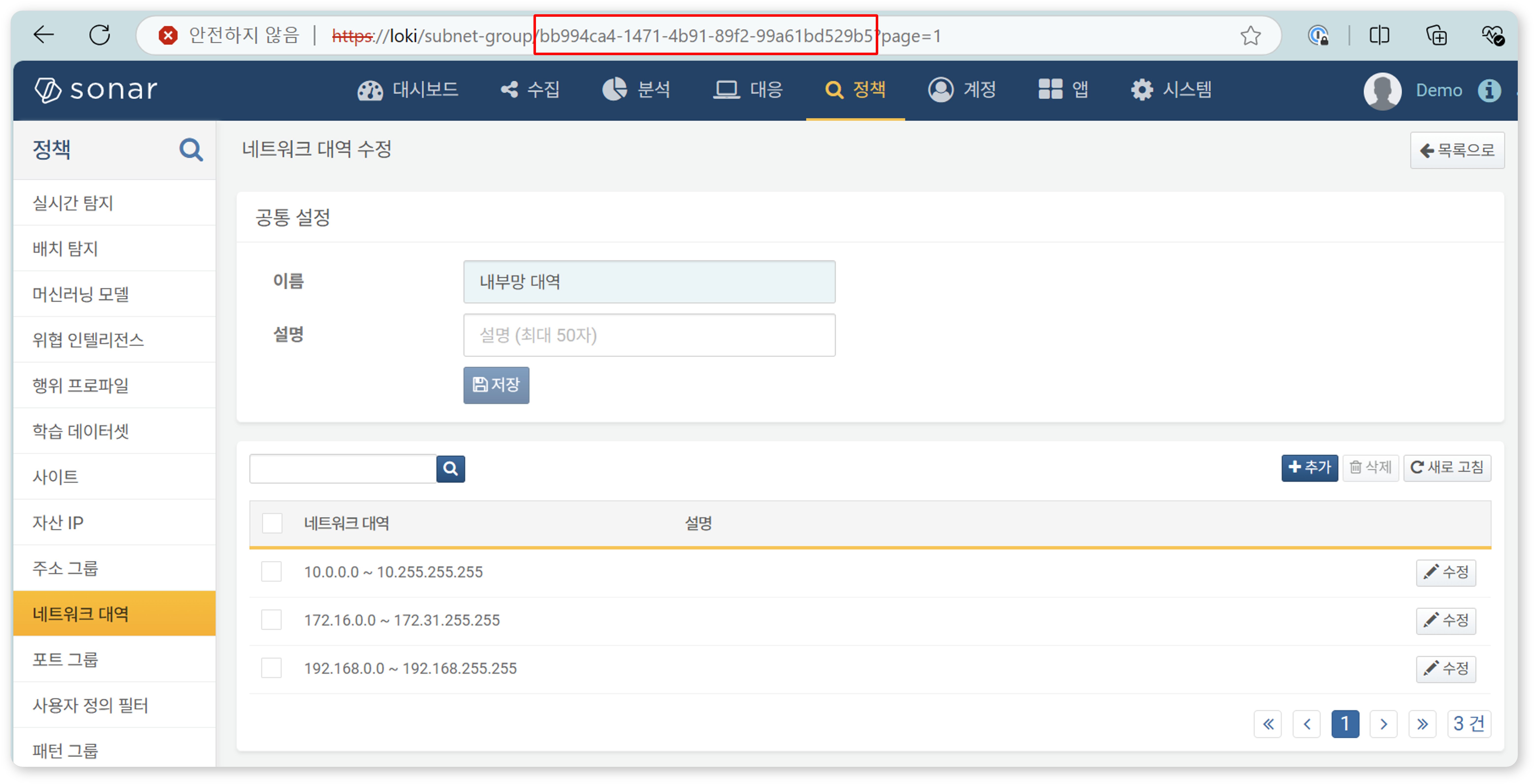
The following summarizes the subnet group-related content that can be used when the input field type is **IP** in the Scenario Builder. For more details, refer to [Rules and Parameters by Field Type](https://docs.logpresso.comnull).

|  |  |  |  |
| --- | --- | --- | --- |
| Rule | Parameter | Input Range | Description |
| IP Address is in Subnet Group | Compare Subnet Group | Select Subnet Group | Filters field values included in the subnet group |

Queries

When adding or modifying detection scenarios in **Policies > Real-Time Detection** or **Policies > Batch Detection**, you can utilize subnet groups with the [matchnet](https://docs.logpresso.comnull) command or the [matchnet()](https://docs.logpresso.comnull) function. Additionally, remember that you can use subnet groups wherever there is a feature to input query statements.

To use the matchnet command or matchnet() function, you need to know the GUID of the subnet group. The GUID can be found in the address bar of your web browser.



#### Deleting a Subnet Group

To delete a subnet group:

Select the checkbox for the row of the subnet group you wish to delete in the [Subnet Group List](https://docs.logpresso.comnull).

Click **Delete** in the toolbar.

In the **Delete Subnet Group** dialog, review the list of subnet groups to be deleted and click **Delete**. Click **Cancel** if you do not wish to delete.

Be cautious when deleting a subnet group referenced in real-time detection or batch detection scenarios, as it may cause the detection scenarios to not function as intended.