

Example: Using Profiler to Set a Baseline

A baseline is a place to start. Baseline data gives you the building blocks for your network security policy. The first time you use Profiler, the Profiler report will provide you with detailed views of the devices and applications that communicate in your network.

You use the baseline to:

- Determine which hosts to protect with security policies.
- Determine the applications that communicate over the network and therefore which services require protection in general.
- Determine specific operating systems and software versions in use and therefore which security policy attack objects are relevant and which may be exempted.
- Determine which security policy rulebases are relevant.
- Determine session contexts that can be safely ignored and those that should be monitored.

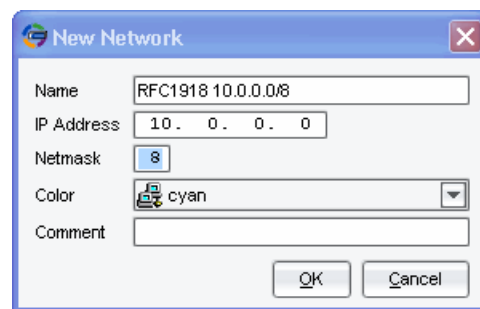
This example assumes a network that uses the private address space defined in RFC 1918: 10.0.0.0/8, 172.16.0.0.12, and 192.168.0.0/16.

To discover hosts and applications in your private network:

1. Use NSM to create network address objects for each of the three private address spaces.

Figure 1 shows the NSM network address object editor.

Figure 1: NSM Network Address Object Editor



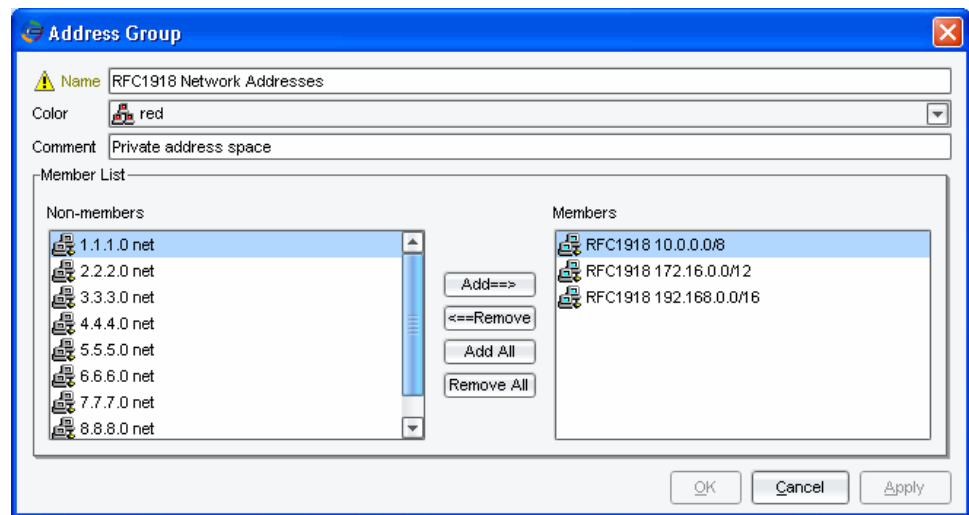
2. Create address objects for any additional networks or hosts that you are aware of.

The Profiler detects host and application information for all traffic that traverses it. If it cannot match the traffic to your network address objects, it assumes you are not tracking the host and populates the source or destination fields as **Non-tracked IP**.

3. Optionally, create a group object to contain the private address space networks.

Figure 2 shows the NSM group object editor.

Figure 2: NSM Group Object Editor



4. In the NSM Device Manager, right-click the IDP appliance and select **IDP Profiler** > **Start Profiler**.

Figure 3 shows how to navigate in NSM Device Manager to start Profiler.

Figure 3: Starting Profiler from NSM Device Manager

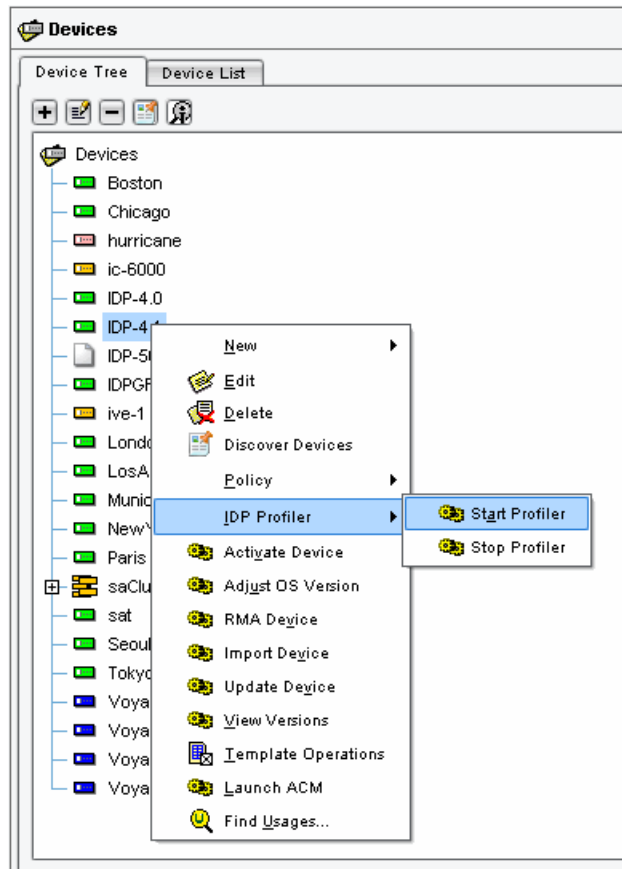
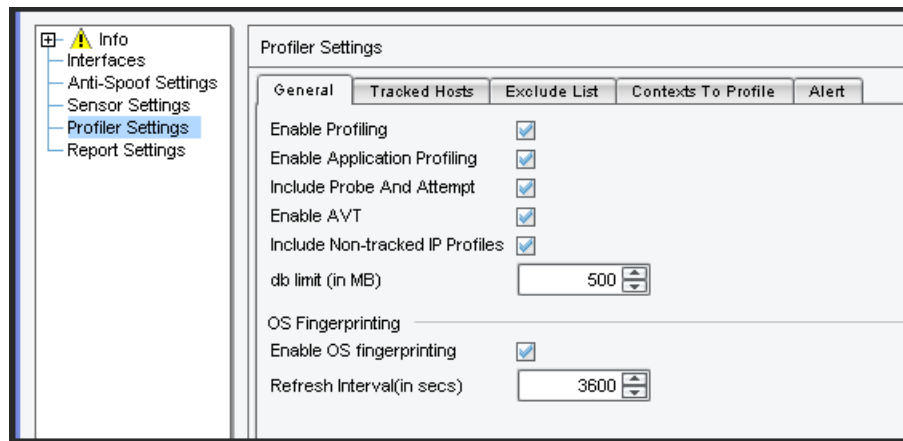


Figure 4 shows the Profiler configuration tabs.

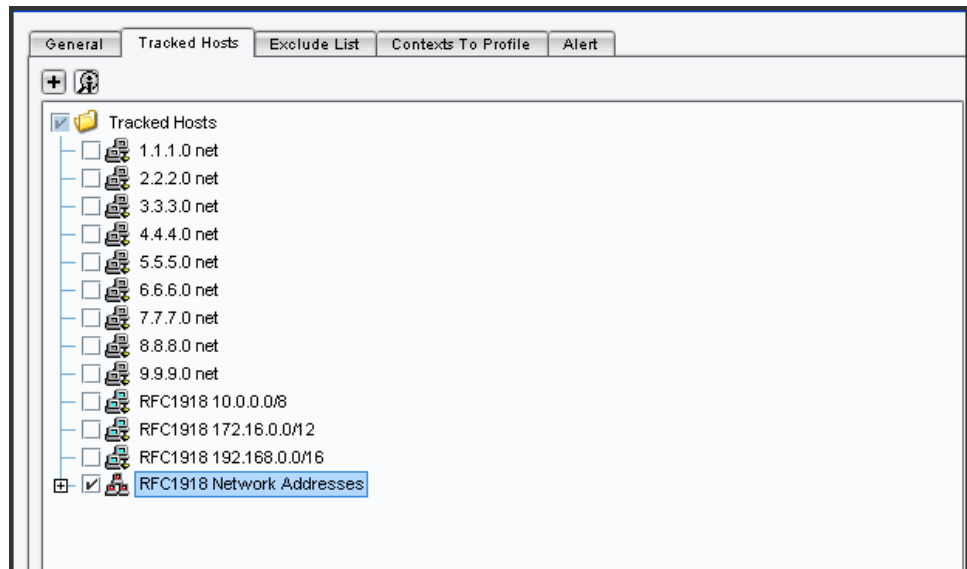
Figure 4: NSM Profiler Configuration Tabs



5. In the General tab, check the boxes to enable profiling, application profiling, OS fingerprinting, and non-tracked IP addresses.

6. Click the **Tracked Hosts** tab and add the address objects you created in Step 1. Figure 5 shows the Tracked Hosts tab.

Figure 5: NSM Profiler Tracked Hosts Tab

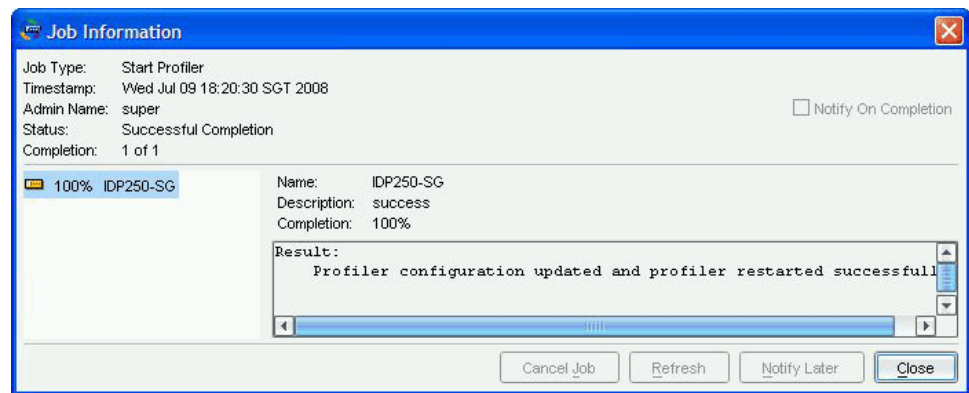


7. Click the **Contexts to Profile** tab and select all contexts.
8. Click the **Alert** tab and clear all alerts. You can use alerts after you have established your baseline but you do not need them in this initial procedure.
9. Click **Apply** to update the Profiler configuration and start the Profiler update job.

The Profiler detects network traffic that traverses the path of the IDP appliance. Consequently, it takes time to build the Profiler database. In most networks, critical services are used frequently and you might see data in five or ten minutes. For best results, let the Profiler run for a full business day to ensure that it has had enough time to monitor all pertinent network traffic.

Figure 6 shows the Job Information window that appears when the Profiler update job is completed.

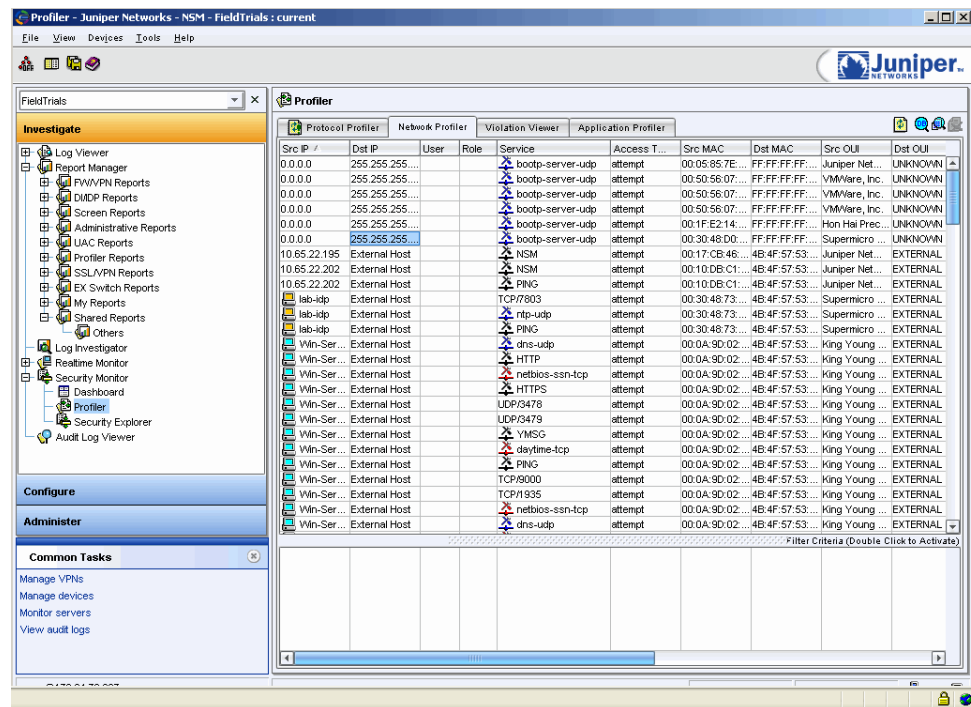
Figure 6: NSM Profiler Update Job Information Window



10. In the NSM navigation tree, select **Investigate > Security Monitor > Profiler** to display the Profiler viewer.
11. Click the **Network Profiler** tab and examine the data gathered about hosts in your network.

Figure 7 shows the Network Profiler tab.

Figure 7: Profiler: Network Profiler Tab



12. Optionally, use the Profiler data to create address objects and groups that you can later use when you create security policy rules.

For example, to create groups for SMTP servers, DNS servers, Windows AD servers, and, HTTP servers:

- Create group objects, such as SMTP, DNS, Windows AD, and HTTP.
- Use NSM UI features to filter and sort Profiler table rows by service.
- Double-click a destination entry to display the host editor, populated with data for the row you clicked.
- If you have created a group for the server type, such as SNMP, assign the host to the group.
- Click **Save**.

Related Topics The following related topic is included in the *IDP Concepts and Examples Guide*:

- Profiler Overview

The following related topic is included in the *IDP Administration Guide*:

- Profiler Task Summary

Published: 2010-01-12