# Chapter 10

# Protecting the Platforms

*Painting: The art of protecting flat surfaces from the weather and exposing them to the critic.*

—Ambrose Bierce (1842–1914)

When it comes to the cost of keeping computers in good working order, there is almost nothing worse than rogue software such as a computer virus to create immeasurable loss of productivity. In this chapter we will go over the Intel® Active Management Technology (Intel AMT) features that are intended to protect the computer and network from software attacks.

Much like repairing computers as discussed in the previous chapter, effective protection of computers and the network is best done with a combination of software- and hardware-based solutions. Many software-only solutions exist today, but they can all be themselves victims of attacks because they run within the operating system they are attempting to defend.

Paring software solutions with Intel AMT, a hardware module that can be trusted regardless of the operating system, forms a much more solid network protection story. The three features covered in this chapter are:

- System defense - hardware packet filtering
- Agent presence - software monitoring
- Heuristic filters - network attack detection

Each of these features work with each other and with software to provide an extra layer of network defense.

## System Defense

Starting with Intel AMT 2.0, Intel introduced the system defense feature, which is mostly a feature of the new Gigabit Ethernet adapter built onto the platform. This new onboard gigabit network adapter can perform shallow packet header inspection and filtering at gigabit speeds. Each time a packet is sent or received by the network interface, it is matched against a set of filters; the action associated with the first filter to match the packet will be performed. If no filter is matched, a specified default action is taken.

This simple hardware traffic matching engine built right into the Intel Gigabit adapter is at the core of the Intel System Defense feature. All the administrators need to do is to use Intel AMT to program the filters on the network adapter. Intel AMT provides a secure and authenticated path for the network administrator to set or clear these filters.

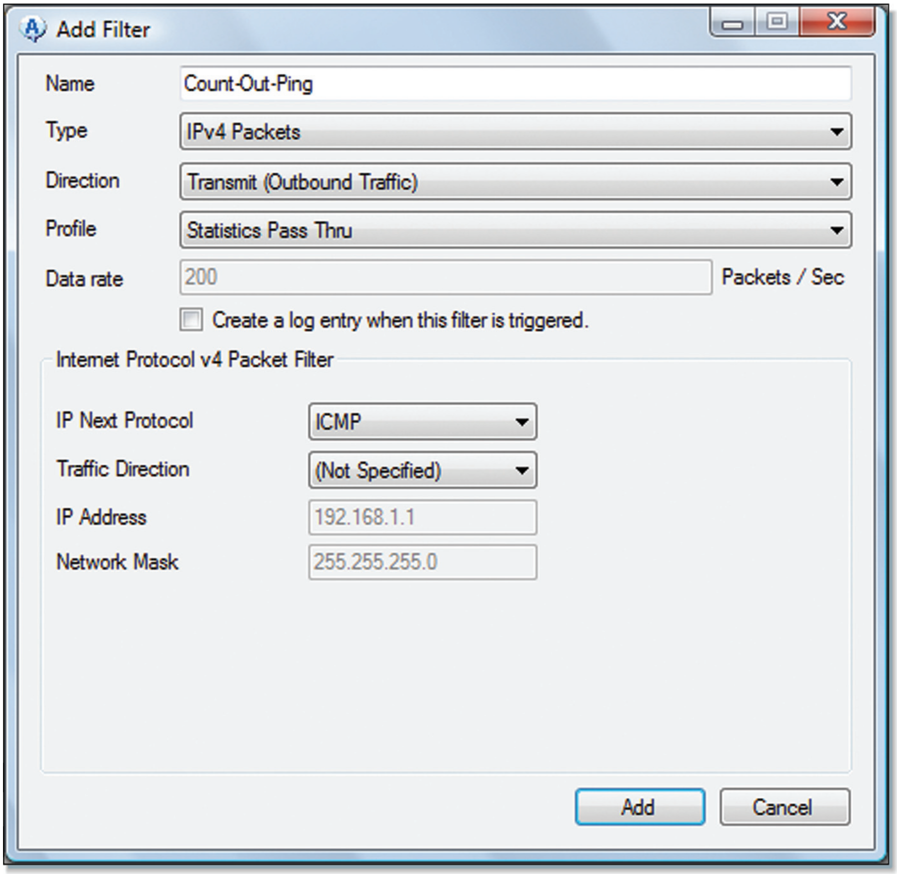
### Network Filters

Filters are the basic entities that are placed in the gigabit adapter that network packets are matched against. Each filter is composed of the following information:

- **Name** – A human readable name for the filter that is at most 16 characters in length.
- **Direction** – A flag indicating if inbound or outbound traffic is to be matched. If traffic much be matched in both directions, two filters must be created.
- **Profile** – Action to be taken can be one of these: allow the packet through, limit this type of packet to a set number per second, or drop the packet. Regardless of the action taken, the packet can also be counted, incrementing one of the hardware counters in the network adapter.
- **Log when triggered** – Log an event in the event log and possibly send an alert when this filter is triggered for the first time.

- **Type** – The type of filter. There are 7 possible filter types:
  - Ethernet
  - IPv4, IPv4/UDP, IPv4/TCP
  - IPv6, IPv6/UDP, IPv6/TCP
- Each of these filter types has a set of additional parameters that must be filled in to perform proper matching.

The detail of how a filter is defined is best described in the Intel AMT SDK, as shown in Figure 10.1. We should note that the definition of a filter varies a little depending if EOI/SOAP or WS-Management is used to communicate with Intel AMT.



Add Filter

Name: Count-Out-Ping

Type: IPv4 Packets

Direction: Transmit (Outbound Traffic)

Profile: Statistics Pass Thru

Data rate: 200 Packets / Sec

□ Create a log entry when this filter is triggered.

Internet Protocol v4 Packet Filter

IP Next Protocol: ICMP

Traffic Direction: (Not Specified)

IP Address: 192.168.1.1

Network Mask: 255.255.255.0

**Figure 10.1** Setting Up a Filter to Count Outgoing ICMP Packets

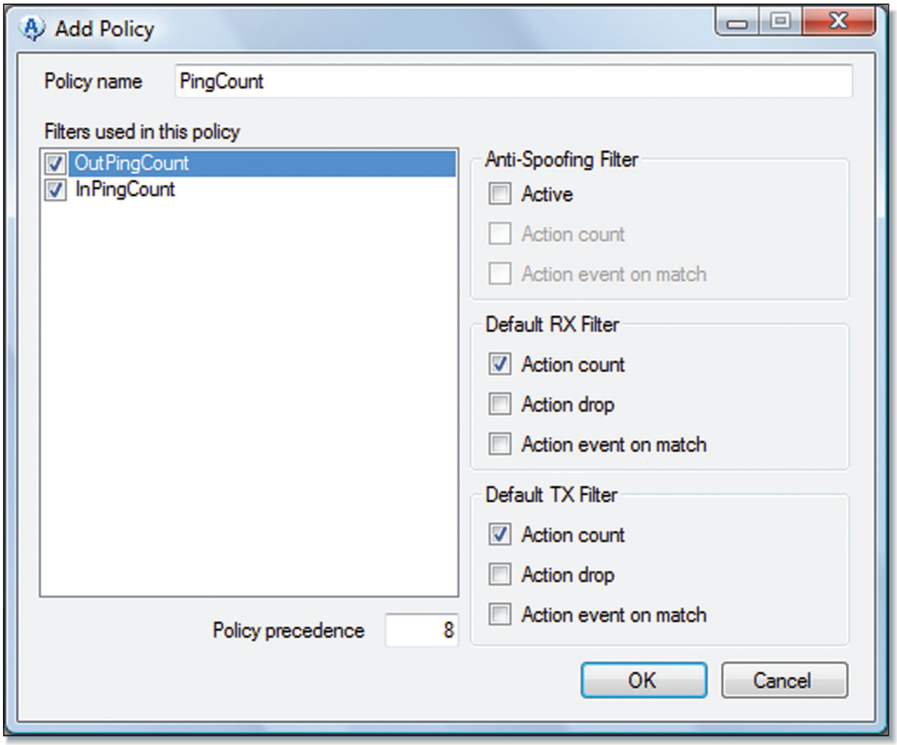
When defining a filter, a common issue involves the confusion over the traffic direction. In Intel AMT Commander, the Direction dropdown list at the top indicates if this filter looks at traffic going in or out of the Ethernet adapter. Further down, in the IPv4 traffic header information, there is a second direction field. This second field indicates which IP address to look at, IPv4 source or target address. The target or outgoing IPv4 address is the address of the other computer on the network. The source or incoming IPv4 address is the address of this local Intel AMT computer. The source (local) and target (remote) address are used the same way, regardless of packet direction.

In general, 16 or more filters can be active in each traffic direction on the Ethernet adapter at any given time. The precise number depends on the version of Intel AMT.

### Network Policies

Once network filters are defined and set up in Intel AMT, they must then be added into a System Defense policy, which is a group of zero or more filters as shown in Figure 10.2. Filters on their own can't be enabled on the hardware; they must be part of a policy and only one System Defense policy can be active at any given time.

A policy also includes three default filters that indicate what to do when none of the network filters match a packet.



Add Policy

Policy name: PingCount

Filters used in this policy

☑ OutPingCount
☑ InPingCount

Anti-Spoofing Filter

□ Active
□ Action count
□ Action event on match

Default RX Filter

☑ Action count
□ Action drop
□ Action event on match

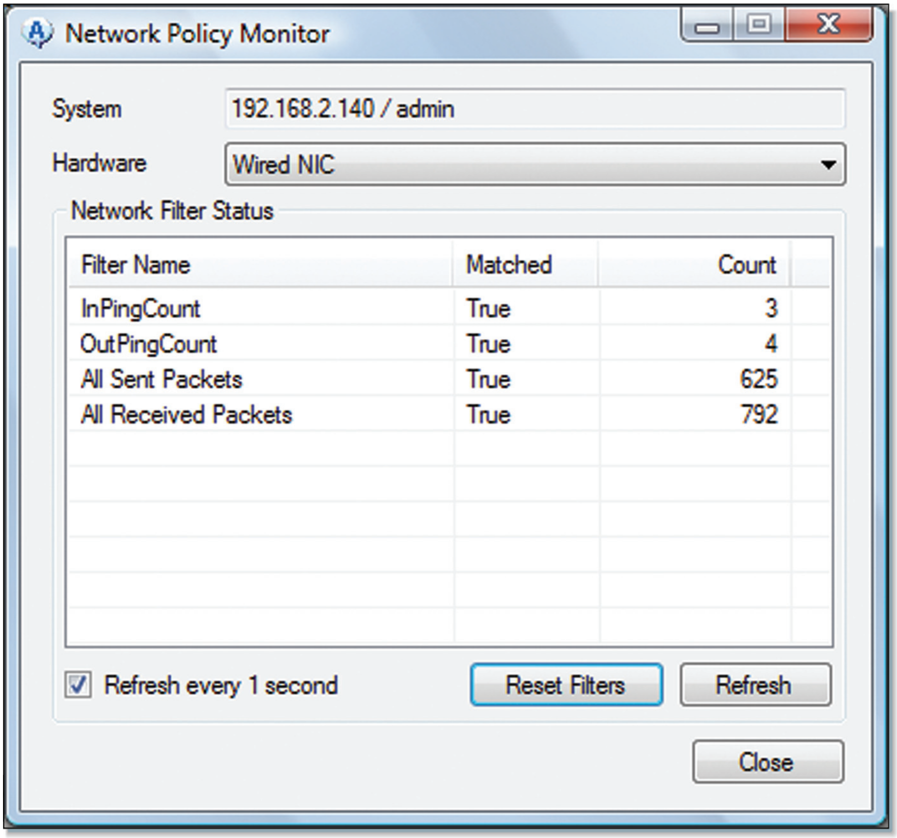
Default TX Filter

☑ Action count
□ Action drop
□ Action event on match

Policy precedence: 8

**Figure 10.2** Intel® AMT Commander Window for Adding a New System Defense Policy

As shown in the example in Figure 10.3, an administrator creates two network filters for counting ICMP packets, one inbound and one outbound. A policy is then created that includes both these filters and sets the default action to count the packets. Once this policy is made active on the network interface, Intel AMT will start counting ICMP packets both inbound and outbound and all packets that don't match the filters both inbound and outbound.



System 192.168.2.140 / admin

Hardware Wired NIC

Network Filter Status

| Filter Name | Matched | Count |
|---|---|---|
| InPingCount | True | 3 |
| OutPingCount | True | 4 |
| All Sent Packets | True | 625 |
| All Received Packets | True | 792 |

☑ Refresh every 1 second

**Figure 10.3** Intel® AMT Commander Screen Showing System Defense Traffic Counters

Because of how Intel System Defense policies can be defined, it is possible to limit traffic on a given port, IP address, or subnet by placing a Pass-through filters for the allowed inbound and outbound traffic and place a Drop All default action on the policy. This way, if none of the filters are matched, the packet is simply dropped. This can be very useful in situations where a computer has been compromised and the administrator wants to severely limit the other network nodes a computer can communicate with.

It is important to note that System Defense filters and policies never apply to Intel AMT traffic. It is not possible for example to block Intel AMT port 16992 using a System Defense filter. In fact, Intel AMT traffic would not even be counted or processed in any way. This means that it is possible to add a new policy with no filters and a default action of Drop All on both send and receive to deny all packets from going to the operating system. Still, Intel AMT and features such as Serial-over-LAN and IDE redirect would still work properly.

### Anti-Spoofing Filter

When setting up a new System Defense policy, each policy comes with three default filters, the default transmit, default receive, and anti-spoofing filters. The anti-spoofing filter only looks at outbound packets and checks to see that the sender IP address matches the IP address of Intel AMT.

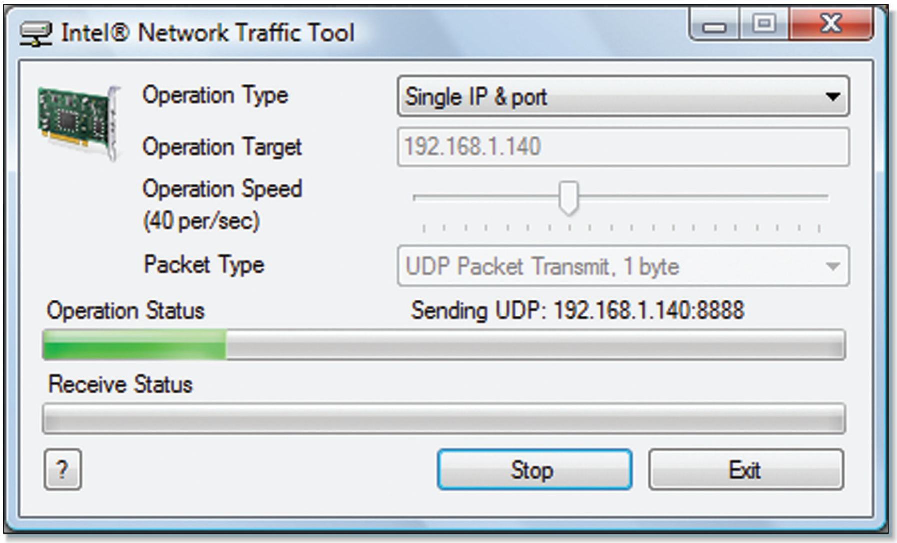
In other words, if the OS attempts to send a packet on the network that have a return address that does not match the real IP address on the Intel AMT computer, the anti-spoofing filter will catch it. As of Intel AMT 5.0, only IPv4 packets are looked at.

Spoofing an IP address is a typical way to attack another computer while trying to mask the real source of the attack. In general, it's a good idea to block such packets. There are rare occasions, especially on servers that are multi-home, for which this filter would not be desirable. For work desktops and laptops, making use of the anti-spoofing filter is a good idea.

### Rate Throttling Filter

A little known feature of Intel AMT System Defense is the rate throttling filter support. To use this feature, simply create a usual filter such as an outgoing UDP match all filter, set the filter profile to Rate Throttling, and set a rate of 10 packets per second. Add this filter as part of a policy and activate the policy.

At this point, no more than 10 packets per second can leave the computer at any time, and surplus packets will be discarded. Someone can test this feature using the Intel AMT Net Traffic tool. This time, run Intel AMT Net Traffic on two computers, the computer using Intel AMT and another one on the network, as shown in Figure 10.4



Intel® Network Traffic Tool

Operation Type: Single IP & port

Operation Target: 192.168.1.140

Operation Speed (40 per/sec)

Packet Type: UDP Packet Transmit, 1 byte

Operation Status: Sending UDP: 192.168.1.140:8888

Receive Status

**Figure 10.4** Intel® Network Traffic Tool Set Up to Send Packets to a Single Target IP Address

By setting the Intel Network Traffic Tool to send packets at a rate of 40 packets per second and the filters limiting it to 10 packets per second, the result will be very clear on the computer receiving the packets. Intel AMT Commander can be used to activate and deactivate the System Defense filter to see the difference in received packets.

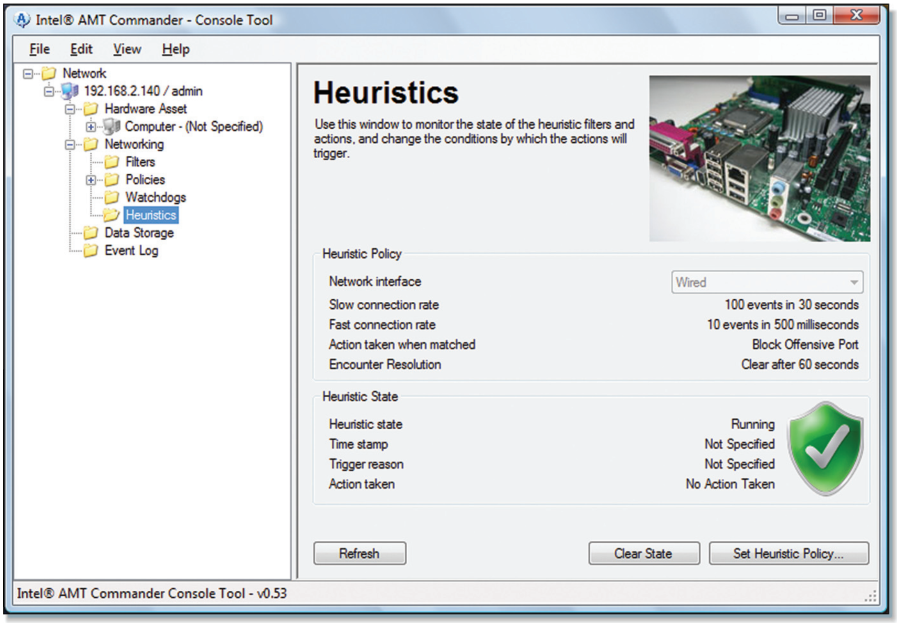
Rate throttling packets can be very useful in preventing unwanted network flooding. It can be used to limit packets sent to a single IP or port, all packets or subnet. Inbound rate throttling can be used to protect running OS applications from packet floods.

## Heuristic Filter

Starting with Intel AMT 3.0, Intel introduced a new feature called the heuristic filter to help defend the network. Viruses can cause wide spread damage on computer systems. In the late 1990s there were stories in the media of viruses causing complete network shutdowns and large corporations would tell employees walking in the office in the morning to stay off computers. These rapidly propagating viruses created a great deal of damage and lost productivity. With Intel AMT 3.x and AMT 5.x, Intel has attempted to provide a new defense against IP address scanning viruses, called heuristic filters.

With this new feature, Intel AMT monitors outgoing network traffic and attempt to detect a IP address scanning pattern and stop it. To be clear, this feature is not a defense against viruses; rather, it blocks the Intel AMT computer from attacking other computers on the network.

At the hardware level, the gigabit Ethernet interface sends a sample of the outgoing traffic to Intel AMT for analysis. Intel AMT only gets a sub-sample because at gigabit speeds, Intel AMT management engine is not sufficiently fast to handle all that traffic. Within that sample, Intel AMT attempts to look for interesting events such as opening a TCP connection or sending a UDP packet to a new IP address. Most of these interesting events are fairly typical and should not be of concern. However, if the frequency of the interesting events rises above a threshold set by an administrator, a potential attack is detected and Intel AMT can take action. In Figure 10.5, Manageability Commander is monitoring the state of the heuristic filter in an Intel AMT 3.0 computer.



Heuristics

Use this window to monitor the state of the heuristic filters and actions, and change the conditions by which the actions will trigger.

Heuristic Policy

| | |
|---|---|
| Network interface | Wired |
| Slow connection rate | 100 events in 30 seconds |
| Fast connection rate | 10 events in 500 milliseconds |
| Action taken when matched | Block Offensive Port |
| Encounter Resolution | Clear after 60 seconds |

Heuristic State

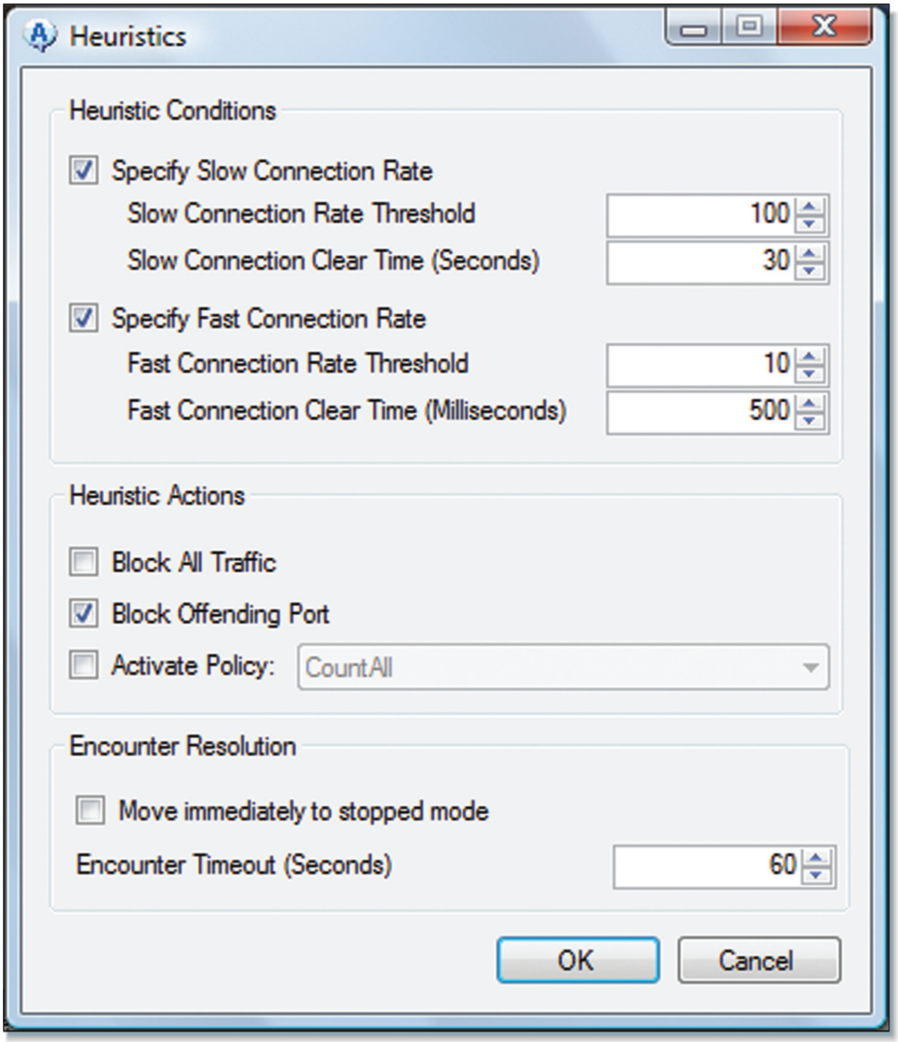
| | |
|---|---|
| Heuristic state | Running |
| Time stamp | Not Specified |
| Trigger reason | Not Specified |
| Action taken | No Action Taken |

**Figure 10.5** Monitoring the State of Heuristic Filters

## Heuristic Policy

The heuristic filter feature is enabled and set up by the network administrator. The feature must be set up and enabled with triggering thresholds and actions to be taken once the filter is activated.

Intel AMT Commander provides an easy way to set up heuristic filter policies and actions as shown in Figure 10.6. Again, this feature is only available on Intel AMT 3.x and 5.x, so Intel AMT Commander will not display this feature when connected to other versions of Intel AMT.



Heuristics

Heuristic Conditions

☑ Specify Slow Connection Rate

Slow Connection Rate Threshold: 100

Slow Connection Clear Time (Seconds): 30

☑ Specify Fast Connection Rate

Fast Connection Rate Threshold: 10

Fast Connection Clear Time (Milliseconds): 500

Heuristic Actions

□ Block All Traffic

☑ Block Offending Port

□ Activate Policy: CountAll

Encounter Resolution

□ Move immediately to stopped mode

Encounter Timeout (Seconds): 60

**Figure 10.6** Intel® AMT Commander Heuristic Policy Setup

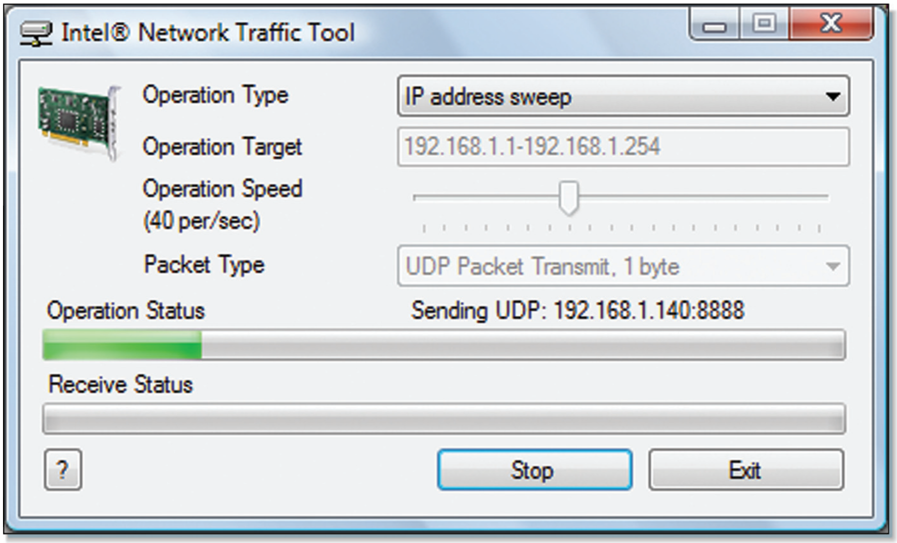
The Intel AMT Commander dialog box is separated into three parts. The heuristic conditions at the top are what will cause the heuristic filter to trigger. The administrator can set up to two thresholds, a slow and a fast one. The slow threshold will count for a given number of interesting events between 1 and 50 seconds. The fast counter count events between 10 to 1000 milliseconds. Two counters allow an administrator more flexibility in setting heuristic policy trigger. The generally recommended values are 100 events in 30 seconds or 10 events in 500 milliseconds. This recommendation comes from looking at previous IP address–scanning viruses.

Once the heuristic trigger is set up, the administrator must specify what action to take. The choices are to block all network traffic, block the offending outgoing port only, and/or enable a specified System Defense policy.

Lastly, the administrator can opt to keep the resulting action permanent, or allow it to expire after a certain time. If the action is permanent, the administrator will have to reset the heuristic filter manually.

### Heuristic Filter Demonstration

In an attempt to demonstrate heuristic filters in real life, the Intel AMT DTK provides a tool called Intel AMT Net Traffic as shown in Figure 10.7.



Intel® Network Traffic Tool

Operation Type: IP address sweep

Operation Target: 192.168.1.1-192.168.1.254

Operation Speed (40 per/sec)

Packet Type: UDP Packet Transmit, 1 byte

Operation Status: Sending UDP: 192.168.1.140:8888

Receive Status

**Figure 10.7** Intel® AMT Network Traffic Tool

It's a small traffic generation tool that can be used to artificially trigger the heuristic filter. Once the heuristic policy is set up and active, run this tool on the computer with Intel AMT and perform an IP address sweep using a range of IP addresses outside the local network subnet.

Why scan outside the local subnet? It so happens that Microsoft Windows will block outgoing traffic within the subnet to IP addresses that don't exist. As a result of this existing filter in the Microsoft operating system, Intel AMT will never see any unusual events within the local subnet.

Intel AMT Commander is built to poll the state of the heuristic filter every 5 seconds when the UI is looking at the heuristic state, so starting the IP address sweep should result in a displayed change in the state without a few seconds.

### Heuristic Filter Limitations

It is important to also know the limitations of the heuristic filter feature. The Intel AMT heuristic filter should not be used as a replacement for OS-level firewall and virus protection software.

Since there is only one heuristic filter and it no longer works once triggered, if the resulting action is to block the offending port only it is possible for another attack on a different port to work. In other words, someone could trigger the heuristic filter using one outbound port and then, while the heuristic filter is not looking anymore, launch an IP address port scan on a different outbound port.

On the other hand, if the action taken is to block all ports, it may be possible to cause a denial of service attack, using Intel AMT to stop all work on this computer.

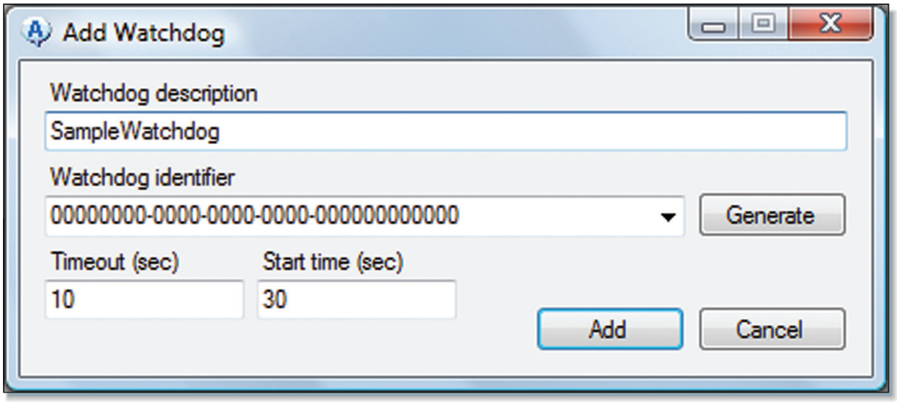
Another limitation of the heuristic filter has to do with how it analyzes the interesting events. Someone playing around with the Intel Net Traffic Tool will notice that if both the target IP address and port change during the scan, the heuristic filter no longer triggers.

## Agent Presence

Proper management of a computer must include management based on both hardware and software. With agent presence, Intel AMT attempts to serve as a trusted entity that can help monitor running applications in the operating system. This is done by creating what is called a *watchdog GUID* in Intel AMT and then having an OS application register and perform a "heartbeat" on that GUID at regular intervals.

This way, Intel AMT can report to the management console the registration and heartbeat state of a given GUID, indicating to the administrator that an OS-level application is running correctly.

To get started, the administrative console must first create a watchdog as shown in Figure 10.8. This is done by calling the ConsoleWatchdogCreate method that is part of the AgentWatchdogRemote SOAP service[1].



Add Watchdog

Watchdog description: SampleWatchdog

Watchdog identifier: 00000000-0000-0000-0000-000000000000

Timeout (sec): 10

Start time (sec): 30

**Figure 10.8** Intel® AMT Commander Window for Adding an Agent Presence Watchdog

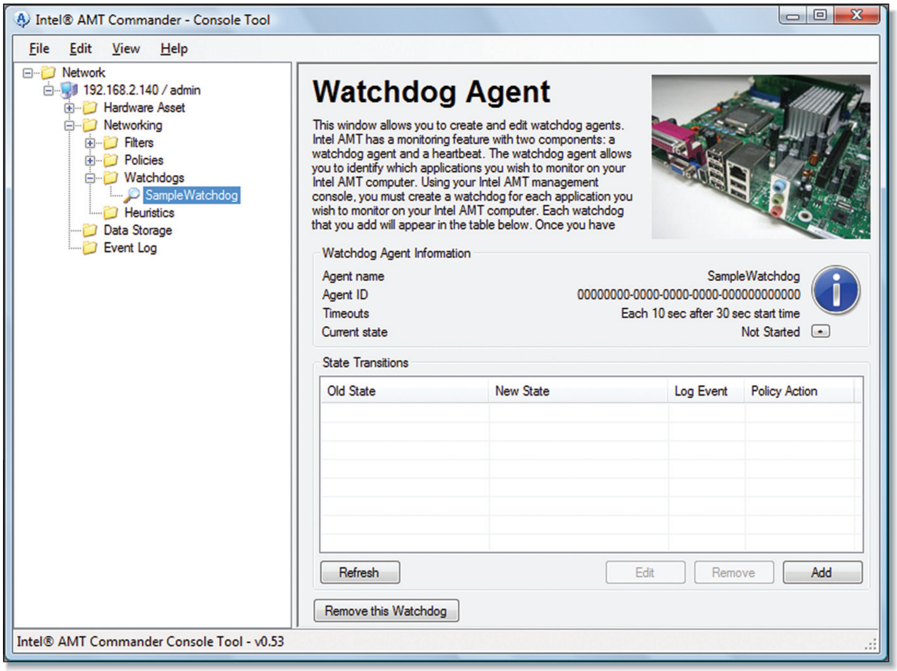
A watchdog must specify a name, GUID, heartbeat time, and start time as shown in Figure 10.9. The human-readable name is only used to help the administrator track this watchdog. The watchdog GUID is important and should uniquely identify an application. The timeout is the maximum amount of time an application has to perform a heartbeat. Beyond this time, something wrong is assumed to have occurred to the application such as an unexpected error and closure. Lastly, the start time is the maximum time expected between the power up of the computer and the start of this application. If a computer is booted up and the application is never loaded, this start time will pass and something incorrect is assumed to have happened. For example, something must have prevented the application from starting up.

Once a watchdog is added to Intel AMT, it can have one of five states:

[1] See the Intel AMT SDK for a complete list of methods and services.

- **Not Started** – Occurs when the watchdog was just added or the computer was just powered on and the watchdog is waiting the start up amount of time specified by the administrator.
- **Stopped** – The OS application performed a correct exit.
- **Running** – The application is correctly running.
- **Expired** – The application was expected to be running, but has not reported. Either the application did not start, or it stopped unexpectedly.
- **Suspended** – The computer is in an Sx sleep state and OS-level applications are not currently running.

A watchdog can change state at any time. The state of a watchdog can be polled by a management console, but these states will be especially useful when looking at performing automatic actions based on state transitions.



Watchdog Agent

This window allows you to create and edit watchdog agents. Intel AMT has a monitoring feature with two components: a watchdog agent and a heartbeat. The watchdog agent allows you to identify which applications you wish to monitor on your Intel AMT computer. Using your Intel AMT management console, you must create a watchdog for each application you wish to monitor on your Intel AMT computer. Each watchdog that you add will appear in the table below. Once you have

Watchdog Agent Information

Agent name: SampleWatchdog
Agent ID: 00000000-0000-0000-0000-000000000000
Timeouts: Each 10 sec after 30 sec start time
Current state: Not Started

State Transitions

| Old State | New State | Log Event | Policy Action |
|---|---|---|---|

**Figure 10.9** Intel® AMT Commander Displaying a Watchdog State

### Application Heartbeat

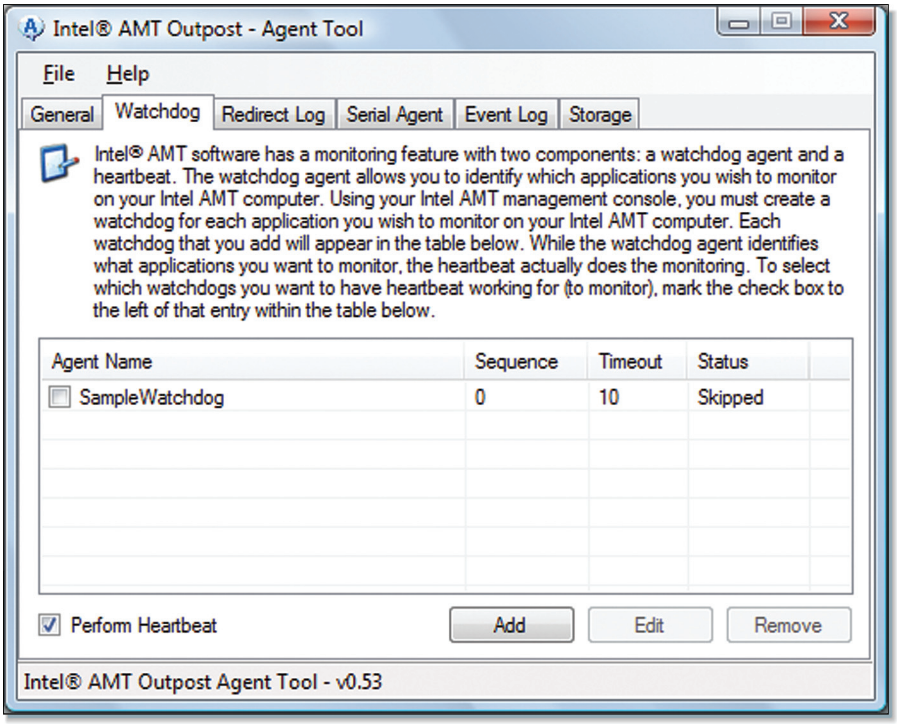
Once a watchdog is created by the management console, it's time to run software that will perform the heartbeat of the watchdog GUID. This software must run on the computer with Intel AMT with an MEI driver and Local Manageability Service (LMS) that are working correctly.

First, the local software must authenticate to the LMS using HTTP or HTTPS and then use the following methods on the AgentWatchdogLocal service:

- **AgentWatchdogRegister** – Register to start performing heartbeats on a watchdog. The registration call will provide the application with the maximum time internal for the watchdog.
- **AgentWatchdogHeartbeat** – Perform a heartbeat on a watchdog; this must be called periodically after registration is made.
- **AgentWatchdogShutdown** – Stop performing heartbeats on a watchdog; must be called before existing the application.

These three methods are simple and allow the application to report to Intel AMT it's proper running state. The registration to a watchdog will also provide the application with a sequence number that must be incremented and used everytime the application performs a heartbeat or shuts down the agent. This sequence number prevents other applications from easily spoofing the heartbeat.

For people who want to try performing agent registration and heartbeat for demonstration's sake, the Intel AMT DTK includes an application called Intel AMT Outpost. This agent tool, shown in Figure 10.10, includes agent presence support.



Intel® AMT software has a monitoring feature with two components: a watchdog agent and a heartbeat. The watchdog agent allows you to identify which applications you wish to monitor on your Intel AMT computer. Using your Intel AMT management console, you must create a watchdog for each application you wish to monitor on your Intel AMT computer. Each watchdog that you add will appear in the table below. While the watchdog agent identifies what applications you want to monitor, the heartbeat actually does the monitoring. To select which watchdogs you want to have heartbeat working for (to monitor), mark the check box to the left of that entry within the table below.

| Agent Name | Sequence | Timeout | Status |
|---|---|---|---|
| □ SampleWatchdog | 0 | 10 | Skipped |

☑ Perform Heartbeat

Intel® AMT Outpost Agent Tool - v0.53

**Figure 10.10** Intel® AMT Outpost Used to Perform Agent Presence Operations

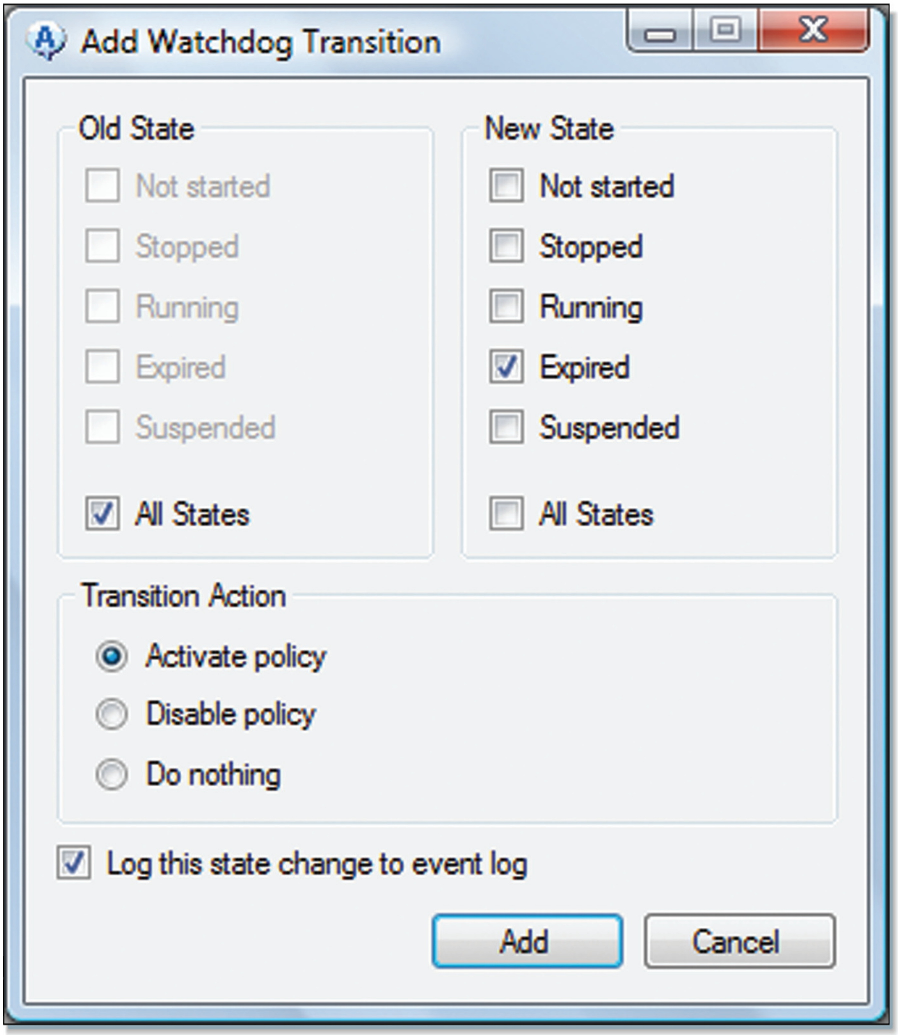
Intel AMT Outpost allows a user to add watchdog GUIDs and perform correct registration and heartbeat by checking the box next to the watchdog. A user can also set up Outpost to perform heartbeat when a given process such as Notepad is running. This is very useful for demonstrations. Ultimately, critical applications such as corporate agents, anti-virus applications, and firewall applications should select and publish a GUID on which they will attempt to perform heartbeat whenever possible. It is also important for software vendors to publish a way for administrators to provide a username and password for the software to locally log in to Intel AMT. Administrators should create a local-only account for the purpose of performing heartbeats.

### Taking Action

Now that we know how to create a new watchdog agent remotely and perform local heartbeat on it, it's time to see what we can do with the watchdog state information.

Intel AMT provides for each watchdog agent a way to attach an action to a state transition. For example, an administrator can specify that whenever a firewall GUID changes to the expired state, an event is logged into the Intel AMT event log and a 'Block All' System Defense policy is activated. When the firewall software goes back online, the System Defense policy can be disabled.

The administrator can set up a rule that states "when going from any state to the expired state, activate the agent presence policy and log the event to the event log." Causing the event to be logged will also cause a network alert to be sent to management consoles if they are subscribed to receive events. In Figure 10.11, we see the dialog box used by Intel AMT Commander to set up such a rule.



Add Watchdog Transition

Old State

□ Not started
□ Stopped
□ Running
□ Expired
□ Suspended

☑ All States

New State

□ Not started
□ Stopped
□ Running
☑ Expired
□ Suspended

□ All States

Transition Action

● Activate policy
○ Disable policy
○ Do nothing

☑ Log this state change to event log

**Figure 10.11** Intel® AMT Commander Window for Configuring an Action Based on a State Transition

A limitation of agent presence actions is that only one system defense policy can be set to be activated per network interface (one for wired, one for wireless). Once selected, the circuit breaker policy will be enabled when a change in transition occurs.

Any transition can be set to disable the current system defense policy, regardless of what the currently active policy is. You can disable the current one, but you can only enable a single set policy.

One way to get around this limitation is for a management console to actively receive the network alert indicating that a state transition has occurred and manually activate or disable a system defense policy. This active approach is more flexible, but requires the computer to be connected on the managed network. For laptops, having Intel AMT activate a policy on its own is much more useful since it will work regardless of where the laptop is.

## Summary

Using a combination of software and hardware is the best way to effectively protect a network of computers from attack. This chapter covered the three Intel AMT system protection features. System defense and heuristic filters can be used right away, without the need of any specialized software running on each PC. Agent presence support should be added to mission critical software to help monitor their correct operation and make sure to take appropriate action if it is not the case. In the end, making correct use of these features can save lots of time and money the next time an unexpected attack occurs.