

## The ImproveNet Initiative for a Community-Based Exchange of Firewall Configurations

*Strengthening your firewall's protection - automatically*

### As Threats Have Increased, So Has the Firewall's Complexity

The rapid growth of Internet usage, as evidenced by the increase in the number of online users, rising connection speeds, and the spread of Web-enabled services and platforms, has unfortunately not all been for the good. Hackers and other malware developers have created a breeding ground for Internet-based attacks targeting confidential data, PC performance, and the integrity of corporate networks. Unpatched vulnerabilities and a lack of timely security updates contribute to increasing security problems.

Software firewalls serve as a reliable deterrent to hacker attacks because they put a virtual shield around the host computer and prevent malicious or unauthorized Internet communications to and from the machine, protecting it from hacker attacks and malware intrusions. While an anti-virus acts reactively by checking and removing a virus from the computer, a firewall is designed to be proactive, preventing the virus from getting onto the computer in the first place by constantly monitoring all connection activity and dropping non-compliant data packets.

Firewalls, because of their relative complexity and sophistication, can often require a degree of technical knowledge on the part of the user in order to be configured in a way that will provide the highest level of security. While antivirus operation is more straightforward – basically, you get a file and make certain it's virus-free by running it past a virus scanner - firewalls need input from you in order to 'know' whether a particular type of Internet access or network activity is permissible.

Novice users are the most affected by firewalls' action prompts because they don't have the experience to know how to respond to them – how would they know whether the "iexplore.exe" program requesting Internet access via port 80 of an HTTP protocol is normal? After seeing a few questions like this, the chances are they will simply give up using the firewall altogether, or simply allow the connection without any deliberation, which is of course not a good solution.

The problem is exacerbated for all users, not just beginners, by the number of applications that require Internet access today. As a result, even experienced users can end up with a misconfigured system and compromised security. Whether it's a lack of time in which to research the correct access parameters or simply a lack of available information, users need help in making their firewall configuration as tight as needed without it getting in the way of online activities.

Agnitum recognized the need to provide users with an easier and more reliable way to help users configure their firewalls correctly, and thus securely. The result was the development of ImproveNet, a system that automates not only most of the firewall configuration through our own security experts' judgment but also the distribution of those configurations to participating users.

### The Essence of the Program

ImproveNet is a system for optionally collecting users' Outpost Firewall Pro access configurations, having Agnitum security experts review them, and then to create new application access rules and global firewall settings that can be distributed back out to users. The goal of the system is to learn about as many

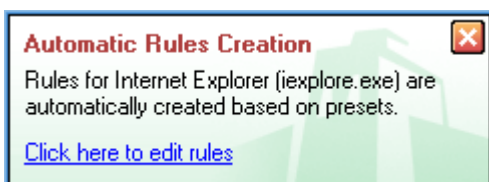
Internet-accessing applications as possible and be able to automatically configure and implement access rules for them for end users.

## ImproveNet and What It Means for You

ImproveNet makes the process of creating Internet access rulesets automatic by distributing new access configurations to users. As it is impossible for one vendor to know about all of the network- and Internet-enabled applications in existence, the community helps accumulate reports and produce precisely secure firewall access rules based on them.

Creating rules for applications in Outpost is now significantly easier than in previous versions or competing firewalls. ImproveNet relieves users of the need to develop all their firewall security rules themselves by giving them the option to network with other Outpost users and Agnitum engineers to share configurations and gain access to universally-applicable Internet access security rules. Users simply check a box in the Outpost interface to give their permission for rules they create to be automatically reported to Agnitum engineers. The engineers check the rules for validity and then automatically distribute them to all other users through the Agnitum Update tool.

Users benefit by seeing far fewer action prompt windows, ensuring a less-interrupt-driven computing experience, because Outpost will apply automatic presets based on the rules, adjusted by other users. And because they do not need to manually create their own rules, the primary cause of firewall failure – configuration errors – is removed, increasing security while reducing user input. Updates are delivered daily, so the need to manually configure rules is minimized.



**This screenshot illustrates the benefits of having ImproveNet - collaborated access rules automatically applied on the user PC – no pop-up prompts; the firewall is automatically configured to work with the Internet-requesting program.**

## Detailed Information

ImproveNet is a network community that brings Outpost users and Agnitum engineers together to optionally share configurations and enable everyone to benefit from universally-applicable Internet access security rules. By participating in the ImproveNet service and having their application rulesets be applied automatically following ImproveNet collaboration, users can adjust their application access rules to protect against the latest threats. These settings are created, transferred and applied automatically if this feature is enabled, so that users no longer need to worry about how to respond to the next action prompt window – because ImproveNet adjustments mean that the window won't appear in the first place.

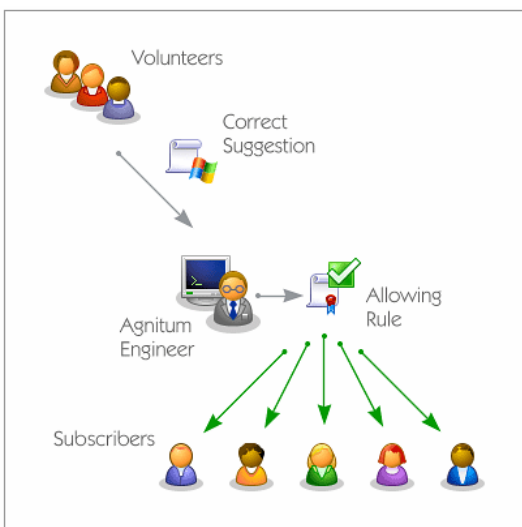
The principle behind the ImproveNet service lies in security experts evaluating the preset access rules in use by the community of Outpost Firewall Pro users. After the rule is checked for validity and approved, it is automatically distributed to all other users through the Agnitum Update tool. Because new rules are created and processed on a daily basis, users have a continuously-updated set of access rules for the majority of Internet-enabled programs, sparing themselves the need to manually create their own rules and removing the possibility of errors in rule structure and application.

Users receive only approved, secure configurations and are safeguarded against malicious or

inappropriate ones. To exclude erroneous configurations from the pool of newly distributed rulesets, Agnitum security experts review every submitted user configuration, evaluate it from a security and interoperability standpoint, and produce the final and the most secure presets based on the information collected. Below is an illustration that shows how different users' configurations are treated and what the final outcome is in relation to the three proposed configuration types submitted by users:

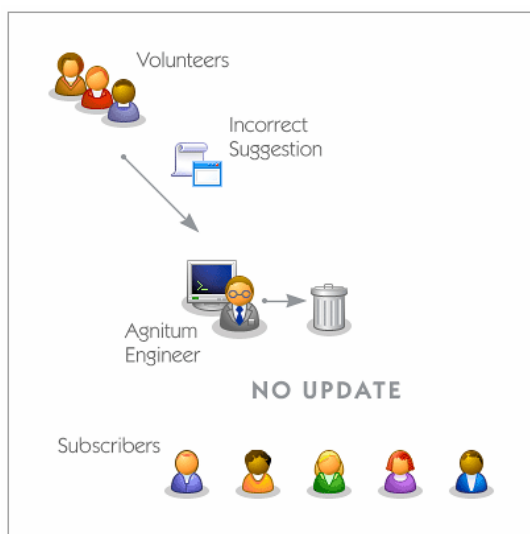
### Scenario #1

An ImproveNet contributing member submits a new application's access configuration to be evaluated by an Agnitum specialist. After the specialist has looked at the user's rule and approved it, the corresponding allowing ruleset is created and distributed to other ImproveNet participants, simplifying the task of making correct access configurations for new programs:



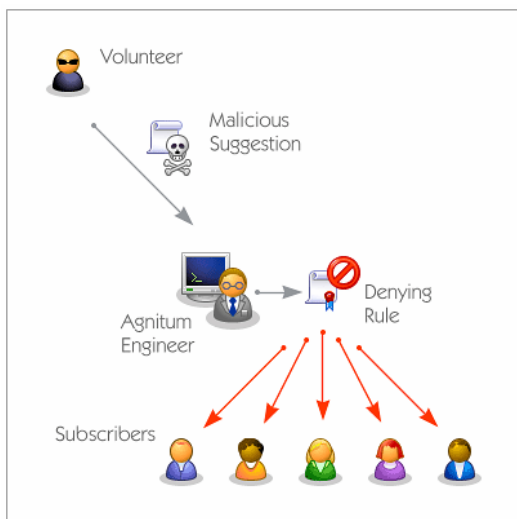
### Scenario #2

The situation is the same as in the previous scenario, but here the volunteer sends out an incorrect or incomplete rule for the program, for which no effective rule can be developed. The Agnitum specialist looks at the rule and, based on his best judgment, determines that no ruleset should be issued. As a result, the volunteer's rule is dropped.



### Scenario #3

In this case, a volunteer sends out a malicious configuration, either by mistake or intentionally, and after the specialist has looked at the rule he specifically decides that a denying ruleset for the application should be created and distributed to subscribers. As a result, recipients get a firewall configuration that automatically prevents network access for a new piece of malware.



### ImproveNet Options

By default, the ImproveNet service is designed to work in conjunction with the automatic application of firewall rules to Outpost Firewall – meaning the process is two-stage. First, the user firewall's network accessing configuration is sent for Agnitum's review, and secondly, the approved configuration is returned to the user community and automatically applied to the users' PCs.

Users can opt to not have new firewall rules applied automatically without their interaction by selecting the appropriate checkbox on the program's interface. In this way, they can still participate in the ImproveNet program by sending out their configurations and thus helping other community members by supplying configuration information, but will see an action prompt following the initiation of a new connection on their computers. New presets will still arrive through the Agnitum Update service, but they won't be automatically applied, and users will have to select the action, even though the action will be recommended based on the information stored in readily available presets.

Advanced users who prefer to make things themselves and control applications' access parameters manually would appreciate the ability to have a recommended set of rules to follow while the final decision is left to them.

### ImproveNet FAQ

#### What is the ImproveNet system and why is it useful for me?

ImproveNet is a system of optionally collecting users' firewall configurations and having Agnitum security experts review them centrally and create new application access rules and global firewall settings to be distributed to users. The goal of the system is to learn about new Internet-accessing applications promptly and prepare automatic configuration rules so you don't have to do it manually.

## **What information is sent to Agnitum from my computer, and how might that change in the future? How can I be confident that no personal information is sent to you?**

The only information sent to Agnitum is data which helps to identify a web-enabled application when it requests network or Internet access, along with the technical details of that connection. In future versions, additional information that impacts new functionality, such as component control, may be added, but you can rest assured that nothing will be transmitted to our engineers that personally identifies you. Here is a complete list of the data sent:

For the application: name, version number, local path, fingerprint (checksum).

For the connection: direction, protocol, port number.

In place of MAC or IP addresses, the following connection type ID is sent: Internet, local (localhost), or local network of class A, B, or C.

## **Why are so few presets available after Outpost is installed?**

We will be updating and expanding the current configuration library with ImproveNet-distributed presets. Program rules are created as necessary. For each application, we will only include rules which have been requested at least once. Application rules are applied only in cases when the information of the particular application (its fingerprints) matches that written in the presets files. If there is no match, the Rules Wizard will be displayed and you can select the appropriate action from the drop-down menu in the usual way.

## **What does automatic application of network access rules mean for me?**

With this system, rules that govern how various applications on your computer access the Internet are automatically configured and applied in Outpost Firewall Pro. This helps eliminate the firewall's pop-up questions when a new connection is initiated on your PC and shifts the task of correctly—and most importantly—securely configuring the firewall to the experts at Agnitum. So not only is managing Outpost Firewall Pro easier now, but you can also be sure that it is as secure as it can be.

You will see far fewer requests for confirmation about how to deal with application communication issues. In addition, the ability to automatically update the rules allows Outpost to block existing third-party vulnerabilities until the vendor is able to issue security updates – so-called zero-hour protection.

Thanks to ImproveNet, if an error in the existing firewall rules is detected, we can fix it and distribute an update almost immediately through the ImproveNet infrastructure.

If for any reason you don't want to use the automatic application of new rules, you can disable it and instead make settings manually, although with a recommended choice which can be optionally followed when the rule creation dialog box appears.

## **How are these rules created and how do I get the updated firewall configuration?**

Based on the configuration sent to us through the ImproveNet program, Agnitum security engineers collect and evaluate information on thousands of network-enabled applications submitted by participating users.

After the evaluation is completed and a set of new automatic access rules is prepared, this configuration is distributed via the Agnitum Update service to users. New rules are automatically applied on the users' machines and Outpost Firewall Pro is set to work automatically with programs listed in the newly-received configuration.

## **Tell me about the auto-rules - how secure are they?**

Thanks to the ImproveNet technology, we know not only about the rules that are missing from users' configurations and the questions their Outpost installation asks, but we also learn about attempts to bypass the protection. Based on reports following the release of Outpost 3.5, we can see that the rulesets are much safer.

Where the former configuration consisted of a large number of rules which were quite insecure because any malicious application could edit the presets file and thus go online, plus the presets file didn't feature program ID check based on its fingerprinting, the new configuration is significantly more secure and has less redundant entries because it only stores what's needed.

Users' configurations now consist only of rules that are required by their particular system setup. And if users install Outpost with a clean configuration and auto-application of rules enabled, new rules are created specifically for the requirements of their system. So the automatic application can be discontinued after a day or two, because the necessary rulesets will already have been created. Users can then tweak those rules using the Rules Wizard alerts if they wish, but there is no real need to do so.

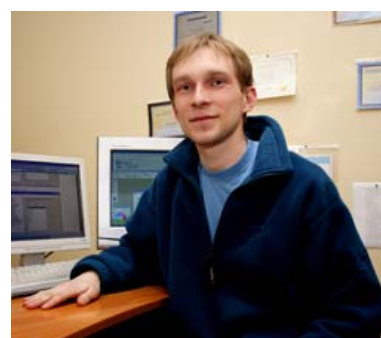
Users can also regularly download new presets. Even if you have auto-application of rules turned off, you will find it useful to refresh the rulesets at intervals to allow for updated Rules Wizard settings for updates of installed applications. We have intentionally tightened up a number of the rules because of the automatic application.

## ImproveNet Summary

Here's the impressive statistics collected for just over one month of ImproveNet operation:

<i>Event/Entry</i>	<i>Description</i>	<i>Data</i>
<b>Start of service</b>	The date when the first batch of rulesets was sent to Outpost users. User configuration collection started a little earlier.	February 21, 2006
<b>Statistics compilation date</b>	The date to which the statistics has been gathered	April 6, 2006
<b>Number of applications covered</b>	Total number of applications included in the automatic firewall rulesets distributed through ImproveNet.	250
<b>Percentage of frequently-used applications covered</b>	The top 50 applications are considered the most frequently used. The percentage represents the number of applications for which automatic rulesets have been assigned compared with the total number of frequently-used applications.	64%
<b>Total number of Internet access requests collected</b>	Aggregate number of connection requests (user prompt windows)	Over 30,000
<b>Percentage of total requests processed</b>	Shows the ratio of processed request to the total number of connection pop-ups displayed throughout the Outpost users' community.	40%

"With ImproveNet, users receive two primary benefits - convenience and increased security. Convenience means that they are not bothered with the firewall's pop-ups while they're online, because most common Internet access rulesets have been developed and applied automatically. Security means that our users can defend against zero-day attacks with new threat-blocking rulesets delivered to their systems automatically. Additionally, ImproveNet enables us to quickly include new network-enabled applications in our configuration database and make them available to our entire user community."



Alexey Belkin, chief software architect and the originator of the ImproveNet concept.