TECHNICAL NOTE

Stormshield Network Firewall

COLLABORATIVE SECURITY

Document version: 1.0

Reference: snentno_collaborative-security

CONTENTS

INTRODUCTION

The Stormshield Network firmware version 1.0 offers the first installment of Stormshield's innovative collaborative security model (Multi-Layer Collaborative Security). This new approach, based on the interaction between the protection engines of the various Stormshield solutions, provides a solid and adapted response to modern threats.

It is now possible, in just one click, to increase the level of protection on a host that has been identified as vulnerable or displaying abnormal behavior directly from the firewall's activity reports and logs. So when critical vulnerabilities are detected, affected hosts can be assigned a strengthened protection profile or specific filter rules (that can be as strict as total isolation).

The Multi-Layer Collaborative Security model – a new vision of security

Modern threats have become increasingly harder for conventional protection systems to detect. Signature-based approaches are proving insufficient against these multi-vector attacks, more often than not created specifically to attain a defined target using 0-day vulnerabilities. A more thorough observation of behavior on networks or on workstations and servers combined with better knowledge of the context of these behaviors allows new threats to be identified more effectively.

The holistic Multi-Layer Collaborative Security model, currently developed by Stormshield, will increase the level of protection by relying on a comprehensive view of behavior and context. It revolves around 3 layers:

- Internal collaboration: interactions between the various protection engines on the same solution (Antivirus, URL filtering, IPS, Vulnerability detection, etc).

  Example: a host presenting a critical vulnerability sets up connections to a website that has been identified in the "botnet" category. These connections have been identified by the intrusion prevention engine as a channel through which the host may be controlled remotely. This host has probably been infected.

- External collaboration: interactions between Stormshield Network Security and Endpoint Security solutions.

  Example: many illegitimate methods of accessing systems on a host which then attempt to set up SSH connections to internal servers. This host is very probably corrupted and can be isolated proactively.

- Threat Intelligence: anonymous collection of alarms and security information on all Stormshield products deployed in order to identify active and unknown threats via the Stormshield Analysis Center, then providing adapted countermeasures on products.

Stormshield Network version 1.0 introduces the manual management of internal collaboration, thereby making it possible to adapt the level of protection according to alarms or detected vulnerabilities.

PRINCIPLE

The administrator determines a security policy dedicated to hosts that have been detected as vulnerable or which need to be isolated. For example, he may create rules that prohibit such hosts from contacting the Internet, but allow them to contact a group of servers that issue upgrades or security patches needed for a remediation. Depending on the criticality of the vulnerabilities detected, rules for total isolation may also be considered.

When Stormshield Network Vulnerability Manager has detected a host as vulnerable, a pop-up menu of the vulnerability report will allow it to be added directly to the predefined remediation or isolation group. If the host does not yet exist in the firewall's object base, it can also be created in this menu.

The selected host will therefore be immediately subject to the specific security policy intended for fixing its vulnerabilities.

Requirements

Features relating to collaborative security require a Stormshield Network Firewall in version 1.0 or higher. If you wish to use these features to isolate vulnerable hosts, the **Stormshield Network Vulnerability Manager** option is also required.

As the Firewall only acts on traffic that passes through it, the architecture will need to be adapted in order to link up hosts to be isolated, remediation servers and the company's critical servers on distinct network interfaces on the firewall (example: dmz1 for critical servers, dmz2 for remediation servers, in for client workstations, etc.). The concept of bridging on Stormshield Network Firewalls allows meeting this need without having to modify the address range.

ISOLATING A VULNERABLE HOST

Configuration of the firewall

The implementation of collaborative security starts off with the preparation of host groups and filter rules dedicated to remediation. In the example given, the filter policy involves remediation rules that implement three host groups (infected hosts, remediation servers and administration hosts).

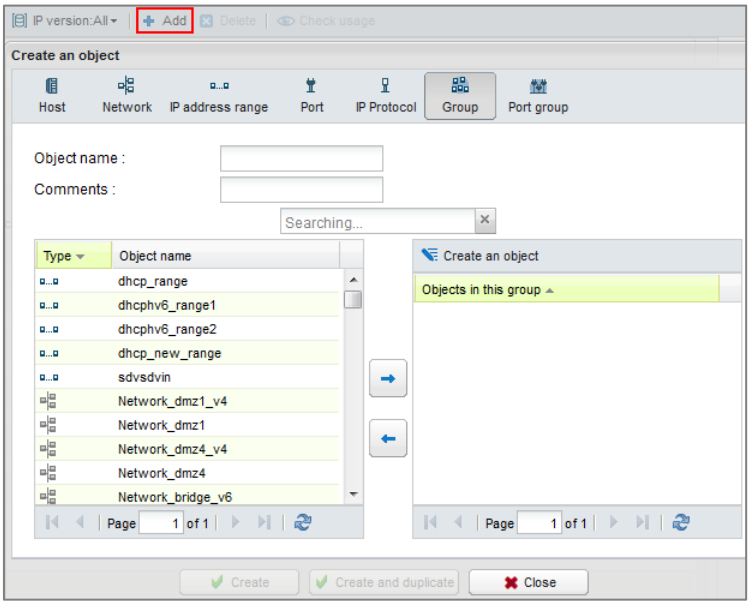
Creating groups

To implement the remediation policy chosen in this example, three object groups are needed:

- A group meant for containing vulnerable hosts (example: **vulnerable_hosts**). The administrator will add hosts detected by SN Vulnerability Manager in real time to this group, which is empty when it is created.
- A group containing servers that distribute updates and security patches (example: **remediation_servers**).
- A group containing the administration workstations allowed to access vulnerable hosts (example: **remediation_admin**).

To create them, in the menu **Configuration** > **Objects** > **Network Objects**, click on **Add** and select the *Group* object:

1. Name the first group and add host objects that it has to contain (or create them directly in the same window),
2. Confirm by clicking on **Create and duplicate**,
3. Add the two other groups following this method,
4. When the last group has been defined, confirm by clicking on **Create**.

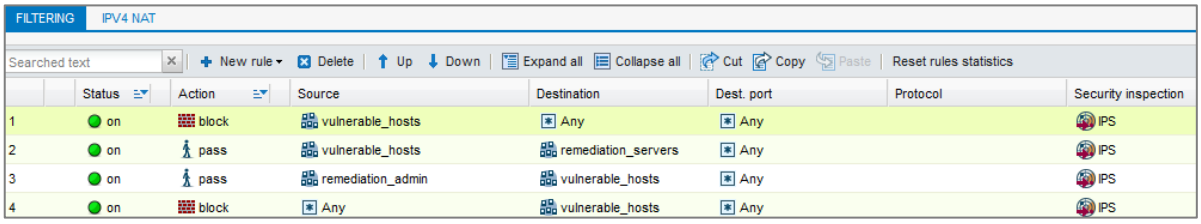


Creating filter rules

In this example of implementing collaborative security, the filter policy requires four rules:

- A rule allowing vulnerable hosts to access remediation servers.
- A rule allowing administration hosts to access vulnerable hosts.
- A rule prohibiting vulnerable hosts from accessing any other destination.
- A rule prohibiting any host other than administration workstations from accessing vulnerable hosts.

In the firewall's filter policy, the group of rules dedicated to remediation would therefore look like this:



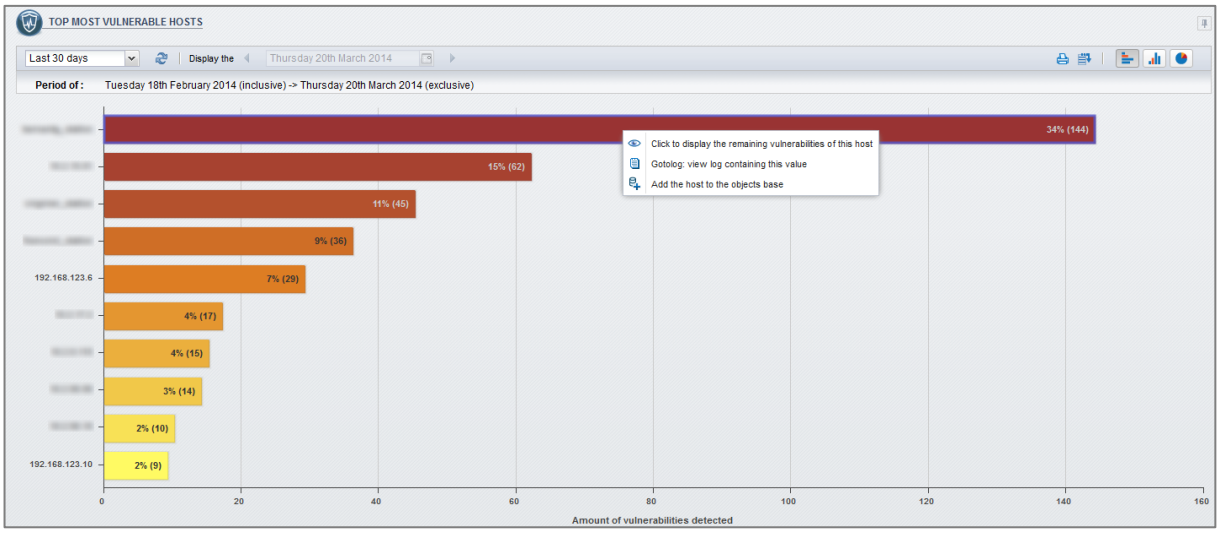
Usage from reports

Displaying the most vulnerable hosts

Select the report **Top most vulnerable hosts** (menu **Reports** > **Vulnerability** > **vulnerable hosts**). Hosts are classified there in descending order according to the number of vulnerabilities detected.

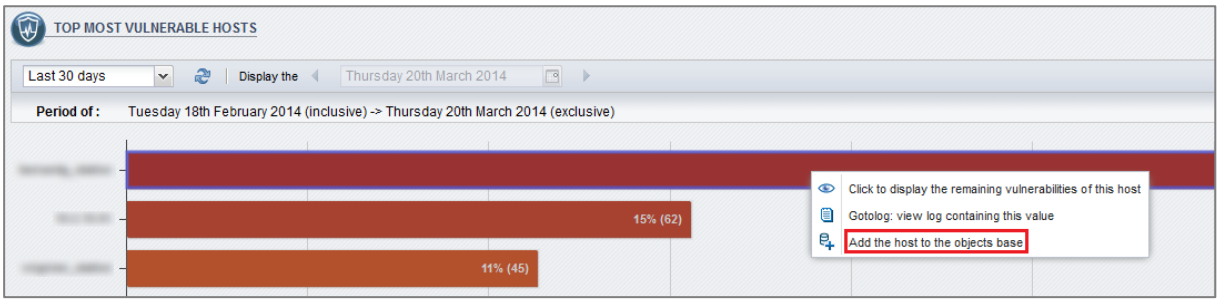
Clicking on the graph of a selected host opens a pop-up menu that offers three actions:

- Click to display remaining vulnerabilities for this host,
- Search for this host in vulnerability logs,
- Add the host to the object base.



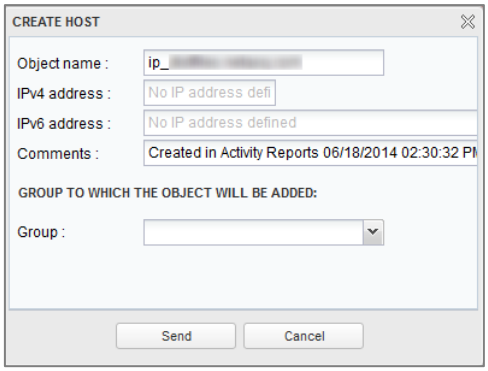
Adding a host to a group

In the pop-up menu, select **Add the host to the Object base**.



Host missing from the firewall's object base

If the host does not already exist in the firewall's object base, the following dialogue box will open:



The field **Object name** is pre-entered (and can be modified) in the form of a prefix "ip_" followed by the host's IPv4 address. The **IPv4 address** field can be pre-entered and can be modified (for hosts that have several IP addresses).

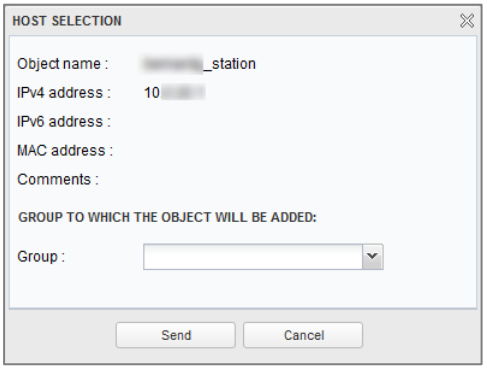
Next, select the group to which you wish to add this host.

By clicking on **Send**, the host will be automatically added to the selected group. If the target group is used in filter rules, they will be immediately applied to the host.

REMARK
The selection of a group is not mandatory. In this case, simply clicking on **Send** will add the host to the firewall's object base.

Host already in the firewall's object base

If the host already exists in the firewall's object base, the following dialogue box will open:



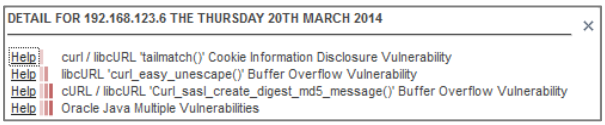
The fields **Object name** and **IPv4 address** are entered and cannot be modified. Only the group must be selected. By clicking on **Send**, the host will be automatically added to this group (example: vulnerable_hosts). If the target group is used in filter rules, they will be immediately applied to the host.

Extra: displaying vulnerabilities on a host

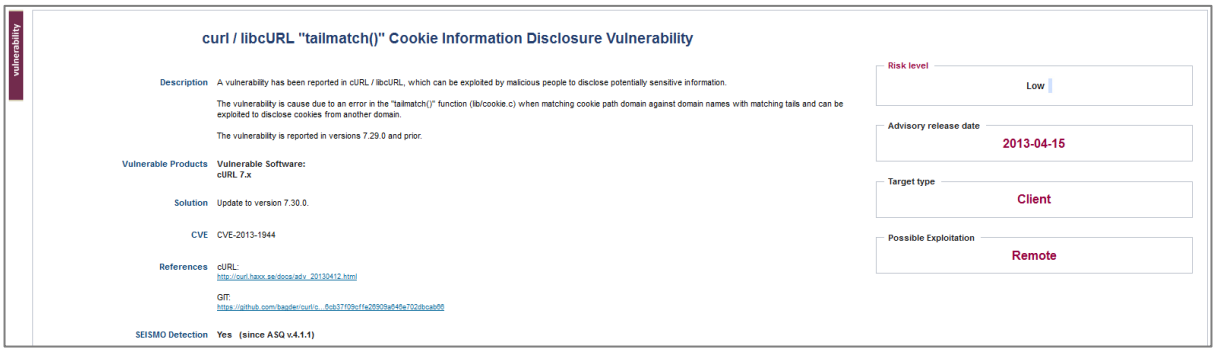
In the report **Top most vulnerable hosts**, you can also find out details of vulnerabilities on a host (list and additional information), and determine the updates or patches to apply to it.

To do this, click on a host's graph and select the entry **Click to display the remaining vulnerabilities of this host** from the pop-up menu.

A pop-up window will then appear in the list of vulnerabilities for the selected host:

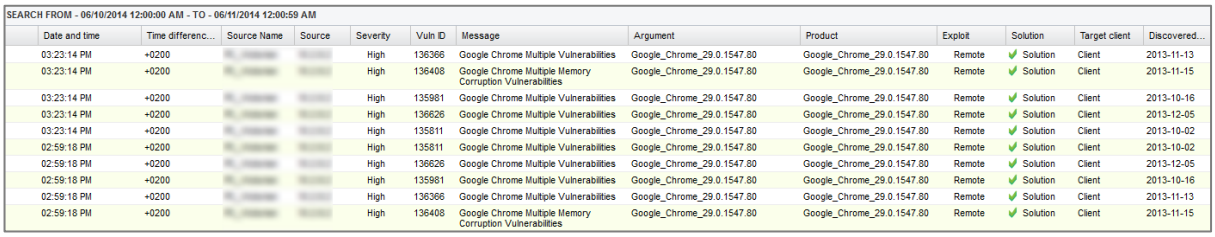


Clicking on the "Help" hyperlink before each vulnerability allows obtaining details about it from the Stormshield Network Security knowledge base (https://kb.stormshield.eu):



Extra: displaying logs relating to vulnerabilities

In the report **Top most vulnerable hosts**, click on the graph of the selected host and choose the entry **Search for this host in the vulnerabilities log** from the pop-up menu. All vulnerability logs regarding this host will then be displayed (contents of the *l_pvm* file).

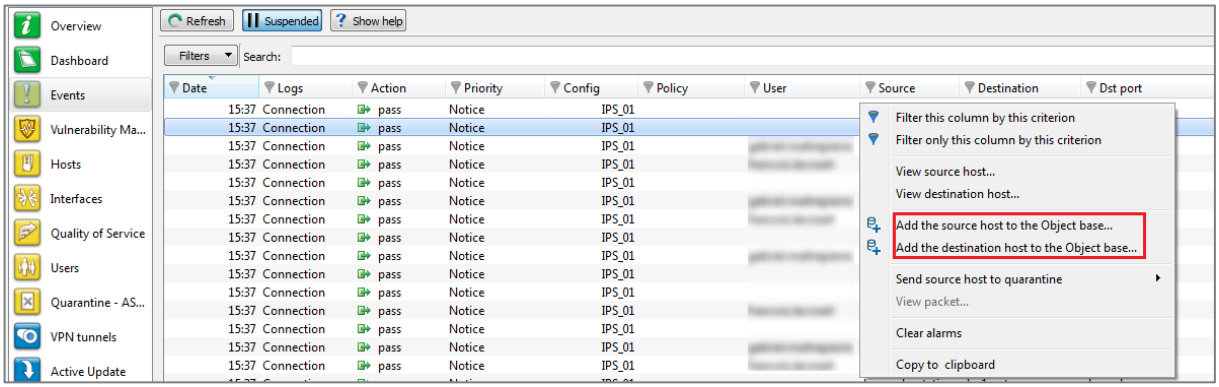


Usage from SN Real-Time monitor

SN Real-Time Monitor also allows directly adding a vulnerable host to a remediation group from the **Events**, **Vulnerability Manager** and **Hosts** views.

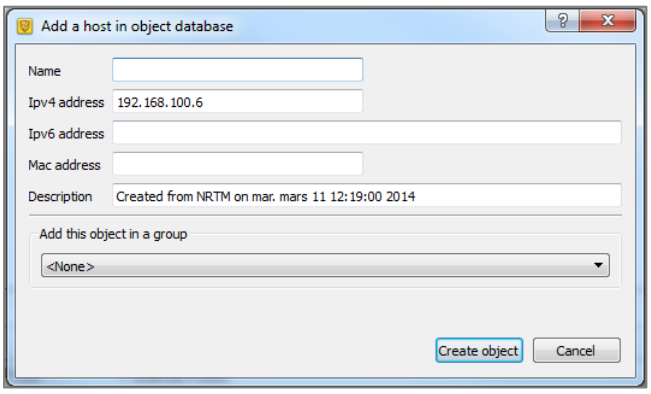
"Events" view

In the Events module, right-click on a row to display the pop-up menu: select the entry **Add the source host to the Object base** or **Add the destination host to the Object base**.



Host missing from the firewall's object base

If the host does not already exist in the firewall's object base, the following dialogue box will open:

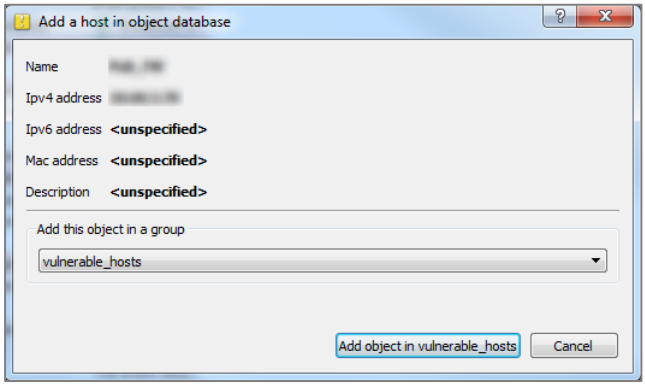


- The **Name** field is to be filled in with the name chosen for the object to be created,
- The **IPv4 address** field is pre-entered and can be modified (for hosts that have several IP addresses),
- If the selected host also has an IPv6 address, it will be pre-entered in the **IPv6 address** field; this value can also be modified (for hosts that have several IP addresses),
- The **Description** field is automatically entered with a comment summarizing the date the object was created and the name of the user who performed the operation. This comment can be can be modified.

Next, select the group to which you wish to add this host. By clicking on **Create object**, the host will be automatically added to the selected group (example: **vulnerable_hosts**). If the target group is used in filter rules, they will be immediately applied to the host.

Host already in the firewall's object base

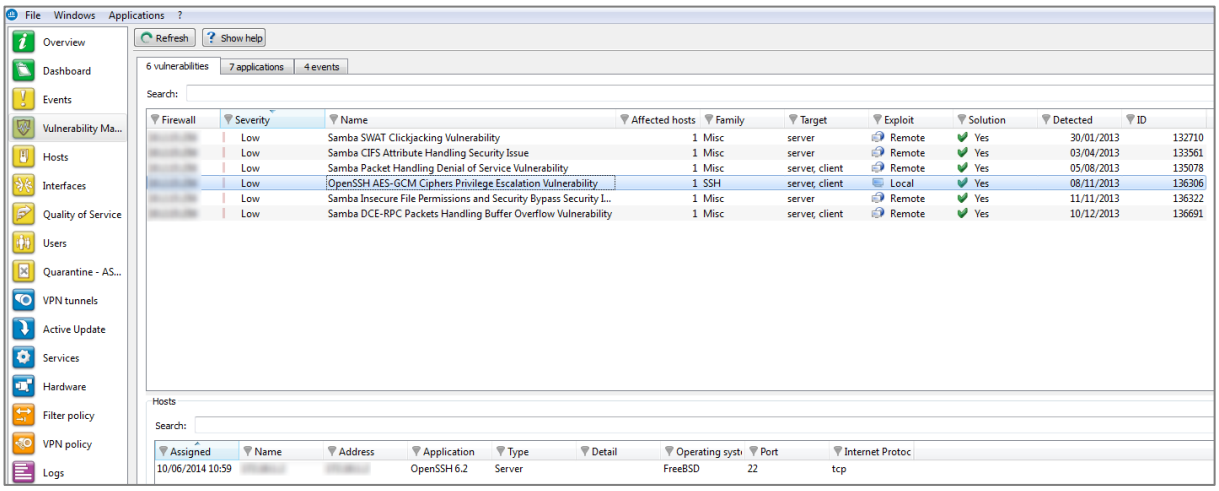
If the host already exists in the firewall's object base, the following dialogue box will open:



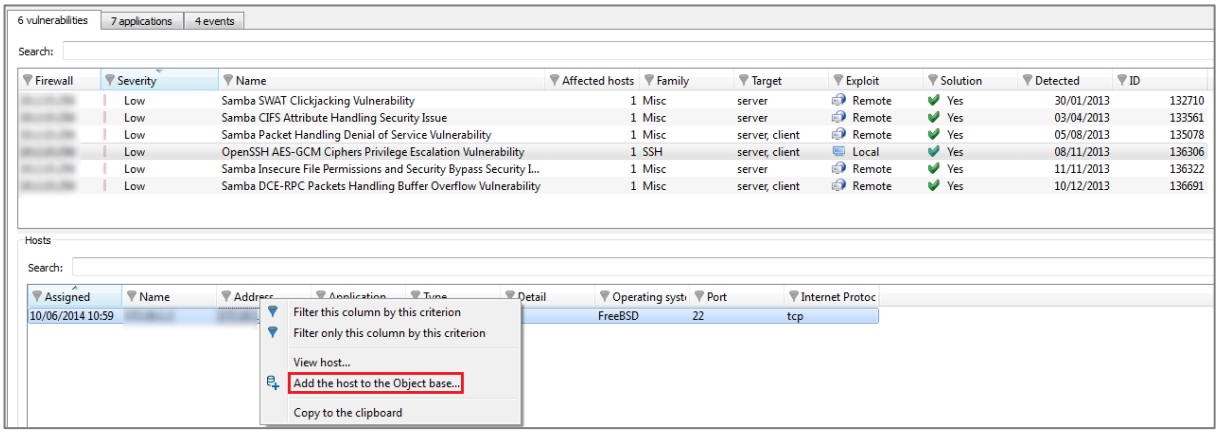
Simply select the group to which you wish to add this host and click on **Add object in *selected_group***. If the target group is used in filter rules, they will be immediately applied to the host.

"Vulnerability manager" view

The *Vulnerabilities* tab in this module lists all the security flaws detected by the firewall. When a vulnerability is selected, all hosts affected by this vulnerability will be displayed in the lower window.



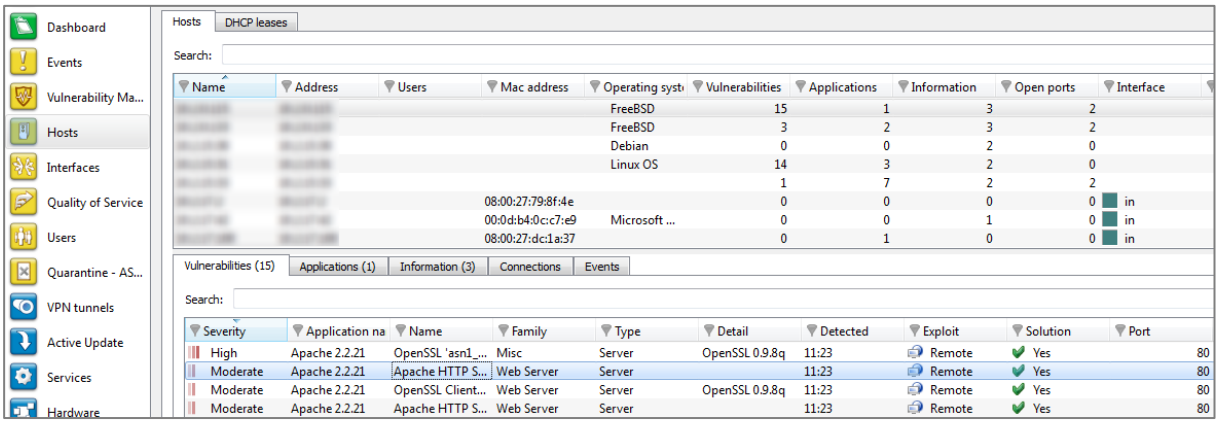
Right-click on the host you wish to add to a remediation group and select the entry **Add the host to the Object base** from the pop-up menu.



If the host does not belong to the firewall's object base, please refer to the paragraph "Events" view > Host missing from the firewall's object base for the values of the various fields. If the host is already in the object base, please refer to the paragraph "Events" view > Host already in the firewall's object base for the values of the various fields.

"Hosts" view

The **Hosts** module lists all of the firewall's known hosts. When a host is selected, all of its vulnerabilities will be listed in the lower window (*Vulnerabilities* tab).



Right-click on a host to display the pop-up menu: select the entry **Add the host to the Object base**.

If the host does not belong to the firewall's object base, please refer to the paragraph "Events" view > Host missing from the firewall's object base for the values of the various fields. If the host is already in the object base, please refer to the paragraph "Events" view > Host already in the firewall's object base for the values of the various fields.

ISOLATING BY OTHER CRITERIA

Other criteria may be involved in deciding to isolate a host fully or partially. This may be, for example, the fact that this host accesses public IP addresses that are deemed untrustworthy according to WHOIS information gathered, or that it has been the source of many alarms from the intrusion prevention engine, or even that it has attempted to log on to malicious sites (botnets).

Configuration of the Firewall

In this example, the filter policy includes a rule that prohibits targeted hosts from accessing the Internet. This rule requires the creation of a specific group (example: **Manually_BlockedHosts**) and may simply look like this:

Usage from activity reports

Display of visited web domains and related WHOIS data

Select the report **Top most visited web sites** (menu **Activity reports** > **Web** > **Visited Web sites**). Domain and public IP addresses are classified there in descending order according to the number of visits.

Clicking on the graph of the selected public IP address opens a pop-up menu that offers four actions:

- URL access,
- Access to WHOIS data regarding the domain,
- Display the URLs category,
- Search this value in logs.

Select the entry **Access to WHOIS data regarding the domain** in this menu. WHOIS data regarding the selected IP address will then be displayed in your Internet browser.

Adding a host to a group

In the report **Top most visited web sites**, click on the graph of the IP address or the URL for which you wish to view connection logs and select the entry **Search this value in logs** in the pop-up menu.

In the *Source name* column of the view displayed, click on the host to be isolated and select the option **Add the host to the Object base** in the pop-up menu. Depending on the appropriate case, the dialogue box is as described in the paragraph Host missing from the firewall's object base or in the paragraph Host already in the firewall's object base.

Select the group meant for isolating hosts (*Manually_BlockedHosts* in the example). The filter rules using this group will be applied immediately to this the host.