

TECHNICAL NOTE Stormshield Network Firewall

COLLABORATIVE SECURITY

Document version: 1.0 **Reference:** snentno collaborative-security





CONTENTS

INTRODUCTION	3
The Multi-Layer Collaborative Security model – a new vision of security	3
PRINCIPLE	4
Requirements	4
ISOLATING A VULNERABLE HOST	5
Configuration of the firewall	5
Creating groups	5
	C C
Displaying the most vulnerable hosts	6
Adding a host to a group	7
Extra: displaying vulnerabilities on a host	8
Extra: displaying logs relating to vulnerabilities	9
Usage from SN Real-Time monitor	9
"Events" view	9
"Vulnerability manager" view	11
"Hosts" view	11
ISOLATING BY OTHER CRITERIA	13
Configuration of the Firewall	13
Usage from activity reports	13
Display of visited web domains and related WHOIS data	13
Adding a host to a group	13



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 popup 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.

Host	Network IP address range	1 Port	I IP Protocol	Group Port group
Object nar Comment	ne:	Searchi	ng	×
Туре 👻	Object name			Sector Create an object
00	dhcp_range		*	Objects in this group
oo	dhcphv6_range1			
oo	dhcphv6_range2			
00	dhcp_new_range			
oo	sdvsdvin			
	Network_dmz1_v4			
	Network_dmz1			
	Network_dmz4_v4		+	
	Network_dmz4			
	Network_bridge_v6		-	
14 4 1	Page 1 of 1	2		A Page 1 of 1 b b 2



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:

FILTE	RING IPV4 NAT						
Searc	hed text	× 🛉 New rule 🕶	🛛 Delete 🕇 Up 👃 Down 🛅	Expand all 🔚 Collapse all 📔	🚰 Cut 😭 Copy 🔄 Paste	Reset rules statistics	
	Status 🖃	Action 🖃	Source	Destination	Dest. port	Protocol	Security inspection
1	🔵 on	block	vulnerable_hosts	* Any	Any		IPS
2	🔵 on	📩 pass	ulnerable_hosts	Remediation_servers	🖹 Any		IPS
3	🔵 on	🕺 pass	Remediation_admin	Nulnerable_hosts	💌 Any		🚳 IPS
4	🔵 on	block	Any	vulnerable_hosts	Any		IPS

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.



TOP MOST V	VULNERABLE HOSTS							Ŧ
Last 30 days	➤ 2 Display the	Thursday 20th March 20	014 🖪 🕨				e) 🖶 📕 🕌 (
Period of :	Tuesday 18th February 2014 ((inclusive) -> Thursday 20th M	arch 2014 (exclusive)					
10000, 1000 100000			15% (6)	2) 🖉 G	lick to display the remaining vulne otolog: view log containing this v	erabilities of this host alue	34%	(144)
		1	1% (45)	₽ A	dd the host to the objects base			
		9% (36)						
192.168.123.6 -		7% (29)						
	4% (17)							
	4% (15)							
	3% (14)							
	2% (10)							
192.168.123.10 -	2% (9)							
1 0	20	5 4	0 60) 80	10	10 12	0 14	0 160

Adding a host to a group

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

TOP MOST VULNERABLE	HOSTS				
Last 30 days 👻 휞	Display the 🔹 Thursday	20th March 2014	•		
Period of : Tuesday 18th	February 2014 (inclusive) -> Th	ursday 20th March 2014 (exclu	usive)		
		1			
				٩	Click to display the remaining vulnerabilities of this host
			15% (62)		Gotolog: view log containing this value
		11% (45)		ę.	Add the host to the objects 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:

CREATE HOST	×
Object name :	ip_
IPv4 address :	No IP address defi
IPv6 address :	No IP address defined
Comments :	Created in Activity Reports 06/18/2014 02:30:32 PM
GROUP TO WHICH T	THE OBJECT WILL BE ADDED:
Group :	v
	Send Cancel

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.

1 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:

HOST SELECTION		\approx
Object name :	_station	
IPv4 address :	10	
IPv6 address :		
MAC address :		
Comments :		
GROUP TO WHICH T	HE OBJECT WILL BE ADDED:	
Group :	~	
		_
	Send Cancel	

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:

DETAIL	FOR 192.168.123.6 THE THURSDAY 20TH MARCH 2014	×
Help Help Help Help	curl / libcURL 'tailmatch()' Cookie Information Disclosure Vulnerability libcURL 'curl_easy_unescape()' Bulfer Overflow Vulnerability cURL / libcURL 'curl_sasl_create_digest_md5_message()' Bulfer Overflow Vulnerability Oracle Java Multiple Vulnerabilities	

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



Inerability	C	url / libcURL "tailmatch()" Cookie Information Disclosure Vulnerability	Risk level	
5	Description	A vulnerability has been reported in cURL / libcURL, which can be exploited by malicious people to disclose potentially sensitive information.		Low
		The vulnerability is cause due to an error in the "talimatch()" function (lb/cookie c) when matching cookie path domain against domain names with matching tails and can be exploited to disclose cookies from another domain.		
		The vulnerability is reported in versions 7.29.0 and prior.	Advisory release date	2013-04-15
	Vulnerable Products	Vulnerable Software: cURL 7.x	Target time	
	Solution	Update to version 7.30 0.	anger gpe	Client
	CVE	CVE-2013-1944	Possible Exploitation	
	References	cURL: Imm Low I have seldogaide . 2013/412 html		Remote
		GIT: https://dtub.com/bagderout/c5ob7100sffa20009a046a1020bca800		
	SEISMO Detection	Yes (since ASQ v.4.1.1)		

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 *I pvm* file).

SEARC	H FROM - 06/10/2014 12	2:00:00 AM - TO - 0	6/11/2014 12:00:5	59 AM									
	Date and time	Time differenc	Source Name	Source	Severity	Vuln ID	Message	Argument	Product	Exploit	Solution	Target client	Discovered
	03:23:14 PM	+0200	R., 10000	10.000	High	136366	Google Chrome Multiple Vulnerabilities	Google_Chrome_29.0.1547.80	Google_Chrome_29.0.1547.80	Remote	V Solution	Client	2013-11-13
	03:23:14 PM	+0200	R., 1999		High	136408	Google Chrome Multiple Memory Corruption Vulnerabilities	Google_Chrome_29.0.1547.80	Google_Chrome_29.0.1547.80	Remote	V Solution	Client	2013-11-15
	03:23:14 PM	+0200	R., 1989	10000	High	135981	Google Chrome Multiple Vulnerabilities	Google_Chrome_29.0.1547.80	Google_Chrome_29.0.1547.80	Remote	V Solution	Client	2013-10-16
	03:23:14 PM	+0200	R. COLUMN	and the second s	High	136626	Google Chrome Multiple Vulnerabilities	Google_Chrome_29.0.1547.80	Google_Chrome_29.0.1547.80	Remote	V Solution	Client	2013-12-05
	03:23:14 PM	+0200	R., 1988	10000	High	135811	Google Chrome Multiple Vulnerabilities	Google_Chrome_29.0.1547.80	Google_Chrome_29.0.1547.80	Remote	V Solution	Client	2013-10-02
	02:59:18 PM	+0200	R. Constant	and the second s	High	135811	Google Chrome Multiple Vulnerabilities	Google_Chrome_29.0.1547.80	Google_Chrome_29.0.1547.80	Remote	V Solution	Client	2013-10-02
	02:59:18 PM	+0200	R., 1999	10000	High	136626	Google Chrome Multiple Vulnerabilities	Google_Chrome_29.0.1547.80	Google_Chrome_29.0.1547.80	Remote	V Solution	Client	2013-12-05
	02:59:18 PM	+0200	R. COLUMN	and the second s	High	135981	Google Chrome Multiple Vulnerabilities	Google_Chrome_29.0.1547.80	Google_Chrome_29.0.1547.80	Remote	V Solution	Client	2013-10-16
	02:59:18 PM	+0200	R., 1988	10000	High	136366	Google Chrome Multiple Vulnerabilities	Google_Chrome_29.0.1547.80	Google_Chrome_29.0.1547.80	Remote	V Solution	Client	2013-11-13
	02:59:18 PM	+0200	R., 1999		High	136408	Google Chrome Multiple Memory Corruption Vulnerabilities	Google_Chrome_29.0.1547.80	Google_Chrome_29.0.1547.80	Remote	V Solution	Client	2013-11-15

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.

i	Overview	C Refresh Suspended	? Show help									
	Dashboard	Filters 🔻 Search:										
1	Events	Date Vertein Vert	Action	Priority	V Config	Policy	Vser	V So	ource	Destination	🛡 Dst port	
<u> </u>		15:37 Connection	pass	Notice	IPS_0	1		-	Cite on Alabia	and unan her this mitaria	_	
1	Vulnerability Ma	15:37 Connection	🖙 pass	Notice	IPS_0	1		<u> </u>	Filter this	Column by this chieno		
	-	15:37 Connection	🖙 pass	Notice	IPS_0	1	phone - all spaces	•	Filter onl	y this column by this cr	iterion	
3	Hosts	15:37 Connection	🖙 pass	Notice	IPS_0	1	frame on the second		View cou	rce hort		
		15:37 Connection	🖙 pass	Notice	IPS_0	1			view sou	ince nostili		
 \${	Interfaces	15:37 Connection	🖙 pass	Notice	IPS_0	1	print of male spaces		View des	tination host		
		15:37 Connection	🖙 pass	Notice	IPS_0	1	Carrier and the result	e.	Add the	source host to the Ohie	ct hase	
2	Quality of Service	15:37 Connection	🖙 pass	Notice	IPS_0	1		A	A du dic	i at at a second		
		15:37 Connection	🖙 pass	Notice	IPS_0	1	print and reading over	4	Add the	destination host to the	Object base	
660	Users	15:37 Connection	🖙 pass	Notice	IPS_0	1			Send sou	irce host to quarantine		•
		15:37 Connection	🖙 pass	Notice	IPS_0	1			1/2			
	Quarantine - AS	15:37 Connection	🖙 pass	Notice	IPS_0	1	frame on the result		view pac	Ket		
	VDN tuppels	15:37 Connection	🖙 pass	Notice	IPS_0	1			Clear ala	rms		
	VENtunnels	15:37 Connection	🖙 pass	Notice	IPS_0	1	printer and approxim]
	Active Undate	15:37 Connection	🖙 pass	Notice	IPS_0	1	Same of the read		Copy to	clipboard		
	neare opulie	45.27.0	-	AL 12	100.0				1.000	1.4		



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:

🖁 Add a host	in object database	<u>g</u>	X
Name			
Ipv4 address	192.168.100.6		
Ipv6 address			
Mac address			
Description	Created from NRTM on mar. mars 11 12:19:00 2014		
Add this obje	ect in a group		
<none></none>			•
		Create object C	ancel
_			

- 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:

🛃 Add a host in object database	8 x
Name	
Ipv4 address	
Ipv6 address <unspecified></unspecified>	
Mac address <unspecified></unspecified>	
Description <unspecified></unspecified>	
Add this object in a group	
vulnerable_hosts	•
	Add object in vulnerable_hosts Cancel

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.

😐 Fil	e Windows Appli	ications	2													
i	Overview	Refresh ? Show help														
	Dashboard	6 vulner	6 vulnerabilities 7 applications 4 events													
2	Events	Search:														
	Mala and The Ma	Firev	vall 🖣	Severity	Vame				Rected hosts Ramily	/ 🛡 Tar	get	🛡 Exploit	Solution	Detected	₩ ID	
	vulnerability ivia	10111	100	Low	Samba SWAT	Clickjacking Vulnerat	oility		1 Misc	serve		Remote	🖌 Yes	30/01/20	13	132710
E	Hosts	10.00	1.100	Low	Samba CIFS A	ttribute Handling See	curity Issue		1 Misc	serve		Remote	💜 Yes	03/04/20	13	133561
	10505	10111	1 N	Low	Samba Packe	Samba Packet Handling Denial of Service Vulnerability			1 Misc	1 Misc server, client 🤿 Remot		i Remote	🖌 Yes	05/08/2013		135078
38	Interfaces	10.00	100	Low	OpenSSH AES	OpenSSH AES-GCM Ciphers Privilege Escalation Vulnerability			1 SSH	serve	; client	🔍 Local	💜 Yes	08/11/20	13	136306
		Low Samba Insecure File Permissions and Security Bypass Securi						ss Security L	1 Misc	serve		Remote	💜 Yes	11/11/2013		136322
5	Quality of Service	Low Samba DCE-RPC Packets Handling Buffer Overflow Vulnerabi					Vulnerability	1 Misc	serve	; client	🗊 Remote	💜 Yes	10/12/20	13	136691	
	Users Quarantine - AS															
0	VPN tunnels															
Ð	Active Update															
2	Services															
	Hardware	Luntz														
5	Filter policy	Search	1:													
1	VPN policy	₹ As	signed	🛡 Name	Address	Application	Туре	🛡 Detail	Operating system	Port	♥ Intern	et Protoc				
	Logs	10/06	6/2014 10:59	111.001.0	171.001.0	OpenSSH 6.2	Server		FreeBSD	22	tcp					

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.

6 vulnerabilities	7 applications	4 events							
Search:									
Firewall	Severity	Vame Vame	Affected hosts	🔻 Family	🔻 Target	🔻 Exploit	Solution	Detected	♥ ID
	Low	Samba SWAT Clickjacking Vulnerability Samba CIFS Attribute Handling Security Issue	1	Misc Misc	server server	Remote Remote	✓ Yes✓ Yes	30/01/2013 03/04/2013	132710 133561
0.000 No 0.000 No 0.000 No	Low Low Low Low	Samba Packet Handling Denial of Service Vulnerability OpenSSH AES-GCM Ciphers Privilege Escalation Vulnerabilit Samba Inscure File Permissions and Security Bypass Securit Samba DCE-RPC Packets Handling Buffer Overflow Vulnera	ty 1 ty L 1 bility 1	Misc SSH Misc Misc	server, client server, client server server, client	 Remote Local Remote Remote 	 ✓ Yes ✓ Yes ✓ Yes ✓ Yes 	05/08/2013 08/11/2013 11/11/2013 10/12/2013	135078 136306 136322 136691
Hosts Search:									
V Assigned	Vame	Address Anolication Tune View host Add the host to the Object base Copy to the clipboard	Detail 💎 Oper FreeBSD	ating syster Po	rt ¶Int tcp	ernet Protoc			

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).



	Dashboard	Hosts	DHCP leas	es									
!	Events	Search	1:										
122	N. 1. 1. 1. 1. 1.	💎 Na	ime	Address	Users	Mac address	P Operating syste	Vulnerabilities	Applications	Information	Open ports	Interface	9
1	Vulnerability Ma	-		March 199			FreeBSD	15	1		3	2	
E	Heate	-		March 199			FreeBSD	3	2		3	2	
	HUSIS			A			Debian	0	(1	2	0	
34	Interfaces	-		and the second s			Linux OS	14	3		2	0	
	Interfoces			B-100				1	5		2	2	
R	Ouality of Service	-		March 1		08:00:27:79:8f:4e		0	(1	0	0 in	
	C	-	1.65	discustion in the second		00:0d:b4:0c:c7:e9	Microsoft	0	(1	1	0 in	
ψų.	Users	100.00	1.00	Barris 1998		08:00:27:dc:1a:37		0	1		0	0 🚺 in	
	Quarantine - AS	Vuln	erabilities (15)	Applications (1)	Information (3)	Connections	Events						
0	VPN tunnels	Sea	rch:										
			Severity	Application na	💎 Name	Family	🔻 Type	💎 Detail	Detected	🔻 Exploit	Solution	Port	
	Active Update		High	Apache 2.2.21	OpenSSL 'asn1_	Misc	Server	OpenSSL 0.9.8q	11:23	Remote	🖌 Yes		80
٢	Constinue		Moderate	Apache 2.2.21	Apache HTTP S.	. Web Server	Server		11:23	Remote	💜 Yes		80
	Services		Moderate	Apache 2.2.21	OpenSSL Client.	. Web Server	Server	OpenSSL 0.9.8q	11:23	Remote	🖌 Yes		80
	Hardware	1	Moderate	Apache 2.2.21	Apache HTTP S.	Web Server	Server		11:23	Remote	💜 Yes		80

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:

🗱 📄 block 🛗 Manually_BlockedHosts 🔹 Any ⊘ Internet 🔹 Any

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.