



STORMSHIELD

NOTE TECHNIQUE

Firewall Stormshield Network

SECURITE COLLABORATIVE

Version du document : 1.0

Référence : snfrtno_securite-collaborative



SOMMAIRE

INTRODUCTION	3
Le modèle Multi-Layer Collaborative Security, une nouvelle vision de la sécurité	3
PRINCIPE	4
Prérequis	4
ISOLEMENT D'UNE MACHINE VULNÉRABLE	5
Configuration du firewall	5
Création des groupes	5
Création des règles de filtrage	6
Utilisation depuis les rapports d'activités	6
Affichages des machines les plus vulnérables	6
Ajout d'une machine à un groupe	7
Complément : affichage des vulnérabilités d'une machine	8
Complément : affichage des traces liées aux vulnérabilités	9
Utilisation depuis SN Real-Time monitor	9
Vue « Événements »	9
Vue « Management de vulnérabilités »	11
Vue « Machines »	12
ISOLEMENT SELON D'AUTRES CRITERES	12
Configuration du Firewall	13
Utilisation depuis les rapports d'activités	13
Affichages des domaines web visités et des données WHOIS liées	13
Ajout d'une machine à un groupe	13



INTRODUCTION

La version de firmware Stormshield Network 1.0 propose la première brique du modèle innovant de sécurité collaborative de Stormshield (Multi-Layer Collaborative Security). Cette nouvelle approche, basée sur l'interaction entre moteurs de protection des solutions Stormshield, offre une réponse concrète et adaptée face aux menaces modernes.

Depuis les rapports d'activités et les journaux de traces du Firewall, il est désormais possible, en un clic, d'augmenter le niveau de protection d'une machine identifiée comme vulnérable ou présentant un comportement anormal. Ainsi, en cas de détection de vulnérabilités critiques, les machines concernées peuvent se voir attribuer un profil de protection renforcée ou des règles de filtrage spécifiques (pouvant aller jusqu'à l'isolement complet).

Le modèle Multi-Layer Collaborative Security, une nouvelle vision de la sécurité

Les menaces modernes sont de plus en plus difficiles à détecter pour les systèmes de protection traditionnels. Les approches par signatures deviennent insuffisantes face à ces attaques multi-vectorielles, souvent créées spécifiquement pour atteindre une cible définie et utilisant des vulnérabilités 0-day. Une étude plus fine des comportements sur les réseaux ou sur les postes et serveurs, alliée à une meilleure connaissance du contexte de ces comportements, permet d'identifier plus efficacement les nouvelles menaces.

Le modèle holistique Multi-Layer Collaborative Security, développé actuellement par Stormshield, augmentera le niveau de protection en s'appuyant sur une vision complète des comportements et du contexte. Il repose sur 3 couches :

- Collaboration Interne : interactions entre les différents moteurs de protection d'une même solution (Antivirus, Filtrage d'URLs, IPS, Détection de Vulnérabilités, ...).
Exemple : une machine présentant une vulnérabilité critique établit des connexions vers un site WEB identifié dans la catégorie « Botnet ». Ces connexions sont identifiées par le moteur de prévention d'intrusion comme étant un canal de prise de contrôle à distance de la machine. Cette machine a probablement été infectée.
- Collaboration Externe : Interactions entre les solutions Stormshield Network Security et Endpoint Security.
Exemple : de nombreux accès systèmes non légitimes sont réalisés sur une machine qui tente ensuite d'établir des connexions SSH vers des serveurs internes. Cette machine est très probablement corrompue et peut être isolée de manière proactive.
- Threat Intelligence : Collecte anonymisée des alertes et informations de sécurité sur tous les produits Stormshield déployés pour identifier des menaces actives et inconnues, via le Centre d'Analyse Stormshield, puis mettre à disposition les contre-mesures adaptées sur les produits.



La version Stormshield Network 1.0 introduit une gestion manuelle de la collaboration interne, permettant ainsi d'adapter le niveau de protection en fonction des alertes ou vulnérabilités détectées.

PRINCIPE

L'administrateur détermine une politique de sécurité dédiée aux machines détectées comme vulnérables ou à isoler. Il crée par exemple des règles interdisant les flux de ces machines vers Internet, mais les autorisant à contacter un groupe de serveurs qui délivrent les mises à jour ou correctifs de sécurité nécessaires à la remédiation. Selon la criticité des vulnérabilités détectées, des règles d'isolement complet peuvent également être envisagées.

Lorsqu'une machine est détectée comme vulnérable par Stormshield Network Vulnerability Manager, un menu contextuel du rapport de vulnérabilités permet de l'ajouter directement au groupe de remédiation ou d'isolement prédéfini. Si la machine n'existe pas encore dans la base objets du firewall, sa création est également possible depuis ce même menu.

La machine sélectionnée est ainsi immédiatement soumise à la politique de sécurité spécifique destinée à corriger ses vulnérabilités.

Prérequis

Les fonctions liées à la sécurité collaborative nécessitent un Firewall Stormshield Network en version 1.0 ou supérieure. Si vous souhaitez utiliser ces fonctions pour isoler des machines vulnérables, l'option **Stormshield Network Vulnerability Manager** est également nécessaire.

Le Firewall n'agissant que sur les flux qui le traversent, il est nécessaire d'adapter son architecture afin de raccorder les machines à isoler, les serveurs de remédiation et les serveurs critiques de l'entreprise sur des interfaces réseaux distinctes du Firewall (exemple : dmz1 pour les serveurs critiques, dmz2 pour les serveurs de remédiation, in pour les postes clients, etc.). La notion de bridge sur les Firewalls Stormshield Network permet de répondre à cette nécessité sans avoir à modifier le plan d'adressage.



ISOLEMENT D'UNE MACHINE VULNÉRABLE

Configuration du firewall

La mise en œuvre de la sécurité collaborative passe tout d'abord par la préparation de groupes de machines et de règles de filtrage dédiés à la remédiation. Dans l'exemple présenté, la politique de filtrage fait appel à des règles de remédiation mettant en œuvre trois groupes de machines (machines infectées, serveurs de remédiation et machines d'administration).

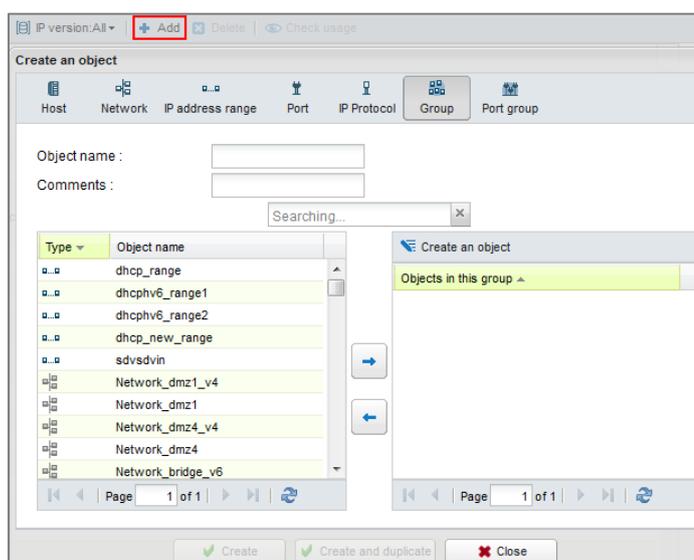
Création des groupes

Pour mettre en œuvre la politique de remédiation choisie dans cet exemple, trois groupes d'objets sont nécessaires :

- Un groupe destiné à contenir les machines vulnérables (exemple : **vulnerable_hosts**). Ce groupe, vide lors de sa création, sera alimenté en temps réel par l'administrateur avec les machines détectées par SN Vulnerability Manager.
- Un groupe contenant les serveurs distribuant les mises à jour et correctifs de sécurité (exemple : **remediation_servers**).
- Un groupe contenant les postes d'administration autorisées à accéder aux machines vulnérables (exemple : **remediation_admin**).

Pour ce faire, dans le menu **Configuration > Objets > Objets Réseaux**, cliquez sur **Ajouter** et choisissez le type d'objet *Groupe* :

1. Nommez le premier groupe et ajoutez-y (ou créez directement dans la même fenêtre) les objets machines qu'il doit contenir,
2. Validez en cliquant sur **Créer et dupliquer**,
3. Ajoutez les deux autres groupes en suivant cette méthode,
4. Lorsque le dernier groupe est défini, validez en cliquant sur **Créer**.





Création des règles de filtrage

Dans cet exemple de mise en œuvre de sécurité collaborative, la politique de filtrage requiert quatre règles:

- Une règle autorisant les machines vulnérables à accéder aux serveurs de remédiation.
- Une règle autorisant les machines d'administration à accéder aux machines vulnérables.
- Une règle interdisant les machines vulnérables à accéder à toute autre destination.
- Une règle interdisant toute autre machine que les postes d'administration à accéder aux machines vulnérables.

Au sein de la politique de filtrage du Firewall, le groupe de règles dédiées à la remédiation prend donc la forme suivante :

	Status	Action	Source	Destination	Dest. port	Protocol	Security inspection
1	on	pass	vulnerable_hosts	remediation_servers	Any		IPS
2	on	pass	remediation_admin	vulnerable_hosts	Any		IPS
3	on	block	vulnerable_hosts	Any	Any		IPS
4	on	block	Any	vulnerable_hosts	Any		IPS

Utilisation depuis les rapports d'activités

Pour accéder aux journaux et rapports d'activités, deux méthodes sont possibles :

- Depuis l'adresse https://adresse_ip_firewall/reports. Cette méthode permet à un utilisateur non familiarisé avec l'interface d'administration des firewalls de consulter directement les traces et rapports.
- Depuis l'interface d'administration du Firewall, en cliquant sur l'icône située dans la partie supérieure droite de l'écran :

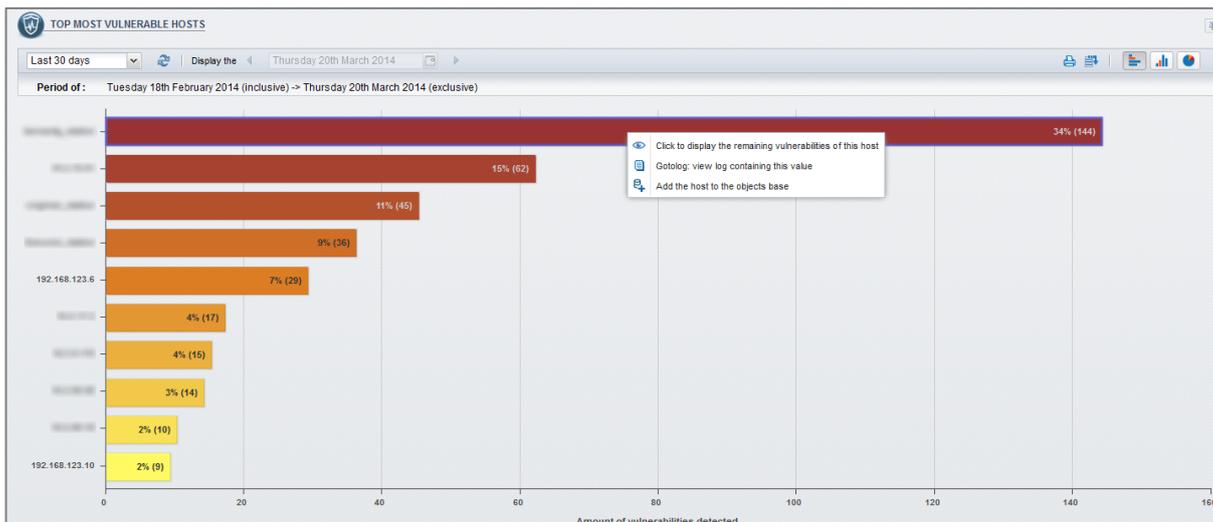


Affichages des machines les plus vulnérables

Sélectionnez le rapport **Top des machines les plus vulnérables** (menu **Rapports d'activités** > **Vulnérabilité** > **Machines vulnérables**). Les machines y sont classées par ordre décroissant selon le nombre de vulnérabilités détectées.

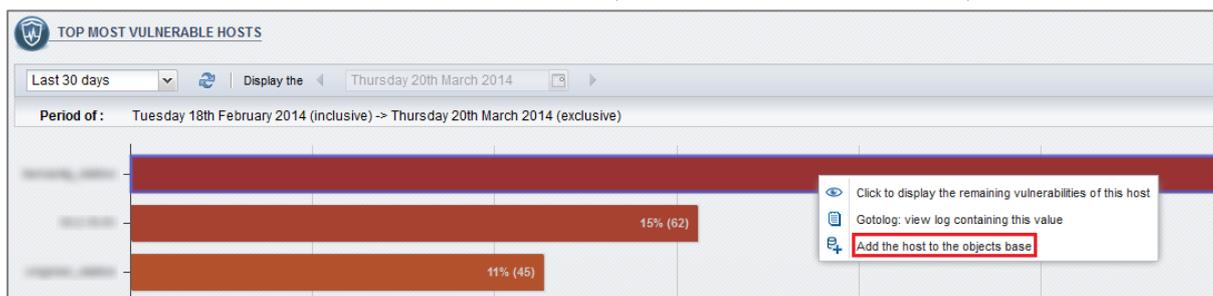
Un clic sur le graphique de la machine choisie ouvre un menu contextuel proposant trois actions :

- Cliquer pour afficher les vulnérabilités subsistantes pour cette machine,
- Rechercher cette machine dans le journal des vulnérabilités,
- Ajouter la machine à la base objets.



Ajout d'une machine à un groupe

Dans le menu contextuel, sélectionnez l'entrée **Ajouter la machine à la base objet**.



Machine absente de la base objets du Firewall

Si la machine n'existe pas déjà dans la base objets du Firewall, la boîte de dialogue suivante s'ouvre :

CREATE HOST ✕

Object name :

IPv4 address :

IPv6 address :

Comments :

GROUP TO WHICH THE OBJECT WILL BE ADDED:

Group :

Le champ **Nom de l'objet** est pré-rempli (et modifiable), sous la forme d'un préfixe « ip_ » suivi de l'adresse IPv4 de la machine. Le champ **Adresse IPv4** peut être pré-rempli et est modifiable (cas d'une machine possédant plusieurs adresses IP).

Sélectionnez ensuite le groupe dans lequel vous souhaitez ajouter cette machine.



En cliquant sur **Créer et ajouter au groupe**, la machine est automatiquement ajoutée au groupe sélectionné. Si le groupe cible est utilisé dans des règles de filtrage, celles-ci sont immédiatement appliquées à la machine.

i REMARQUE

La sélection d'un groupe n'est pas obligatoire. Dans ce cas, en cliquant sur le bouton **Créer l'objet**, la machine sera simplement ajoutée à la base objets du Firewall.

Machine déjà présente dans la base objets du Firewall

Si la machine existe déjà dans la base objets du Firewall, la boîte de dialogue suivante s'ouvre :

HOST SELECTION

Object name : [redacted]_station

IPv4 address : 10 [redacted]

IPv6 address :

MAC address :

Comments :

GROUP TO WHICH THE OBJECT WILL BE ADDED:

Group : [dropdown menu]

Send Cancel

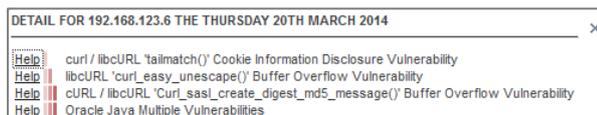
Les champs **Nom de l'objet** et **Adresse IPv4** sont renseignés et non modifiables. Seul le groupe doit être sélectionné. En cliquant sur **Envoyer**, la machine est automatiquement ajoutée à ce groupe (exemple : **vulnerable_hosts**). Si le groupe cible est utilisé dans des règles de filtrage, celles-ci sont immédiatement appliquées à la machine.

Complément : affichage des vulnérabilités d'une machine

Depuis le rapport **Top des machines les plus vulnérables**, vous pouvez également connaître le détail des vulnérabilités d'une machine (liste et informations complémentaires), et déterminer les mises à jour ou correctifs à lui appliquer.

Pour ce faire, cliquez sur le graphique d'une machine et choisissez l'entrée **Cliquez pour afficher les vulnérabilités subsistantes pour cette machine** du menu contextuel.

Une fenêtre Pop-Up affiche alors la liste des vulnérabilités de la machine sélectionnée:



Un clic sur l'hyperlien « Aide » précédant chaque vulnérabilité permet d'en obtenir le détail sur la base de connaissances de sécurité Stormshield Network (<https://kb.stormshield.eu>):

curl / libcURL "tailmatch()" Cookie Information Disclosure Vulnerability

Description A vulnerability has been reported in curl / libcURL, which can be exploited by malicious people to disclose potentially sensitive information.
The vulnerability is caused due to an error in the "tailmatch()" function (libc/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.

Vulnerable Products Vulnerable Software: curl 7.x

Solution Update to version 7.30.0.

CVE CVE-2013-1944

References
 curl: http://curl.haxx.se/docs/adv_20130412.html
 GIT: <https://github.com/bagder/curl/commit/80d37109c1fc209595d49e70280e600>

SEISMO Detection Yes (since ASQ v4.4.1)

Risk level Low

Advisory release date 2013-04-15

Target type Client

Possible Exploitation Remote

Complément : affichage des traces liées aux vulnérabilités

Depuis le rapport **Top des machines les plus vulnérables**, cliquez sur le graphique de la machine choisie et choisissez l'entrée **Rechercher cette machine dans le journal des Vulnérabilités** du menu contextuel. L'ensemble des traces du journal des vulnérabilités concernant cette machine est alors affiché (contenu du fichier *lpvm*).

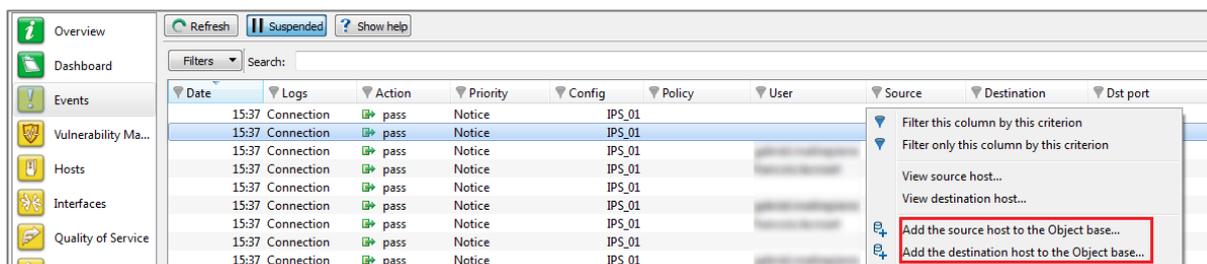
Date and time	Time differenc...	Source Name	Source	Severity	Vuln ID	Message	Argument	Product	Exploit	Solution	Target client	Discovered...
03:23:14 PM	+0200			High	136366	Google Chrome Multiple Vulnerabilites	Google_Chrome_29.0.1547.80	Google_Chrome_29.0.1547.80	Remote	✓ Solution	Client	2013-11-13
03:23:14 PM	+0200			High	136408	Google Chrome Multiple Memory Corruption Vulnerabilites	Google_Chrome_29.0.1547.80	Google_Chrome_29.0.1547.80	Remote	✓ Solution	Client	2013-11-15
03:23:14 PM	+0200			High	135981	Google Chrome Multiple Vulnerabilites	Google_Chrome_29.0.1547.80	Google_Chrome_29.0.1547.80	Remote	✓ Solution	Client	2013-10-16
03:23:14 PM	+0200			High	136626	Google Chrome Multiple Vulnerabilites	Google_Chrome_29.0.1547.80	Google_Chrome_29.0.1547.80	Remote	✓ Solution	Client	2013-12-05
03:23:14 PM	+0200			High	135811	Google Chrome Multiple Vulnerabilites	Google_Chrome_29.0.1547.80	Google_Chrome_29.0.1547.80	Remote	✓ Solution	Client	2013-10-02
02:59:18 PM	+0200			High	135811	Google Chrome Multiple Vulnerabilites	Google_Chrome_29.0.1547.80	Google_Chrome_29.0.1547.80	Remote	✓ Solution	Client	2013-10-02
02:59:18 PM	+0200			High	136626	Google Chrome Multiple Vulnerabilites	Google_Chrome_29.0.1547.80	Google_Chrome_29.0.1547.80	Remote	✓ Solution	Client	2013-12-05
02:59:18 PM	+0200			High	135981	Google Chrome Multiple Vulnerabilites	Google_Chrome_29.0.1547.80	Google_Chrome_29.0.1547.80	Remote	✓ Solution	Client	2013-10-16
02:59:18 PM	+0200			High	136366	Google Chrome Multiple Vulnerabilites	Google_Chrome_29.0.1547.80	Google_Chrome_29.0.1547.80	Remote	✓ Solution	Client	2013-11-13
02:59:18 PM	+0200			High	136408	Google Chrome Multiple Memory Corruption Vulnerabilites	Google_Chrome_29.0.1547.80	Google_Chrome_29.0.1547.80	Remote	✓ Solution	Client	2013-11-15
02:30:10 PM	+0200			High	136626	Google Chrome Multiple Vulnerabilites	Google_Chrome_29.0.1547.80	Google_Chrome_29.0.1547.80	Remote	✓ Solution	Client	2013-12-05

Utilisation depuis SN Real-Time monitor

SN Real-Time Monitor permet également d'ajouter directement une machine vulnérable à un groupe de remédiation depuis les vues Événements, Management de vulnérabilités et Machines.

Vue « Événements »

Dans le module Événements, faites un clic droit sur une ligne d'enregistrement pour afficher le menu contextuel : choisissez alors l'entrée **Ajouter la machine source à la base objets** ou **Ajouter la machine destination à la base objets**.



The screenshot shows the 'Events' view in the SN Real-Time monitor. A table displays connection logs with columns for Date, Logs, Action, Priority, Config, Policy, User, Source, Destination, and Dst port. A context menu is open over one of the rows, showing options like 'Filter this column by this criterion' and 'Add the source host to the Object base...'. The latter option is highlighted with a red box.



Machine absente de la base objets du Firewall

Si la machine vulnérable n'existe pas déjà dans la base objets du Firewall, la boîte de dialogue suivante s'ouvre :

The screenshot shows a dialog box titled "Add a host in object database". It contains the following fields and controls:

- Name: [Empty text box]
- Ipv4 address: 192.168.100.6
- Ipv6 address: [Empty text box]
- Mac address: [Empty text box]
- Description: Created from NRTM on mar. mars 11 12:19:00 2014
- Group selection: "Add this object in a group" dropdown menu with "<None>" selected.
- Buttons: "Create object" and "Cancel" at the bottom right.

- Le champ **Nom de l'objet** est à compléter avec le nom choisi pour l'objet à créer,
- Le champ **Adresse IPv4** est pré-rempli et modifiable (cas d'une machine possédant plusieurs adresses IP),
- Si la machine sélectionnée possède également une adresse IPv6, celle-ci est pré-renseignée dans le champ **Adresse IPv6** ; cette valeur est également modifiable (cas d'une machine possédant plusieurs adresses IP),
- Le champ **Description** est automatiquement rempli à l'aide d'un commentaire type reprenant la date de création de l'objet et le nom de l'utilisateur ayant réalisé l'opération. Ce commentaire est modifiable.

Sélectionnez ensuite le groupe dans lequel vous souhaitez ajouter cette machine. En cliquant sur **Créer et ajouter au groupe**, la machine est automatiquement ajoutée au groupe choisi (exemple : **vulnerable_hosts**). Si le groupe cible est utilisé dans des règles de filtrage, celles-ci sont immédiatement appliquées à la machine.

Machine déjà présente dans la base objets du Firewall

Si la machine vulnérable existe déjà dans la base objets du Firewall, la boîte de dialogue suivante s'ouvre :

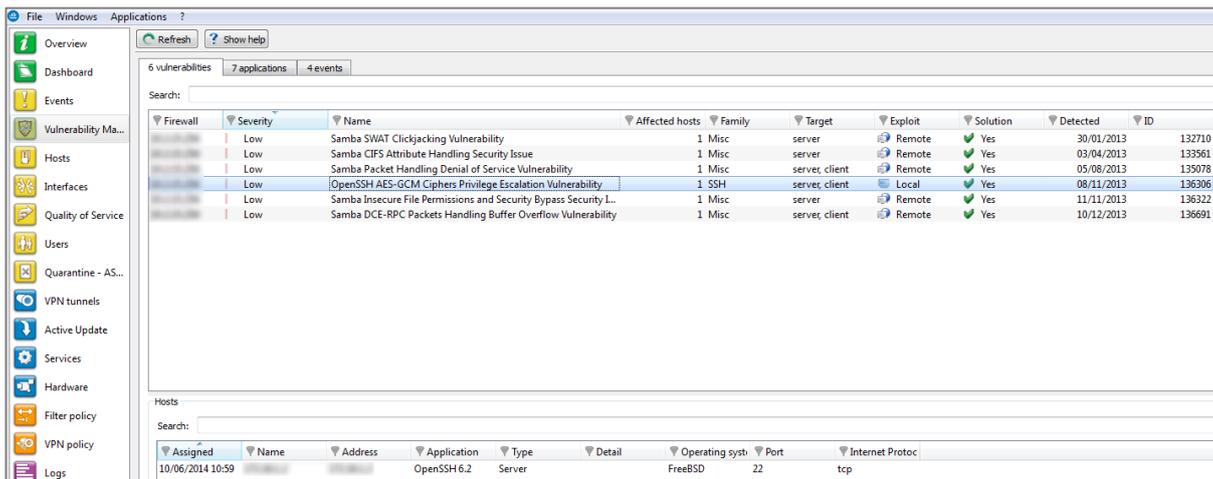
The screenshot shows the same dialog box as above, but with the following differences:

- Name: [Blurred text]
- Ipv4 address: [Blurred text]
- Ipv6 address: <unspecified>
- Mac address: <unspecified>
- Description: <unspecified>
- Group selection: "Add this object in a group" dropdown menu with "vulnerable_hosts" selected.
- Buttons: "Add object in vulnerable_hosts" and "Cancel" at the bottom right.

Il suffit de sélectionner le groupe dans lequel vous souhaitez ajouter cette machine et cliquer sur le bouton **Ajouter l'objet dans groupe_sélectionné**. Si le groupe cible est utilisé dans des règles de filtrage, celles-ci sont immédiatement appliquées à la machine.

Vue « Management de vulnérabilités »

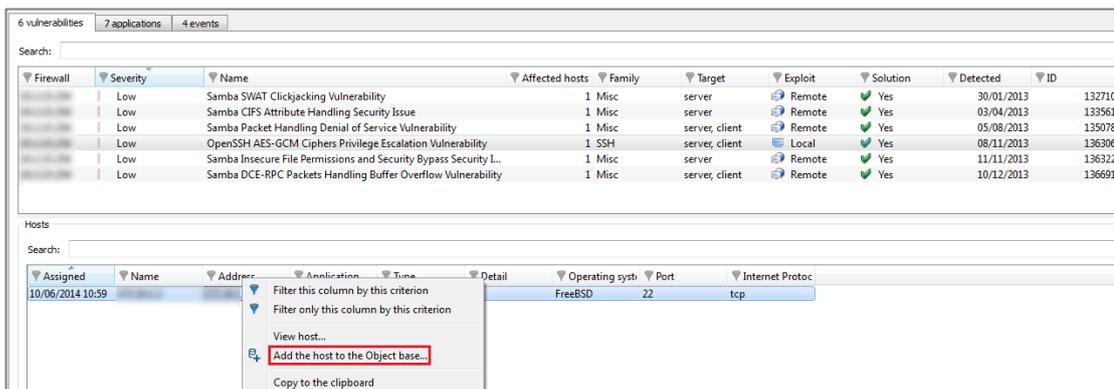
L'onglet *Vulnérabilités* de ce module liste l'ensemble des failles de sécurité détectées par le Firewall. Lorsqu'une vulnérabilité est sélectionnée, toutes les machines concernées par cette faille sont affichées dans la fenêtre inférieure.



Severity	Name	Affected hosts	Family	Target	Exploit	Solution	Detected	ID
Low	Samba SWAT Clickjacking Vulnerability	1 Misc	Misc	server	Remote	Yes	30/01/2013	132710
Low	Samba CIFS Attribute Handling Security Issue	1 Misc	Misc	server	Remote	Yes	03/04/2013	133561
Low	Samba Packet Handling Denial of Service Vulnerability	1 Misc	Misc	server, client	Remote	Yes	05/08/2013	135078
Low	OpenSSH AES-GCM Ciphers Privilege Escalation Vulnerability	1 SSH	SSH	server, client	Local	Yes	08/11/2013	136306
Low	Samba Insecure File Permissions and Security Bypass Security L...	1 Misc	Misc	server	Remote	Yes	11/11/2013	136322
Low	Samba DCE-RPC Packets Handling Buffer Overflow Vulnerability	1 Misc	Misc	server, client	Remote	Yes	10/12/2013	136691

Assigned	Name	Address	Application	Type	Detail	Operating syst.	Port	Internet Protoc.
10/06/2014 10:59			OpenSSH 6.2	Server		FreeBSD	22	tcp

Faites un clic droit sur la machine que vous souhaitez ajouter dans un groupe de remédiation, et choisissez l'entrée **Ajouter la machine à la base objet** du menu contextuel.



Assigned	Name	Address	Application	Type	Detail	Operating syst.	Port	Internet Protoc.
10/06/2014 10:59			OpenSSH 6.2	Server		FreeBSD	22	tcp

Si la machine n'appartient pas à la base objets du Firewall, référez-vous au paragraphe [Vue « Événements » > Machine absente de la base objets du Firewall](#) pour les valeurs des différents champs. Si la machine est déjà présente dans la base objets, reportez-vous au paragraphe [Vue « Événements » > Machine déjà présente dans la base objets du Firewall](#) pour les valeurs des différents champs.



Vue « Machines »

Le module Machines liste l'ensemble des machines connues du Firewall. Lorsqu'une machine est sélectionnée, l'ensemble de ses vulnérabilités est listé dans la fenêtre inférieure (onglet *Vulnérabilités*).

The screenshot shows the Stormshield interface. The left sidebar contains navigation icons for Dashboard, Events, Vulnerability Ma..., Hosts, Interfaces, Quality of Service, Users, Quarantine - AS..., VPN tunnels, Active Update, Services, and Hardware. The main area is divided into two sections. The top section, titled 'Hosts', shows a table of machines with columns for Name, Address, Users, Mac address, Operating syst, Vulnerabilities, Applications, Information, Open ports, and Interface. The bottom section, titled 'Vulnerabilities (15)', shows a table of vulnerabilities with columns for Severity, Application na, Name, Family, Type, Detail, Detected, Exploit, Solution, and Port.

Name	Address	Users	Mac address	Operating syst	Vulnerabilities	Applications	Information	Open ports	Interface
				FreeBSD	15	1	3	2	
				FreeBSD	3	2	3	2	
				Debian	0	0	2	0	
				Linux OS	14	3	2	0	
					1	7	2	2	
			08:00:27:79:8f:4e		0	0	0	0	in
			00:0d:b4:0c:c7:e9	Microsoft ...	0	0	1	0	in
			08:00:27:dc:1a:37		0	1	0	0	in

Severity	Application na	Name	Family	Type	Detail	Detected	Exploit	Solution	Port
High	Apache 2.2.21	OpenSSL 'asn1_...	Misc	Server	OpenSSL 0.9.8q	11:23	Remote	Yes	80
Moderate	Apache 2.2.21	Apache HTTP S...	Web Server	Server		11:23	Remote	Yes	80
Moderate	Apache 2.2.21	OpenSSL Client...	Web Server	Server	OpenSSL 0.9.8q	11:23	Remote	Yes	80
Moderate	Apache 2.2.21	Apache HTTP S...	Web Server	Server		11:23	Remote	Yes	80

Faites un clic droit sur une machine pour afficher le menu contextuel : choisissez alors l'entrée **Ajouter la machine à la base objets**.

Si la machine n'appartient pas à la base objets du Firewall, référez-vous au paragraphe [Vue « Événements » > Machine absente de la base objets du Firewall](#) pour les valeurs des différents champs. Si la machine est déjà présente dans la base objets, reportez-vous au paragraphe [Vue « Événements » > Machine déjà présente dans la base objets du Firewall](#) pour les valeurs des différents champs.

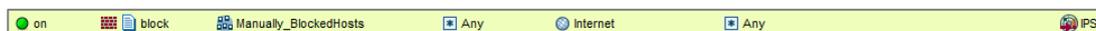


ISOLEMENT SELON D'AUTRES CRITERES

D'autres critères peuvent intervenir dans le choix d'isoler partiellement ou totalement une machine. Cela peut-être, par exemple, le fait que cette machine accède à des adresses IP publiques jugées non dignes de confiance selon les informations WHOIS recueillies, ou qu'elle soit à l'origine de nombreuses alarmes du moteur de prévention d'intrusion, ou encore qu'elle tente de se connecter à des sites malveillants (botnets).

Configuration du Firewall

Dans cet exemple, la politique de filtrage fait appel à une règle interdisant les machines ciblées à accéder à Internet. Cette règle nécessite la création d'un groupe spécifique (exemple : **Manually_BlockedHosts**) et pourra prendre simplement la forme suivante :



Utilisation depuis les rapports d'activités

Affichages des domaines web visités et des données WHOIS liées

Sélectionnez le rapport **Top des domaines web les plus visités** (menu **Rapports d'activités > Web > Domaines Web visités**). Les domaines et adresses IP publiques y sont classés par ordre décroissant selon le nombre de visites.

Un clic sur le graphique de l'adresse IP publique choisie ouvre un menu contextuel proposant quatre actions :

- Accéder à l'URL,
- Accéder aux données WHOIS relatives au domaine,
- Afficher la catégorie d'URLs,
- Rechercher cette valeur dans les traces.

Choisissez l'entrée **Accédez aux données WHOIS relatives au domaine** dans ce menu. Les données WHOIS concernant l'adresse IP sélectionnée sont alors affichées dans votre explorateur Internet.

Ajout d'une machine à un groupe

Dans le rapport **Top des domaines web les plus visités**, cliquez sur le graphique de l'adresse IP ou l'URL pour laquelle vous souhaitez visualiser les traces de connexions et choisissez l'entrée **Rechercher cette valeur dans les traces** du menu contextuel.

Dans la colonne *nom de la source* de la vue affichée, cliquez sur la machine à isoler et choisissez l'entrée **Ajouter la machine à la base objet** du menu contextuel. Selon le cas rencontré, la boîte de dialogue est celle décrite dans le paragraphe **Machine absente de la base objets du Firewall** ou dans le paragraphe **Machine déjà présente dans la base objets du Firewall**.



Sélectionnez le groupe dédié à l'isolement (*Manually_BlockedHosts* dans l'exemple). Les règles de filtrage utilisant ce groupe sont immédiatement appliquées à la machine.