STORMSHIELD

COLLABORATIVE SECURITY

Network Security

Endpoint Security

Data Security

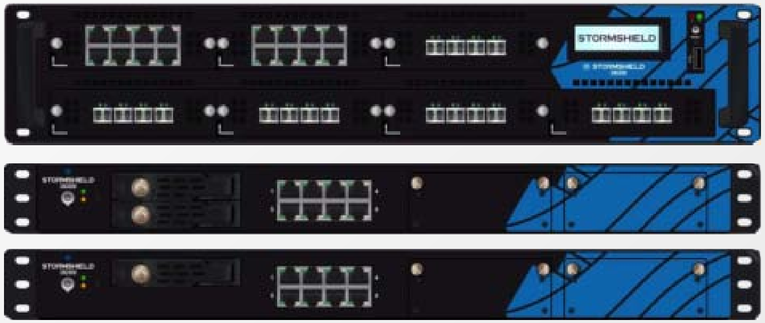
STORMSHIELD

Hardware

Stormshield Network Security

GAMME EXISTANTE

GRANDS COMPTES DATACENTERS



PETITES ENTREPRISES, AGENCES, FILIALES

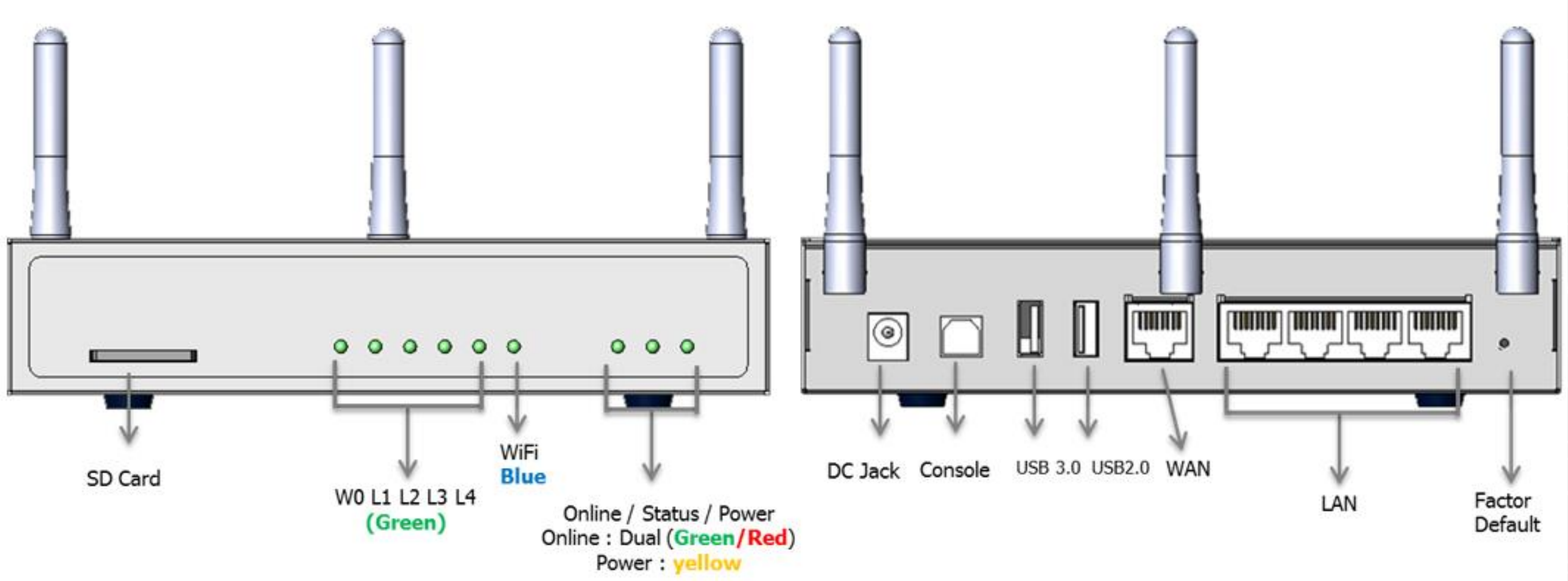
MOYENNES ENTREPRISES AGENCES

APPLIANCES VIRTUELLES ET APPLICATION CLOUD UTM - AWS

CiTRIX ready

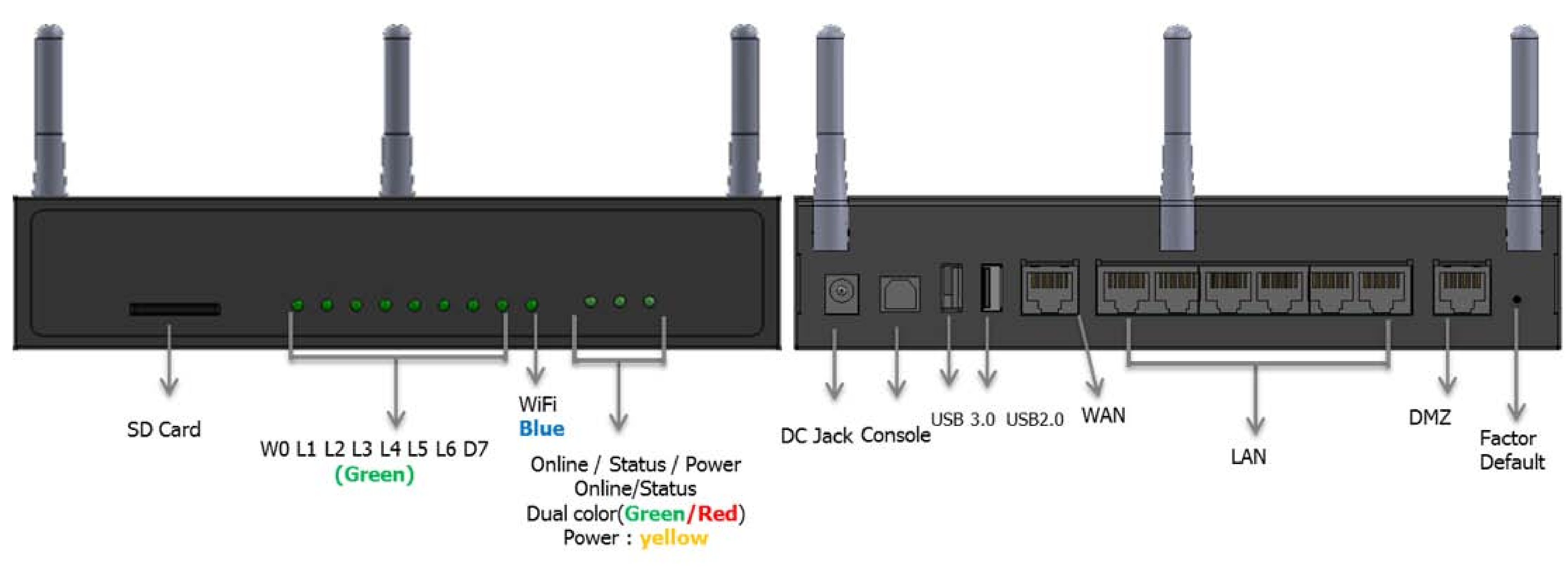
vmware READY

SN160 / SN160W



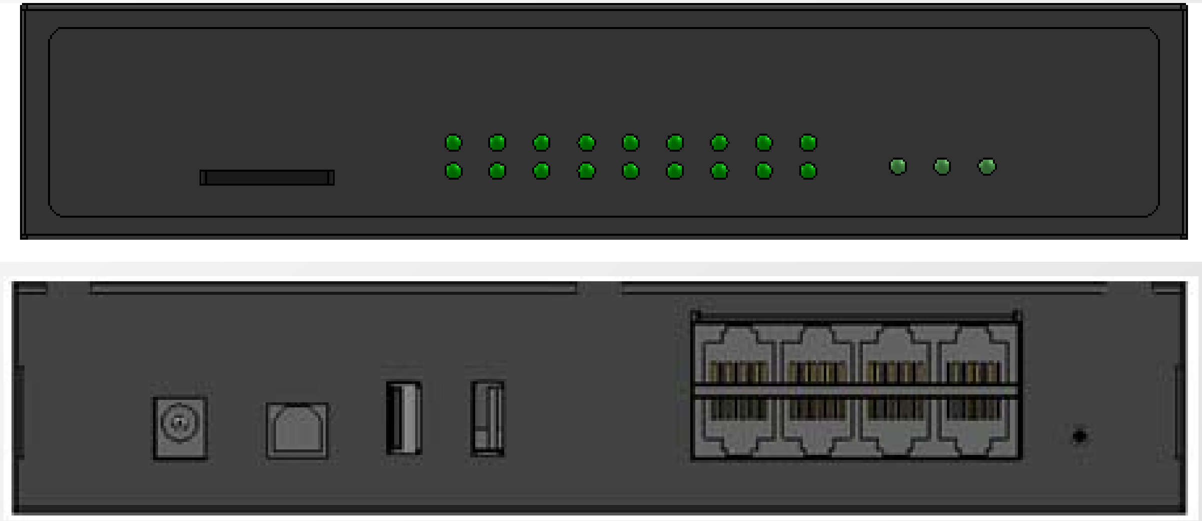
Performances (Mbits/s)	FW	IPS	HTTP	AV	VPN
SN150	400	200	150	30	80
SN160 (expected values)	**1000**	**400**	**350**	**125**	**250**

SN210 / SN210W



Performances (Mbits/s)	FW	IPS	HTTP	AV	VPN
SN200	600	500	400	125	250
SN210 (expected values)	**1500**	**600**	**500**	**250**	**400**

SN310



Performances (Mbits/s)	FW	IPS	HTTP	AV	VPN
SN300	800	700	600	150	300
SN310 (expected values)	**2500**	**1000**	**800**	**350**	**600**

STORMSHIELD

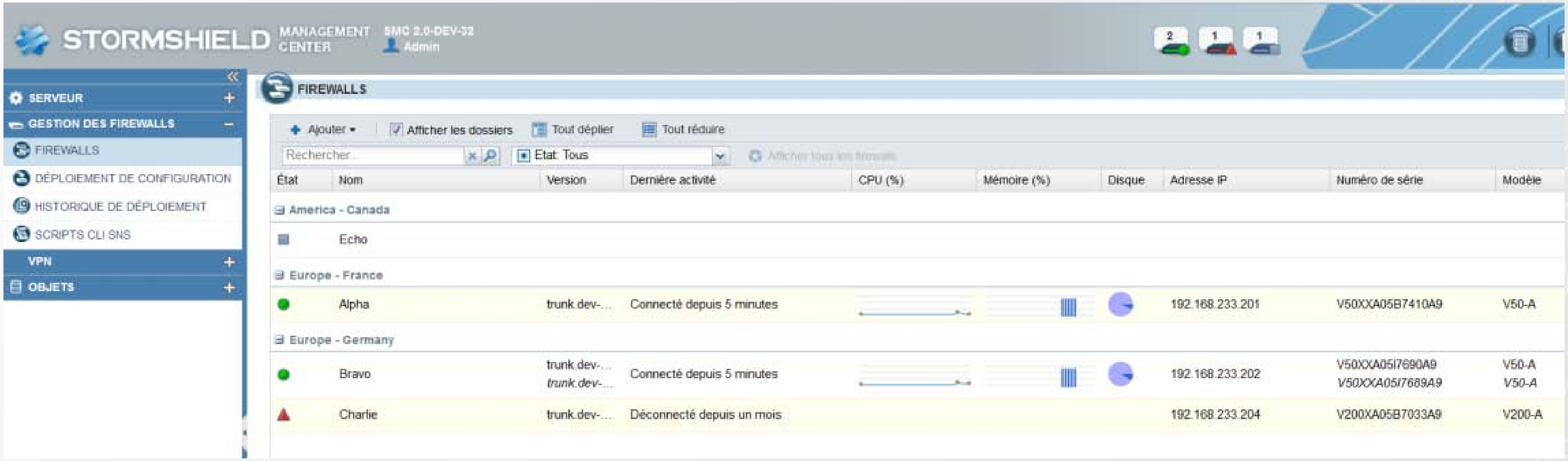
Tour d’horizon V3

Stormshield Network Security

Stormshield Management Center

Stormshield Network Security

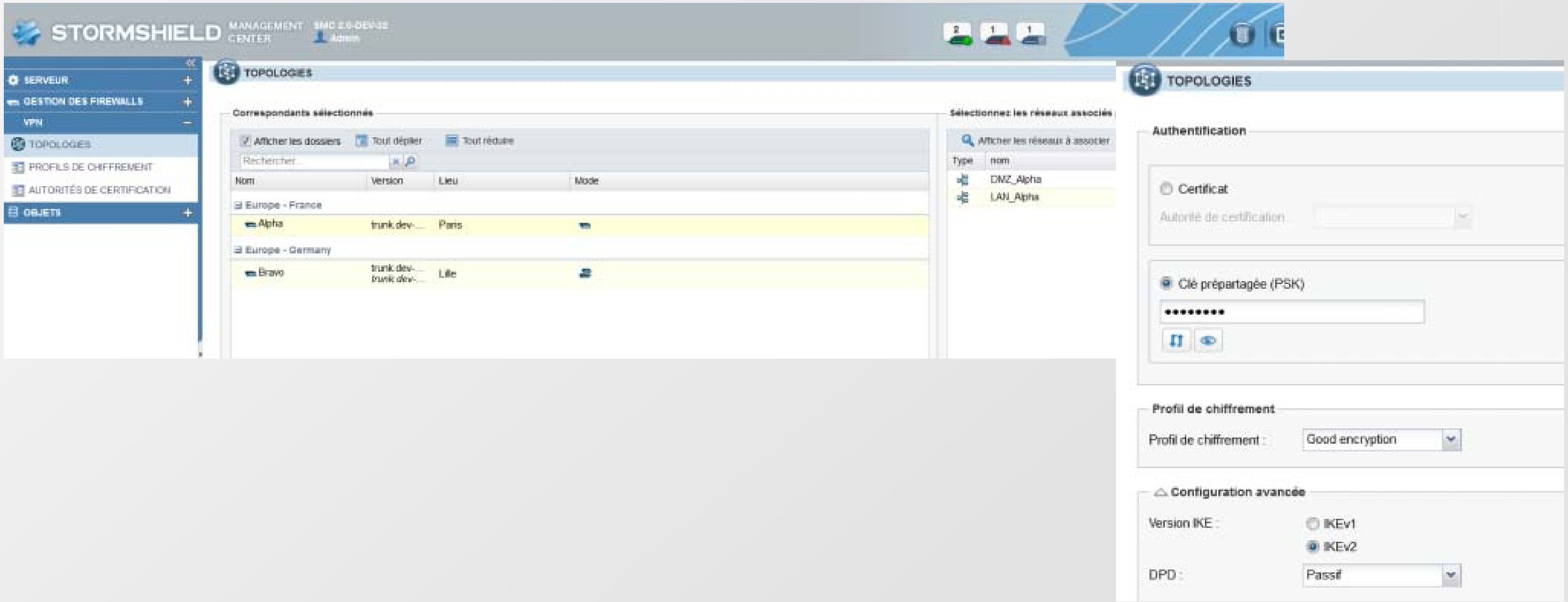
STORMSHIELD



☑ Afficher les dossiers

Etat: Tous

État	Nom	Version	Dernière activité	CPU (%)	Mémoire (%)	Disque	Adresse IP	Numéro de série	Modèle
⊟ America - Canada									
■	Echo								
⊟ Europe - France									
●	Alpha	trunk.dev-…	Connecté depuis 5 minutes				192.168.233.201	V50XXA05B7410A9	V50-A
⊟ Europe - Germany									
●	Bravo	trunk.dev-… *trunk.dev-…*	Connecté depuis 5 minutes				192.168.233.202	V50XXA05I7690A9 *V50XXA05I7689A9*	V50-A *V50-A*
▲	Charlie	trunk.dev-…	Déconnecté depuis un mois				192.168.233.204	V200XA05B7033A9	V200-A



Correspondants sélectionnés

Nom	Version	Lieu	Mode
⊟ Europe - France			
Alpha	trunk.dev-…	Paris	
⊟ Europe - Germany			
Bravo	trunk.dev-… trunk.dev-…	Lille	

Sélectionnez les réseaux associés

Type	nom
	DMZ_Alpha
	LAN_Alpha

Authentification

○ Certificat

Autorité de certification

● Clé prépartagée (PSK)

•••••••••

Profil de chiffrement

Profil de chiffrement : Good encryption

Configuration avancée

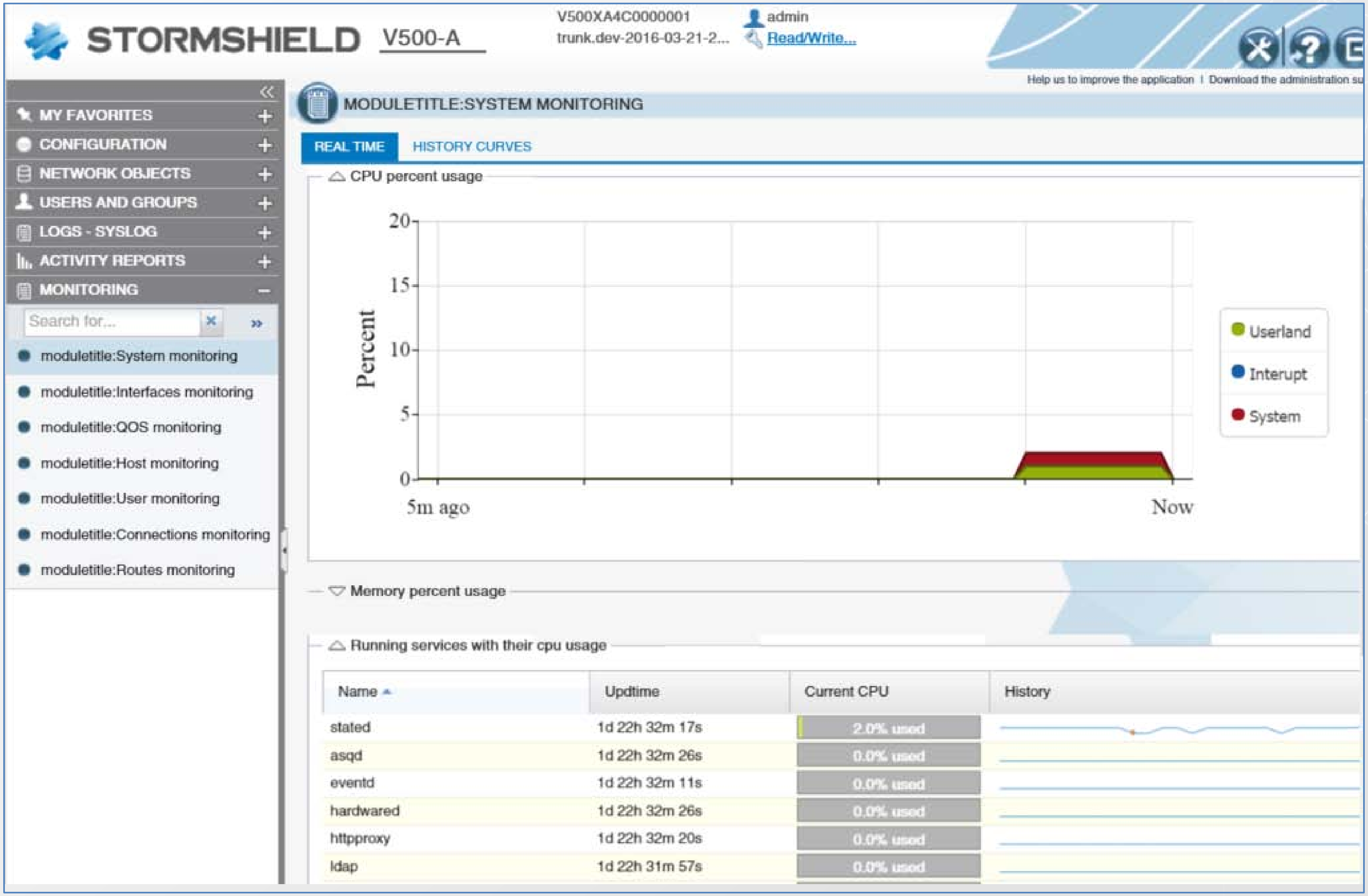
Version IKE : ○ IKEv1 ● IKEv2

DPD : Passif

Une interface Web

Administration / Reporting / Monitoring

STORMSHIELD


STORMSHIELD V500-A
V500XA4C0000001
trunk.dev-2016-03-21-2...
admin
Read/Write...
Help us to improve the application | Download the administration su
MY FAVORITES
CONFIGURATION
NETWORK OBJECTS
USERS AND GROUPS
LOGS - SYSLOG
ACTIVITY REPORTS
MONITORING
Search for...
moduletitle:System monitoring
moduletitle:Interfaces monitoring
moduletitle:QOS monitoring
moduletitle:Host monitoring
moduletitle:User monitoring
moduletitle:Connections monitoring
moduletitle:Routes monitoring
MODULETITLE:SYSTEM MONITORING
REAL TIME
HISTORY CURVES
CPU percent usage
Percent
20
15
10
5
0
5m ago
Now
Userland
Interupt
System
Memory percent usage
Running services with their cpu usage

Name ▲	Updtime	Current CPU	History
stated	1d 22h 32m 17s	2.0% used	
asqd	1d 22h 32m 26s	0.0% used	
eventd	1d 22h 32m 11s	0.0% used	
hardwared	1d 22h 32m 26s	0.0% used	
httpproxy	1d 22h 32m 20s	0.0% used	
ldap	1d 22h 31m 57s	0.0% used	

STORMSHIELD

Courbes temps réel et historique

Administration / Reporting / Monitoring

COURBES TEMPS REEL ET HISTORIQUE

SYSTEME

Pourcentage d’utilisation CPU et Température

Pourcentage d’utilisation mémoire (Temps réel)

Services utilisés ainsi que leur charge CPU

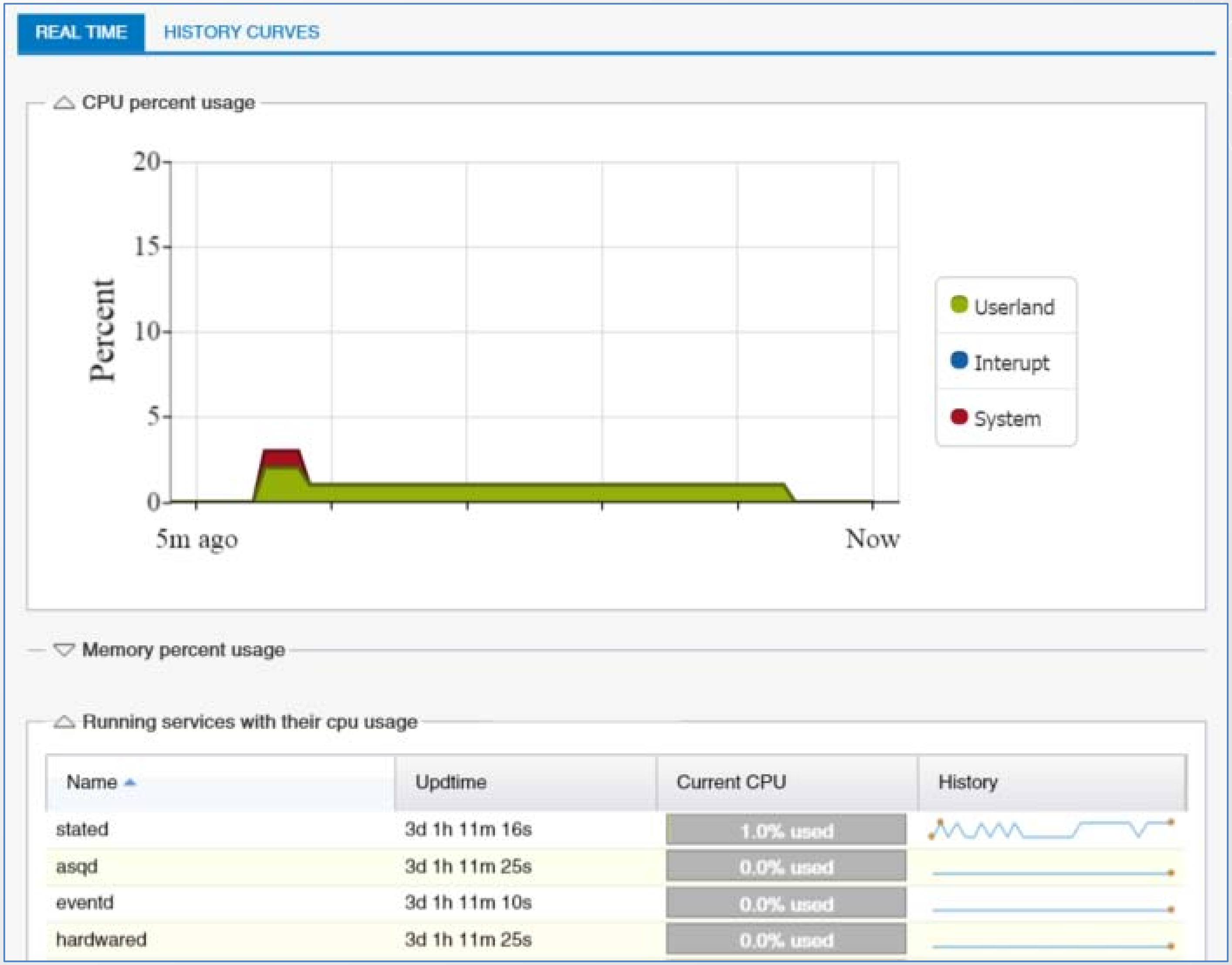
INTERFACES

Débits

Connexions

QoS

MONITEUR TEMPS REEL



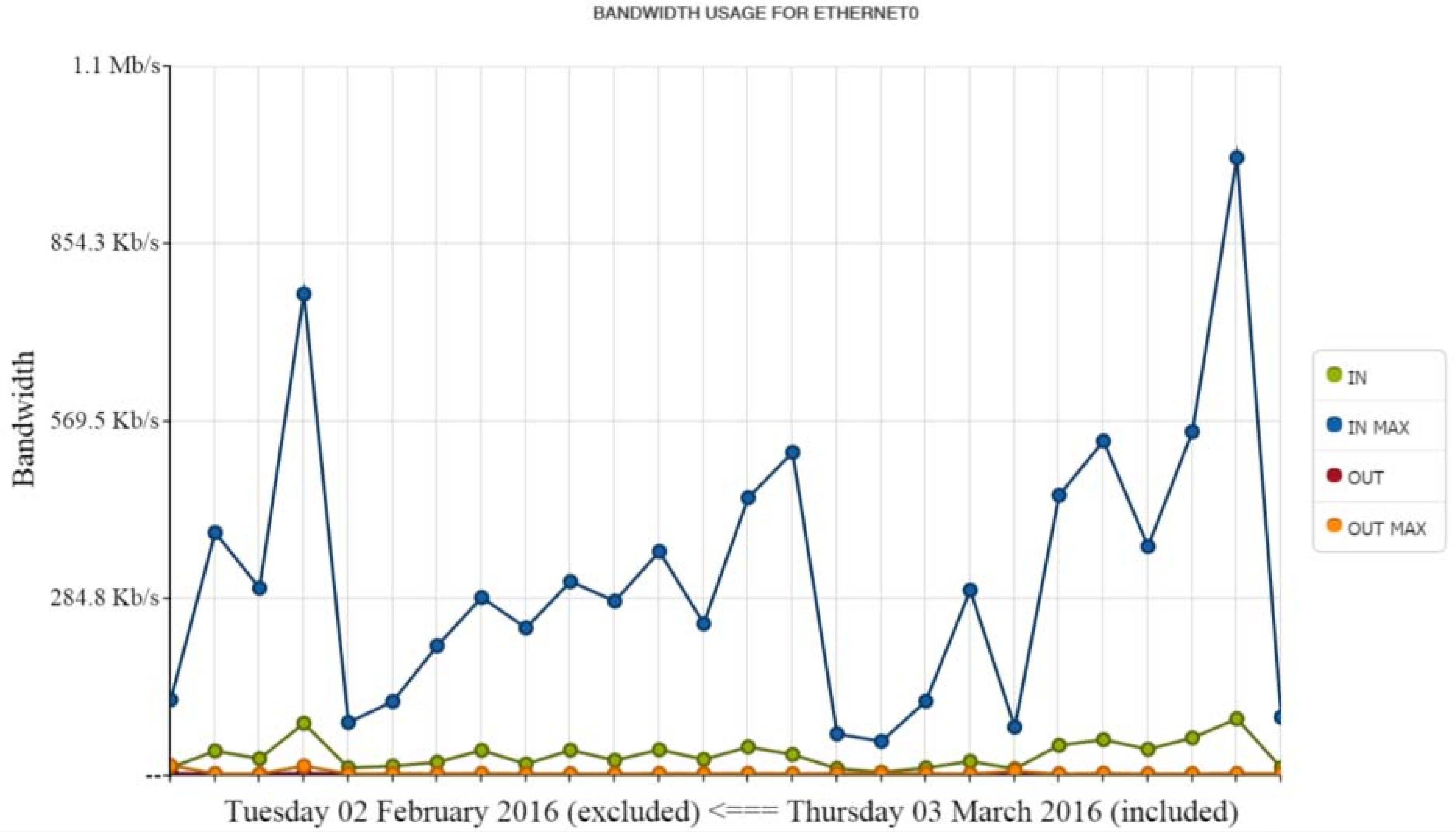
△ CPU percent usage

▽ Memory percent usage

△ Running services with their cpu usage

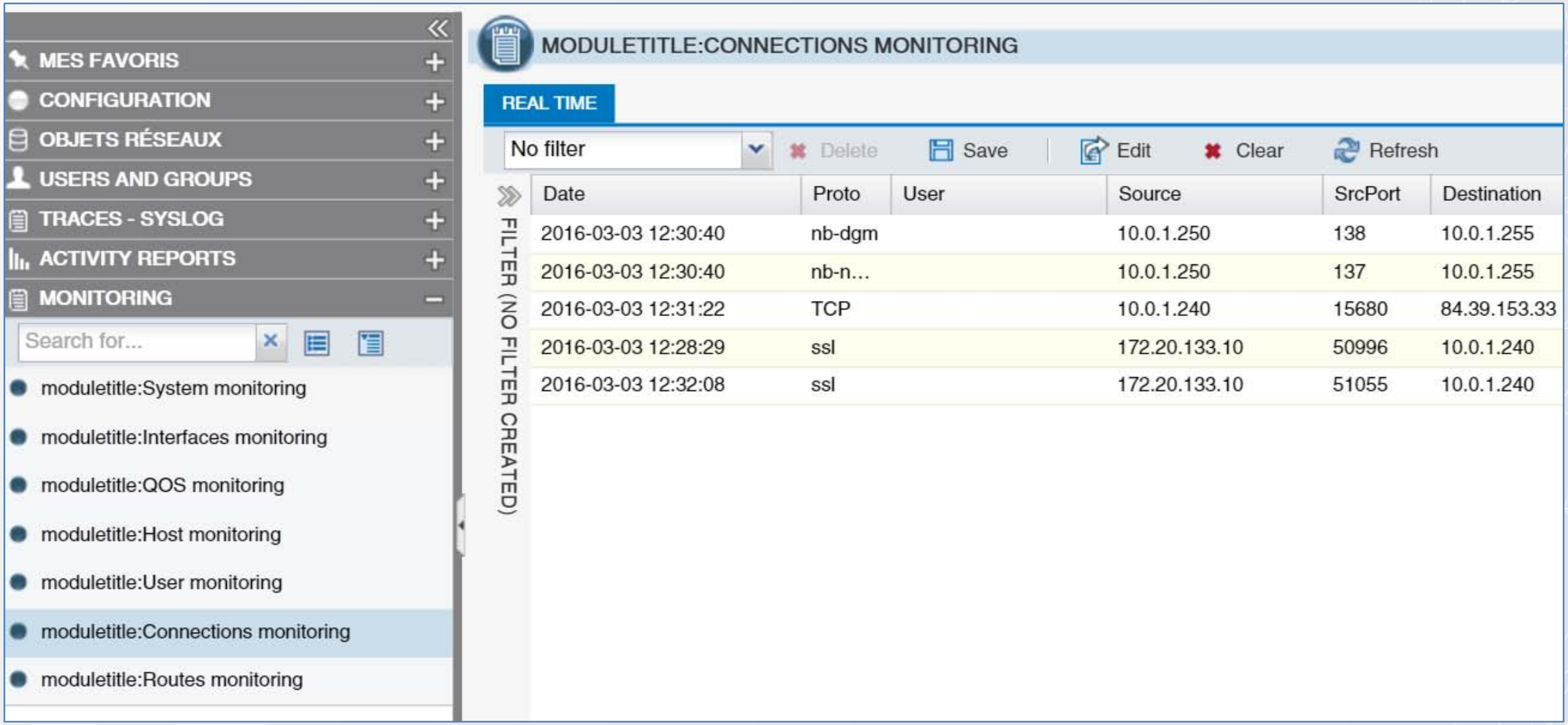
Name ▲	Updtime	Current CPU	History
stated	3d 1h 11m 16s	1.0% used	
asqd	3d 1h 11m 25s	0.0% used	
eventd	3d 1h 11m 10s	0.0% used	
hardwared	3d 1h 11m 25s	0.0% used	

COURBES D'HISTORIQUE



MONITEUR TEMPS REEL

Hôtes, Utilisateurs connections et routes sont désormais disponibles dans l'interface Web


MES FAVORIS
CONFIGURATION
OBJETS RÉSEAUX
USERS AND GROUPS
TRACES - SYSLOG
ACTIVITY REPORTS
MONITORING
Search for...
moduletitle:System monitoring
moduletitle:Interfaces monitoring
moduletitle:QOS monitoring
moduletitle:Host monitoring
moduletitle:User monitoring
moduletitle:Connections monitoring
moduletitle:Routes monitoring
MODULETITLE:CONNECTIONS MONITORING
REAL TIME
Delete
Save
Edit
Clear
Refresh
FILTER (NO FILTER CREATED)

No filter

Date	Proto	User	Source	SrcPort	Destination
2016-03-03 12:30:40	nb-dgm		10.0.1.250	138	10.0.1.255
2016-03-03 12:30:40	nb-n...		10.0.1.250	137	10.0.1.255
2016-03-03 12:31:22	TCP		10.0.1.240	15680	84.39.153.33
2016-03-03 12:28:29	ssl		172.20.133.10	50996	10.0.1.240
2016-03-03 12:32:08	ssl		172.20.133.10	51055	10.0.1.240

Optimisation de l’Authentification

Stormshield Network Security

AUTHENTIFICATION MULTI-DOMAINE

INCLUS DANS LA V3

-4 Domaines/LDAP externes ET 1 base interne en simultané

-Suppression de diverses limitations
(Groupe de groupe, appartenance à trop de groupes; etc…)

-Possibilité d'utiliser les caractères spéciaux (« espace », « @ »)

-…

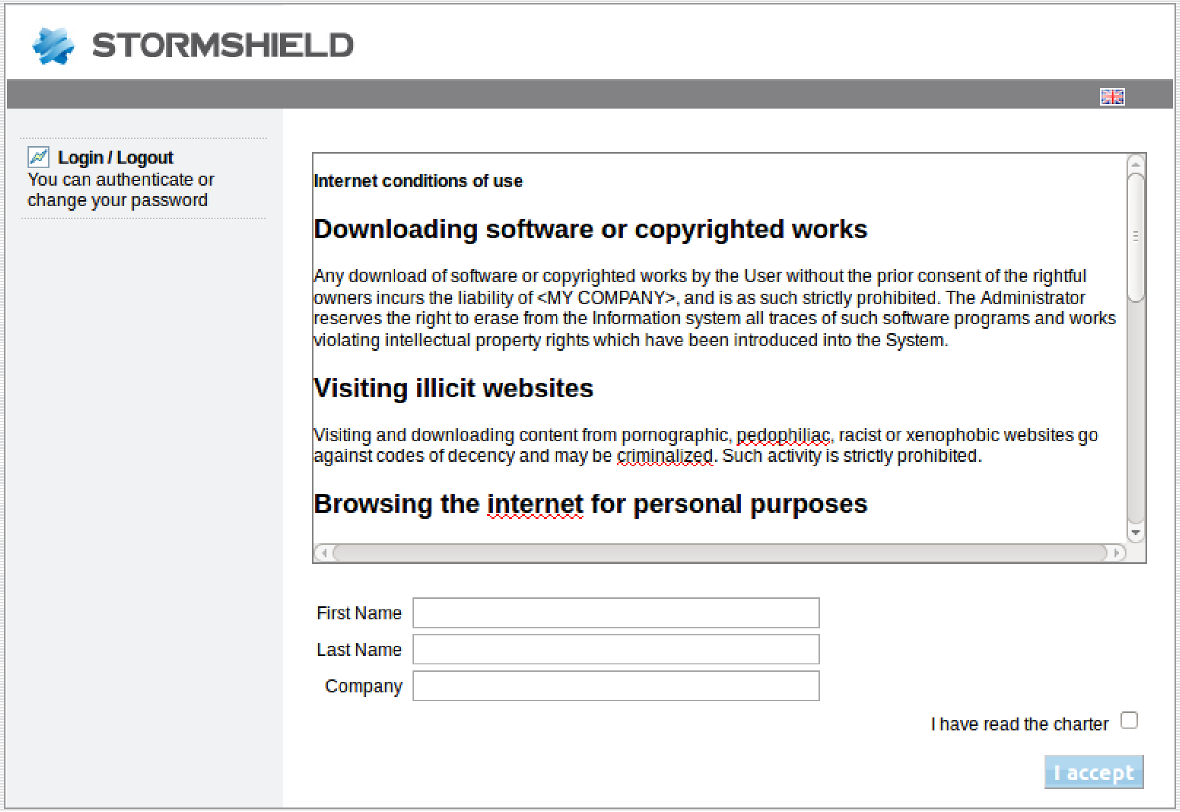
STORMSHIELD

Portail d’Authentification

Stormshield Network Security

MODE INVITE (1/3)

Mode existant depuis la V1 (Charte internet)
Ajout de nouveaux champs personnalisés (Nom, …)



Login / Logout
You can authenticate or change your password

Internet conditions of use

Downloading software or copyrighted works

Any download of software or copyrighted works by the User without the prior consent of the rightful owners incurs the liability of <MY COMPANY>, and is as such strictly prohibited. The Administrator reserves the right to erase from the Information system all traces of such software programs and works violating intellectual property rights which have been introduced into the System.

Visiting illicit websites

Visiting and downloading content from pornographic, pedophiliac, racist or xenophobic websites go against codes of decency and may be criminalized. Such activity is strictly prohibited.

Browsing the internet for personal purposes

First Name	
Last Name	
Company	

I have read the charter □

MODE INVITE (2/3)

NOUVEAU PORTAIL DE CREATION D’UTILISATEURS TEMPORAIRES

-Champs à renseigner tels que le nom, prénom, etc…

-Mot de passe

-Durée d’accès

-Assignation à un groupe utilisateur personnalisé (par exemple: « Internet uniquement »)

-…

MODE INVITE (2/3)

NOUVEAU PORTAIL DE TYPE SPONSORING

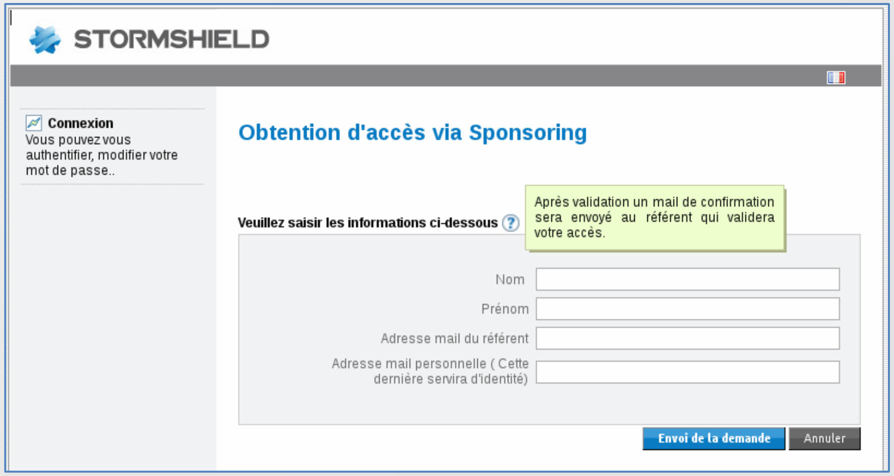
-Se connecter au WIFI (Accès ouvert)

-Renseignement des informations du formulaire

-Indiquer un contact interne (e-mail)

-Le contact recoit un e-mail avec toutes les informations et un lien pour accepter la demande d'accès

-Si accepté, l'invité sera automatiquement redirigé vers la page web demandée à l'origine



Connexion
Vous pouvez vous authentifier, modifier votre mot de passe..

Obtention d'accès via Sponsoring

Veuillez saisir les informations ci-dessous (?)

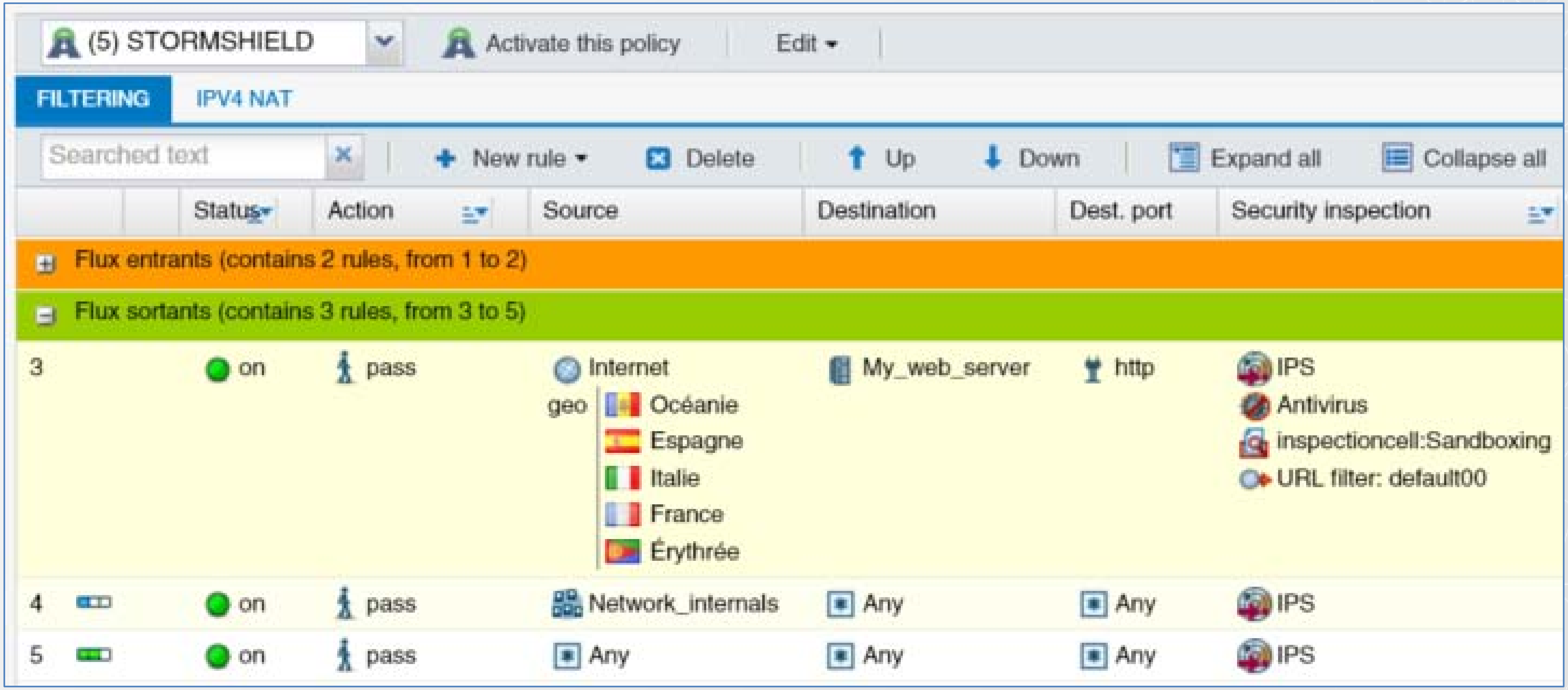
Après validation un mail de confirmation sera envoyé au référent qui validera votre accès.

Nom	
Prénom	
Adresse mail du référent	
Adresse mail personnelle (Cette dernière servira d'identité)	

Géolocalisation

Stormshield Network Security

GEOLOCALISATION



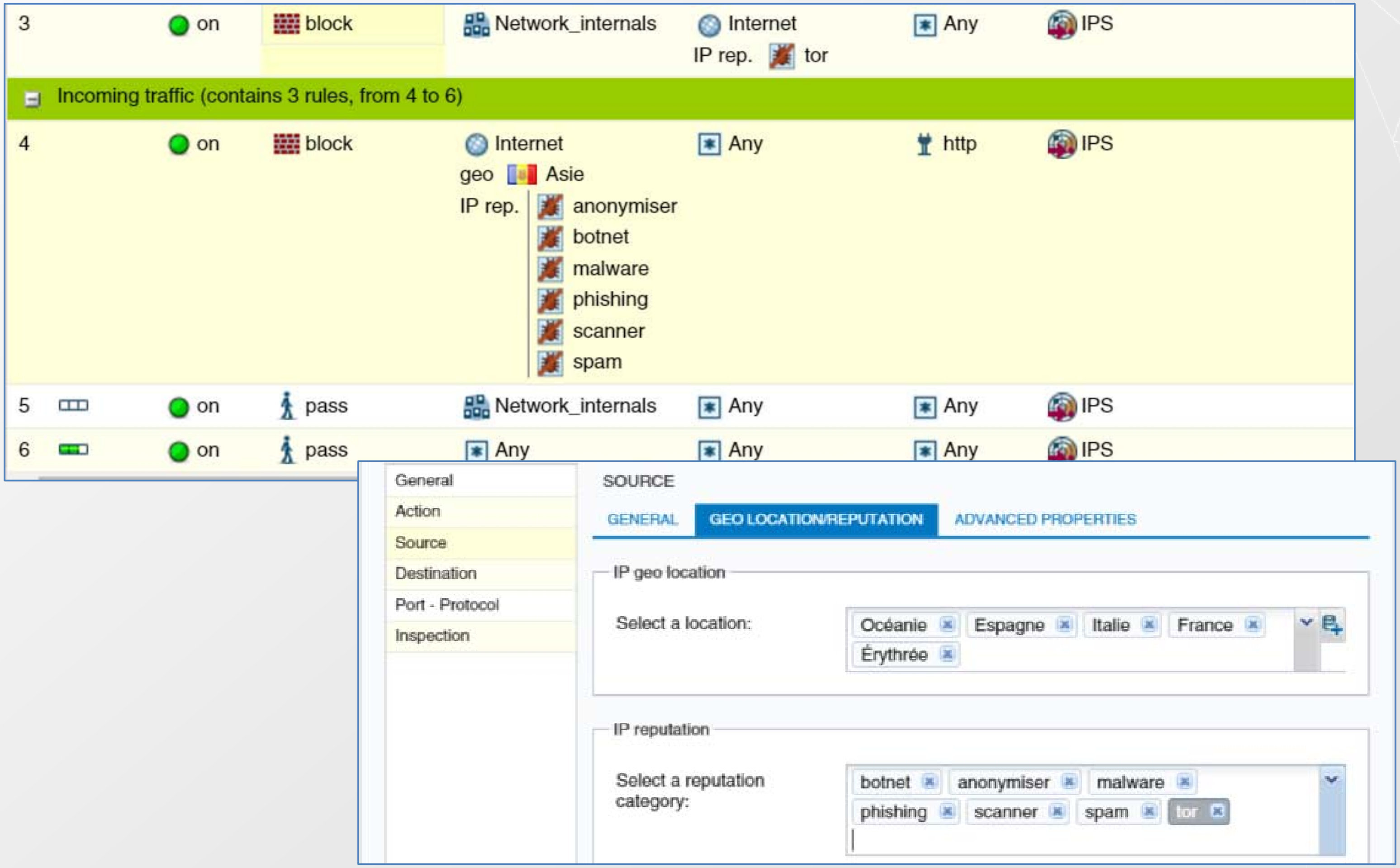
		Status	Action	Source	Destination	Dest. port	Security inspection
⊞ Flux entrants (contains 2 rules, from 1 to 2)							
⊟ Flux sortants (contains 3 rules, from 3 to 5)							
3		● on	pass	Internet geo Océanie Espagne Italie France Érythrée	My_web_server	http	IPS Antivirus inspectioncell:Sandboxing URL filter: default00
4		● on	pass	Network_internals	Any	Any	IPS
5		● on	pass	Any	Any	Any	IPS

STORMSHIELD

IP Réputation

Stormshield Network Security

IPREPUTATION



3		on	block	Network_internals	Internet IP rep. tor	Any	IPS
Incoming traffic (contains 3 rules, from 4 to 6)							
4		on	block	Internet geo Asie IP rep. anonymiser botnet malware phishing scanner spam	Any	http	IPS
5	▭▭▭	on	pass	Network_internals	Any	Any	IPS
6	▬	on	pass	Any	Any	Any	IPS

SOURCE

IP geo location

Select a location: Océanie, Espagne, Italie, France, Érythrée

IP reputation

Select a reputation category: botnet, anonymiser, malware, phishing, scanner, spam, tor

STORMSHIELD

Host Réputation

Stormshield Network Security

SYSTÈME DE SCORE

LE SCORE POURRA ETRE UTILISE DANS UNE POLITIQUE DE FILTRAGE

Sera basé dans un premier temps sur:

-Analyse Antivirale

-Analyse IPS

-BreachFighter (sandboxing)

Autres ajouts

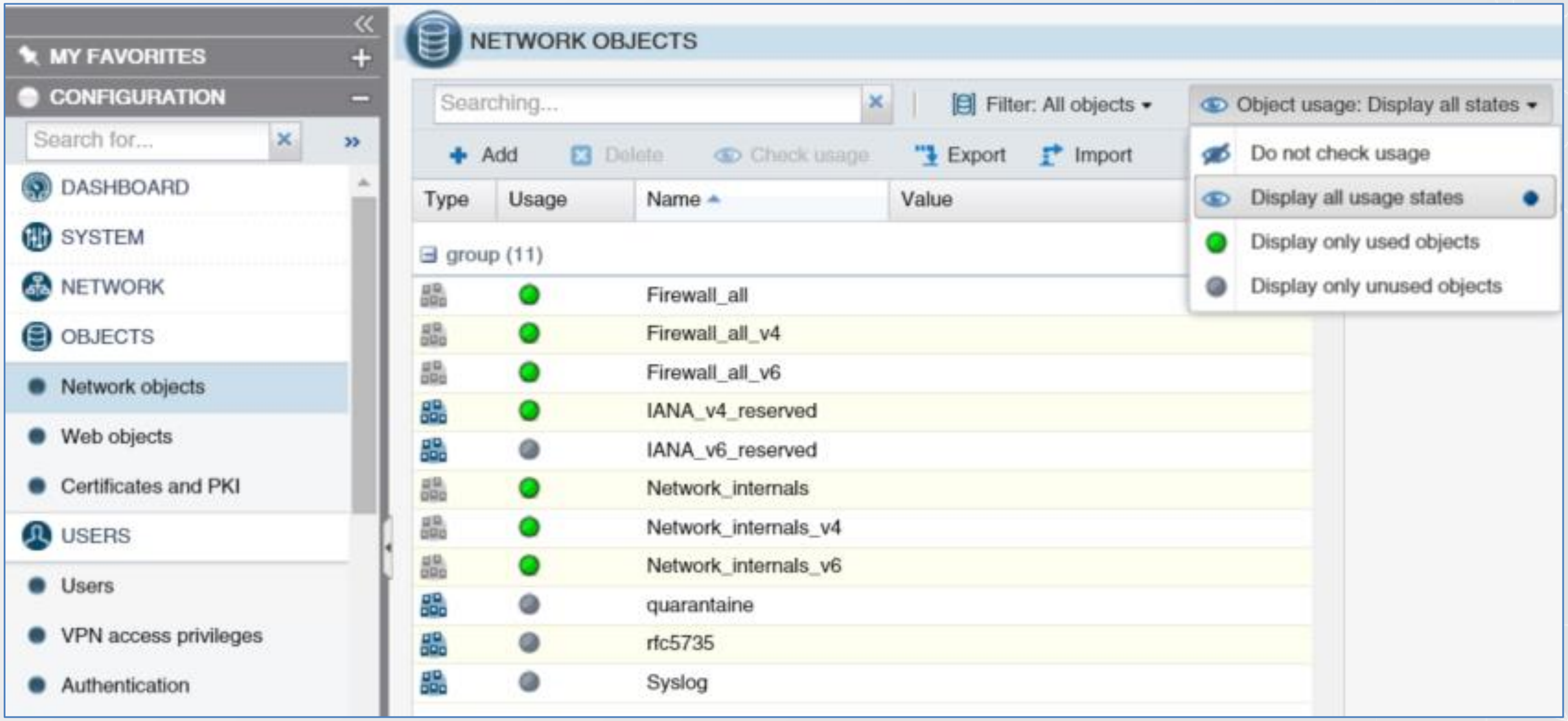
Stormshield Network Security

BASE D’OBJETS

-Visualisation rapide des objets utilisés et non-utilisés

-Import/Export des objets (.csv)

-L’affichage de tous les objets est plus rapide et plus complet qu’auparavant



MY FAVORITES +

CONFIGURATION −

Search for... ✕ »

DASHBOARD

SYSTEM

NETWORK

OBJECTS

- Network objects
- Web objects
- Certificates and PKI

USERS

- Users
- VPN access privileges
- Authentication

NETWORK OBJECTS

Searching... ✕ | Filter: All objects ▾ | Object usage: Display all states ▾

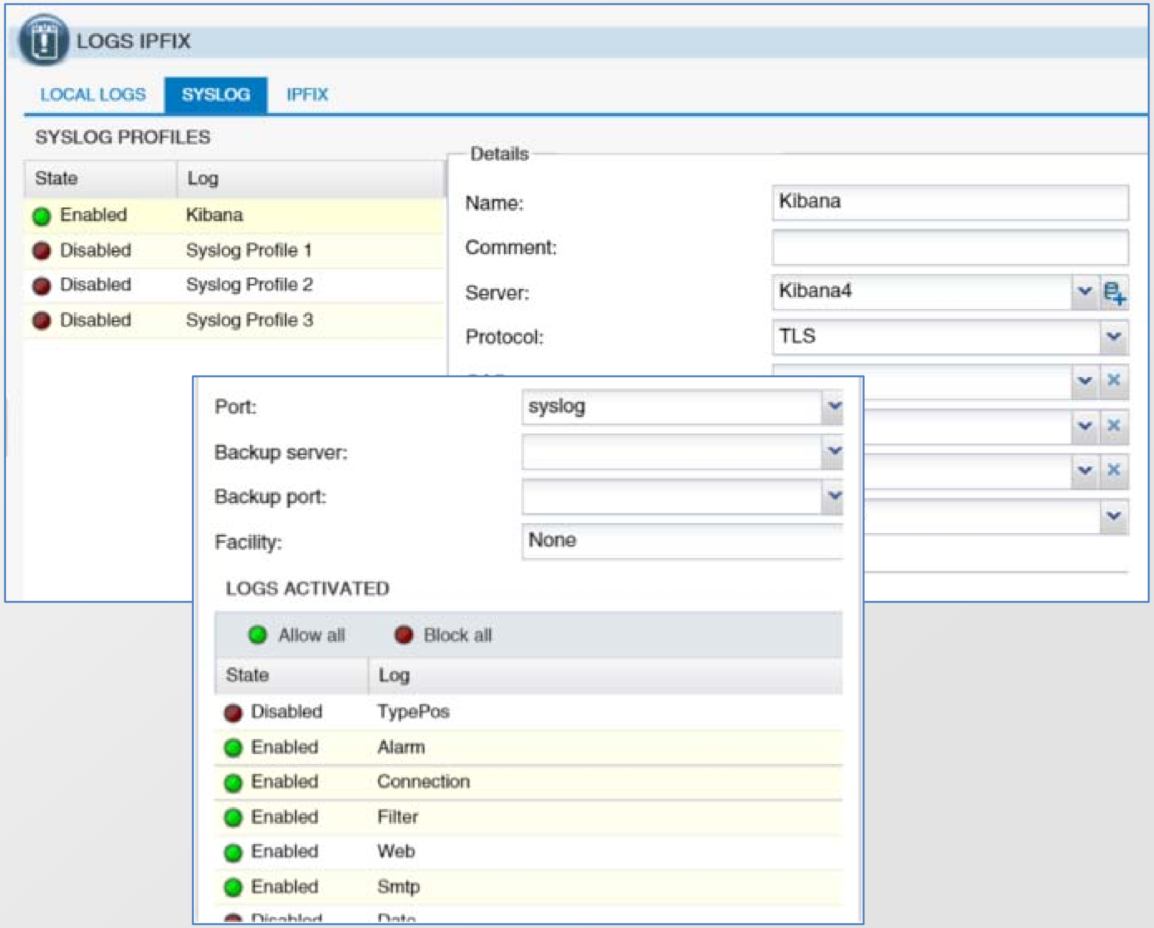
+ Add | Delete | Check usage | Export | Import

- Do not check usage
- Display all usage states ●
- 🟢 Display only used objects
- ⚪ Display only unused objects

Type	Usage	Name ▴	Value
group (11)			
	🟢	Firewall_all	
	🟢	Firewall_all_v4	
	🟢	Firewall_all_v6	
	🟢	IANA_v4_reserved	
	⚪	IANA_v6_reserved	
	🟢	Network_internals	
	🟢	Network_internals_v4	
	🟢	Network_internals_v6	
	⚪	quarantaine	
	⚪	rfc5735	
	⚪	Syslog	

SYSLOG TCP/TLS

-Chiffrement des communications Syslog



LOGS IPFIX

SYSLOG PROFILES

State	Log
● Enabled	Kibana
● Disabled	Syslog Profile 1
● Disabled	Syslog Profile 2
● Disabled	Syslog Profile 3

Details

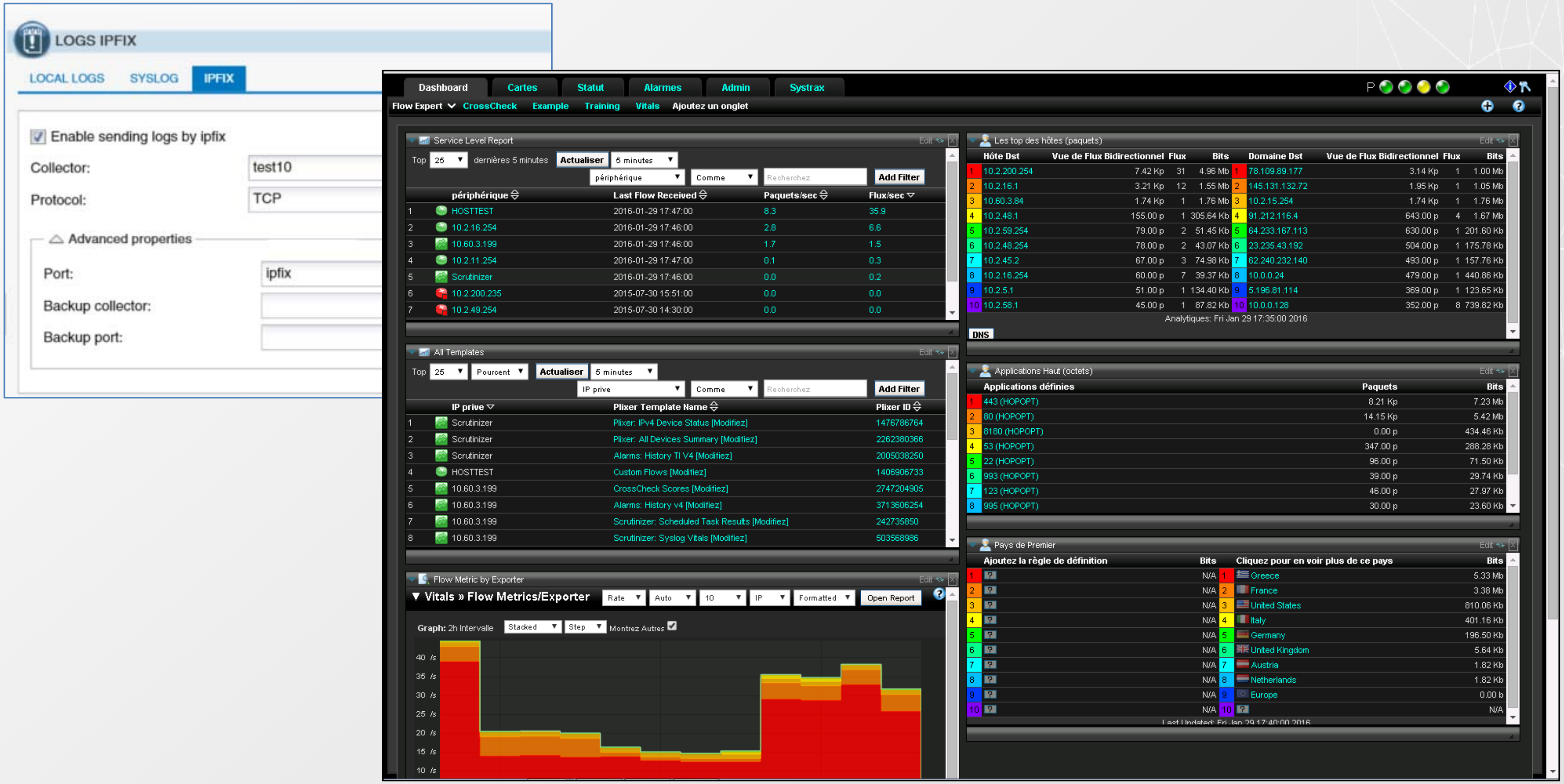
Name:	Kibana
Comment:	
Server:	Kibana4
Protocol:	TLS
Port:	syslog
Backup server:	
Backup port:	
Facility:	None

LOGS ACTIVATED

State	Log
● Disabled	TypePos
● Enabled	Alarm
● Enabled	Connection
● Enabled	Filter
● Enabled	Web
● Enabled	Smtp
● Disabled	Data

STORMSHIELD

IPFIX/NETFLOW



LOGS IPFIX

☑ Enable sending logs by ipfix

Collector: test10

Protocol: TCP

Advanced properties

Port: ipfix

Backup collector:

Backup port:

Service Level Report

Top 25 dernières 5 minutes Actualiser 5 minutes

périphérique Comme Recherchez Add Filter

	périphérique	Last Flow Received	Paquets/sec	Flux/sec
1	HOSTTEST	2016-01-29 17:47:00	8.3	35.9
2	10.2.16.254	2016-01-29 17:46:00	2.8	6.6
3	10.60.3.199	2016-01-29 17:46:00	1.7	1.5
4	10.2.11.254	2016-01-29 17:47:00	0.1	0.3
5	Scrutinizer	2016-01-29 17:46:00	0.0	0.2
6	10.2.200.235	2015-07-30 15:51:00	0.0	0.0
7	10.2.49.254	2015-07-30 14:30:00	0.0	0.0

All Templates

Top 25 Pourcent Actualiser 5 minutes

IP prive Comme Recherchez Add Filter

	IP prive	Plixer Template Name	Plixer ID
1	Scrutinizer	Plixer: IPv4 Device Status [Modifiez]	1476786764
2	Scrutinizer	Plixer: All Devices Summary [Modifiez]	2262380366
3	Scrutinizer	Alarms: History TI V4 [Modifiez]	2005038250
4	HOSTTEST	Custom Flows [Modifiez]	1406906733
5	10.60.3.199	CrossCheck Scores [Modifiez]	2747204905
6	10.60.3.199	Alarms: History v4 [Modifiez]	3713606254
7	10.60.3.199	Scrutinizer: Scheduled Task Results [Modifiez]	242735850
8	10.60.3.199	Scrutinizer: Syslog Vitals [Modifiez]	503568986

Flow Metric by Exporter

▼ Vitals » Flow Metrics/Exporter

Rate Auto 10 IP Formatted Open Report

Graph: 2h Intervalle Stacked Step Montrez Autres ☑

Les top des hôtes (paquets)

	Hôte Dst	Vue de Flux Bidirectionnel	Flux	Bits		Domaine Dst	Vue de Flux Bidirectionnel	Flux	Bits
1	10.2.200.254	7.42 Kp	31	4.96 Mb	1	78.109.89.177	3.14 Kp	1	1.00 Mb
2	10.2.16.1	3.21 Kp	12	1.55 Mb	2	145.131.132.72	1.95 Kp	1	1.05 Mb
3	10.60.3.84	1.74 Kp	1	1.76 Mb	3	10.2.15.254	1.74 Kp	1	1.76 Mb
4	10.2.48.1	155.00 p	1	305.64 Kb	4	91.212.116.4	643.00 p	4	1.67 Mb
5	10.2.59.254	79.00 p	2	51.45 Kb	5	64.233.167.113	630.00 p	1	201.60 Kb
6	10.2.48.254	78.00 p	2	43.07 Kb	6	23.235.43.192	504.00 p	1	175.78 Kb
7	10.2.45.2	67.00 p	3	74.98 Kb	7	62.240.232.140	493.00 p	1	157.76 Kb
8	10.2.16.254	60.00 p	7	39.37 Kb	8	10.0.0.24	479.00 p	1	440.86 Kb
9	10.2.5.1	51.00 p	1	134.40 Kb	9	5.196.81.114	369.00 p	1	123.65 Kb
10	10.2.58.1	45.00 p	1	87.82 Kb	10	10.0.0.128	352.00 p	8	739.82 Kb

Analytiques: Fri Jan 29 17:35:00 2016

DNS

Applications Haut (octets)

	Applications définies	Paquets	Bits
1	443 (HOPOPT)	8.21 Kp	7.23 Mb
2	80 (HOPOPT)	14.15 Kp	5.42 Mb
3	8180 (HOPOPT)	0.00 p	434.46 Kb
4	53 (HOPOPT)	347.00 p	288.28 Kb
5	22 (HOPOPT)	96.00 p	71.50 Kb
6	993 (HOPOPT)	39.00 p	29.74 Kb
7	123 (HOPOPT)	46.00 p	27.97 Kb
8	995 (HOPOPT)	30.00 p	23.60 Kb

Pays de Premier

	Ajoutez la règle de définition	Bits		Cliquez pour en voir plus de ce pays	Bits
1	?	N/A	1	Greece	5.33 Mb
2	?	N/A	2	France	3.38 Mb
3	?	N/A	3	United States	810.06 Kb
4	?	N/A	4	Italy	401.16 Kb
5	?	N/A	5	Germany	196.50 Kb
6	?	N/A	6	United Kingdom	5.64 Kb
7	?	N/A	7	Austria	1.82 Kb
8	?	N/A	8	Netherlands	1.82 Kb
9	?	N/A	9	Europe	0.00 b
10	?	N/A	10	?	N/A

Last Updated: Fri Jan 29 17:40:00 2016

SIGNATURES D’APPLICATIONS PERSONNALISEES

Vous aurez la possibilité de créer vos propres signatures

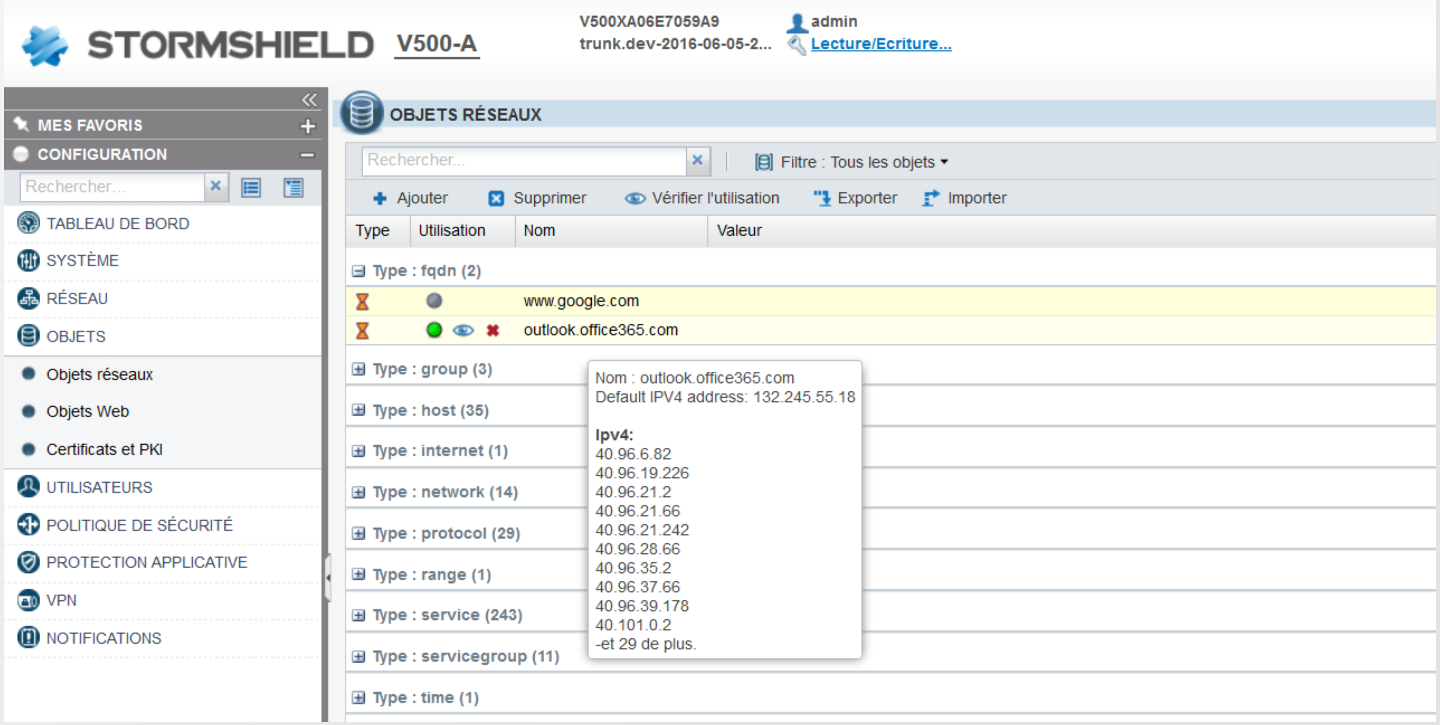
PASS THE HASH

Renforcement de la méthode d’authentification par règles de filtrage

Protocoles CIFS et DCERPC. Nous vérifions si le login utilisateur est présent dans la requête envoyés par la station de travail

OBJETS FQDN

Il devient possible d’utiliser des Objets FQDN dans les règles de filtrage afin de prendre en compte toutes les adresses renvoyés par la requête DNS,



Type	Utilisation	Nom	Valeur
⊟ Type : fqdn (2)			
⧗	●	www.google.com	
⧗	● 👁 ✖	outlook.office365.com	
⊞ Type : group (3)			
⊞ Type : host (35)			
⊞ Type : internet (1)			
⊞ Type : network (14)			
⊞ Type : protocol (29)			
⊞ Type : range (1)			
⊞ Type : service (243)			
⊞ Type : servicegroup (11)			
⊞ Type : time (1)			

Nom : outlook.office365.com
Default IPV4 address: 132.245.55.18

Ipv4:
40.96.6.82
40.96.19.226
40.96.21.2
40.96.21.66
40.96.21.242
40.96.28.66
40.96.35.2
40.96.37.66
40.96.39.178
40.101.0.2
-et 29 de plus.

STORMSHIELD

Merci

Stormshield Network Security

WWW.STORMSHIELD.EU