

Version en ligne

OFFERTE !

pendant 1 an

+ QUIZ 

Stormshield

Configuration et mise en œuvre
de votre pare-feu

En téléchargement



Exemples
de configuration



informatique technique




Collection

epsilon

Alejandro CASTAÑO FERNÁNDEZ



Les éléments à télécharger sont disponibles à l'adresse suivante :
<http://www.editions-eni.fr>
Saisissez la référence de l'ouvrage **EPSTORM** dans la zone de recherche et validez. Cliquez sur le titre du livre puis sur le bouton de téléchargement.

Chapitre 1
Introduction

- 1. Objectifs du livre 15
- 2. Public visé 16
- 3. Connaissances préalables recommandées 16
- 4. Organisation de l'ouvrage..... 18
- 5. Conventions d'écriture 19

Chapitre 2
La gamme Stormshield Network Security

- 1. Qu'est-ce que Stormshield ? 21
 - 1.1 Un portefeuille de produits pour une réponse globale
aux besoins de sécurité des environnements IT/OT 22
 - 1.1.1 Protection des réseaux physiques
et des infrastructures virtualisées 22
 - 1.1.2 Protection des données 22
 - 1.1.3 Protection des postes et des serveurs 22
 - 1.2 Certifications et qualifications françaises
des produits de sécurité 23
- 2. Recommandations de sécurisation
d'un pare-feu SNS. Guide ANSSI 24
 - 2.1 Administration du pare-feu 25
 - 2.2 Configuration réseau 25
 - 2.3 Configuration des services 25
 - 2.4 Politique de filtrage réseau et NAT 26
 - 2.5 Certificats et PKI 26

2 **Stormshield**

Configuration et mise en œuvre de votre pare-feu

2.6	VPN IPSec	26
2.7	Supervision	27
2.8	Sauvegarde	27
2.9	Journalisation	27
2.10	Gestion du parc	27
3.	Stormshield Academy, certifications	
	Stormshield Network Security (SNS)	28
3.1	Cursus SNS	29
3.2	Partenariat avec les grandes écoles et universités	30
4.	Gestion des produits SNS	31
4.1	Espace client	31
4.1.1	Base de connaissances Stormshield	34
4.2	Documentation	35
4.3	Création d'un ticket	36
4.4	RMA (Return Merchandise Authorization, ou Procédure d'échange matériel)	39
4.4.1	Garantie standard	39
4.4.2	Garantie Express	40
4.4.3	Échange DOA (Dead On Arrival, « Mort dès son arrivée »)	40
4.4.4	Serenity for all (Sérénité pour tous)	40
4.5	Licence	40
4.5.1	Administration	41
4.5.2	Modules	41
4.5.3	Options	42
4.5.4	Global	43
4.5.5	Matériel	44
4.5.6	Limites	44
4.5.7	Réseau	44
4.5.8	Proxy	45
4.5.9	Services	46
4.5.10	VPN (Virtual Private Network)	47

4.6	Types d'offres	47
4.6.1	Remote Office Security Pack	47
4.6.2	UTM Security Pack	48
4.6.3	Premium UTM Security Pack	48
4.6.4	Enterprise Security Pack	48
4.6.5	Pay-as-you-go (Payer au fur et à mesure)	48
5.	Modèles de la gamme SNS	49
5.1	SN160(W)	50
5.1.1	Descriptif	50
5.1.2	Spécifications techniques	50
5.2	SN210(W)	52
5.2.1	Descriptif	52
5.2.2	Spécifications techniques	52
5.3	SN310	54
5.3.1	Descriptif	54
5.3.2	Spécifications techniques	54
5.4	SN510	55
5.4.1	Descriptif	55
5.4.2	Spécifications techniques	56
5.4.3	Options matérielles	57
5.5	SN710	57
5.5.1	Descriptif	57
5.5.2	Spécifications techniques	57
5.5.3	Options matérielles	58
5.6	SN910	59
5.6.1	Descriptif	59
5.6.2	Spécifications techniques	59
5.7	SN2100	61
5.7.1	Descriptif	61
5.7.2	Spécifications techniques	61
5.7.3	Options matérielles	62

5.8	SN3100	63
5.8.1	Descriptif	63
5.8.2	Spécifications techniques	63
5.8.3	Options matérielles	65
5.9	SN6100	65
5.9.1	Descriptif	65
5.9.2	Spécifications techniques	65
5.9.3	Options matérielles	67
5.10	SNi40	67
5.10.1	Descriptif	67
5.10.2	Spécifications techniques	67
5.10.3	Options matérielles	68
5.11	Machines virtuelles	69
5.11.1	Descriptif	69
5.11.2	Modèles et performances	69
5.11.3	Prérequis concernant les hyperviseurs	71

Chapitre 3

Interfaces de gestion

1.	Objectifs du chapitre	73
2.	Configuration par défaut présente sur l'UTM physique	74
2.1	Authentification	74
2.2	Réseau	74
2.3	Filtrage	75
3.	Interface graphique (IHM ou GUI)	75
4.	Configuration par défaut sur une VM	80
4.1	Déploiement d'une EVA sur VMware	80
4.2	Déploiement d'une VM sur Virtualbox	91

- 5. Interface CLI 97
 - 5.1 Accès en console 97
 - 5.1.1 Sur une UTM physique 97
 - 5.1.2 Sur une UTM virtuelle 97
 - 5.2 Accès avec un client SSH 98
 - 5.2.1 Putty sur Windows 99
 - 5.2.2 Client SSH sur Linux 101
 - 5.3 Accès en SRP 102
 - 5.3.1 Depuis une UTM 102
 - 5.3.2 Depuis un poste GNU/Linux 103
 - 5.3.3 Depuis un poste Windows 104
- 6. Interface centralisée (SMC) 108

Chapitre 4
Configuration

- 1. Introduction 109
- 2. Menu "admin" 110
 - 2.1 Obtenir ou libérer le droit d'écriture 111
 - 2.1.1 Obtenir le droit d'écriture 111
 - 2.1.2 Libérer le droit d'écriture 115
 - 2.2 Obtenir ou libérer le droit d'accès
aux données personnelles (logs) 117
 - 2.3 Préférences 121
 - 2.3.1 Restaurer les paramètres de connexion 122
 - 2.3.2 Paramètres de connexion 122
 - 2.3.3 Paramètres de l'application 122
 - 2.4 Se déconnecter 123
- 3. Système 124
 - 3.1 Configuration 124
 - 3.1.1 Configuration générale 124
 - 3.1.2 Administration du firewall 129
 - 3.1.3 Paramètres réseau 132

6 **Stormshield**

Configuration et mise en œuvre de votre pare-feu

3.2	Administrateurs	134
3.2.1	Administrateurs	134
3.2.2	Compte Admin	137
3.2.3	Gestion de tickets	138
3.3	Licence	140
3.3.1	Général	140
3.3.2	Détails de la licence	142
3.4	Maintenance	143
3.4.1	Mise à jour du système	143
3.4.2	Sauvegarder	146
3.4.3	Restaurer	148
3.4.4	Configuration	149
3.5	Active update (Mises à jour automatiques)	152
3.5.1	Configuration avancée	153
3.6	Haute disponibilité	154
3.6.1	Créer un groupe de firewalls (cluster)	156
3.6.2	Joindre un cluster	160
3.7	Management Center	165
3.7.1	Rattachement du firewall au serveur SMC	166
3.8	Console CLI	168
4.	Réseau	169
4.1	Interfaces	169
4.1.1	Interfaces externes ou internes (protégées)	170
4.1.2	Paramètres des interfaces	171
4.1.3	Interface ethernet	173
4.1.4	Interface bridge	174
4.1.5	Interface VLAN	177
4.1.6	Interface GRETAP	181
4.1.7	Interface Modem Ppoe	181
4.1.8	Interface Modem PPTP	184
4.1.9	Interface USB/Ethernet (Clé USB/Modem)	186
4.1.10	Interface d'agrégation de liens (LACP)	189

- 4.2 Interfaces virtuelles 192
 - 4.2.1 Interfaces VTI 192
 - 4.2.2 Interfaces GREtun 193
 - 4.2.3 Loopback 194
- 4.3 Routage 195
 - 4.3.1 Routage statique 195
 - 4.3.2 Routage dynamique 196
 - 4.3.3 Routes de retour 198
- 4.4 Routage multicast 199
- 4.5 DNS dynamique 201
- 4.6 DHCP 202
 - 4.6.1 Serveur DHCP 202
 - 4.6.2 Relai DHCP 205
- 4.7 Proxy Cache DNS 206
- 5. Objets 208
 - 5.1 Objets réseau 208
 - 5.1.1 Objet de type Machine (hôte) 209
 - 5.1.2 Objet de type FQDN (Nom DNS) 211
 - 5.1.3 Objet de type Réseau 212
 - 5.1.4 Objet de type Plage d'adresses IP 213
 - 5.1.5 Objet de type Routeur 214
 - 5.1.6 Objet de type Groupe (hôtes et réseaux) 216
 - 5.1.7 Objet de type Protocole IP 218
 - 5.1.8 Objet de type Port 220
 - 5.1.9 Objet de type Groupe de ports 221
 - 5.1.10 Objet de type Groupe de régions 222
 - 5.1.11 Objets de type Temps 223
 - 5.2 Objets Web 225
 - 5.2.1 URL 225
 - 5.2.2 Nom de certificat (Common Name) 226
 - 5.2.3 Groupe de catégories 227
 - 5.2.4 Base d'URL 229

8 **Stormshield**

Configuration et mise en œuvre de votre pare-feu

5.3	Certificats et PKI	236
5.3.1	Création d'une CA (Root CA)	240
5.3.2	Ajout d'une CA	243
6.	Utilisateurs	246
6.1	Utilisateurs	246
6.2	Comptes temporaires	247
6.3	Droits d'accès	248
6.3.1	Accès par défaut	249
6.3.2	Accès détaillé	250
6.3.3	Serveur PPTP	250
6.4	Authentification	251
6.4.1	Méthodes disponibles	251
6.4.2	Politique d'authentification	257
6.4.3	Portail captif	259
6.4.4	Profils du portail captif	259
6.5	Enrôlement	261
6.6	Configuration des annuaires	263
7.	Politique de sécurité	268
7.1	Filtrage et NAT	269
7.1.1	Onglet Filtrage	269
7.1.2	Onglet NAT	282
7.2	Filtrage URL	284
7.3	Filtrage SSL	285
7.4	Filtrage SMTP	288
7.5	Qualité de service	289
7.6	Règles implicites	291
8.	Protection applicative	293
8.1	Applications et protections	293
8.2	Protocoles	295
8.3	Profils d'inspection	297
8.4	Management de vulnérabilités	298

8.5	Réputation des machines	299
8.5.1	Configuration	299
8.5.2	Machines	300
8.6	Antivirus	300
8.6.1	Kaspersky	300
8.6.2	Clamav	301
8.7	Antispam	302
8.7.1	Général	302
8.7.2	Domaines en liste blanche	303
8.7.3	Domaines en liste noire	304
9.	VPN	304
9.1	VPN IPSec	304
9.1.1	Politique de chiffrement - tunnels	305
9.1.2	Correspondants	306
9.1.3	Identification	308
9.1.4	Profils de chiffrement	309
9.2	VPN SSL Portail	311
9.3	VPN SSL	312
9.4	Serveur PPTP	314
10.	Notifications	315
10.1	Traces-Syslog-IPFix	315
10.2	Agent SNMP	319
10.3	Alertes e-mail	321
10.4	Événements système	323
10.5	Messages de blocage	324
10.6	Configuration des rapports	326
10.7	Configuration de la supervision	327

Chapitre 5 Monitoring

1. Introduction	329
2. Tableau de bord	330
2.1 Réseau	331
2.2 Propriétés.	331
2.3 Services	332
2.4 Protections	332
2.5 Indicateurs de santé	333
3. Logs - Journaux d'audit.	333
4. Rapports	335
5. Supervision	339

Chapitre 6 Gestion centralisée SMC

1. Introduction	343
2. Installation	344
2.1 Téléchargement de la machine virtuelle SMC	344
2.2 Installation	345
2.3 Assistant d'installation en ligne de commande	346
2.4 Assistant d'installation par l'interface graphique du SMC	348
3. Gestion de SMC	351
3.1 Installation d'une licence valide.	351
3.2 Paramètres.	353
3.3 Maintenance	354
3.4 Administrateurs	355
3.5 Journaux/traces	356
4. Supervision	357

- 5. Configuration 361
 - 5.1 Firewalls et dossiers 361
 - 5.1.1 Filtrage 361
 - 5.1.2 Topologies VPN 362
 - 5.2 Certificats 365
 - 5.3 Profils de chiffrement 367
 - 5.3.1 Ajout d'un profil de chiffrement 367
- 6. Objets réseau 368
- 7. Déploiement 369
- 8. Maintenance 370
- 9. Scripts CLI SNS 370

Chapitre 7
Exemples de configuration

- 1. Introduction 371
- 2. Réseau 371
 - 2.1 GRETAP 371
 - 2.1.1 Firewall Lille 372
 - 2.1.2 Firewall Paris 375
 - 2.1.3 Vérification de la connectivité
entre les deux réseaux identiques 375
 - 2.2 Gretun, interface virtuelle 377
- 3. Politique de sécurité 377
 - 3.1 Filtrage et NAT 377
 - 3.2 Règles implicites 383
 - 3.2.1 Règles implicites plugin 387
 - 3.2.2 HA 388
 - 3.2.3 Requêtes ident (port TCP/113) 390
 - 3.2.4 Serveur PPTP 390
 - 3.2.5 GRE 391
 - 3.2.6 SRP 391

3.2.7	SSH	392
3.2.8	OpenVPN (VPN SSL « full »)	393
3.2.9	VPN IPSec	393
3.2.10	Fwdefault	394
3.3	Proxy SSL	395
3.3.1	Création d'une règle de filtrage	397
3.3.2	Création de l'Autorité de certification	399
3.3.3	Paramétrage du proxy SSL	400
3.3.4	Ajout de la CA dans un navigateur Mozilla Firefox	401
3.3.5	Filtrage SSL	404
3.3.6	Filtrage URL	406
3.3.7	Alarmes IPS	407
4.	Utilisateurs	409
5.	VPN SSL	411
5.1	Configuration sur le SNS	411
5.2	Configuration sur client	414

Chapitre 8

Débogage

1.	Introduction	419
2.	Outils d'aide au diagnostic	419
2.1	Connaître l'adresse IP d'un hôte	419
2.1.1	Microsoft Windows	419
2.1.2	GNU/Linux	420
2.1.3	SNS	422
2.2	Tester la connectivité réseau entre deux hôtes	424
2.3	Résolution DNS d'un hôte	426
2.3.1	Microsoft Windows	426
2.3.2	GNU/Linux	428
2.3.3	SNS	429

2.4	Table de routage	430
2.4.1	Microsoft Windows	430
2.4.2	GNU/Linux	431
2.5	Prendre des captures	432
2.5.1	GNU/Linux et SNS	432
2.5.2	Microsoft Windows	436
3.	Récupération de la configuration	440
3.1	Réinitialisation du mot de passe de l'utilisateur admin	440
3.2	Récupération de la configuration par defaultconfig	441
4.	Réseau	444
4.1	Bridge	444
4.1.1	Enregistrement des hôtes	444
4.1.2	Mode protégé du bridge	445
4.2	Routage	445
4.2.1	Interface de sortie	445
5.	Objets	446
5.1	Régénération des CA présentes dans l'UTM	446
6.	IPS	447
6.1	Commandes sfctl (Stateful control)	447
6.1.1	Règles de filtrage et NAT	447
6.1.2	Correspondance des règles	449
6.1.3	Hôtes	450
6.1.4	Connexions	450
6.1.5	Utilisateurs	452
6.1.6	Routage vis-à-vis de l'IPS	452
6.1.7	Autres commandes sfctl	453
	Index	455



Chapitre 6

Gestion centralisée SMC

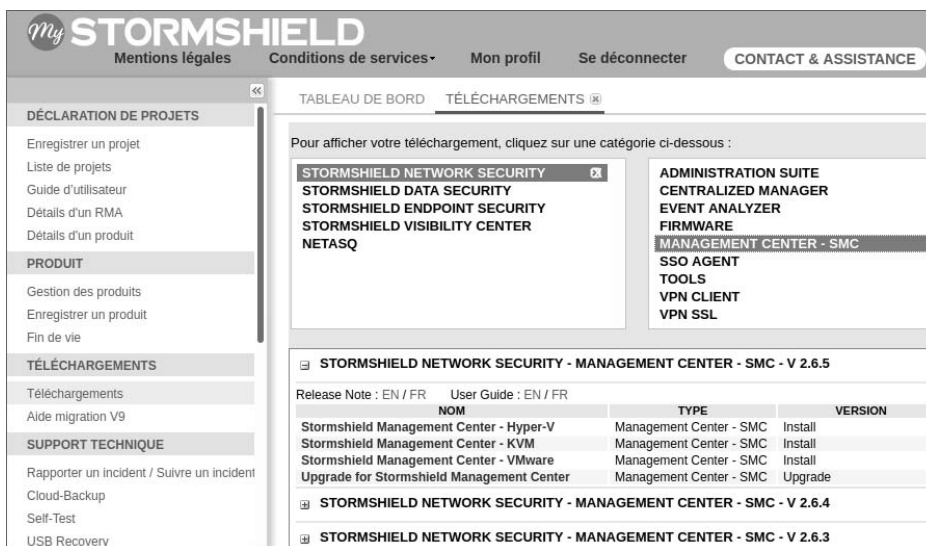
1. Introduction

De nos jours, les entreprises et d'autres opérateurs sensibles optent pour une gestion centralisée de la sécurité informatique. Quelques avantages se dégagent de cette approche. Le premier est de disposer d'une configuration homogène sur tout notre parc informatique. En effet, des éléments de sécurité tels qu'un firewall qui ne seraient pas trop utilisés et/ou oubliés peuvent représenter le maillon faible de toute une infrastructure informatique. Une seule interface de gestion simplifiera la mise en place, entre autres, de tunnels VPN IPSec entre les différents correspondants. Un unique point pour vérifier, par exemple, les versions des logiciels peut être aussi un point très positif.

2. Installation

2.1 Téléchargement de la machine virtuelle SMC

■ Depuis l'espace client Stormshield, qui se trouve à l'adresse <https://mystormshield.eu>, vous pouvez télécharger la machine virtuelle SMC. Il faut suivre le chemin **Téléchargements** - **Téléchargements** - **Stormshield Network Security - Management Center - SMC** et en bas de l'écran vous pouvez télécharger la machine virtuelle :



The screenshot shows the Stormshield client interface. The main content area is titled "TÉLÉCHARGEMENTS" and contains a list of download categories. The "MANAGEMENT CENTER - SMC" category is selected, showing a list of download items. The first item is "STORMSHIELD NETWORK SECURITY - MANAGEMENT CENTER - SMC - V 2.6.5". Below this, there is a table with columns for "NOM", "TYPE", and "VERSION".

NOM	TYPE	VERSION
Stormshield Management Center - Hyper-V	Management Center - SMC	Install
Stormshield Management Center - KVM	Management Center - SMC	Install
Stormshield Management Center - VMware	Management Center - SMC	Install
Upgrade for Stormshield Management Center	Management Center - SMC	Upgrade

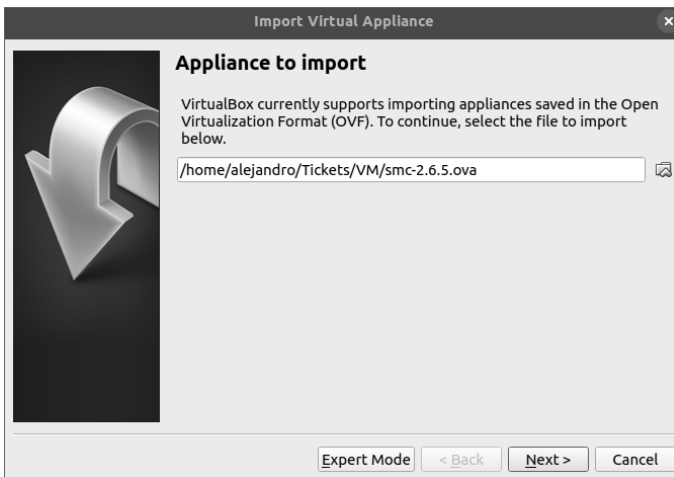
Vous avez le choix entre différents types de machines virtuelles :

- Hyper -V
- KVM
- VMware

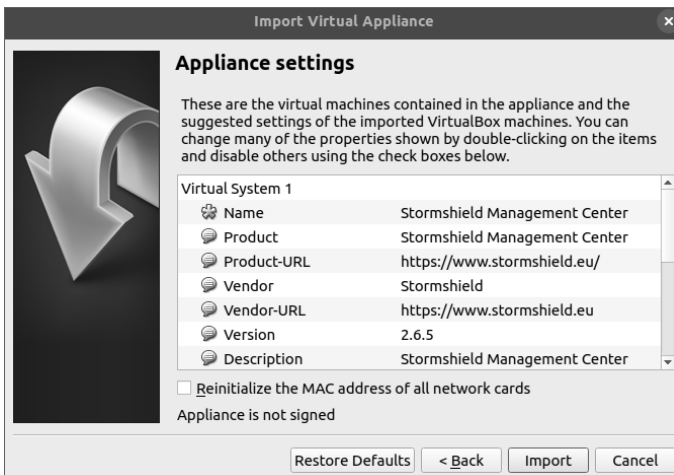
2.2 Installation

Dans notre exemple, nous allons utiliser Virtualbox pour installer SMC ; vous avez le choix, comme vu plus haut, d'autres hyperviseurs.

▣ Vous devez importer le fichier ova dans Virtual Box.



▣ En cliquant sur **Next**, quelques informations sont affichées à l'écran et vous pouvez cliquer sur **Import** :



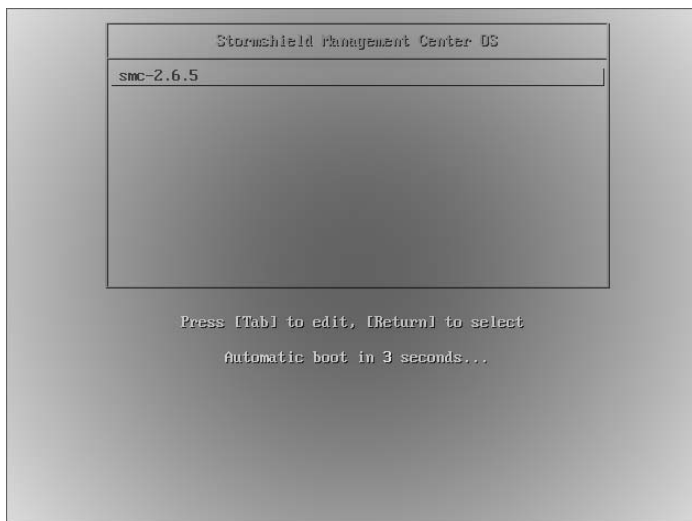
► Vous devez accepter les termes et les conditions de la licence du SMC :



2.3 Assistant d'installation en ligne de commande

Nous allons utiliser l'assistant de configuration en ligne de commandes pour configurer les paramètres de base de SMC (configuration initiale).

► Une fois la machine virtuelle importée, lancez-la.



- ▶ Appuyez sur n'importe quelle touche pour entrer dans l'assistant de configuration lorsque vous verrez le message :

```
[...]  
Press a key to enter manual server setup (5s)  
[...]
```

- ▶ La première chose à faire est de choisir la langue du clavier, dans notre cas **fr** :

```
Press a key to enter manual server setup (5s)  
  
-----  
|  M I N I M A L   W I Z A R D   C O N F I G U R A T I O N   |  
-----  
Please enter your keyboard layout (fr, us, ch, de, es, it, pl) [us]: _
```

- ▶ Juste après avoir renseigné la langue de votre clavier, vous devez entrer l'adresse IP de l'interface *eth0* (sans le masque de réseau, puis le masque de réseau), la passerelle (si nécessaire) et le serveur DNS :

```
Summary (eth0)  
- Address: 192.168.1.249  
- Netmask: 255.255.255.0  
- Gateway: 192.168.1.1  
- DNS: 8.8.8.8  
Are you sure you want to set these network settings (yes/no) [yes]: _
```

- ▶ Désormais, vous devez vous occuper du fuseau horaire. On vous demande si vous souhaitez utiliser un serveur NTP ou rester en date manuelle sur votre SMC.

```
Please enter your date/time settings  
  
- Current timezone: Europe/Paris  
- Do you want to configure timezone? (yes/no) [no]: no  
  
- Do you want to set date/time manually or with NTP (manual/ntp) [manual]? manual  
- Enter date and hour [2020-08-03 23:08:48]:  
TIMEZONE=Europe/Paris  
NTPSERVERS=none  
LOCALDATE=2020-08-03 23:08:51  
  
End of initial configuration. Press ENTER to continue...
```

- Une fois que l'assistant a fini, authentifiez-vous avec le login **root** et le mot de passe **root** en console.

```
Stormshield Management Center version: 2.6.5

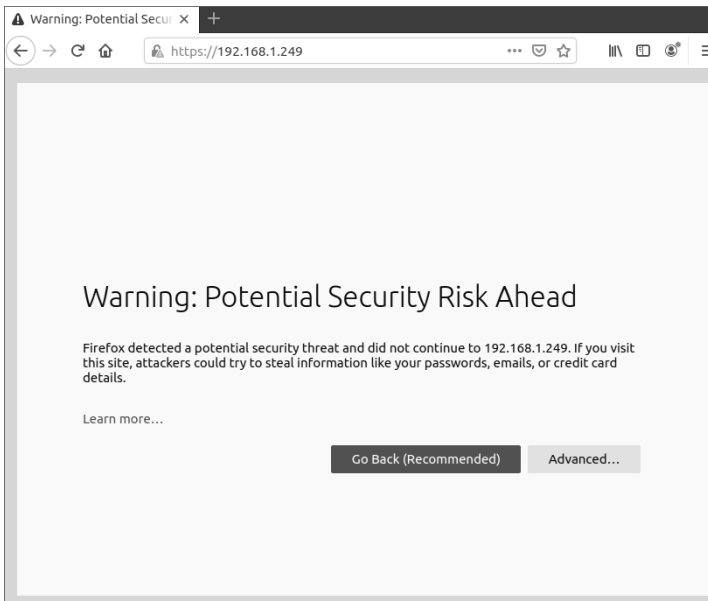
You can access your server at:
https://192.168.1.249

smc login: root
Password:
Last login: Mon Aug 3 23:12:22 CEST 2020 on tty1
[root@smc] - {} >
```

2.4 Assistant d'installation par l'interface graphique du SMC

Désormais nous passons à la deuxième partie de la configuration d'un SMC. Celle-ci se fait en GUI.

- Sur un navigateur web, entrez l'adresse IP telle qu'elle est affichée sur la console SMC. Une alerte est levée par votre navigateur, car il s'agit d'un site en HTTPS et le serveur SMC présente un certificat autosigné :



- En acceptant cette alerte, vous obtenez un assistant de configuration SMC en interface graphique. Il n'y a que trois pas à suivre : le premier vous demande si vous souhaitez initialiser le serveur SMC d'une manière manuelle ou depuis une sauvegarde. Puis, il demande la langue de l'interface web et du clavier :

ASSISTANT D'INITIALISATION DU SERVEUR SMC (ÉTAPE 1/3)

Je veux initialiser mon serveur :

Manuellement
 Depuis une sauvegarde

Sélectionnez une sauvegarde à restaurer :

Langue de l'interface web : Français

Disposition du clavier (console) : Français (fr)

« Précédent Suivant »

- L'étape suivante permet de changer la configuration réseau. Vous n'en avez pas besoin car elle a déjà été faite en console.

CONFIGURATION DU RÉSEAU (ÉTAPE 2/3)

Adresse IP : 192.168.1.249

Masque : 255.255.255.0

Passerelle par défaut : 192.168.1.1

Nom d'hôte : smc

Adresse du serveur DNS : 8.8.8.8

« Précédent Suivant »