FAQ Formation CSNA

Dernière Mise à jour : **14/06/2019**

Table des matières

Formation à distance CSNA 2
Plateforme en ligne https://institute.stormshield.eu 2
Ressources complémentaires utiles pour la formation 2
Organisation de la formation 2
Installation/configuration du Kit OVA 2
Quels sont les pré-requis pour l'installation du kit de machines virtuelles OVA ? 2
Prise en main du kit : questions diverses 3
Labs : questions diverses 3
Dépannage : questions diverses 4
Autres formations Stormshield 4
Certifications 4
Partenariat établissement 5
Questions sur le matériel 5
Performances, documentation technique 5

Formation à distance CSNA

Plateforme en ligne https://institute.stormshield.eu

Qui doit on contacter si nous n'avons pas reçu nos identifiants pour le site Institute?

Dans un premier temps, veuillez redemander un mot de passe sur la page d'accueil **https://institute.stormshield.eu,** en indiquant votre email académique. Si l'email n'est pas reconnu, il convient de signaler la situation en écrivant à institute@stormshield.eu

Que trouve-t-on sur ce site ?

Vous avez accès à plusieurs rubriques (voir diaporama pour détails p 20)

1. téléchargement des ressources officielles de formation : archive OVA avec les VM et pdf du cours
2. téléchargement des documents spécifiques à cette session Certa : en particulier le pdf d'aide à l'installation en complément du tutoriel vidéo de stormshield et les webinaires
3. lien vers l'examen en ligne (70 questions 1h30)

Quelle est la dernière version du support de cours CSNA?

CSNA_v3_Livre_de_formation_2018_05_17.pdf

Ressources complémentaires utiles pour la formation

https://frama.link/formationStormshieldCSNACerta

Organisation de la formation

Y-a-il une organisation prévue ou chacun fait à son rythme ?

Stormshield organise des webinaires d'accompagnement pour répondre aux questions diverses, la liste de diffusion peut être utilisée pour animer la formation et sollicitez vos pairs, vous pouvez le faire également à plusieurs au sein d'un même établissement, à vous de trouver votre rythme. Nous donnons des conseils de phasage ci-après pour ceux qui ne pourraient bloquer une semaine dessus.

Quelle est la durée approximative nécessaire ?

5 jours pleins (dont lecture attentive du support de cours) + 1 journée de révisions

Quelle progression si on le fait en plusieurs étapes ?

phase 1 aller jusqu'au lab 3 (réseau et routage) : compter 1,5 jours dont installation et prise en main de la plateforme virtuelle et des parefeux SNS (menus...)
phase 2 lab 4,5,6 (NAT, filtrage port, filtrage url) : compter 1,5 jours
phase 3 lab 7,8,9 (authentification, VPN, VPN SSL) : compter 1,5 jours
NB : durées comprenant les temps de lectures, vous pouvez aussi faire les labs d'un seul coup après étude du cours en amont, je déconseille de vous jeter sur les labs sans avoir lu le cours et regardé les exemples, les menus de l'interface

Installation/configuration du Kit OVA

Quels sont les pré-requis pour l'installation du kit de machines virtuelles OVA ?

Le kit de machines virtuelles est prévu pour être installé **sur Virtual Box** (version 5.2 et ultérieures) sur une seule machine hôte physique qui va simuler deux compagnies **A** et **B** et le **Trainer**.
Deux options sont possibles : la machine Windows qui permet d'accéder à la configuration des VM appliances SNS est la machine physique qui héberge les VM ou une VM que vous ajoutez au kit. Il est possible également d'installer le kit OVA sur une machine hôte linux, l'outil realtime monitor ne fonctionnant que sous windows, il faudra alors une VM Windows pour certaines manipulations.

- Prévoir **10 Go** d'espace disque libre pour télécharger l'archive, la décompresser puis importer les VM (**5Go** sur le disque cible)
- Prévoir **8Go de RAM** au minimum, 16 Go si vous utilisez une VM Windows pour l'administration

Que conseillez-vous d'utiliser pour accéder aux interfaces web de configuration des parefeux : la machine hôte ou une nouvelle machine virtuelle ?

Une **machine hôte** sous **windows** (de préférence à cause des difficultés d'installation parfois des VM sous d'autres systèmes, notamment la gestion du réseau sous linux et virtual box et de l'outil realtime monitor qui fonctionne sous windows) mais vous pouvez faire les tests avec une vm également, cela dépend de la mémoire de votre PC hôte (tabler alors sur 16 Go). Une VM légère sous linux (type TinyLinux) pour faire les tests de clients des Cies A et B peut être également intéressante.

Dans les étapes de configuration après installation de l'archive, il est écrit : désactiver une carte Virtual Host # 2 ou 3 sur la machine physique. Pourquoi désactiver un des réseaux ? Pourquoi y a-t-il un souci quand les deux Host-Only VirtualBox sont actifs ?

Lorsque je suis sur CieA en mode usine, le SNS A a une IP en 10.0.0.254 ; c'est la même adresse sur la seconde carte de CieB (cf ci-après), donc **on ne peut pas les activer simultanément => conflit d'adresse IP**

Par la suite, une fois le réseau opérationnel, si en tant que CieA, j'envoie un ping sur le réseau interne de CieB, cela ne marchera pas car le PC va utiliser la carte directement connectée au réseau interne de B.

Donc, on place le pc hôte soit sur le lan de A soit sur celui de B, mais pas les 2 en même temps ^^

En effet, pour démarrer une VM qui est derrière une interface de type Virtual Host, il est nécessaire que cette interface Virtual Host soit active, sinon, le démarrage échoue. Par la suite, on désactive l'interface de la compagnie avec laquelle on ne joue pas, alternativement.

Vous pouvez conserver les @IP statiques pour Cie A et Cie B et désactiver alternativement une carte ou l'autre.

Une fois l'infrastructure démarrée, je peux prendre en main l'interface Web des 3 SNS depuis mon poste physique avec les adresses :

*** 192.168.56.50 pour le trainer**

*** 192.168.56.10 pour company A**

*** 192.168.56.20 pour company B**

Les autres adresses des SNS Company A et B m'étonnent beaucoup : 10.0.0.254/8 !!

Est-ce normal au début ?

Oui on vous livre les VM dans le même état que si c'était des boîtiers physiques qui par défaut sont en mode bridge (à l'intérieur du boîtier toutes les cartes sont pontées par défaut), avec cette adresse par défaut qu'on peut joindre en se reliant physiquement à un port interne du boîtier (in, dmz1 et dmz2 sont considérées comme internes) cad jamais se brancher sur le port OUT/WAN sinon l'IP de la machine cliente est blacklistée (détection de tentative d'intrusion) et il faut remettre à zéro le boîtier!!

Qui doit on contacter si nous avons des problèmes pour le paramétrage des VM ?

Si la lecture attentive du document Installation-architecture-virtuelle-SNS-complement-d-information-v1.1.pdf et le visionnage du module elearning disponible via le fichier read_me.html fourni avec l'OVA ne vous ont pas permis d'avoir un environnement fonctionnel, vous pouvez contacter l'email institute@stormshield.eu en fournissant tous les éléments du problème rencontré tel que les étapes de reproduction du problème, les messages d'erreur ainsi que des captures d'écran.

Prise en main du kit : questions diverses

Je n'ai pas compris le rôle de l'environnement Trainer.

L'environnement trainer joue le rôle de la passerelle par défaut et accès à internet lorsque la NAT a été implémentée sur les firewalls des Compagnies A et B

Est-ce normal qu'une fois les VM démarrées je n'ai plus Internet sur le poste physique ?

Oui c'est normal jusqu'au lab sur les règles de nat

Depuis les Virtual WorkStation je n'ai pas accès à Internet. Est-ce normal ?

Oui c'est normal jusqu'au lab sur les règles de nat

Dans le doc d'installation, vous parlez de brancher la carte 4 du sns trainer sur la carte physique et non filaire. Est-ce possible d'utiliser la carte Wifi, notamment si c'est mon mode d'accès à internet ?

Oui wifi ou filaire pas de différence du point de vue de VMWare

À partir de la VM debian fournie, peut-on avoir un navigateur ?

Pas de navigateur sur la Debian, car pas d'interface graphique, juste la commande **wget**, il est possible d'installer **lynx**.

Labs : questions diverses

Lab 1 - Y-a-t-il une différence entre les partitions de secours et les partitions de sauvegarde ?

Non c'est la même structure de données. Ces deux partitions ont du sens avec du matériel physique où vous pouvez conserver la version n-1 du firmware et/ou de votre configuration pour un retour arrière facilité en cas de souci avec la mise-à-jour/modification.

Lab 5 - Comment tracer la NAT ?

Pour tracer la NAT dans une règle, il faut ouvrir l'onglet "**Options**" de la règle (double-clic) et choisir l'option désirée dans la liste déroulante "**tracer**" ou lever une alarme, il est possible de tracer la NAT dans un tunnel IPSec en cochant la case correspondante.

Lab 7 - Comment tester le portail captif et l'enrôlement ? Je n'y accède pas depuis mon navigateur, ce qui me semble normal puisque je ne suis pas dans le "in".

Après que les VMs aient toutes démarrées, on peut désactiver toutes les interfaces virtuelles, **sauf une côté in**, et se connecter sur le portail captif du firewall situé derrière (cf webinaire vidéo d'Avril et document complémentaire).

Dépannage : questions diverses

Je ne peux plus accéder à mon firewall via l'interface web.
Comment faire pour supprimer toutes les règles de filtrage en ligne de commandes ?
Sur un boitier physique il faut connecter le câble console et accéder en mode console, sur une VM, accéder en console (même login et mdp que via l'interface graphique)
En invite de commande, taper « **enfilter 10** » par exemple pour activer la politique de sécurité numéro 10 (la **Pass All** d'origine), l'accès à l'interface graphique redevient opérationnel et la configuration peut être modifiée.

Autres formations Stormshield

Dans le cadre du CERPEP, est-ce que des formations en présentielles sont envisagées ? (pour la formation administrateur CSNA)
C'est une question actuellement en discussion, on envisage la Toussaint 2019 dans plusieurs académies et printemps/été 2020 dans le cadre de la réforme du BTSSIO

Dans le cadre du CERPEP, est-ce que des formations en présentielles sont envisagées ? (pour la formation Expert)

- **Juillet 2019** chez Stormshield à Lyon pour les formateurs certa et les "pionnniers" de la formation 2018
- **Toussaint 2019** chez Stormshield à Paris pour les plus motivés d'entre vous
- **Courant 2020** dans plusieurs académies lorsque les formateurs certa auront été formés au 3ème niveau de certification

Certifications

Est-il possible d'avoir des exemples des questions posées dans l'examen avant de démarrer une tentative ?
Non simplement un test exemple pour savoir différencier choix unique de choix multiple.
En voici 2 pour illustrer :

- En combien de phases un tunnel VPN IPsec s'établit-il? (vous sélectionnez une réponse dans la liste de propositions)
- Si aucune règle de filtrage ne correspond au paquet reçu par le parefeu, quelle sera l'action par défaut ? (vous sélectionnez une réponse dans la liste de propositions)

Les examens sont en français ou en anglais ?
L'examen est ouvert par défaut **en Français**, mais les 2 langues sont possibles. Il est possible de demander à le remplacer par l'examen Anglais en écrivant à institute@stormshield.eu
Comment se passe le test en ligne ?
70 questions en 90 minutes, il est possible de marquer les questions pour y revenir à la fin à l'aide de la case à cocher "Réviser cette question plus tard"
L'accès à tout document est autorisé, ayez bien le support sous la main pour effectuer des recherches dans le pdf, ça peut aider
Comment bien se préparer ?
Lire attentivement le support de cours, réaliser les labs, se dire que vous avez éventuellement la possibilité de le repasser, notamment si vous souhaitez atteindre les 80% pour devenir instructeur officiel après la formation et certification Expert.
Y-a-t-il des questions dont les réponses ne se trouvent pas dans le cours ?
Oui sur les fondamentaux du réseau mais ça ne représente pas plus de 10% des questions et cela fait partie des pré-requis d'accès à cette formation CSNA
Comme la validité d'une certification est de 3 ans, il faut que nous repassions à nouveau les examens et les 80% tous les 3 ans, sinon nous perdons le centre de certification de notre établissement ?
Vous ne pourrez plus présenter d'étudiants à l'examen ou utiliser les supports officiels et le kit pour les étudiants si vous n'êtes plus certifié. En revanche si vous passez entre temps la certification expert, c'est celle-ci qui fait foi et sa date de validité est aussi de 3 ans. Vous n'aurez à repasser que la dernière certification acquise

Partenariat établissement

Pour l'acquisition de matériel ou pour devenir centre de certification Stormshield, il convient de mettre en place une convention de partenariat entre Stormshield et l'établissement. La présentation de ce partenariat et le contrat de partenariat sont disponibles sur Institute.

Questions sur le matériel

Comment acheter du matériel Stormshield pour les enseignements de BTS SIO?

Il convient de mettre en place un partenariat entre l'établissement et Stormshield pour accéder à des conditions spécifiques. Le document de présentation du partenariat est disponible sur la plateforme Institute et sur la page partenariat-stormshield (pdf) du site du réseau Certa.

Quel matériel choisir ?

Le SN210W répond à 100% du besoin pour dispenser une formation CSNA.

Le SN310 permet en plus la mise en place d'un Cluster en Haute Disponibilité. Cette fonctionnalité peut être utile pour la mise en place de projets tutorés.

Il peut être intéressant de mixer l'acquisition du matériel (8 SN210 + 4 SN310).

Où trouve-t-on les tarifs partenariat des boitiers parefeu ?

Le tarif partenariat pour les différents matériels est détaillé dans le document de présentation du partenariat p 13, il constitue une remise substantielle sur les boitiers + un abonnement à certaines options de licence pendant la durée du partenariat. Vous trouverez une liste de revendeur dans le "Guide-du-programme-Stormshield-Institute" disponible sur Institute.

Peut-on utiliser les boîtiers au tarif partenariat pour une utilisation en production pour le lycée ?

NON. Les conditions proposées dans le cadre du partenariat concernent des appliances à vocation pédagogique et qui ne seront pas mises en production. Pour du matériel en production, administré par des équipes IT, il convient de voir en direct avec votre partenaire Stormshield.

Peut-on utiliser les boîtiers au tarif partenariat pour une utilisation pour la sortie Internet du BTS SIO ?

OUI. Si ce boîtier est utilisé **exclusivement** pour cet usage et qu'il est **administré directement par les enseignants**, il peut être acheté et maintenu dans le cadre du partenariat Institute au niveau établissement.

Quels sont les tarifs des boitiers pour une utilisation en production ?

Nous vous invitons à contacter votre revendeur pour identifier le modèle et les options de licence répondant à votre besoin. Vous trouverez une liste de revendeur dans le "Guide-du-programme-Stormshield-Institute" disponible sur Institute..

Quelles sont les limitations des VM du kit CSNA ?

Les VM du kit disposent d'un abonnement à certaines options de licence valables jusqu'à la fin de l'année civile. Les limitations concernent le nombre d'accès simultanés, le nombre de VPN… qui font qu'elles ne peuvent être utilisées en production, raison pour laquelle Stormshield vous autorise à les diffuser à vos étudiants.

Disposons-nous de fonctionnalités normalement sous licences (IPS, VPN-SSL, filtrage d'URL, anti-virus etc.) ?

Les VM du kit comme les produits acquis dans le cadre du partenariat établissement disposent d'un abonnement à certaines options de licence pendant la durée du partenariat, en sont exclues : anti-virus Kaspersky, filtrage d'URL avancé et BreachFighter.

Performances, documentation technique

Peut-on avoir accès au document PDF des datasheets de toute la gamme (caractéristiques techniques, débits IMIX, performances avec sans antivirus, etc.) ?

Vous trouverez ces information sur le site web corporate de Stormshield:
https://www.stormshield.com/fr/documentation/?_sft_type_security=reseaux&_sft_rc_type=fiche-produit

Les débits ne semblent pas faits en IMIX (58%/33%/8% en 48/494/1500 bytes) : pourquoi ?

C'est un choix "marketing"; les données fournies sont celles demandées par la majorité nos clients.

Quelles sont les parties (fonctionnalités) qui sont couvertes par le développement EAL4+ (et celles sous EAL3+) ?

Pour la partie EAL4+ : https://www.ssi.gouv.fr/entreprise/certification_cc/fonction-de-filtrage-de-la-suite-logicielle-stormshield-firewall-version-2-2-6/

Pour la partie EAL3+ : https://www.ssi.gouv.fr/entreprise/certification_cc/suite-logicielle-stormshield-firewall-version-2-2-6/