PROCEDURE D'INSTALLATION : CONFIGURATION SYSLOG STORMSHIELD

PROJET

CUB

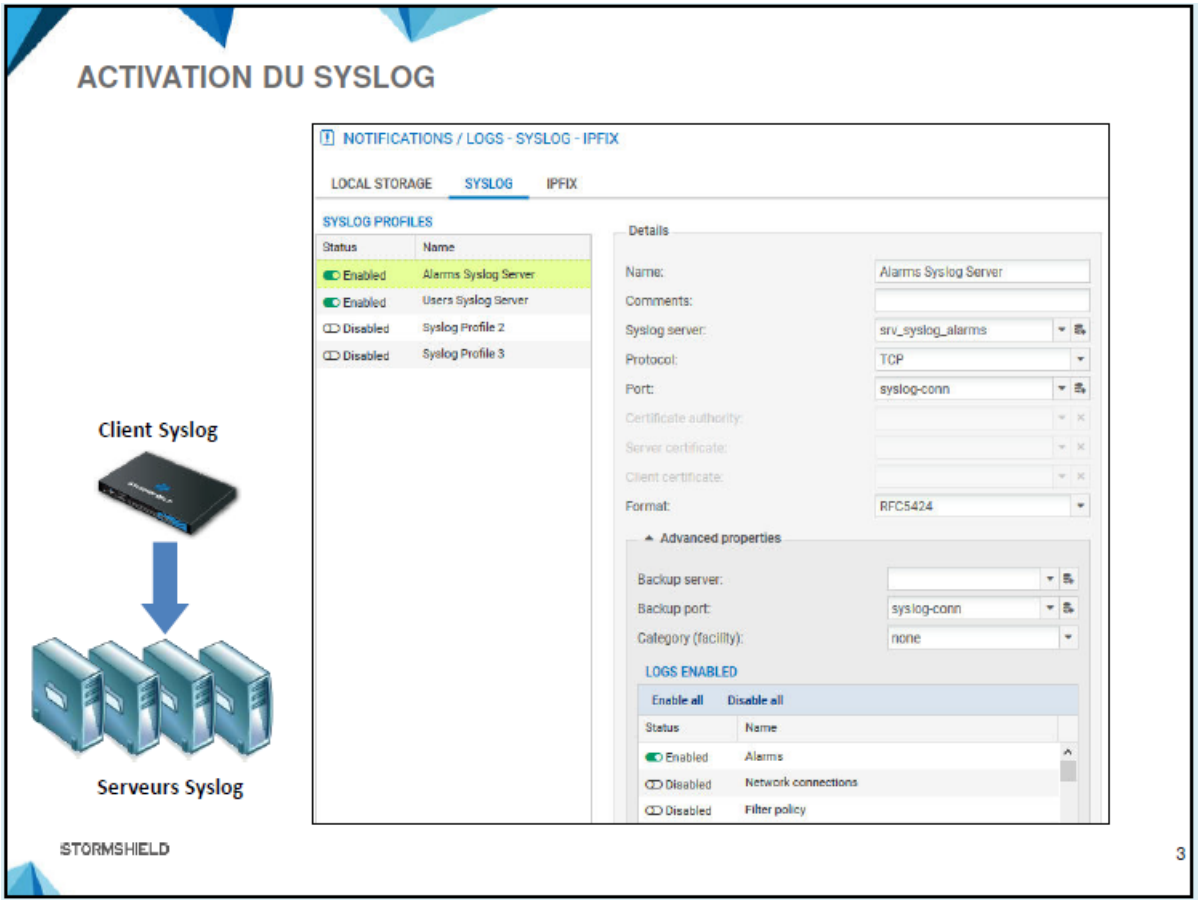
- **Objectif :** Assurer la sécurité du réseau via le filtrage du trafic, le chiffrement des communications (VPN), la gestion sécurisée, la surveillance des événements et la sauvegarde des configurations, afin de garantir la confidentialité, l'intégrité et la disponibilité des systèmes.

- **Prérequis**

  - **Système d’exploitation**
    - OS Stormshield

  - **Ressources matérielles (minimum recommandé)**
    - **CPU** : 1 cœurs
    - **RAM** : 1 Go
    - **Disque** : 32 Go (SSD recommandé)
    - **Connexion réseau** : 1 Gbit/s

Activation du Syslog

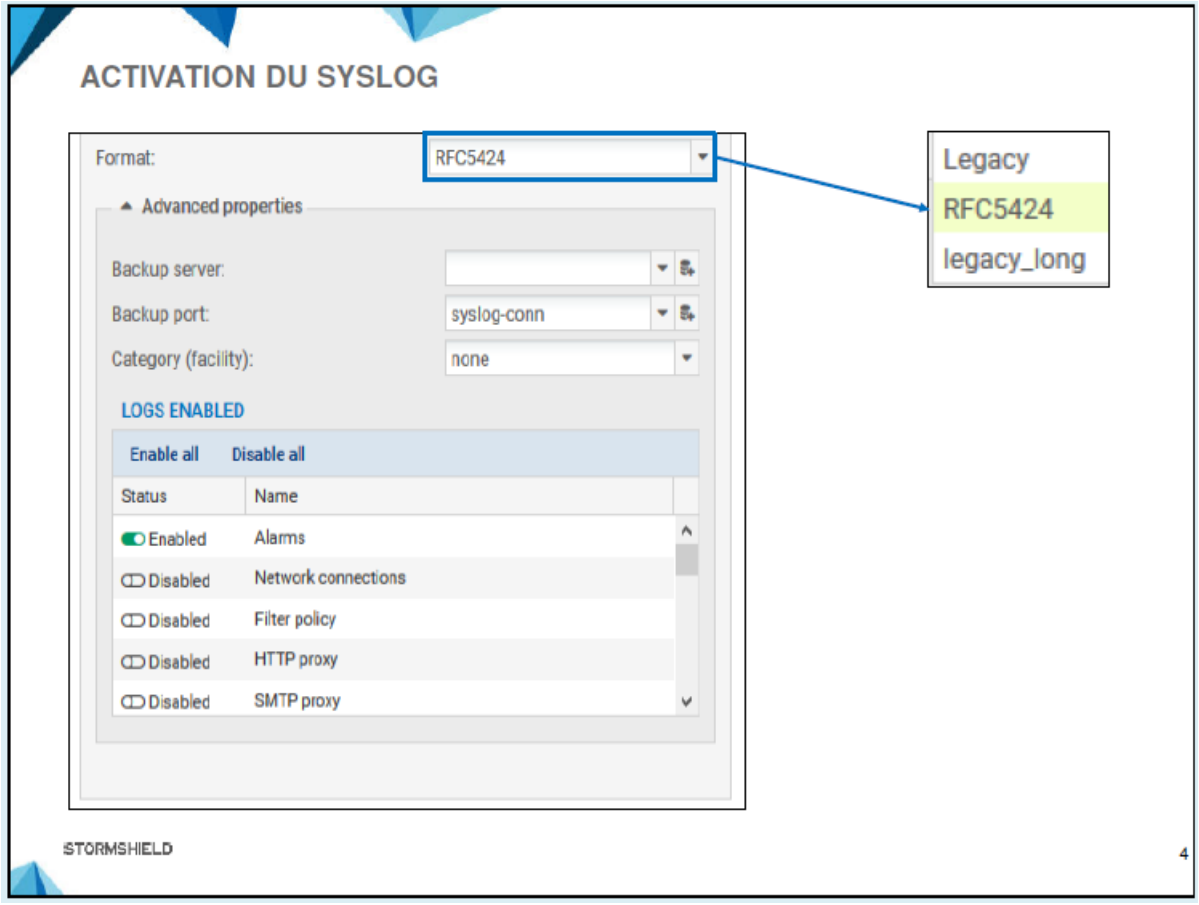


Les firewalls Stormshield Network embarquent un client SYSLOG qui peut être activé pour transmettre des traces vers des serveurs SYSLOG externes. Il est possible d'activer jusqu'à 4 serveurs SYSLOG en même temps en personnalisant le protocole de transmission, le format et les catégories de traces pour chaque serveur.

La configuration de ces serveurs s'effectue dans le menu **CONFIGURATION ⇒ NOTIFICATIONS ⇒ Traces - Syslog - IPFIX ⇒ onglet SYSLOG** (un serveur par profil). Dans chaque profil, vous pouvez configurer les paramètres suivants :

- **Nom** : du profil syslog,
- **Commentaire** (facultatif),
- **Serveur Syslog** : objet machine portant l'adresse IP du serveur Syslog,
- **Protocole** : utilisé pour la transmission des traces : UDP, TCP et TLS,

- **Port** : de destination, utilisé pour la transmission des traces. Les ports standards : syslog (UDP/514), syslog-conn (TCP/601), syslog-tls (TCP/6514),
- **Autorité de certification (obligatoire)** : Le certificat de la CA qui a signé les certificats du firewall et du serveur Syslog,
- **Certificat serveur (optionnel)** : le certificat qui doit être présenté par le serveur Syslog pour s'authentifier auprès du firewall,
- **Certificat client (optionnel)** : le certificat qui doit être présenté par le firewall pour s'authentifier auprès du serveur Syslog,



Format : Le format syslog utilisé :

- LEGACY : limité à 1024 caractères par message syslog.
- LEGACY-LONG : Le message syslog n'est pas limité.
- RFC5424 : respectant le format défini par la RFC 5424.

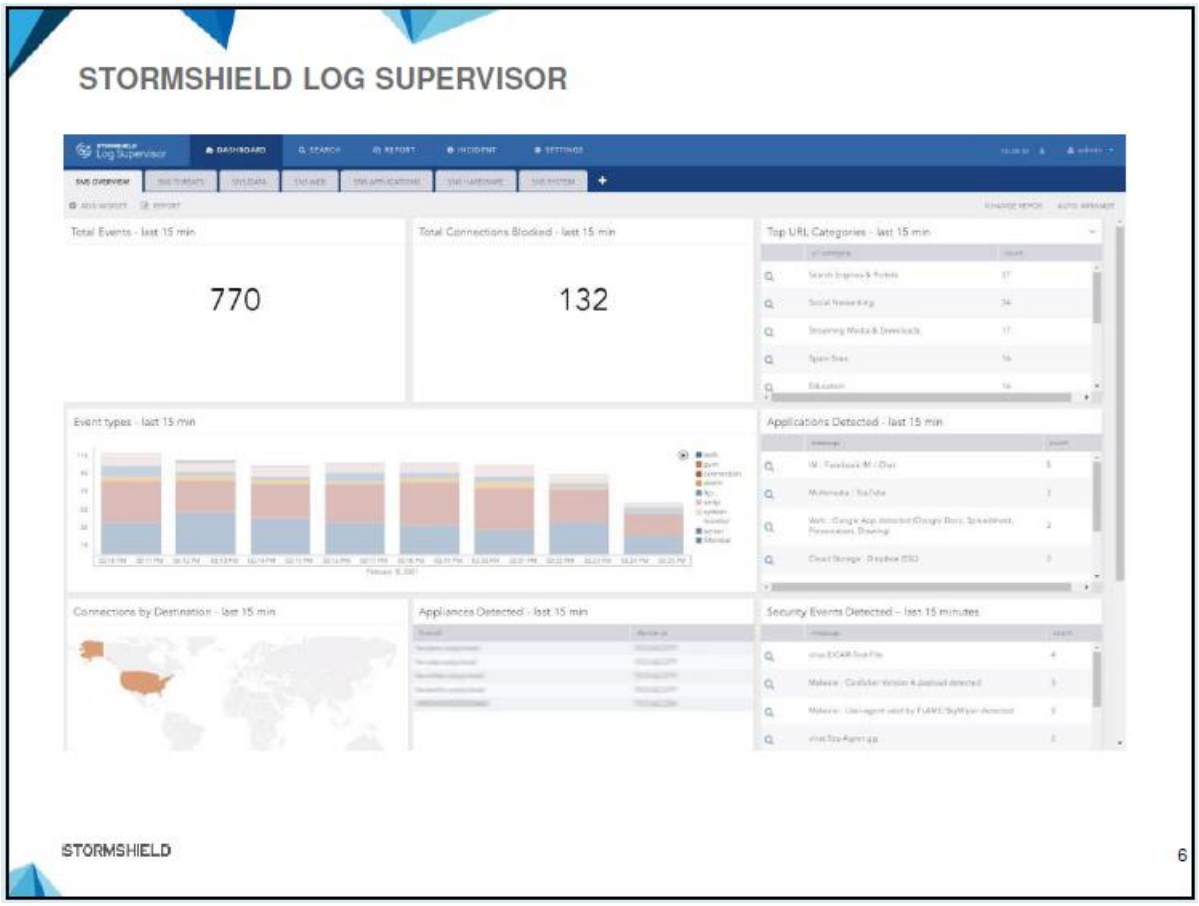
Dans l'encadré **configuration avancée**, les paramètres suivants peuvent être configurés :

- **Serveur de secours**,
- **Port de secours**,
- **Catégorie (facility)** : identifiant ajouté au début d'u□e ligne de trace pour identifier un firewall dans le cas où le serveur Syslog reçoit les traces de plusieurs firewalls,
- **TRACES ACTIVÉES** : permet de sélectionner les catégories de traces qui seront transmises au serveur SYSLOG en double cliquant sur la partie **État** de chaque famille pour activer ou désactiver l'envoi.

NOTE :

- Les paramètres Autorité de certification, Certificat serveur et Certificat client sont activés seulement si le protocole TLS est sélectionné.
- Les paramètres Serveur de secours et Port de secours peuvent être utilisés seulement si les protocoles TCP ou TLS sont sélectionnés.

Stormshield Log Supervisor (SLS)



Stormshield Log Supervisor est une solution de gestion de traces. Elle collecte les données de streaming qui proviennent des firewalls Stormshield Network Security, les analyse, et fournit des aperçus de vos données en temps réel. SLS permet un contrôle strict des réseaux d'entreprise distribués depuis un seul emplacement et offre des capacités de synthétisation des risques sous-jacents liés aux attaques distribuées complexes sur les réseaux de grande taille. Stormshield Log Supervisor peut être déployé sur deux environnements virtuels :

- VMware ESXi avec le Stormshield Log Supervisor OVA,
- Microsoft Hyper-V avec le Stormshield Log Supervisor Hyper-V VHD.