

Procédure de sauvegarde ESA Safelists/Blocklists

Contenu

[Introduction](#)

[Conditions préalables](#)

[Conditions requises](#)

[Composants utilisés](#)

[Générez les fichiers de sauvegarde SLBL](#)

Introduction

Ce document décrit comment sauvegarder Safelists/Blocklists (SLBL) sur l'appliance de sécurité du courrier électronique de Cisco (ESA).

Conditions préalables

Conditions requises

Aucune spécification déterminée n'est requise pour ce document.

Composants utilisés

Les informations dans ce document sont basées sur l'appliance de sécurité du courrier électronique de Cisco (ESA) et toutes les versions d'AsyncOS.

Les informations contenues dans ce document ont été créées à partir des périphériques d'un environnement de laboratoire spécifique. Tous les périphériques utilisés dans ce document ont démarré avec une configuration effacée (par défaut). Si votre réseau est opérationnel, assurez-vous que vous comprenez l'effet potentiel de toute commande.

Générez les fichiers de sauvegarde SLBL

De l'interface web ESA, naviguez vers la **base de données d'administration système > de fichier de configuration > d'utilisateur Safelist/Blocklist (quarantaine de Spam)**. Vous pouvez générer des fichiers de sauvegarde de cet emplacement.

Note: Si vous avez plusieurs ESAs dans la batterie, vous devez télécharger les fichiers de sauvegarde à chaque unité de opposition.

Sélectionnez la commande de **slblconfig** dans le CLI afin d'importer et exporter la configuration SLBL :

```
> slblconfig
```

```
End-User Safelist/Blocklist: Enabled
```

```
Choose the operation you want to perform:
```

- IMPORT - Replace all entries in the End-User Safelist/Blocklist.
- EXPORT - Export all entries from the End-User Safelist/Blocklist.

```
[> export
```

```
End-User Safelist/Blocklist export has been initiated...
```

```
Please wait while this operation executes.
```

```
End-User Safelist/Blocklist successfully exported to  
slbl-782BCB64XXYY-1234567-20140717T020032.csv (200B).
```

Vous devez alors accéder à l'ESA par l'intermédiaire du Protocole FTP (File Transfer Protocol) afin de récupérer et retenir la configuration de création récente et exportée SLBL :

```
$ ftp user@myesa.local  
Connected to myesa.local.  
220 myesa.local.rtp Cisco IronPort FTP server (V8.5.6) ready  
331 Password required.  
Password:  
230 Login successful.  
Remote system type is UNIX.  
Using binary mode to transfer files.  
ftp> hash  
Hash mark printing on (1024 bytes/hash mark).  
ftp> bin  
200 Type set to Binary.  
ftp> cd configuration  
250 CWD command successful.  
ftp> ls  
227 Entering Passive Mode (172,16,1,1,XX,YYY)  
150 Opening ASCII mode data connection for file list  
drwxrwx--- 2 root config 512 Oct 14 2013 iccm  
-rw-rw---- 1 admin config 1117 Oct 14 2013 profanity.txt  
-rw-rw---- 1 admin config 90 Oct 14 2013 proprietary_content.txt  
-rw-rw---- 1 admin config 2119 Oct 14 2013 sexual_content.txt  
-rw-rw---- 1 admin config 28025 Oct 14 2013 ASYNCOS-MAIL-MIB.txt  
-rw-rw---- 1 admin config 1292 Oct 14 2013 IRONPORT-SMI.txt  
-r--r--r-- 1 root wheel 436237 Jul 9 16:51 config.dtd  
drwxrwx--- 2 root config 512 May 28 20:23 logos  
-rw-rw---- 1 root config 1538 May 30 17:25 HAT_TEST  
-rw-r----- 1 admin config 18098688 Jul 9 16:59 warning.msg  
-r--r--r-- 1 root wheel 436710 Jul 9 16:51 cluster_config.dtd  
-rw-rw---- 1 nobody config 200 Jul 16 22:00  
slbl-782BCB64XXYY-1234567-20140717T020032.csv  
#  
226 Transfer Complete  
ftp> get slbl-782BCB64XXYY-1234567-20140717T020032.csv  
local: slbl-782BCB64XXYY-1234567-20140717T020032.csv remote:  
slbl-782BCB64XXYY-1234567-20140717T020032.csv  
227 Entering Passive Mode (172,16,1,1,XX,YYY)
```

```
150 Opening Binary mode data connection for file
'slbl-782BCB64XXYY-1234567-20140717T020032.csv'
#
226 Transfer Complete
200 bytes received in 00:00 (8.63 KiB/s)
ftp> exit
221 Goodbye.
```

Votre fichier de sauvegarde est maintenant transféré localement. Vous pouvez ouvrir et visualiser les entrées SLBL comme nécessaires.