Procedura di backup degli elenchi di sicurezza/blocchi ESA

Sommario

Introduzione

Questo documento descrive come eseguire il backup di Safelist/Blocklist (SLBL) su Cisco Email Security Appliance (ESA).

Prerequisiti

Requisiti

Nessun requisito specifico previsto per questo documento.

Componenti usati

Il riferimento delle informazioni contenute in questo documento è Cisco Email Security Appliance (ESA) e tutte le versioni di AsyncOS.

Le informazioni discusse in questo documento fanno riferimento a dispositivi usati in uno specifico ambiente di emulazione. Su tutti i dispositivi menzionati nel documento la configurazione è stata ripristinata ai valori predefiniti. Se la rete è operativa, valutare attentamente eventuali conseguenze derivanti dall'uso dei comandi.

Genera file di backup SLBL

Dall'interfaccia Web dell'ESA, selezionare **System Administration > Configuration File > End-User Safelist/Blocklist Database (Spam Quarantine).** È possibile generare file di backup da questo percorso.

Nota: Se nel cluster sono presenti più ESA, è necessario caricare i file di backup in ciascuna unità opposta.

Immettere il comando **slblconfig** nella CLI per importare ed esportare la configurazione 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).
```

Èquindi necessario accedere all'ESA tramite il protocollo FTP (File Transfer Protocol) per recuperare e conservare la configurazione SLBL appena creata ed esportata:

```
$ 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.
```

Il file di backup è ora trasferito localmente. È possibile aprire e visualizzare le voci SLBL in base alle esigenze.