Procedimento de backup ESA Safelists/Blocklists

Índice

Introdução

Este documento descreve como suportar Safelists/Blocklists (SLBL) na ferramenta de segurança do email de Cisco (ESA).

Pré-requisitos

Requisitos

Não existem requisitos específicos para este documento.

Componentes Utilizados

A informação neste documento é baseada em ferramenta de segurança do email de Cisco (ESA) e em todas as versões de AsyncOS.

As informações neste documento foram criadas a partir de dispositivos em um ambiente de laboratório específico. Todos os dispositivos utilizados neste documento foram iniciados com uma configuração (padrão) inicial. Se a sua rede estiver ativa, certifique-se de que entende o impacto potencial de qualquer comando.

Gerencia arquivos de backup SLBL

Da interface da WEB ESA, navegue ao **base de dados da administração do sistema > do arquivo de configuração > do utilizador final Safelist/Blocklist (quarentena do Spam).** Você pode gerar arquivos de backup deste lugar.

Nota: Se você tem diversos ESA no conjunto, você deve transferir arquivos pela rede os arquivos de backup a cada unidade de oposição.

Incorpore o comando do **slblconfig no** CLI a fim importar e exportar a configuração 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).
```

Você deve então alcançar o ESA através do File Transfer Protocol (FTP) a fim recuperar e reter a configuração recém-criado, exportada 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.
```

Seu arquivo de backup é transferido agora localmente. Você pode abrir e ver as entradas SLBL como necessárias.