

Infra Blog

By Rob Heygele

Backup ASA config with PowerShell

11/04/2016 [LEAVE A COMMENT \(HTTPS://HEGGEL4.WORDPRESS.COM/2016/04/11/BACKUP-ASA-CONFIG-WITH-POWERSHELL/#RESPOND\)](https://heggel4.wordpress.com/2016/04/11/backup-asa-config-with-powershell/#RESPOND)

During my years in the networking business one of my frustrations is that it is very hard to backup the configuration of an ASA. There are some commercial products like Solarwinds that can accomplish this goal, but it costs money. An open source alternative like Rancid is also available but is pretty hard to configure.

Determined to find a solution I started searching the internet and came across some PowerShell scripts. I'm not a PowerShell specialist, but I do know how to put together the separate scripts. So to be clear, I did not invent the scripts I just put them together.

So let's take a look at the script:

Read-Host "Enter Password" -AsSecureString | ConvertFrom-SecureString | Out-File c:\<map>\cred01.txt

I don't want to send the password of the ASA user plain over the network. So with the above line I make sure the password is encrypted. It is possible to convert the password back to plain text, but then you'll need access to the server. So it is not rock-solid, but safer than sending the password in plain text over the internet. If you make sure that the user account only has minimal rights on the ASA, there is minimal chance of getting unwanted guests on your ASA. The line converts the plain password to an encrypted password and writes it to a .txt file.

\$ASApw = Get-Content "c:\<map>\cred01.txt" | ConvertTo-SecureString #-AsPlainText #-Force

\$BSTR = [System.Runtime.InteropServices.Marshal]::SecureStringToBSTR(\$ASApw)

\$ASApw = [System.Runtime.InteropServices.Marshal]::PtrToStringAuto(\$BSTR)

The above three lines are needed to convert the encrypted password from the credentials file. This is needed because the ASA is unable to read an encrypted password.

\$ASAIP = "<ip address>"

\$ASAUser = "<username>"

\$ASAEnablepw = \$ASApw

#Modifies the ASA firewall

#Starts by writing a "commands" file#

echo en >>unicode.txt

echo \$ASAEnablepw >>unicode.txt

echo "conf t" >>unicode.txt

echo "no pager" >>unicode.txt

echo "show run" >>unicode.txt

echo "pager 24" >>unicode.txt

echo "copy running-config startup-config" >>unicode.txt

echo "running-config" >>unicode.txt

echo exit >>unicode.txt

echo exit >>unicode.txt

#Converts the file to ASCII format (separate file)#

\$lines = gc "unicode.txt"

\$lines | out-file -encoding Ascii -filepath commands.txt

The above lines write the actual ASA commands to the commands.txt file.

#Using the command file and plink.exe connects and runs the commands#

c:/Windows/System32/plink.exe -ssh -l \$ASAUser -pw \$ASApw \$ASAIP -m commands.txt > "c:\<map>\ASA.txt"

-To make things work you need to download the Plink tool. It is the command line version of Putty. It can be downloaded from the Cisco website. I put the tool in the c:\windows\system32 folder, but you can place it everywhere you want. This line writes the configuration ASA to an .txt file.

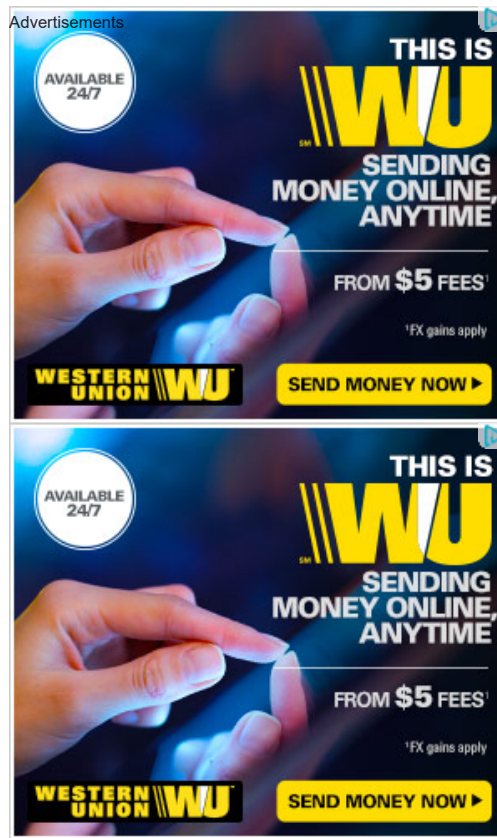
#removes the files it created earlier#

del unicode.txt

del commands.txt

As you can see it's actually a pretty easy script and above all it's free.

To make a daily backup, create a task through "Task scheduler".



FILED UNDER CISCO, CONFIGURATION, MONITORING, SECURITY

Create a free website or blog at WordPress.com.