自動化向けの Cisco Secure Firewall ASA HTTP インターフェイス

最終更新：2022 年 6 月 21 日

自動化向けの Cisco Secure Firewall ASA HTTP インターフェイス

通常、ネットワーク管理者は CLI や ASDM を使用して ASA を操作します。

同時に複数のファイアウォールを管理したり、一部の管理手順を自動化したりする必要性が生じることがよくあります。

ASA を含むほとんどのネットワークアプライアンスを操作する方法の 1 つは、CLI を使用することです。自動ツールは Telnet または SSH でデバイスに接続し、一度に 1 つずつコマンドを認証して実行できます。ただし、この方法にはいくつかの欠点があります。このツールは、Telnet や SSH 接続の状態を維持する必要があり、接続が失われた場合は、ログインプロセスを繰り返す必要があります。CLI を使用すると、一度に 1 つのコマンドしか送信できないため、特にファイアウォールが管理ステーションから遅延している場合、多くのファイアウォールを管理するには時間がかかります。

ASA を操作するためのより効率的な代替方法は HTTP です。HTTP を使用すると、自動化ツールは特定形式の URL にアクセスすることで、ASA でコマンドを実行できます。HTTP インターフェイスを使用すると、複数のコマンドを一度に送信して、リモートファイアウォールの管理効率を大幅に向上させることもできます。

このドキュメントでは、HTTP を使用して実行できるいくつかの一般的なタスクについて説明します。コマンドラインの curl ユーティリティの例をドキュメント内で示しますが、Python などのプログラミング言語の HTTP ライブラリを使用すると、同じ手順を簡単に実行できます。

HTTP アクセスの有効化

ローカルユーザーの作成後、HTTP 認証を有効にして、HTTP サーバーを有効にします。デフォルト設定を使用している場合、最初の ASDM アクセス用の管理インターフェイスに対して HTTP サーバーがすでに有効になっていることがあります。

（注） https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20190501-asa-csrf のセキュリティアドバイザリの修正として、ASA は特定の User-Agent ヘッダーを持つクライアントからの HTTP 基本認証のみを受け入れます。許可されたユーザー文字列のデフォルトリストは、**show running-config all http** コマンドを実行して表示できます。

```
http server basic-auth-client ASDM
http server basic-auth-client CSM
http server basic-auth-client REST API Agent
```

このドキュメントの例では、User-Agent を **ASDM** に設定し、基本認証を使用します。別の User-Agent 文字列を許可するには、**http server basic-auth-client** コマンドを使用して文字列を追加します。

手順

ステップ 1 ローカル ユーザを作成します。

username *username* [**password** *password*] [**privilege** *priv_level*]

または、AAA サーバーを使用してユーザー認証を設定することもできます。

例：

```
ciscoasa(config)# username api password api privilege 15
```

ステップ 2 ローカルデータベースを使用して HTTP 認証を有効にします。

aaa authentication http console LOCAL

または、AAA サーバーを使用してユーザー認証を設定することもできます。

例：

```
ciscoasa(config)# aaa authentication http console LOCAL
```

ステップ 3 HTTP サーバーを有効にして、ネットワークからのアクセスを許可します。

http server enable

http *source_IP_address mask source_interface*

例：

```
ciscoasa(config)# http server enable
ciscoasa(config)# http 0.0.0.0 0.0.0.0 inside
```

例

```
username deanwinchester password 67Impala privilege 15
http server enable
http 10.1.1.0 255.255.255.0 management
aaa authentication http console LOCAL
```

構成管理

このセクションでは、HTTPインターフェイスを使用してASA設定を表示および編集する方法を示します。

ASA 設定の取得

ASA で URL **/admin/config** にアクセスすると、現行の完全な ASA 設定を取得できます。

例

```
$ curl -k -A ASDM https://api:api@172.31.1.5/admin/config
!
ASA Version 9.12(2)9
!
hostname asa1
domain-name vik.local
enable password *** pbkdf2
passwd ** encrypted
multicast-routing
names
name 192.168.1.55 asa1.vblan.com
----- SNIP -----
```

単一コマンドの実行

HTTP経由でASAにアクセスする場合、ASAは、EXECモードとコンフィギュレーションモードの両方のコマンドを同じ方法で受け入れます。コンフィギュレーションモードに切り替える必要はありません。

コマンドは URL 内で直接指定するため、URL エンコードが必要です。たとえば、スペースは + 記号に置き換える必要があります。https://www.urlencoder.org/ など、この変換を対話方式で実行するための多くのオンラインツールがあります。

例：***show*** コマンド

```
$ curl -k -A ASDM https://api:api@172.31.1.5/admin/exec/show+version

Cisco Adaptive Security Appliance Software Version 9.12(2)9
Firepower Extensible Operating System Version 2.6(1.152)
Device Manager Version 7.12(1)

Compiled on Mon 30-Sep-19 13:11 PDT by builders
```

```
System image file is "disk0:/asa9-12-2-9-smp-k8.bin"
Config file at boot was "startup-config"

asa1 up 19 days 20 hours

Hardware:   ASA5515, 8192 MB RAM, CPU Clarkdale 3058 MHz, 1 CPU (4 cores)
            ASA: 4096 MB RAM, 1 CPU (1 core)
Internal ATA Compact Flash, 8192MB
BIOS Flash MX25L6445E @ 0xffbb0000, 8192KB

Encryption hardware device : Cisco ASA Crypto on-board accelerator (revision 0x1)
                             Boot microcode        : CNPx-MC-BOOT-2.00
                             SSL/IKE microcode     : CNPx-MC-SSL-SB-PLUS-0005
                             IPSec microcode       : CNPx-MC-IPSEC-MAIN-0026
                             Number of accelerators: 1
Baseboard Management Controller (revision 0x1) Firmware Version: 2.4
--- SNIP ---
```

例：コンフィギュレーション コマンド

エラーや警告がない限り、コマンドを実行しても何も出力されないことに注意してください。

```
$ curl -k -A ASDM https://api:api@172.31.1.5/admin/exec/domain-name+lab.com
```

例：コマンドエラー

```
$ curl -k -A ASDM
https://api:api@172.31.1.5/admin/exec/aaa+authentication+http+console+LOCAL
Range already exists.
```

複数コマンドの実行

1つのコマンドと同様のURL構文を使用して、複数の連続したコマンドを実行できます。複数のコマンドは、スラッシュ（/）で区切ります。

例

```
$ curl -k -A ASDM
https://api:api@172.31.1.5/admin/exec/object+network+curl-test/host+1.2.3.4

$ curl -k -A ASDM https://api:api@172.31.1.5/admin/exec/show+run+object+id+curl-test
object network curl-test
 host 1.2.3.4
```

コマンドの一括実行

多くのコマンドを同時に送信する必要がある場合、ASA では /admin/config への HTTP POST として受け入れることができます。

例

以下の例は、テキストファイルに保存された ACL を作成する方法を示しています。

```
$ cat config.txt
```

```
access-list test123 extended permit tcp any any eq www
access-list test123 extended permit tcp any any eq ftp
access-list test123 extended permit tcp any any eq https

$ curl -k -A ASDM https://api:api@172.31.1.5/admin/config --data-binary @config.txt
Cryptochecksum (changed): 5362c464 e7b04911 a0427d83 367676fc
Config OK

$ curl -k -A ASDM https://api:api@172.31.1.5/admin/exec/show+run+access-list+test123
access-list test123 extended permit tcp any any eq www
access-list test123 extended permit tcp any any eq ftp
access-list test123 extended permit tcp any any eq https
```

イメージ管理

ASA HTTPインターフェイスを使用して、フラッシュメモリ内のファイルを管理することもできます。

ファイルをダウンロードする

すべてのイメージは、URL：**/admin/disk0/***filename* からアクセスできます。

例

以下の例では、dap.xml がダウンロードされます。

```
$ curl -k -A ASDM https://api:api@172.31.1.5/admin/disk0/dap.xml
<?xml version="1.0" encoding="UTF-8" standalone="yes"?>
<dapRecordList>
<dapRecord>
<dapName>
<value>Userspoof</value>
</dapName>
<dapViewsRelation>
<value>and</value>
</dapViewsRelation>
<advancedView>
<value>assert(function()
  return (endpoint.registry["WinUserName"].value ~= aaa.cisco.username)
end)()</value>
--- SNIP ---
```

ファイルのアップロード

HTTP POST を **/admin/disk0/***filename* に実行すると、ファイルがアップロードされます。既存ファイルの上書きを示すプロンプトは表示されないことに注意してください。 ASAは既存ファイルを通知なしに上書きします。

例

以下の例は、セキュアクライアントを ASA にアップロードする方法を示しています。

```
$ curl -k -A ASDM
https://api:api@172.31.1.5/admin/disk0/anyconnect-win-4.9.05042-webdeploy-k9.pkg
```

```
--data-binary @anyconnect-win-4.9.05042-webdeploy-k9.pkg
76380273 bytes uploaded
```

証明書の管理（Certificate Management）

ASA にインストールされる証明書には、アイデンティティと CA の 2 種類があります。

ASA は、アイデンティティ証明書を PKCS12 ファイル形式で受け入れます。PKCS12 ファイルはバイナリ形式であるため、最初に Base64 にエンコードする必要があります。Linux や Unix ベースのシステムでは、OpenSSL ユーティリティを使用して Base64 エンコードを実行できます。Windows では、certutil を -encode オプションとともに使用します。

CLI で ASA に証明書をインストールする場合、ASA は対話型プロンプトを使用して証明書を受け入れます。HTTP インターフェイスを使用して証明書を適用する場合は、**nointeractive** キーワードを指定する必要があります。

アイデンティティ証明書のインストール

例

Base64 エンコードとそれに続く ID 証明書のインストールの例を以下に示します。

```
$ openssl base64 -e -in cert.p12 -out cert.pem
$ echo crypto ca import test-tp pkcs12 pkcs12password nointeractive > cert.txt
$ cat cert.pem >>cert.txt
$ echo quit >>cert.txt
$ cat cert.txt
crypto ca import test-tp pkcs12 Lenovo321 pkcs12password nointeractive
MIILmQIBAzCCC18GCSqGSIb3DQEHAaCCC1AEggtMMIILSDCCBf8GCSqGSIb3DQEH
BqCCBfAwggXsAgEAMIIF5QYJKoZIhvcNAQcBMBwGCiqGSIb3DQEMAQYwDgQIMN+G
--- SNIP ---
HuKDMSUwIwYJKoZIhvcNAQkVMRYEFAR7qSZN47HvCRU/82AiUyRwwyojMDEwITAJ
BgUrDgMCGgUABBSIt7Y5piQ1yqlpPOGZWOAUAXMT+gQIV+Oe+uTn7nwCAggA
quit
$ curl -k -A ASDM https://api:api@172.31.1.5/admin/config --data-binary @cert.txt
Enter the PKCS12 data in base64 representation....
.INFO: Import PKCS12 operation completed successfully
.
Cryptochecksum (changed): 19dd8321 c0cc9f6a 2690799c e4e58e79
Config OK
```

CA 証明書のインストール

例

```
$ echo crypto ca trustpoint test-tp >cert.txt
$ echo enrollment terminal >>cert.txt
$ echo crypto ca authenticate test-tp nointeractive >>cert.txt
$ cat ca-cert.pem >>cert.txt
$ echo quit >>cert.txt
$ cat cert.txt
crypto ca trustpoint test-tp
enrollment terminal
```

```
crypto ca authenticate test-tp nointeractive
-----BEGIN CERTIFICATE-----
MIIFWTCCBEGgAwIBAgITGQAAAESL6p0sIJ47EgAAAAAARDANBgkqhkiG9w0BAQsF
ADA/MRMwEQYKCZImiZPyLGQBGRYDY29tMRUwEwYKCZImiZPyLGQBGRYFdmJsYW4x
--- SNIP ---
XbyWLIGppq++4MFx2JZ3/cBQ26zuu4PKIHKXWnJdOVsAHLrTnYD5jzJlF2q1d1dP
zf9XqoNta0ArpWGs1jFm9fPG/KvgK5iGEmPwbT4=
-----END CERTIFICATE-----
quit

$ curl -k -A ASDM https://api:api@172.31.1.5/admin/config --data-binary @cert.txt
Enter the certificate in base64 representation....
End with the word "quit" on a line by itself.

INFO: Certificate has the following attributes:
Fingerprint:     98bc0332 2e157f21 6abfd738 2598145d

Trustpoint CA certificate accepted.

Cryptochecksum (changed): d426ce12 9be43c52 138896b6 7b954a43
Config OK
```

翻訳について
このドキュメントは、米国シスコ発行ドキュメントの参考和訳です。リンク情報につきましては、日本語版掲載時点で、英語版にアップデートがあり、リンク先のページが移動/変更されている場合がありますことをご了承ください。あくまでも参考和訳となりますので、正式な内容については米国サイトのドキュメントを参照ください。