Manual:Hotspot HTTPS example

From MikroTik Wiki

Contents

Summary

Using Hotspot server without enabled HTTPs login, may result in fail to redirect a client to the Hotspot authentication page if the requested page uses HTTPS protocol. To avoid such scenario, the “HTTPS login” should be enabled.

Hotspot HTTPs login provides:

- Extra security using SSL key encryption.
- Ability to redirect clients from HTTPS URLs.

This page contains information how to use SSL certificate to enable HTTPS login on Hotspot server. It is possible to use trusted certification authority (CA) signed certificate as well as no cost, self-signed certificate.

Self-signed certificates

Self-signed certificates can be made with no costs, and without public CA involvement. There are multiple free tools available for creating such certificates. The following examples will show how to use OpenSSL on linux machine, and RouterOS CLI to generate and sign your own certificates.

RouterOS example:

First we need to make our own CA who will sign the cerificates

```
/certificate
add name=ca-template common-name=myCa key-usage=key-cert-sign,crl-sign
sign ca-template name=myCa
```

Now create a certificate for Hotspot

```
/certificate
add name=Hotspot-template common-name=Hotspot
sign Hotspot-template ca=myCa name=Hotspot
```

Make server certificate trusted

```
set [find name=Hotspot] trusted=yes
```

OpenSSL example:

Here is OpenSSL example, to generate free self-signed certificate. First create a privat key

```
openssl genrsa -des3 -out Hotspot.key 1024
```

Generate certificate signing request

```
openssl req -new -key Hotspot.key -out Hotspot.csr
```

Sign created certificate signing request

```
openssl x509 -req -days 365 -in Hotspot.csr -signkey Hotspot.key -out Hotspot.crt
```

Import certificates:

Now you need to upload and import created key and certificate (CRT file) to the router

```
/certificate> import file-name=Hotspot.crt
passphrase: ****
     certificates-imported: 1
     private-keys-imported: 0
            files-imported: 1
       decryption-failures: 0
  keys-with-no-certificate: 0
```

and the key

```
/certificate> import file-name=Hotspot.key
passphrase: ****
     certificates-imported: 0
     private-keys-imported: 1
            files-imported: 1
       decryption-failures: 0
  keys-with-no-certificate: 0
```

Certificates are ready for use in Hotspot login.

Note: By using self signed certificate, SSL redirect warnings will still be present. As part of SSL protocol, cause hotspot captive portal will be seen as Man-in-the-Middle by SSL.

Trusted Certificate authority

To use HTTPs login without displaying SSL warning on client browser, requires use of Trusted CA signed certificate. Certificate import procedure is the same as described in previous example.

Note: Browser will still warn end-user about redirection even with CA signed certificate! This warning message cannot be avoided.

Note: Such HTTPS sites like google, facebook, etc that use SSL HSTS will show ssl error and will refuse to continue. In such case end-user should try to access different site.

Hotspot HTTPs login

When you have successfully imported certificate and private key on the router, first you need to enable ssl service and add the name of the certificate in /ip service:

```
/ip service set www-ssl certificate=Hotspot disabled=no
```

Next step is to enable HTTPs login on your Hotspot.

```
/ip hotspot profile set hsprof1 login-by=https ssl-certificate=Hotspot
```

Now all HTTPs requests from unauthorised clients will be redirected to your Hotspot login page.

Note: Such HTTPS sites as google, facebook, etc that use SSL HSTS will still be showing ssl error, and will completely refuse to continue. In such case the end user should try to access different sites.

SSL certificate key size impact on CPU load

SSL certificate key size will impact load on www service on hotspot server. Effects of this is seen from hosts that have not yet been authenticated with server. In this situation various services on these hosts like Dropbox for example are trying to contact their servers and are constantly bouncing against hotspot server. Per experiment ~60hosts with only Dropbox installed on them could cause up to 50-60% CPU load on lower end mipsbe devices like RB951 or similar models.

one option to avoid that would be to disable HTTPs redirect with this firewall rule:

```
/ip firewall nat add chain=hs-unauth action=return protocol=tcp dst-port=443 place-before=0
```

side effect of course will be that https site no longer will be redirected to captive portal, but it will also avoid un nesecary load on deivce.

- Second option is to use smaller size ssl key.

Retrieved from "https://wiki.mikrotik.com/index.php?title=Manual:Hotspot_HTTPS_example&oldid=29260"

Categories: Manual | Hotspot | Examples | IP | Create Certificates

- This page was last edited on 5 May 2017, at 12:08.