

HTTPS

WNAM

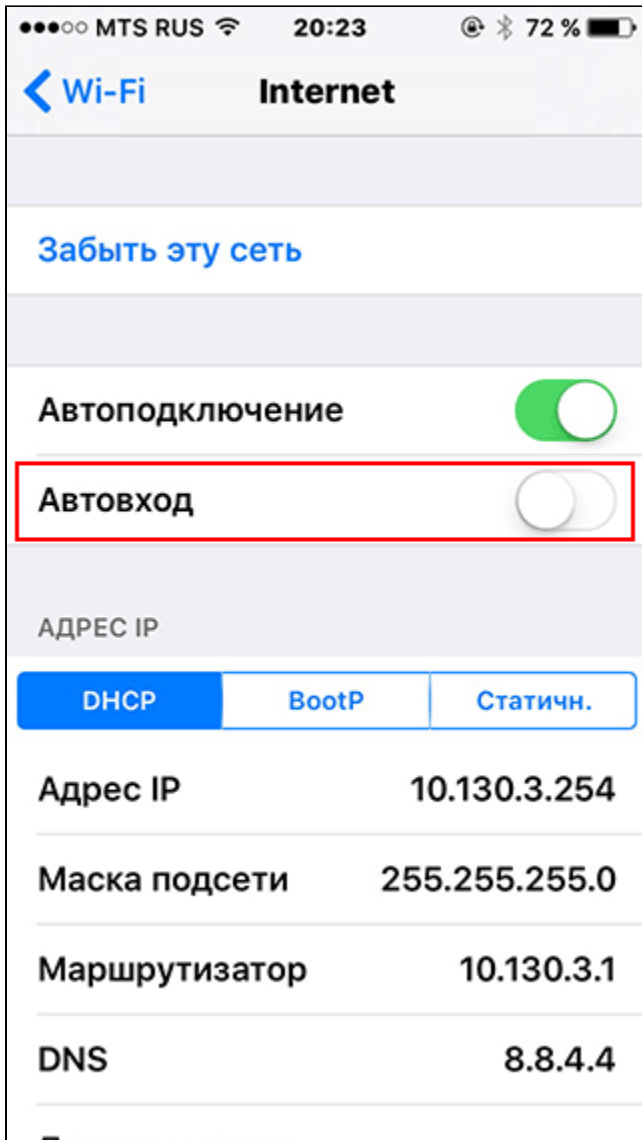
IP- . . . c Android iOS:

- Android http://www.gstatic.com/generate_204.
- iOS () www.ibook.info, www.appleiphonecell.com, captive.apple.com ..

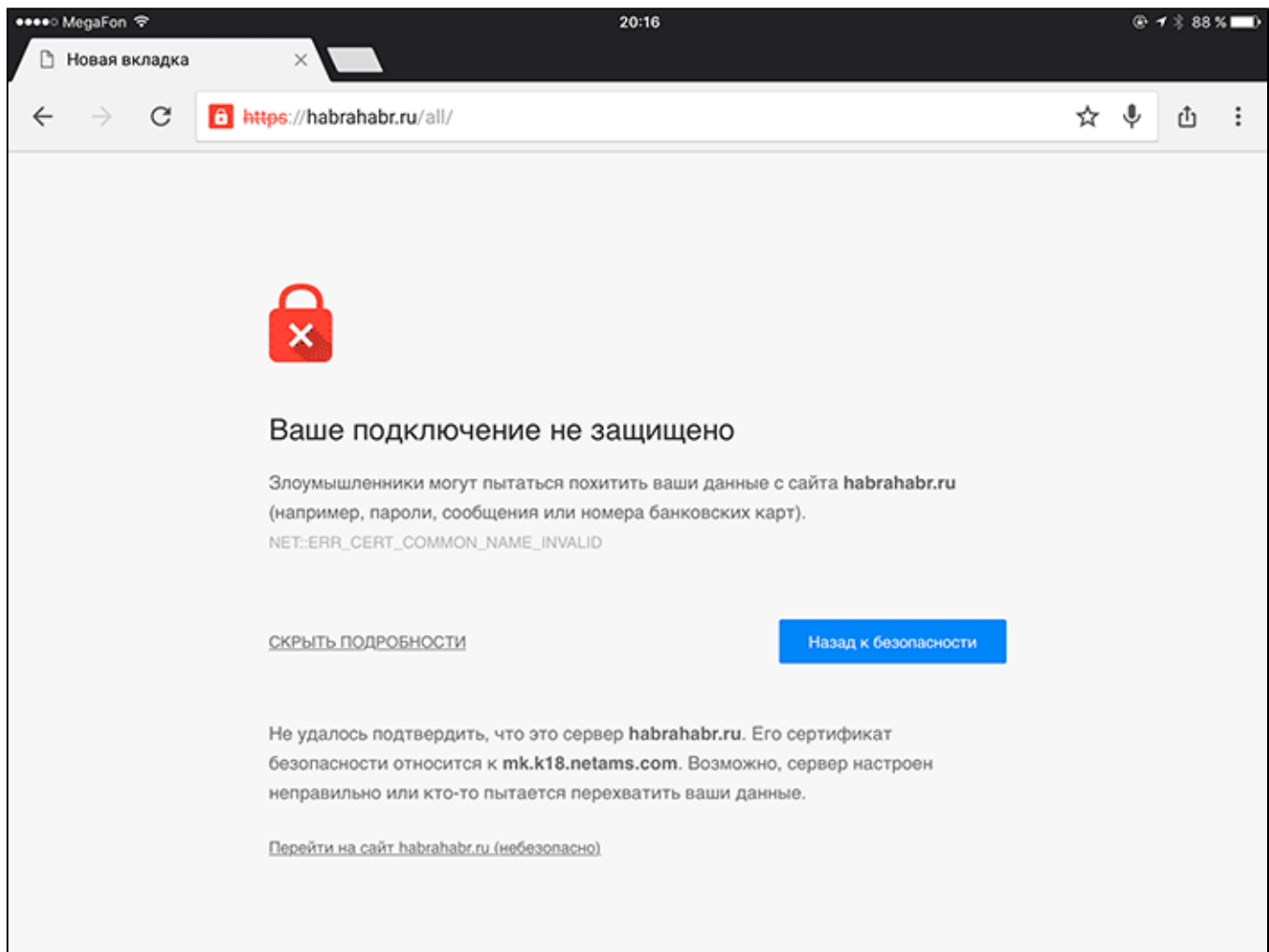
.. . . (-), . . . Captive Network Assistant (CNA).

.. - , CNA . (Cisco, Aruba) CNA Bypass, "" , , . - .

CNA iOS "" , .



CNA, Wi-Fi (Google, Yandex). HTTPS, () . HTTP . , (, Linux-, Mikrotik ..) HTTPS-. , , SSL- , WNAM. HTTPS-



MITM (Man-In-The-Middle), . . . :

- https- . HTTPS (.. SSL) IP-, DNS-, 443.
- (Mikrotik) (-), .
- TCP- SSL-, . , , .
- "", .. , (auth.provider.ru), (, google.com).
- , Wi-Fi, , .

! - WNAME. SSL HTTPS-.

(,) HTTPS- . :

- WNAME HTTP- ;
- HTTPS-;
- HTTPS- - tomcat, WNAME ;
- HTTPS- , .

! , HTTPS- WNAME, . , HTTPS, , HTTPS- CNA.

HTTPS- SSL. :

- , "",
- , Synamtec, Thawte, Verisign, Comodo .. 1 ;
- Let's Encrypt WoSign (90).

, . Letsencrypt , . , . IP-, DNS- , Split DNS DNS- Wi-Fi .

, Mikrotik 172.16.130.9 mk.k18.netams.com, WNAM 172.16.130.13 debian64.k18.netams.com. 2- Wildcard- (*.mydomain.ru).

, Letsencrypt, :

```
# openssl x509 -in cert.pem -text -noout

Certificate:
  Data:
    Version: 3 (0x2)
    Serial Number:
    03:0c:ab:c8:e6:3a:0c:7e:5a:e5:ff:23:ab:5f:cf:9b:15:a5
    Signature Algorithm: sha256WithRSAEncryption
    Issuer: C=US, O=Let's Encrypt, CN=Let's Encrypt Authority X3
    Validity
      Not Before: May 15 14:45:00 2016 GMT
      Not After : Aug 13 14:45:00 2016 GMT
    Subject: CN=mk.k18.netams.com
    Subject Public Key Info:
      Public Key Algorithm: rsaEncryption
      Public-Key: (2048 bit)
      Modulus:
        ...
      Exponent: 65537 (0x10001)
      X509v3 extensions:
        X509v3 Key Usage: critical
        Digital Signature, Key Encipherment
        X509v3 Extended Key Usage:
        TLS Web Server Authentication, TLS Web Client Authentication
        X509v3 Basic Constraints: critical
        CA:FALSE
        X509v3 Subject Key Identifier:
        C4:B9:60:6C:08:8E:00:AB:9D:F9:40:59:09:1A:16:B3:62:3C:71:36
        X509v3 Authority Key Identifier:
        keyid:A8:4A:6A:63:04:7D:DD:BA:E6:D1:39:B7:A6:45:65:EF:F3:A8:EC:A1

    Authority Information Access:
      OCSP - URI:http://ocsp.int-x3.letsencrypt.org/
      CA Issuers - URI:http://cert.int-x3.letsencrypt.org/

    X509v3 Subject Alternative Name:
      DNS:mk.k18.netams.com
    X509v3 Certificate Policies:
      Policy: 2.23.140.1.2.1
      Policy: 1.3.6.1.4.1.44947.1.1.1
      CPS: http://cps.letsencrypt.org
      User Notice:
        Explicit Text: This Certificate may only be relied upon by Relying Parties and
        only in accordance with the Certificate Policy found at https://letsencrypt.org
        /repository/

    Signature Algorithm: sha256WithRSAEncryption
    ...
```

nginx, tomcat 8080 nginx -. ().

tomcat

JKS, -. fullchain1.pem privkey1.pem PKCS#12 debian64.p12. : Password.

```
openssl pkcs12 -export -in fullchain1.pem -inkey privkey1.pem -out debian64.
p12 -name tomcat
```

JKS c :

```
keytool -importkeystore -deststorepass Password -destkeypass Password -  
destkeystore debian64.jks -srckeystore debian64.p12 -srcstoretype PKCS12 -  
srcstorepass Password -alias tomcat
```

tomcat:

```
cp debian64.jks /etc/tomcat7/
```

- /etc/tomcat7/server.xml , :

```
<Connector port="443" protocol="org.apache.coyote.http11.  
Http11Protocol" URIEncoding="UTF-8" keystoreFile="/etc/tomcat7/debian64.  
jks" keystorePass="Password" keyAlias="tomcat" keyPass="Password"  
maxThreads="150" SSLEnabled="true" scheme="https" secure="true" clientAuth="  
false" sslProtocol="TLS" />
```

- HTTPS (443):

```
touch /etc/authbind/byport/443  
chmod 500 /etc/authbind/byport/443  
chown tomcat7 /etc/authbind/byport/443
```

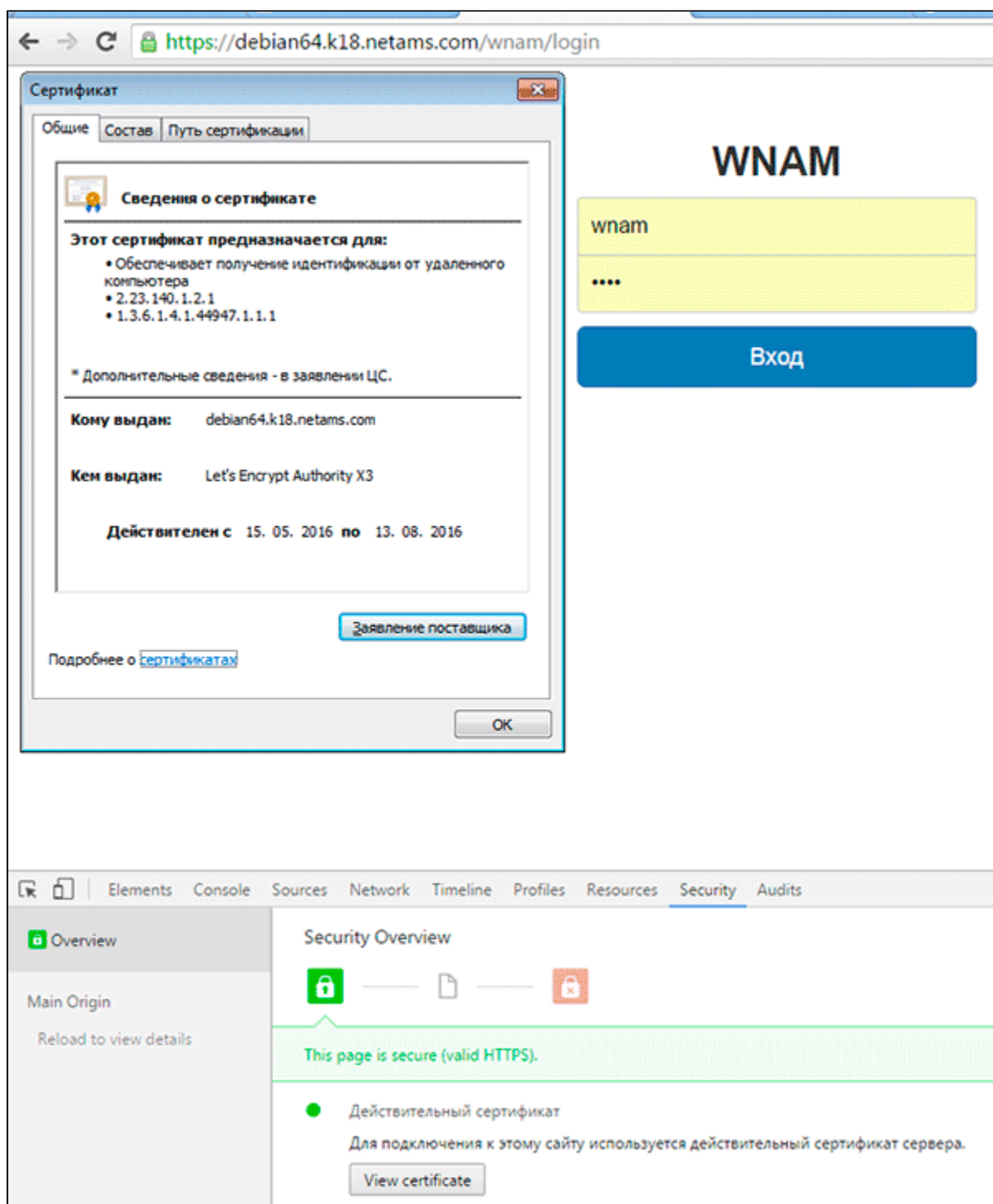
:-

```
/etc/init.d/tomcat7 restart
```

- /var/log/tomcat7/catalina.out :

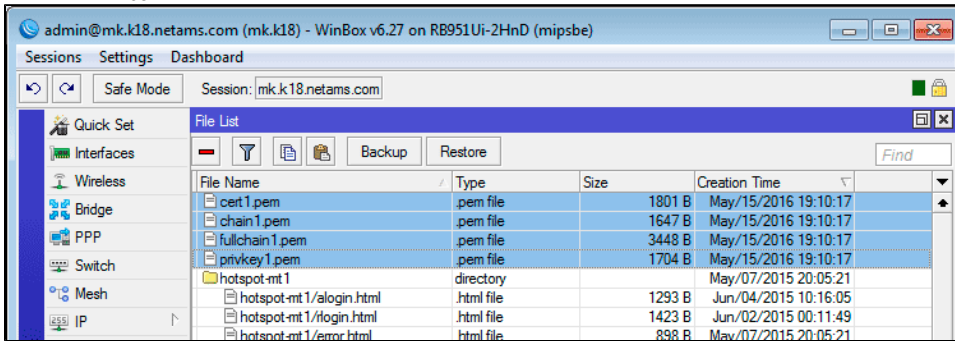
```
INFO: Deployment of web application archive /var/lib/tomcat7/webapps/ROOT.  
war has finished in 52,197 ms  
15, 2016 6:58:21 PM org.apache.coyote.AbstractProtocol start  
INFO: Starting ProtocolHandler ["http-bio-80"]  
15, 2016 6:58:21 PM org.apache.coyote.AbstractProtocol start  
INFO: Starting ProtocolHandler ["http-bio-443"]  
15, 2016 6:58:21 PM org.apache.catalina.startup.Catalina start  
INFO: Server startup in 54766 ms
```

WNAM https://wnam/home, SSL-, .

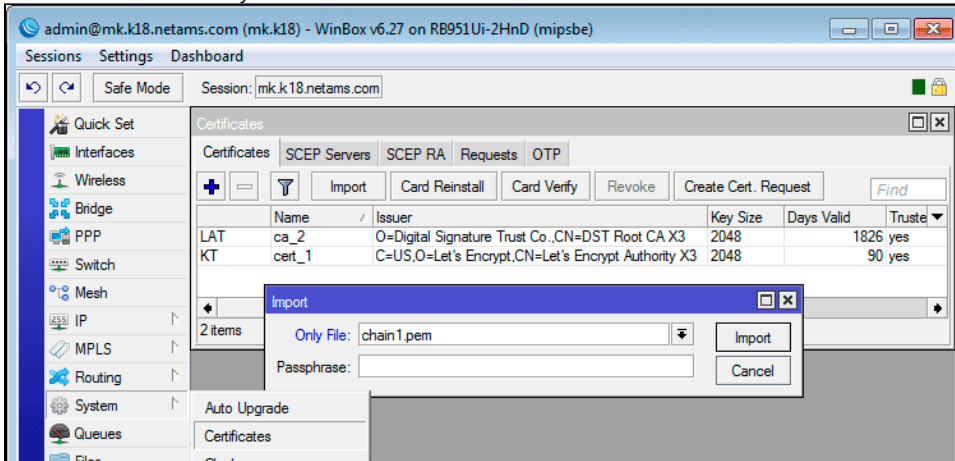


Mikrotik.

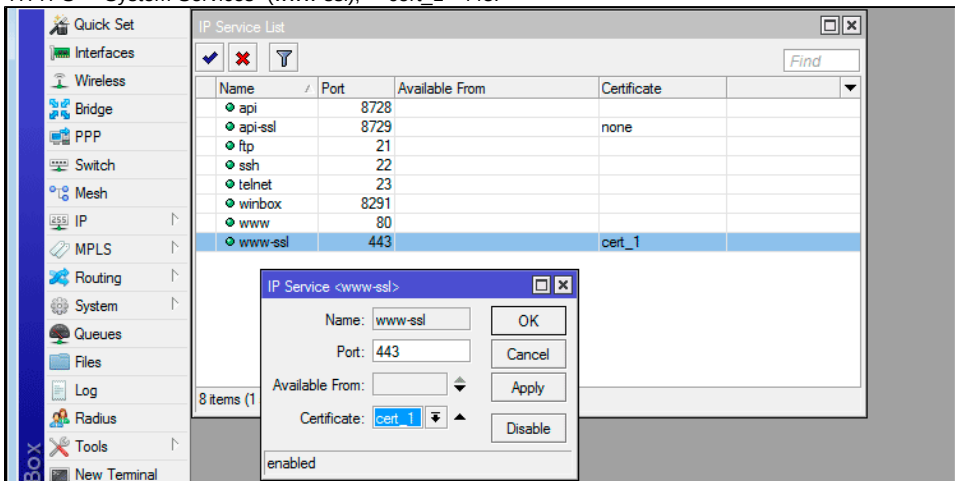
1. Winbox.



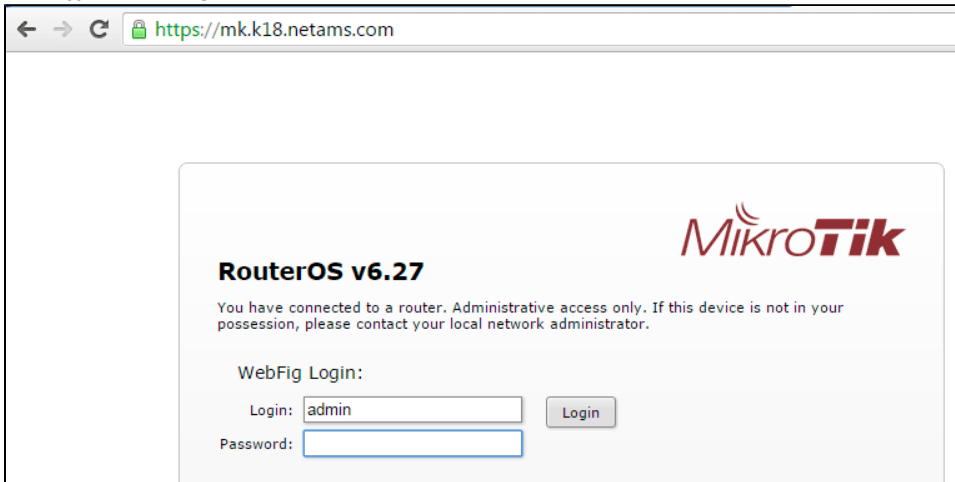
2. Winbox HTTP Web "System-Certificates".



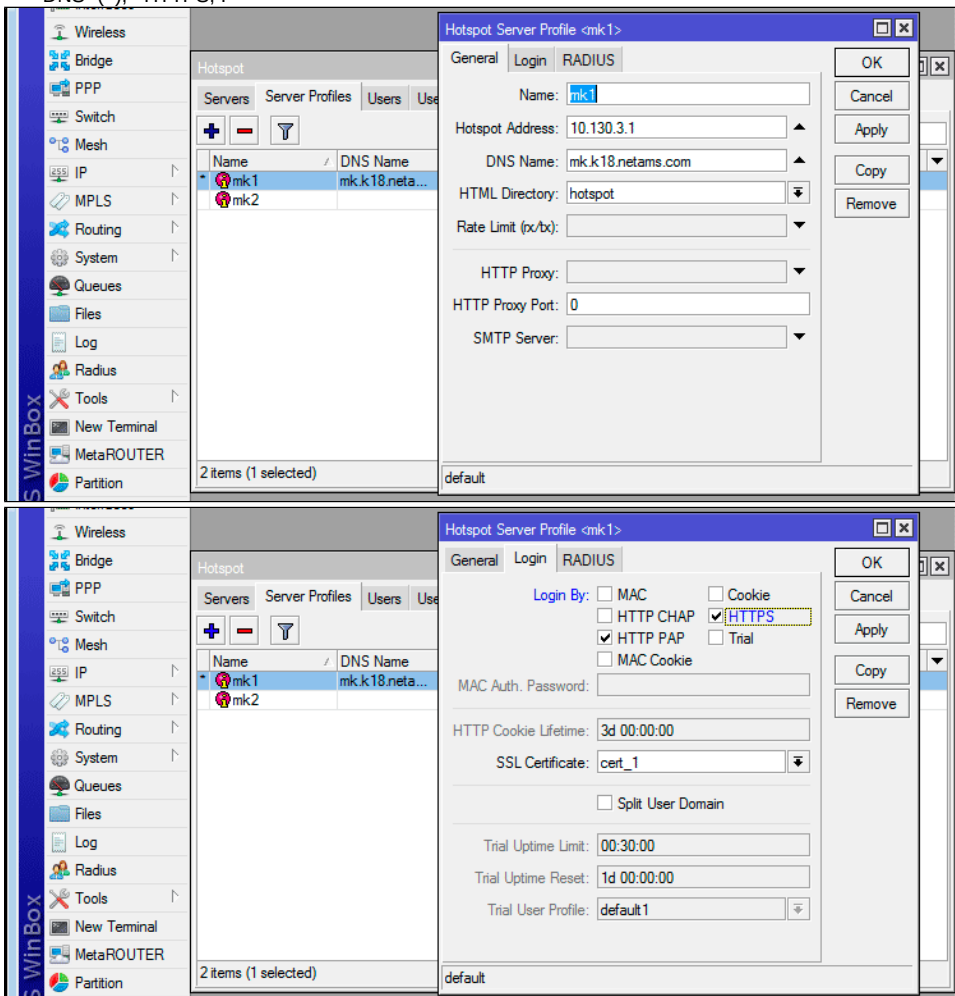
3. HTTPS "System-Services" (www-ssl), cert_1 443.



4. Mikrotik HTTPS.



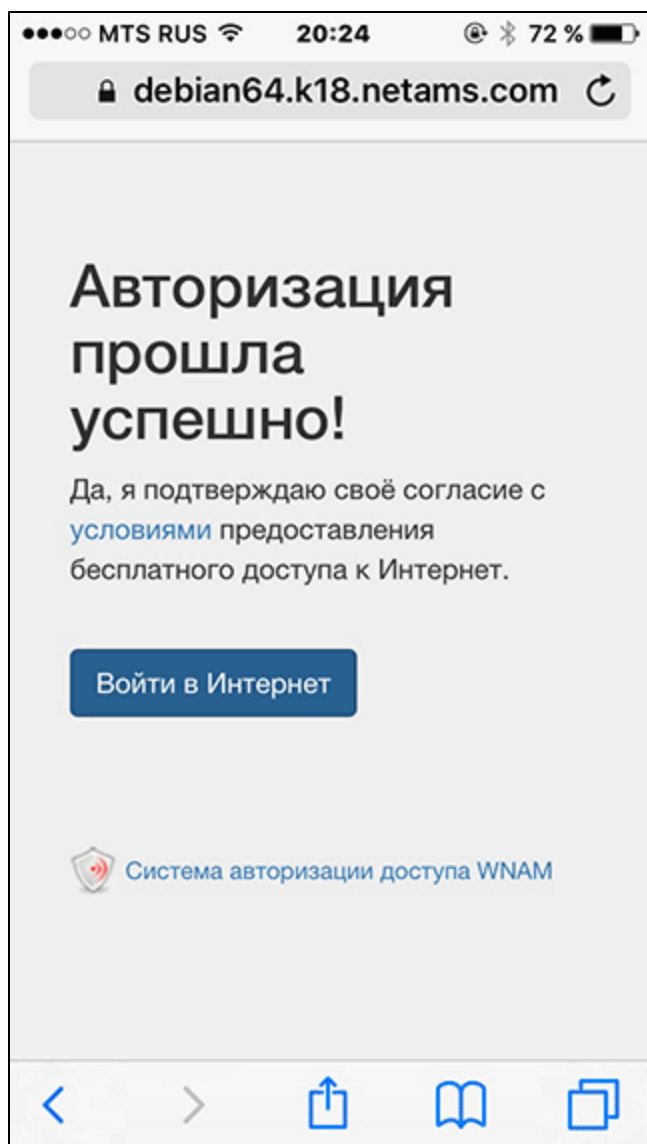
5. DNS- (), HTTPS, .



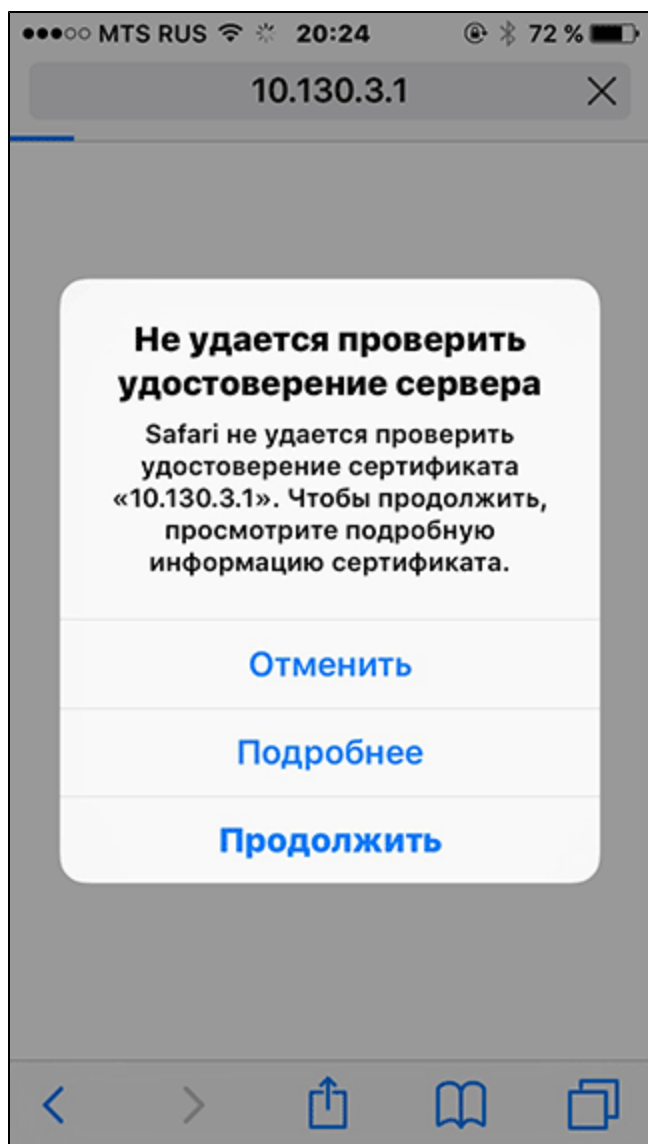
6. hotspot/rlogin.html, Mikrotik, HTTPS- DNS-, :

```
<form name="wnamlogin" action="https://debian64.k18.netams.com/cp/mikrotik" method="post">
<input type="hidden" name="server-address" value = "mk.k18.netams.com:443" />
```

HTTPS- HTTPS- Mikrotik. SSL-.



rlogin.html, .



, WNAME. Let's Encrypt 90, 1.