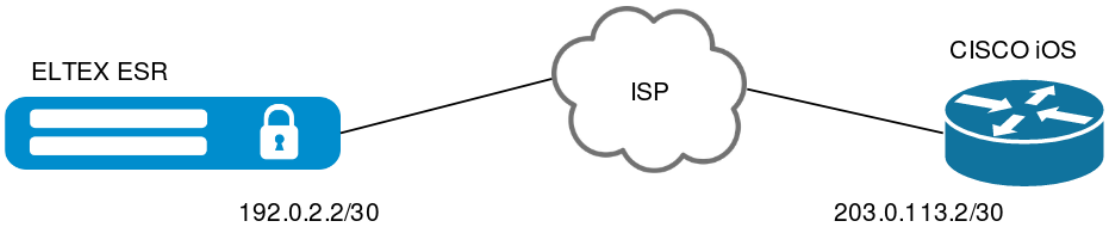
IPsec Site-to-Site VPN Eltex ESR Cisco iOS RSA Signature

IPsec Site-to-Site VPN.



IPsec VPN :

1. ELTEX ESR CISCO iOS.
2. / - (Certificate Authority, CA).
3. CISCO iOS
4. IPsec CISCO iOS
5. ( ) ELTEX ESR
6. ELTEX ESR
7. IPsec ELTEX ESR

ELTEX ESR UDP 500,4500 ESP self IPsec VPN:

```
esr# show running-config

object-group service IPsec
port-range 500
port-range 4500
exit

object-group network MAIN
ip address-range 192.0.2.2
exit

security zone untrusted
exit
security zone trusted
exit
```

```
interface gigabitethernet 1/0/1
security-zone untrusted
ip address 192.0.2.2/30
exit
interface gigabitethernet 1/0/2
security-zone trusted
ip address 192.168.10.1/24
exit
security zone-pair untrusted self
rule 10
description "IPsec"
action permit
match protocol udp
match destination-address MAIN
match destination-port IPsec
enable
exit
rule 20
description "ESP"
action permit
match protocol esp
match destination-address MAIN
enable
exit
rule 30
description "ICMP"
action permit
match protocol icmp
match destination-address MAIN
enable
exit
exit

security zone-pair trusted untrusted
rule 10
description "PERMIT ALL"
action permit
enable
exit
exit

ip route 0.0.0.0/0 192.0.2.1
```

CISCO iOS :

```
!
hostname cisco
!
ip domain name cisco.eltex.org
!
interface FastEthernet0/0
ip address 203.0.113.2 255.255.255.252
duplex auto
speed auto
!
interface FastEthernet0/1
ip address 172.16.10.1 255.255.255.0
duplex auto
speed auto
!
ip route 0.0.0.0 0.0.0.0 203.0.113.1
!
```

: , .

(NTP):

esr# **set date 12:00:00 14 November 2019**

cisco# **clock set 12:01:00 14 Nov 2019**

/ - (Certificate Authority, CA)

openssl.

: self-signed , CA , .

:

openssl genrsa -out ca.key 2048

```
self-signed :
```

openssl req -new -x509 -sha1 -days 3650 -key ca.key -out ca.crt

CA (ca.crt) CA (ca.key) VPN .

CISCO iOS

CISCO iOS:

cisco(config)#**crypto key generate rsa general-keys**

How many bits in the modulus [512]: **2048**

% Generating 1024 bit RSA keys …[OK]

CA myca:

cisco(config)#**crypto ca trustpoint myca**
cisco(ca-trustpoint)#**enrollment terminal**
cisco(ca-trustpoint)#**crl optional**
cisco(ca-trustpoint)#**exit**

CA :

cat ca.crt

-----BEGIN CERTIFICATE-----
MIID7TCCAtWgAwIBAgIJANdwKZKV0XNmMA0GCSqGSIb3DQEBBQUAMIGMMQswCQYD
...
yg==
-----END CERTIFICATE-----

:
cisco(config)#**crypto ca authenticate myca**

Enter the base 64 encoded CA certificate.
End with a blank line or the word “quit” on a line by itself

-----BEGIN CERTIFICATE-----
MIID7TCCAtWgAwIBAgIJANdwKZKV0XNmMA0GCSqGSIb3DQEBBQUAMIGMMQswCQYD
...
yg==
-----END CERTIFICATE-----

% Do you accept this certificate? [yes/no]: **yes**
Trustpoint CA certificate accepted.
% Certificate successfully imported

(CSR, certificate signing request):

cisco(config)#**crypto ca enroll myca**

% Include the router serial number in the subject name? [yes/no]: **yes**
% The serial number in the certificate will be: 13A594C9
% Include an IP address in the subject name? [no]: **no**
Display Certificate Request to terminal? [yes/no]: **yes**
Certificate Request follows:

MIIBkzCB/QIBADAzMTEwDwYDVQQFEwgxM0E1OTRDOTAeBgkqhkiG9w0BCQIWEWNp
...
sdHxeJkU4jMILCs7dPzkzPPDpJID9NU=

.csr openssl:

cat > cisco.csr

-----BEGIN CERTIFICATE REQUEST-----
MIIBkzCB/QIBADAzMTEwDwYDVQQFEwgxM0E1OTRDOTAeBgkqhkiG9w0BCQIWEWNp
...
sdHxeJkU4jMILCs7dPzkzPPDpJID9NU=
-----END CERTIFICATE REQUEST-----

(esr.csr) CA (ca.key), :

openssl x509 -req -days 3650 -sha1 -in cisco.csr -CA ca.crt -CAkey ca.key -set_serial 01 -out certs/cisco.crt

:

cat cisco.crt

-----BEGIN CERTIFICATE-----
...
-----END CERTIFICATE-----

CISCO iOS:

cisco(config)#**crypto ca import myca certificate**

Enter the base 64 encoded certificate.
End with a blank line or the word “quit” on a line by itself

—BEGIN CERTIFICATE—
...
—END CERTIFICATE—

% Router Certificate successfully imported

IPsec CISCO iOS

DN :

cisco(config)#**crypto isakmp identity dn**

ISAKMP (1):

cisco(config)#**crypto isakmp policy 10**
cisco(config-isakmp)#**encryption 3desc**
cisco(config-isakmp)#**authentication rsa-sig**
cisco(config-isakmp)#**group 2**

IPsec (2):

cisco(config)#**crypto ipsec transform-set TS esp-des esp-sha-hmac**
cisco(cfg-crypto-trans)#**exit**

, ACL, :

cisco(config)#**crypto map CMAP 10 ipsec-isakmp**
cisco(config-crypto-map)#**set peer 192.0.2.2**
cisco(config-crypto-map)#**set transform-set TS**
cisco(config-crypto-map)#**match address cryptoacl**
cisco(config-crypto-map)#**exit**
cisco(config)#**ip access-list extended cryptoacl**
cisco(config-ext-nacl)#**permit ip 172.16.10 0.0.0.255 192.168.10.0 0.0.0.255**

:

cisco(config)#**int fastEthernet 0/0**
cisco(config-if)#**crypto map CMAP**
cisco(config-if)#**exit**

ELTEX ESR

, . openssl.cfg:

```
[req]
default_bits = 2048
default_keyfile = esr.key
distinguished_name = req_distinguished_name
req_extensions = req_ext

[req_distinguished_name]
commonName = Common Name (eg, YOUR name)
commonName_default = esrvpn.eltex.org

countryName = Country Name (2 letter code)
countryName_default = RU

stateOrProvinceName = State or Province Name (full name)
stateOrProvinceName_default = Novosibirsk

localityName = Locality Name (eg, city)
localityName_default = NSK

0.organizationName = Organization Name (eg, company)
0.organizationName_default = ELTEX

[req_ext]
subjectAltName = @alt_names

[alt_names]
DNS.1 = esr.eltex.org
```

(CSR, certificate signing request) openssl.cfg:

openssl req -new -nodes -out esr.csr -config openssl.cfg

(esr.key) (esr.csr).

(esr.csr) CA (ca.key), :

openssl x509 -req -days 3650 -sha1 -in esr.csr -CA ca.crt -CAkey ca.key -set_serial 01 -out esr.crt

(esr.crt).

(ca.crt) , (esr.key) (esr.crt) ELTEX ESR

(esr.key esr.crt), CA (ca.crt) CISCO iOS (cisco.crt) USB Flash, TFTP/FTP/SFTP/SCP.

USB Flash :

esr# **sh storage-devices usb**

:

esr# **dir usb://<FLASH_NAME>**

CA:

esr# **copy usb://<FLASH_NAME>:/ca.crt certificate:ca/ca.crt**

esr# **copy usb://<FLASH_NAME>:/esr.key certificate:server-key/esr.key**

esr# **copy usb://<FLASH_NAME>:/esr.crt certificate:server-crt/esr.crt**

esr# **copy usb://<FLASH_NAME>:/esr.crt certificate:server-crt/cisco.crt**

:

esr-# **sh crypto certificates ca**

File name Issuer From To

---------- ---------- ---------- ----------

ca.crt ru1?0???U????novosibirsk 11 14 03:02:48 2019 GMT 11 11 03:02:48 2029 GMT

esr# **sh crypto certificates server-key**

esr.key Private key: (2048 bit)

esr-# **sh crypto certificates server-crt**

File name Issuer From To

---------- ---------- ---------- ----------

cisco.crt ru1?0???U????novosibirsk 11 14 03:36:48 2019 GMT 11 11 03:36:48 2029 GMT

esr.crt ru1?0???U????novosibirsk 11 14 03:25:58 2019 GMT 11 11 03:25:58 2029 GMT

IPsec ELTEX ESR

ISAKMP (1):

esr(config)# **security ike proposal IKEPROP**
esr(config-ike-proposal)# **encryption algorithm 3des**
esr(config-ike-proposal)# **dh-group 2**
esr(config-ike-proposal)# **exit**

:

esr(config)# **security ike policy IKEPOLICY**
esr(config-ike-policy)# **certificate ca ca.crt**
esr(config-ike-policy)# **certificate local-crt esr.crt**
esr(config-ike-policy)# **certificate local-crt-key esr.key**
esr(config-ike-policy)# **certificate remote-crt cisco.crt**
esr(config-ike-policy)# **authentication method public-key**
esr(config-ike-policy)# **proposal IKEPROP**
esr(config-ike-policy)# **exit**

IPsec:

esr(config)# **security ike gateway IKEGW**
esr(config-ike-gw)# **ike-policy IKEPOLICY**
esr(config-ike-gw)# **local address 192.0.2.2**
esr(config-ike-gw)# **local network 192.168.10.0/24**
esr(config-ike-gw)# **remote address 213.0.113.2**
esr(config-ike-gw)# **remote network 172.16.10.0/24**
esr(config-ike-gw)# **mode policy-based**
esr(config-ike-gw)# **exit**

IPsec (2)

esr(config)# **security ipsec proposal IPSECPROP**
esr(config-ipsec-proposal)# **encryption algorithm des**
esr(config-ipsec-proposal)# **pfs dh-group 2**
esr(config-ipsec-proposal)# **exit**

esr(config)# **security ipsec policy IPSECPOLICY**
esr(config-ipsec-policy)# **proposal IPSECPROP**
esr(config-ipsec-policy)# **exit**

IPsec - (route):

esr(config)# **security ipsec vpn IPSECVPN**
esr(config-ipsec-vpn)# **mode ike**
esr(config-ipsec-vpn)# **ike establish-tunnel route**
esr(config-ipsec-vpn)# **ike gateway IKEGW**
esr(config-ipsec-vpn)# **ike ipsec-policy IPSECPOLICY**
esr(config-ipsec-vpn)# **enable**
esr(config-ipsec-vpn)# **exit**

IPsec VPN

IP LAN :

esr# **ping 172.16.10.1 source ip 192.168.10.1**

PING 172.16.10.1 (172.16.10.1) from 192.168.10.1 : 56(84) bytes of data.

.!!!!

--- 172.16.10.1 ping statistics ---

5 packets transmitted, 4 received, 20% packet loss, time 4039ms

rtt min/avg/max/mdev = 4.544/24.296/74.151/28.867 ms

IPsec VPN :

esr# **sh security ipsec vpn status**

Name Local host Remote host Initiator spi Responder spi State

---------- ---------- ---------- ---------- ---------- ----------

IPSECVPN 192.0.2.2 213.0.113.2 0x35475c4c0ed0c90f 0x26487c26958d84a4 **Established**

esr# **sh security ipsec vpn status IPSECVPN**

Currently active IKE SA:

Name: IPSECVPN

State: Established

Version: v1-only

Unique ID: 1

Local host: 192.0.2.2

Remote host: 213.0.113.2

Role: Initiator

Initiator spi: 0x35475c4c0ed0c90f

Responder spi: 0x26487c26958d84a4

Encryption algorithm: des

Authentication algorithm: sha1

Diffie-Hellman group: 2

Established: 12 seconds ago

Rekey time: 12 seconds

Reauthentication time: 2 hours, 44 minutes and 5 seconds

Child IPsec SAs:

Name: IPSECVPN

State: Installed

Protocol: esp

Mode: Tunnel

Encryption algorithm: des

Authentication algorithm: sha1

Rekey time: 42 minutes and 7 seconds

Life time: 59 minutes and 48 seconds

Established: 12 seconds ago

Traffic statistics:

Input bytes: 336

Output bytes: 336

Input packets: 4

Output packets: 4
