Configuring Client-to-Lan IPsec VPN using certificates between SRX and Windows Firewall with Advanced Security

Version 1.0
December 2014
Overview

This example shows the configuration of a Client-to-Lan VPN between a Juniper Networks SRX device and Windows client using the Windows Firewall VPN client.

Setup Prerequisites

- DEP (Dynamic End Point) configuration on SRX
- Tunnel mode in SRX
- IKEv1 (Win client supports only IKEv1)
- IPSec using certificates for authentication
- Perfect Forward Secrecy group2
- Client using Windows firewall with Advanced Security
- Windows Machine Certificate Store
- SRX using separate zones for all interfaces
- SRX using S0 and LAN-side interfaces in default VR and gateway interface is in custom VR.
- Microsoft CA server for certificate signing

Included Platforms and Software Versions

This document applies to Junos 11.4 and subsequent releases for all SRX devices

Topology

Configuration Steps

- Enroll device certificate on SRX
- Configure SRX using a certificate-based VPN
- Configuring Windows certificate services (optional)
- Enrolling client CA certificate
- Enrolling client device certificate
- Creating dial-up VPN in Windows
Enroll Certificates on SRX

1. Configure the CA

   [edit]
   root@srx# set security pki ca-profile ROOT ca-identity mscal
   root@srx# set security pki ca-profile ROOT enrollment url http://2.2.2.2/certsrv/mscep/mscep.dll
   root@srx# commit

   Note:
   The system will use the CDP of the received client certificate for CRL validation by default.
   Refer: “Understanding Certificate Revocation Lists”
   https://www.juniper.net/techpubs/en_US/junos12.1x47/topics/concept/certificate-crl-understanding.html

   “Example: Manually loading a CRL onto the Device”

   “Example: Configuring a Certificate Authority Profile with CRL Locations”

2. Enroll the CA certificate

   root@srx> request security pki ca-certificate enroll ca-profile ROOT
   Type yes at the prompt to load the CA certificate

3. Generate a key pair for Device certificate

   root@srx> request security pki generate-key-pair certificate-id ZTH_HUB

4. Enroll the local certificate

   root@srx> request security pki local-certificate enroll ca-profile ROOT certificate-id ZTH_HUB domain-name vpn-srx240-05.juniper.net email vpn-srx240-05@juniper.net ip-address 1.1.1.1 subject “C=US,DC=juniper,ST=CA,L=Sunnyvale,0=Juniper,OU=engineering,CN=vpn-srx240-05”

Configure SRX

1. Configure the interfaces

   root@srx# set interfaces ge-0/0/1.0 family inet address 1.1.1.1/24
   root@srx# set interfaces ge-0/0/3.0 family inet address 192.168.10.1/24
   root@srx# set interfaces st0.1 family inet

2. Configure Ike Phase1

   root@srx# set security ike proposal IKE_PROP authentication-method rsa-signatures
   root@srx# set security ike proposal IKE_PROP dh-group group2
   root@srx# set security ike proposal IKE_PROP authentication-algorithm sha
   root@srx# set security ike proposal IKE_PROP encryption-algorithm aes-128-cbc
   root@srx# set security ike proposal IKE_PROP lifetime-seconds 3600
   root@srx# set security ike policy IKE_POL mode main
   root@srx# set security ike policy IKE_POL proposals IKE_PROP
   root@srx# set security ike policy IKE_POL certificate local-certificate ZTH_HUB
   root@srx# set security ike policy IKE_POL certificate peer-certificate-type x509-signature
   root@srx# set security ike gateway CORP_GW ike-policy IKE_POL
   root@srx# set security ike gateway CORP_GW dynamic distinguished-name wildcard C=US
   root@srx# set security ike gateway CORP_GW local-identity inet 1.1.1.1
   root@srx# set security ike gateway CORP_GW external-interface ge-0/0/1
   root@srx# set security ike gateway CORP_GW version v1-only

   © Juniper Networks, Inc. 3
3. Configure Ike Phase 2

```
root@srx# set security ipsec proposal IPSEC_PROP protocol esp
dev
root@srx# set security ipsec proposal IPSEC_PROP authentication-algorithm hmac-sha1-96
root@srx# set security ipsec proposal IPSEC_PROP encryption-algorithm aes-128-cbc
dev
root@srx# set security ipsec proposal IPSEC_PROP lifetime-seconds 3600
dev
root@srx# set security ipsec policy IPSEC_POL perfect-forward-secrecy keys group2
dev
root@srx# set security ipsec policy IPSEC_POL proposals IPSEC_PROP
dev
root@srx# set security ipsec vpn CORP_VPN bind-interface st0.1
root@srx# set security ipsec vpn CORP_VPN ike gateway CORP_GW
dev
root@srx# set security ipsec policy IPSEC_POL proposals IPSEC_PROP
```

4. Configure security policies

```
root@srx# set security policies from-zone vpn to-zone trust policy P1 match source-address any
root@srx# set security policies from-zone vpn to-zone trust policy P1 match destination-address any
root@srx# set security policies from-zone vpn to-zone trust policy P1 match application any
root@srx# set security policies from-zone trust to-zone vpn policy P2 match source-address any
root@srx# set security policies from-zone trust to-zone vpn policy P2 match destination-address any
root@srx# set security policies from-zone trust to-zone vpn policy P2 match application any
root@srx# set security policies from-zone trust to-zone vpn policy P2 then permit
```

5. Configure security zones

```
root@srx# set security zones security-zone untrust host-inbound-traffic system-services ike
root@srx# set security zones security-zone untrust host-inbound-traffic system-services ping
root@srx# set security zones security-zone untrust interfaces ge-0/0/1.0

root@srx# set security zones security-zone trust host-inbound-traffic system-services all
root@srx# set security zones security-zone trust host-inbound-traffic protocols all
root@srx# set security zones security-zone trust interfaces ge-0/0/3.0

root@srx# set security zones security-zone vpn host-inbound-traffic system-services all
root@srx# set security zones security-zone vpn host-inbound-traffic protocols all
root@srx# set security zones security-zone vpn interfaces st0.1
```

6. Configure routing-instance

```
root@srx# set routing-instances INTERNET instance-type virtual-router
root@srx# set routing-instances INTERNET interface ge-0/0/1.0
root@srx# set routing-instances INTERNET routing-options static route 0/0 next-hop 1.1.1.2
```

7. Configure route back to VPN tunnel interface for peer IP address

```
root@srx# set routing-options static route 2.2.2.2/32 next-hop st0.1
```
SRX Configuration Results

root@srx# show interfaces
ge-0/0/1 {
  unit 0 {
    family inet {
      address 1.1.1.1/24;
    }
  }
}
ge-0/0/3 {
  unit 0 {
    family inet {
      address 192.168.10.1/24;
    }
  }
}
st0 {
  unit 1 {
    family inet;
  }
}

[edit]
root@srx# show security
pki {
  ca-profile ROOT {
    ca-identity mscal;
    enrollment {
      url http://2.2.2.2/certsrv/mscep/mscep.dll;
    }
  }
}
ike {
  proposal IKE_PROP {
    authentication-method rsa-signatures;
    dh-group group2;
    authentication-algorithm sha1;
    encryption-algorithm aes-128-cbc;
    lifetime-seconds 3600;
  }
  policy IKE_POL {
    mode main;
    proposals IKE_PROP;
    certificate {
      local-certificate ZTH_HUB;
      peer-certificate-type x509-signature;
    }
  }
  gateway CORP_GW {
    ike-policy IKE_POL;
    dynamic {
      distinguished-name {
        wildcard C-US;
      }
    }
    local-identity inet 1.1.1.1;
    external-interface ge-0/0/1;
    version v1-only;
  }
}
ipsec {
    proposal IPSEC_PROP {
        protocol esp;
        authentication-algorithm hmac-shal-96;
        encryption-algorithm aes-128-cbc;
        lifetime-seconds 3600;
    }
    policy IPSEC_POL {
        perfect-forward-secrecy {
            keys group2;
        }
        proposals IPSEC_PROP;
    }
    vpn CORP_VPN {
        bind-interface st0.1;
        ike {
            gateway CORP_GW;
            ipsec-policy IPSEC_POL;
        }
    }
}

policies {
    from-zone vpn to-zone trust {
        policy P1 {
            match {
                source-address any;
                destination-address any;
                application any;
            }
            then {
                permit;
            }
        }
    }
    from-zone trust to-zone vpn {
        policy P2 {
            match {
                source-address any;
                destination-address any;
                application any;
            }
            then {
                permit;
            }
        }
    }
}

zones {
    security-zone untrust {
        host-inbound-traffic {
            system-services {
                ike;
                ping;
            }
        }
    }
    security-zone trust {
        host-inbound-traffic {
            system-services {

```
Configuring Windows Certificate Services (optional)

The same Windows machine may be used as a VPN client and as a CA server. This depends on user requirements and if CA server functionality is available on same Windows machine. It is possible to have the localcert signed by a different CA server as long as the CA is common to both the Windows client certificate and the SRX device certificate.

How to create Microsoft CA in Windows:

**Enrolling Client CA Certificate**

Refer to “Download the Trusted Root CA certificate” & “Import the Trusted Root (CA) Certificate” sections


**Enrolling Client Device Certificate**

Refer to “How To: Install a Certificate for Use with IP Security”

http://support.microsoft.com/kb/253498

or

Refer to “Create a Custom Certificate Request” for submitting a PCKS file for submitting to CA.


**Note:** For this example, the device certificate request must include Country of US to allow SRX wildcard matching of C=US in certificate.

**Configuring VPN in Windows Firewall Client**

1. **Launch Windows Firewall with Advanced Security**

   Click Windows Menu
   Select Control Panel
   Select Windows Firewall
   Click Advanced Settings

2. **Create new connection security rule**

   Select Connection Security Rules
   Select ‘New Rule’ on right side
Select ‘Tunnel’ and click Next

Select ‘Client-to-Gateway’ and click Next

Select ‘Require authentication for inbound and outbound connections’ and click Next
Enter SRX gateway IP address for 'Remote Tunnel Endpoint' and click Next.

Select 'Computer Certificate' and select the 'Signing Algorithm as RSA and Certificate type (depends on your CA setup). Click Browse.
Select CA certificate and click OK and then click Next.

In this example we are using WIN-5QR2LUTHF1-CA. This is the Root Certificate from the Windows Machine store and is the CA used to sign both the SRX’s certificate and the Windows client device certificate.

NOTE: If you do not see your CA refer to the following Microsoft articles to add to list
Adding certificates to the Trusted Root Certification Authorities store for a local computer

Adding certificates to the Trusted Root Certification Authorities store for a local computer

Select all options and click Next
Enter a Name and Description and click Finish

3. Define the Protected network ranges

Select the newly created rule and click Properties under Actions
Select Computers tab
Enter Client NIC IP address as Endpoint 1
Enter Remote network behind SRX as Endpoint 2

4. Define the Tunnel Endpoints

Select Advanced Tab and click on Customize for Ipsec tunneling
Edit endpoints to reflect the Local tunnel endpoint being the Window client address and Remote tunnel endpoint is the SRX’s external interface. Click OK then click Apply the OK.

5. Enable perfect forward secrecy

Open an Elevated CMD prompt
Click on Windows Menu
Enter search phrase CMD.exe into Search field
Right click on the resulting cmd.exe file
Select ‘Run as Administrator’

Enter the following command to enable FFS

C:\Users\Administrator>netsh advfirewall consec set rule name="Test1" new qmsecmethod= esp:sha1-aes128
C:\Users\Administrator>netsh advfirewall consec set rule name="Test1" new qmpfs= dhgroup2

Windows Configuration Results

C:\Users\Administrator>netsh advfirewall consec show rule name="Test1"

Rule Name: Test1
-----------------------------------------------
Enabled: Yes
Profiles: Domain,Private,Public
Type: Static
Mode: Tunnel
LocalTunnelEndpoint: 2.2.2.2
RemoteTunnelEndpoint: 1.1.1.1
Endpoint1: 2.2.2.2/32
Endpoint2: 192.168.10.0/24
Protocol: Any
Action: RequireInRequireOut
Auth1: ComputerCert
Auth1CAName: CN=RIN-5VQR2LUTHF1-CA
Auth1CertMapping: No
Auth1ExcludeCName: No
Auth1CertType: Root
Auth1HealthCert: No
MainModeSecMethods: DHGroup2-AES128-SHA1,DHGroup2-3DES-SHA1
QuickModeSecMethods:  ESP:SHA1-AES128+60Min+100000KB
ExemptIPsecProtectedConnections:  No
ApplyAuthorization:  No

Verifying Setup and Usage

1) Verify the machine cert-store to make sure that private key is attached to required certificates as indicated by the presence of a small key on the certificate icon.

Open Certificate Manager by clicking the Start button Picture of the Start button, typing certmgr.msc into the Search box, and then pressing ENTER.

2) Verify logs in Windows firewall client:
Go to event viewer and check for security logs under Windows logs

3) Verify SRX tunnel status

root@srx# run show security ike sa
Index State Initiator cookie Responder cookie Mode Remote Address
6646446 UP 6c5848b0dc4aeae8 6e722f256cb17955 Main 2.2.2.2

[edit]
root@srx# run show security ike sa detail
IKE peer 2.2.2.2, Index 6646446, Gateway Name: ZTH_HUB_GW
   Role: Responder, State: UP
   Initiator cookie: 6c5848b0dc4aeae8, Responder cookie: 6e722f256cb17955
   Exchange type: Main, Authentication method: RSA-signatures
   Local: 1.1.1.1:500, Remote: 2.2.2.2:500
   Lifetime: Expires in 1789 seconds
   Peer ike-id: C-US, DC=juniper, ST=CA, L=Sunnyvale, O=Juniper, OU=engineering, CN=mjain-win2k8-1
   Xauth user-name: not available
   Xauth assigned IP: 0.0.0.0
   Algorithms:
      Authentication : hmac-sha256-128
      Encryption : aes128-cbc
      Pseudo random function: hmac-sha256
      Diffie-Hellman group : DH-group-2
   Traffic statistics:
      Input bytes : 2596
      Output bytes : 1896
      Input packets: 5
      Output packets: 4
   IPSec security associations: 1 created, 0 deleted
   Phase 2 negotiations in progress: 1

   Negotiation type: Quick mode, Role: Responder, Message ID: 0
   Local: 1.1.1.1:500, Remote: 2.2.2.2:500
Local identity: 1.1.1.1
Remote identity: C=US, DC=juniper, ST=CA, L=Sunnyvale, O=Juniper, OU=engineering, CN=mjain-win2k8-1
Flags: IKE SA is created

[edit]
root@srx# run show security ipsec sa
Total active tunnels: 1
ID    Algorithm       SPI      Life:sec/kb  Mon lsys Port  Gateway
<268173314 ESP:aes-cbc-128/sha1 9d445798 3582/  99999 - root 500 2.2.2.2
>268173314 ESP:aes-cbc-128/sha1 e80f1c05 3582/  99999 - root 500 2.2.2.2

[edit]
root@srx# run show security ipsec sa detail
ID: 268173314 Virtual-system: root, VPN Name: ZTH_HUB_VPN
Local Gateway: 1.1.1.1, Remote Gateway: 2.2.2.2
Local Identity: ipv4_subnet(any:0, [0..7]=192.168.10.0/24)
Remote Identity: ipv4(any:0, [0..3]=2.2.2.2)
Version: IKEv1
DF-bit: clear, Bind-interface: st0.1
Port: 500, Nego#: 10, Fail#: 0, Def-Del#: 0 Flag: 0x608a29
Tunnel events:
Wed Oct 08 2014 00:16:50 -0700: IPSec SA negotiation successfully completed (1 times)
Wed Oct 08 2014 00:16:50 -0700: Tunnel is ready. Waiting for trigger event or peer to trigger negotiation (1 times)
Direction: inbound, SPI: 9d445798, AUX-SPI: 0
Hard lifetime: Expires in 3578 seconds
Lifesize Remaining: 99999 kilobytes
Soft lifetime: Expires in 3015 seconds
Mode: Tunnel(0 0), Type: dynamic, State: installed
Anti-replay service: counter-based enabled, Replay window size: 64
Direction: outbound, SPI: e80f1c05, AUX-SPI: 0
Hard lifetime: Expires in 3578 seconds
Lifesize Remaining: 99999 kilobytes
Soft lifetime: Expires in 3015 seconds
Mode: Tunnel(0 0), Type: dynamic, State: installed
Anti-replay service: counter-based enabled, Replay window size: 64

4) Verify SRX Certificates

[edit]
root@srx# run show security pki ca-certificate
Certificate identifier: ROOT
Issued to: WIN-5VQR2LUTHF1-CA, Issued by: CN = WIN-5VQR2LUTHF1-CA
Validity:
    Not before: 10-3-2014 22:04 UTC
    Not after: 10-3-2019 23:14 UTC
Public key algorithm: rsaEncryption(2048 bits)

Certificate identifier: ikev2natt
Issued to: pond-win, Issued by: CN = pond-win
Validity:
    Not before: 11-22-2013 23:26 UTC
    Not after: 11-22-2018 23:35 UTC
Public key algorithm: rsaEncryption(2048 bits)
root@srx# run show security pki ca-certificate ca-profile ROOT detail

Certificate identifier: ROOT
Certificate version: 3
Serial number: 2efe46115e3f418e46b1f7b7f648584e
Issuer:
  Common name: WIN-5VQR2LUTHF1-CA
Subject:
  Common name: WIN-5VQR2LUTHF1-CA
Subject string:
  CN=WIN-5VQR2LUTHF1-CA
Validity:
  Not before: 10-3-2014 22:04 UTC
  Not after: 10-3-2019 22:14 UTC
Public key algorithm: rsaEncryption(2048 bits)
16:de:d3:ff:3c:0a:3c:ff:1c:82:02:77:dc:92:f4:70:00:0c:4c
f8:00:8d:51:c3:02:03:01:00:01
Signature algorithm: sha1WithRSAEncryption
Use for key: CRL signing, Certificate signing, Digital signature
Fingerprint:

[edit]
root@srx# run show security pki local-certificate certificate-id ZTH_HUB detail

Certificate identifier: ZTH_HUB
Certificate version: 3
Serial number: 61053ed5000000000004
Issuer:
  Common name: WIN-5VQR2LUTHF1-CA
Subject:
  Organization: Juniper, Organizational unit: engineering, Country: US, State: CA, Locality: Sunnyvale,
  Common name: vpn-srx240-05, Domain component: juniper
Subject string:
  C=US, DC=juniper, ST=CA, L=Sunnyvale, O=Juniper, OU=engineering, CN=vpn-srx240-05
  Alternate subject: "vpn-srx240-05@juniper.net", vpn-srx240-05.juniper.net, 1.1.1.1
Validity:
  Not before: 10-3-2014 22:45 UTC
  Not after: 10-3-2015 22:55 UTC
Public key algorithm: rsaEncryption(1024 bits)
5e:ae:7a:3c:78:34:1f:a6:bf:3c:ae:6e:3f:7b:3d:02:03:01:00:01
Signature algorithm: sha1WithRSAEncryption
Distribution CRL:
  file://WIN-5VQR2LUTHF1/CertEnroll/WIN-5VQR2LUTHF1-CA.crl
Fingerprint:

5) Windows Tunnels status SRX Certificates

To check the tunnel status on Win client please go to event viewer -> windows logs -> security and then check the Audit success for Quick mode.

An IPsec quick mode security association was established.

Local Endpoint:
- Network Address: 2.2.2.2
- Network Address mask: 255.255.255.255
- Port: 0
- Tunnel Endpoint: 2.2.2.2

Remote Endpoint:
- Network Address: 192.168.10.0
- Network Address Mask: 255.255.255.0
- Port: 0
- Private Address: 0.0.0.0
- Tunnel Endpoint: 1.1.1.1

Cryptographic Information:
- Integrity Algorithm - AH: -
- Integrity Algorithm - ESP: SHA-1
- Encryption Algorithm: AES-128

Security Association Information:
- Lifetime - seconds: 3600
- Lifetime - data: 100000
- Lifetime - packets: 2147483647
- Mode: Tunnel
- Role: Initiator
- Quick Mode Filter ID: 83470
- Main Mode SA ID: 2171
- Quick Mode SA ID: 1108

Additional Information:
- Inbound SPI: 3325224778
- Outbound SPI: 717234676
- Virtual Interface Tunnel ID: 0
- Traffic Selector ID: 0

To check the tunnel status on Win client please go to event viewer -> windows logs -> security and then check the Audit success for Main mode.

An IPsec main mode security association was established. Extended mode was not enabled. A certificate was used for authentication.
Principal Name: mjain-win2k8-1
Network Address: 2.2.2.2
Keying Module Port: 500

Local Certificate:
SHA Thumbprint: 11f73620578fa9b4b5a7359b48c29fb534b5f229
Issuing CA: WIN-5VQR2LUTHF1-CA
Root CA: CN=WIN-5VQR2LUTHF1-CA

Remote Endpoint:
Principal Name: vpn-srx240-05.juniper.net
Network Address: 1.1.1.1
Keying Module Port: 500

Remote Certificate:
SHA thumbprint: e19d5bfa66f6588fb6303405546995778a26669b
Issuing CA: WIN-5VQR2LUTHF1-CA
Root CA: CN=WIN-5VQR2LUTHF1-CA

Cryptographic Information:
Cipher Algorithm: AES-128
Integrity Algorithm: SHA 256
Diffie-Hellman Group: DH group 2

Security Association Information:
Lifetime (minutes): 30
Quick Mode Limit: 0
Main Mode SA ID: 2171

Additional Information:
Keying Module Name: IKEv1
Authentication Method: Certificate
Role: Initiator
Impersonation State: Not enabled
Main Mode Filter ID: 83452

**E&U, SAN for IKE-ID:**

<table>
<thead>
<tr>
<th>VPN Server Certificate</th>
<th>RE ID Type</th>
<th>RE ID Value</th>
<th>Client Verify</th>
<th>Required on VPN Connection</th>
</tr>
</thead>
<tbody>
<tr>
<td>CN = hostname</td>
<td>local-identity: hostname</td>
<td>hostname</td>
<td>CN</td>
<td>hostname from CN</td>
</tr>
<tr>
<td>CN = IP Address</td>
<td>local-identity: address inet</td>
<td>IP Address</td>
<td>CN</td>
<td>IP Address from CN</td>
</tr>
<tr>
<td>CN = hostname SAN = DNS Name</td>
<td>local-identity: hostname</td>
<td>hostname</td>
<td>SAN</td>
<td>DNS Name from SAN</td>
</tr>
<tr>
<td>CN = IP Address SAN = DNS Name</td>
<td>local-identity: address inet</td>
<td>IP Address</td>
<td>CN</td>
<td>IP Address from CN</td>
</tr>
<tr>
<td>CN = IP Address SAN = DNS Name</td>
<td>local-identity: hostname</td>
<td>hostname</td>
<td>SAN</td>
<td>DNS Name from SAN</td>
</tr>
<tr>
<td>CN = hostname SAN = DNS Name SAN = IP Address</td>
<td>local-identity: hostname</td>
<td>hostname</td>
<td>SAN = DNS Name</td>
<td>DNS Name from SAN</td>
</tr>
<tr>
<td>CN = IP Address SAN = DNS Name SAN = IP Address</td>
<td>local-identity: hostname</td>
<td>hostname</td>
<td>SAN = DNS Name</td>
<td>DNS Name from SAN</td>
</tr>
<tr>
<td>VPN Server Certificate EKU</td>
<td>Accepted by Windows Firewall Client</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>----------------------------</td>
<td>-----------------------------------</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>IP security IKE intermediate Server Authentication</td>
<td>Yes</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>IP security IKE intermediate</td>
<td>No</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>IP security IKE intermediate Client Authentication</td>
<td>No</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Server Authentication</td>
<td>Yes</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Client Authentication</td>
<td>No</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Server Authentication Client Authentication</td>
<td>Yes</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>IP security IKE intermediate Server Authentication</td>
<td>Yes</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Client Authentication</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>None</td>
<td>No</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>