Deploying Netscreen-Remote with Smart-cards

Version 1.0

January, 2008
Introduction

This document describes the setup process for Netscreen-Remote 8.9 (10.8.0) when smart cards are used to authenticate VPN sessions. This document focuses on setup of the SafeNet iKey 2000 on the Windows XP platform using a Microsoft CA server. Similar procedures will apply to setting up other smart cards such as Schlumberger PCMCIA smart card, Datakey CSV and other smart cards using DataKey driver and third-party CA servers such as VeriSign and Entrust.

Included Platforms and ScreenOS

This application note demonstrates setup on ScreenOS 5.4.0r8 and Netscreen-Remote 8.9. However, it also applies to following ScreenOS version and Netscreen-Remote version:

- ScreenOS 5.0
- ScreenOS 5.1
- ScreenOS 5.2
- ScreenOS 5.3
- ScreenOS 5.4
- ScreenOS 6.0
- Netscreen-Remote 8.7 or higher

The product list includes the following:

- NS5000
- ISG1000/2000
- NS500/200/50/25
- SSG550m/550/520m/520/320/350/140
- NS5GT
- SSG5/20

Overview

A smart card is a device with a memory chip for securely storing private keys and certificates; some units have built-in random number and certificate generation chips. The beauty of a smart card is a user can insert their smart card in any computer for VPN authentication.

Smart card stores the private key in its on-board memory. Most of the time this key is encrypted with a passphrase. When the private key is used, it requires the user to enter this passphrase to retrieve. This enhances the security of storing the private key.
Network Diagram

Refer to Figure 1 below for Network Topology used for this configuration example.

Figure 1.

Step 1: Initialize the iKey

Before an old iKey is used, it needs to be initialized.

Initialize iKey is to delete all existing keys and certificates, and setup a new passphrase.

To manage keys and certificates on the iKey, you need to have CIP utilities installed on your PC.

(This program can be found on the installation CD from iKey 2000)
To initialize iKey, first execute the CIP utilities program and plug your iKey into the USB port. Select the slot that shows you the iKey connected. Right click and select “Initialize Token”.

The warning will be prompted, click “Continue Initialization”.

The program will start to initialize. Your iKey, all old keys and certificates will be erased. The passcode will be preconfigured as “PASSWORD”.

Then you need to change the passphrase as soon as possible.
To select a new passphrase, you need select the slot that contain your iKey from CIP utilities, right click to select “Change passphrase”. 
A window will prompt you to enter the passphrase. Key in “PASSWORD” and click OK. This will help you to login to the iKey.
Then, a change passphrase window will be prompted.
Key in the old passphrase: “PASSWORD” and new passphrase that you selected.
Click OK to complete.

**Step 2: Generate and load certificate on iKey**

To generate a certificate for the iKey, you need to connect the iKey to the USB port on your computer, unless it is still there from step 1. Certificates can be generated via the web interface of the Microsoft CA server.
When you have accessed to the web interface of CA server, select “Request a certificate” and click Next.

Then select “Advanced request” and click Next.
Select “Submit a certificate request to this CA using a form”, then click Next.

Enter this information: (only change the fields below, and leave all other fields at the default setting.)

Name: (name of the user)
Email: (email of the user)
Intended Purpose: IPSec Certificate
CSP: Datakey RSA CSP
Key Size: 1024
Hash Algorithm: MD5

Then click Submit.
A login window will be prompted, as you need to access to iKey. Enter the passphrase and click OK.

When the certificate has been generated, click on “Install this certificate”.
After a few minutes, a successful message will be prompted. Your iKey is now installed with the certificate that you just requested from the CA server.
When you login to CIP utilities, you can see the installed certificate.

Step 3: Load CA certificate into Netscreen-Remote

In addition to loading the certificate to the iKey, you need to load the CA certificate on the Netscreen-Remote client. To do this, you need to access the web interface of the CA server.

Select "Retrieve the CA certificate or certificate revocation list" and click next.

Select “Retrieve the CA certificate or certificate revocation list” and click next.
Step 4: Configure Netscreen-Remote

After the certificate is loaded on the iKey and you retrieved the CA certificate/CRL, you can go ahead to start configuring your Netscreen-Remote for a VPN connection.

To start configuring VPN connection on Netscreen-Remote, you need to launch the Security Policy Editor.

Right click My connections, select Add > Connection.
Enter the following information:

ID Type: IP subnet
Subnet: 192.168.1.0
Mask: 255.255.255.0
Use: (checked), Secure Gateway Tunnel
ID Type: Any,
Gateway IP Address, 172.27.6.136 (IP address of ‘untrust’ interface of IPSec gateway.)
Click on the “+” next to New Connection to expand the detail.

Select My Identity and enter the following:

- **Select Certificate:** Select automatically during IKE negotiation
- **ID Type:** Distinguished Name
Click on the “+” next to the Security Policy and enter the following:

Select Phase 1 Negotiation Mode: Aggressive Mode
Enable Perfect Forward Secrecy: Checked
Click on the “+” next to Authentication (Phase 1), enter following:

- **Authentication Method**: RSA Signatures
- **Encrypt Alg**: Triple DES
- **Hash Alg**: SHA-1
- **Key Group**: Diffie-Hellman Group 2
Click on the “+” next to Key Exchange (Phase 2), enter following:

- Encapsulation Protocol (ESP): Checked
- Encrypt Alg: Triple DES
- Hash Alg: SHA-1
- Encapsulation: Tunnel

**Step5: Configure IPSec gateway**

In this application note, the Group IKE ID will be used in the IPSec gateway. With a Group IKE ID configuration, the security administrator doesn’t need to create individual users for the dial-up VPN connection. It allows groups of users to share a common IKE identity when using certificates, as the certificate will provide the individual’s accountability and authentication.
The first step in configuring the Group IKE ID on a Juniper firewall is to define an IKE user.

WebUI:
Select Objects > Users > Local and then click New.
Enter following and click OK.
   User Name: test1
   IK User: Checked
   Number of Multiple Logins with Same ID: 5
   Use Distinguished Name for ID: Selected
   OU: SPG

CLI:
   set user "test1" uid 3
   set user "test1" ike-id asni-dn wildcard "CN=,OU=SPG,O=,L=,ST=,C=,Email=,DC=," share-limit 5
   set user "test1" type ike
   set user "test1" "enable"
Then define the User group to contain this IKE user.

**WebUI:**

Select Object > Users > Local Groups and click New.
Enter following:
- Group Name: test1-gp
- Select the IKE user from Available Member and click "<<", then click OK.

**CLI:**

```bash
set user-group "test1-gp" id 2
set user-group "test1-gp" user "test1"
```
Then you need to load the CA certificate and CRL onto the firewall.

**WebUI:**

Select Object > Certificates, select Cert and click Browse. 
Select the CA certificate from the file browser and then click Load 
Select CRL and click Browse. 
Select the CRL file from the file browser and then click Load.

**CLI:**

exec pki x509 tftp 1.1.1.1 cert-name ca.cer 
exec pki x509 tftp 1.1.1.1 crl-name ca.crl 
(This will copy the file from tftp server 1.1.1.1)
Next, we need to define P1 gateway.

WebUI:

Select VPNS > AutoKey Advanced > Gateway and click New.
Enter following:

- Gateway Name: g1
- Security Level: Custom (Selected)
- Dialup User Group: Selected
- Group: test1-gp
- Outgoing Interface: ethernet0/2

Then click Advanced.

Enter the following:

- Phase 1 Proposal: rsa-g2-3des-sha
- Mode (Initiator): Aggressive (Selected)
- Preferred Certificate:
  - Peer CA: (select the CA certificate loaded in previous step.)
  - Peer Type: X509-SIG

Then click Return, followed by OK.
CLI:

set ike gateway "g1" dialup "test1-gp" Aggr local-id "172.27.6.136" outgoing-interface "ethernet0/2" proposal "rsa-g2-3des-sha"
set ike gateway "g1" cert peer-ca 1
(1 is the number of CA certificate of remote peer)

Then define the VPN properties:

WebUI:

Select VPNS > AutoKey IKE and click New.
Enter following and click OK.
VPN name: v1
  Security Level: Standard
  Remote Gateway: Predefined (Selected), g1
Then click OK

CLI:

set vpn "v1" gateway "g1" no-replay tunnel idletime 0 sec-level standard
Next we will define the address object for the subnet 192.168.1.0/24. This object will be used in the policy to determine the proxy ID of the VPN.

WebUI:
Select Objects > Addresses > List, then choose Trust and click New. Enter following and click OK.

Address Name: lan
Address/Domain Name: IP address/Netmask (selected), 192.168.1.0/24

CLI:

set address "Trust" "lan" 192.168.1.0 255.255.255.0
Lastly, we need to define the policy for the dial-up VPN.

WebUI:

Select Policies and with following, then click New.
From: Untrust
To: Trust
Then enter following and click OK.
   Source Address: Address Book Entry (Selected), Dial-up VPN
   Destination Address: Address Book Entry (Selected), lan
   Action: Tunnel
   VPN: v1
Then click OK

CLI:

set policy id 1 from "Untrust" to "Trust" "Dial-Up VPN" "lan" "ANY" tunnel vpn "v1"
Verifying Configuration

Simple verification for the setup is to connect the dial-up VPN from Netscreen-Remote with the iKey in place.

Before connecting the VPN, start the Netscreen-Remote Log Viewer to observe the connection status.

Make sure the iKey is connected on the USB port. Right click the Netscreen-Remote icon in the system tray. Then select Connect and My Connections\New Connection. This will force Netscreen-Remote to make connection to IPSec gateway.

During the connection, the login prompt will appear, as Netscreen Remote needs to access the iKey to retrieve the certificate. Enter the passphrase for iKey.

When the connection is successful, similar output to the following will be reported in the Netscreen-Remote Log Viewer:

1-31: 21:34:28.626 My Connections\New Connection - Initiating IKE Phase 1 (IP ADDR=172.27.6.136)
1-31: 21:34:55.180 My Connections\New Connection - SENDING>>>> ISAKMP OAK AG (SA, KE, NON, ID, CERT_REQ 10x, VID 6x)
1-31: 21:35:11.273 My Connections\New Connection - RECEIVED<<< ISAKMP OAK AG (SA, VID 3x, KE, NON, ID, CERT, CERT_REQ, SIG)
1-31: 21:35:11.273 My Connections\New Connection - Peer supports Dead Peer Detection Version 1.0
1-31: 21:35:11.273 My Connections\New Connection - Dead Peer Detection enabled
1-31: 21:35:11.273 My Connections\New Connection - Received certificate *0185092D06000069 + rsa-key + SSG140. + SSG140's Juniper Networks SPG ID*,
1-31: 21:35:11.553 My Connections\New Connection - Using auto-selected user certificate *tester's Juniper Networks SPG ID*.
1-31: 21:35:11.553 My Connections\New Connection - Initiating IKE Phase 2 with Client IDs (message id: C686E22E)
1-31: 21:35:12.452 My Connections\New Connection - Initiator = IP ADDR=172.27.6.124, prot = 0 port = 0
1-31: 21:35:12.452 My Connections\New Connection - Responder = IP SUBNET/MASK=192.168.1.0/255.255.255.0, prot = 0 port = 0
In addition, a ping test can be used to confirm the connectivity.

C:\Documents and Settings\tleung>ping 192.168.1.1

Pinging 192.168.1.1 with 32 bytes of data:

Reply from 192.168.1.1: bytes=32 time=2ms TTL=64
Reply from 192.168.1.1: bytes=32 time=1ms TTL=64
Reply from 192.168.1.1: bytes=32 time=2ms TTL=64
Reply from 192.168.1.1: bytes=32 time=1ms TTL=64

Ping statistics for 192.168.1.1:
   Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
   Approximate round trip times in milli-seconds:
      Minimum = 1ms, Maximum = 2ms, Average = 1ms