Laborbericht - NVS - 5CHIF	
Name: Juri Schreib	**Datum:** 2016-10-18
HW-Beschreibung: Aufgabenstellung 5CHIF 18.10.2016	
Ziel: Erfüllung der Aufgabenstellung	

Configure and Verify a Site-to-Site IPsec VPN Using CLI

Part 1: Configure IPsec Parameters on R1

Step 1: Test Connectivity

Ping from PC-A to PC-C

```
Packet Tracer PC Command Line 1.0
C:\>ping 192.168.1.3

Pinging 192.168.1.3 with 32 bytes of data:

Reply from 192.168.1.3: bytes=32 time=5ms TTL=128
Reply from 192.168.1.3: bytes=32 time<1ms TTL=128
Reply from 192.168.1.3: bytes=32 time=2ms TTL=128
Reply from 192.168.1.3: bytes=32 time=5ms TTL=128

Ping statistics for 192.168.1.3:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 5ms, Average = 3ms
```

Step 2: Enable the Security Technology Package

Das Kommando zur aktivierung es technology-packages wird wie in der Angabe im Konfigurationsmodus ausgeführt license boot module c1900 technology-package

```
R1(config)#license boot module c1900 technology-package securityk9
PLEASE  READ THE  FOLLOWING TERMS  CAREFULLY. INSTALLING THE LICENSE OR
LICENSE  KEY  PROVIDED FOR  ANY CISCO  PRODUCT  FEATURE  OR  USING SUCH
PRODUCT  FEATURE  CONSTITUTES  YOUR  FULL ACCEPTANCE  OF  THE FOLLOWING
TERMS. YOU MUST NOT PROCEED FURTHER IF YOU ARE NOT WILLING TO  BE BOUND
BY ALL THE TERMS SET FORTH HEREIN.

Use of this product feature requires  an additional license from Cisco,
together with an additional  payment.  You may use this product feature
on an evaluation basis, without payment to Cisco, for 60 days. Your use
of the  product,  including  during the 60 day  evaluation  period,  is
subject to the Cisco end user license agreement
http://www.cisco.com/en/US/docs/general/warranty/English/EU1KEN_.html
If you use the product feature beyond the 60 day evaluation period, you
must submit the appropriate payment to Cisco for the license. After the
60 day  evaluation  period,  your  use of the  product  feature will be
governed  solely by the Cisco  end user license agreement (link above),
together  with any supplements  relating to such product  feature.  The
above  applies  even if the evaluation  license  is  not  automatically
terminated  and you do  not receive any notice of the expiration of the
evaluation  period.  It is your  responsibility  to  determine when the
evaluation  period is complete and you are required to make  payment to
Cisco for your use of the product feature beyond the evaluation period.

Your  acceptance  of  this agreement  for the software  features on one
product  shall be deemed  your  acceptance  with  respect  to all  such
software  on all Cisco  products  you purchase  which includes the same
software.  (The foregoing  notwithstanding, you must purchase a license
for each software  feature you use past the 60 days evaluation  period,
so  that  if you enable a software  feature on  1000  devices, you must
purchase 1000 licenses for use past  the 60 day evaluation period.)

Activation  of the  software command line interface will be evidence of
your acceptance of this agreement.


ACCEPT? [yes/no]: yes
% use 'write' command to make license boot config take effect on next boot

R1(config)#: %IOS_LICENSE_IMAGE_APPLICATION-6-LICENSE_LEVEL: Module name = C1900
Next reboot level = securityk9 and License = securityk9
```

securityk9

Die running-config wird gespeichert und der Router wird neugeladen

```
copy running-config startup-config
reload
```

```
R1#copy running-config startup-config
Destination filename [startup-config]?
Building configuration...
[OK]
R1#reload
Proceed with reload? [confirm]
```

Sicher gehen, dass das technology package aktiviert ist

```
show version
```

```
Technology Package License Information for Module:'c1900'

-----------------------------------------------------------------
Technology    Technology-package          Technology-package
              Current       Type          Next reboot
-----------------------------------------------------------------
ipbase        ipbasek9      Permanent     ipbasek9
security      securityk9    Evaluation    securityk9
data          disable       None          None
```

Step 3: Identify interesting traffic on R1

Es wir eine Access list configuriert, welche später genutzt wird, damit IPSec VPN weiß, welcher Traffic verschlüsselt werden soll und welcher nicht

```
access-list 110 permit ip 192.168.1.0 0.0.0.255 192.168.3.0 0.0.0.255
```

Step 4: Configure the IKE Phase 1 ISAKMP policy on R1.

Die Befehle werden wie in der Angabe ausgeführt. Ein neuer shared crypto key wird konfiguriert.

```
crypto isakmp policy 10
encryption aes 256
authentication pre-share
group 5
exit
crypto isakmp key vpnpa55 address 10.2.2.2
```

Step 5: Configure the IKE Phase 2 IPsec policy on R1.

Eine VPN transform-set und die crypto map werden erstellt.

```
crypto ipsec transform-set VPN-SET esp-aes esp-sha-hmac
crypto map VPN-MAP 10 ipsec-isakmp
description VPN connection to R3
set peer 10.2.2.2
set transform-set VPN-SET
match address 110
```

Die eingegebenen Kommandos in Schritt 4 und 5

```
R1(config)#crypto isakmp policy 10
R1(config-isakmp)#encryption aes 256
R1(config-isakmp)#authentication pre-share
R1(config-isakmp)#group 5
R1(config-isakmp)#exit
R1(config)#crypto isakmp key vpnpa55 address 10.2.2.2
R1(config)#crypto ipsec transform-set VPN-SET esp-aes esp-sha-hmac
R1(config)#crypto map VPN-MAP 10 ipsec-isakmp
% NOTE: This new crypto map will remain disabled until a peer
        and a valid access list have been configured.
R1(config-crypto-map)#description VPN connection to R3
R1(config-crypto-map)#set peer 10.2.2.2
R1(config-crypto-map)#set transform-set VPN-SET
R1(config-crypto-map)#match address 110
R1(config-crypto-map)#
```

Step 6: Configure the crypto map on the outgoing interface

```
interface s0/0/0
crypto map VPN-MAP
```

```
R1(config-crypto-map)#interface s0/0/0
R1(config-if)#crypto map VPN-MAP
*Jan  3 07:16:26.785: %CRYPTO-6-ISAKMP_ON_OFF: ISAKMP is ON
R1(config-if)#
```

Part 2: Configure IPsec Parameters on

R3

Die selbe Konfiguration wird nun am Router R3 vorgenommen. Es werden nurmehr

Step 1: Enable the Security Technology Package

Wie beim ersten Router wird das Technology Package aktiviert

Config Mode license boot module c1900 technology-package securityk9

Enable Mode

```
copy running-config startup-config
reload
```

Sicher gehen, dass das technology package aktiviert ist

```
show version
```

```
Technology Package License Information for Module:'c1900'

-----------------------------------------------------------------
Technology    Technology-package          Technology-package
              Current       Type          Next reboot
-----------------------------------------------------------------
ipbase        ipbasek9      Permanent     ipbasek9
security      securityk9    Evaluation    securityk9
data          disable       None          None
```

Step 2: Configure router R3 to support a site-to-site VPN with R1.

```
access-list 110 permit ip 192.168.3.0 0.0.0.255 192.168.1.0 0.0.0.255
```

Step 3: Configure the IKE Phase 1 ISAKMP properties on R3.

Die Befehle werden wie in der Angabe ausgeführt. Ein neuer shared crypto key wird konfiguriert.

```
crypto isakmp policy 10
encryption aes 256
authentication pre-share
group 5
exit
crypto isakmp key vpnpa55 address 10.1.1.2
```

Step 4: Configure the IKE Phase 2 IPsec policy on R3.

Eine VPN transform-set und die crypto map werden erstellt.

```
crypto ipsec transform-set VPN-SET esp-aes esp-sha-hmac
```

```
crypto map VPN-MAP 10 ipsec-isakmp
description VPN connection to R3
set peer 10.1.1.2
set transform-set VPN-SET
match address 110
exit
```

Die eingegebenen Kommandos in den Schritten 2 bis 4

```
R3(config)#access-list 110 permit ip 192.168.3.0 0.0.0.255 192.168.1.0 0.0.0.255
R3(config)#crypto isakmp policy 10
R3(config-isakmp)#encryption aes 256
R3(config-isakmp)#authentication pre-share
R3(config-isakmp)#group 5
R3(config-isakmp)#exit
R3(config)#crypto isakmp key vpnpa55 address 10.1.1.2
R3(config)#crypto ipsec transform-set VPN-SET esp-aes esp-sha-hmac
R3(config)#crypto map VPN-MAP 10 ipsec-isakmp
% NOTE: This new crypto map will remain disabled until a peer
        and a valid access list have been configured.
R3(config-crypto-map)#description VPN connection to R3
R3(config-crypto-map)#set peer 10.1.1.2
R3(config-crypto-map)#set transform-set VPN-SET
R3(config-crypto-map)#match address 110
R3(config-crypto-map)#exit
R3(config)#
```

Step 5: Configure the crypto map on the outgoing interface

```
interface s0/0/1
crypto map VPN-MAP
```

```
R3(config)#interface s0/0/1
R3(config-if)#crypto map VPN-MAP
*Jan  3 07:16:26.785: %CRYPTO-6-ISAKMP_ON_OFF: ISAKMP is ON
R3(config-if)#
```

Part 3: Verify the IPsec VPN

Step 1: Verify the tunnel prior to interesting traffic.

```
show crypto ipsec sa
```

```
% Ambiguous command:  "s"
R1#show crypto ipsec sa

interface: Serial0/0/0
    Crypto map tag: VPN-MAP, local addr 10.1.1.2

   protected vrf: (none)
   local  ident (addr/mask/prot/port):
(192.168.1.0/255.255.255.0/0/0)
   remote  ident (addr/mask/prot/port):
(192.168.3.0/255.255.255.0/0/0)
   current_peer 10.2.2.2 port 500
    PERMIT, flags={origin_is_acl,}
   #pkts encaps: 0, #pkts encrypt: 0, #pkts digest: 0
   #pkts decaps: 0, #pkts decrypt: 0, #pkts verify: 0
   #pkts compressed: 0, #pkts decompressed: 0
   #pkts not compressed: 0, #pkts compr. failed: 0
   #pkts not decompressed: 0, #pkts decompress failed: 0
   #send errors 0, #recv errors 0

     local crypto endpt.: 10.1.1.2, remote crypto endpt.:10.2.2.2
     path mtu 1500, ip mtu 1500, ip mtu idb Serial0/0/0
     current outbound spi: 0x0(0)

     inbound esp sas:

     inbound ah sas:

     inbound pcp sas:

     outbound esp sas:

     outbound ah sas:

     outbound pcp sas:
```

Es wurden noch keine Pakete durch den Tunnel verschickt

Step 2: Create interesting traffic.

```
Pinging 192.168.3.3 with 32 bytes of data:

Request timed out.
Request timed out.
Reply from 192.168.3.3: bytes=32 time=2ms TTL=126
Reply from 192.168.3.3: bytes=32 time=10ms TTL=126

Ping statistics for 192.168.3.3:
    Packets: Sent = 4, Received = 2, Lost = 2 (50% loss),
Approximate round trip times in milli-seconds:
    Minimum = 2ms, Maximum = 10ms, Average = 6ms
```

Der Computer mit der IP Adresse 192.168.3.3 wurde erfolgreich gepingt

Step 3: Verify the tunnel after interesting traffic.

```
show crypto ipsec sa
```

```
R1#show crypto ipsec sa

interface: Serial0/0/0
    Crypto map tag: VPN-MAP, local addr 10.1.1.2

   protected vrf: (none)
   local  ident (addr/mask/prot/port):
(192.168.1.0/255.255.255.0/0/0)
   remote  ident (addr/mask/prot/port):
(192.168.3.0/255.255.255.0/0/0)
   current_peer 10.2.2.2 port 500
    PERMIT, flags={origin_is_acl,}
   #pkts encaps: 3, #pkts encrypt: 3, #pkts digest: 0
   #pkts decaps: 2, #pkts decrypt: 2, #pkts verify: 0
   #pkts compressed: 0, #pkts decompressed: 0
   #pkts not compressed: 0, #pkts compr. failed: 0
   #pkts not decompressed: 0, #pkts decompress failed: 0
   #send errors 1, #recv errors 0

     local crypto endpt.: 10.1.1.2, remote crypto endpt.:10.2.2.2
     path mtu 1500, ip mtu 1500, ip mtu idb Serial0/0/0
     current outbound spi: 0xAD88AF3A(2911416122)

     inbound esp sas:
      spi: 0x7797A416(2006426646)
 --More--
```

Es wurden verschlüsselte Pakete geloggt.

Step 4: Create uninteresting traffic.

```
C:\>ping 192.168.2.3

Pinging 192.168.2.3 with 32 bytes of data:

Request timed out.
Reply from 192.168.2.3: bytes=32 time=1ms TTL=126
Reply from 192.168.2.3: bytes=32 time=1ms TTL=126
Reply from 192.168.2.3: bytes=32 time=1ms TTL=126

Ping statistics for 192.168.2.3:
    Packets: Sent = 4, Received = 3, Lost = 1 (25% loss),
Approximate round trip times in milli-seconds:
    Minimum = 1ms, Maximum = 1ms, Average = 1ms
```

Der Computer mit der IP Adresse 192.168.2.3 wurde erfolgreich gepingt

Step 5: Verify the tunnel.

```
R1#show crypto ipsec sa

interface: Serial0/0/0
    Crypto map tag: VPN-MAP, local addr 10.1.1.2

   protected vrf: (none)
   local  ident (addr/mask/prot/port):
(192.168.1.0/255.255.255.0/0/0)
   remote  ident (addr/mask/prot/port):
(192.168.3.0/255.255.255.0/0/0)
   current_peer 10.2.2.2 port 500
    PERMIT, flags={origin_is_acl,}
   #pkts encaps: 3, #pkts encrypt: 3, #pkts digest: 0
   #pkts decaps: 2, #pkts decrypt: 2, #pkts verify: 0
   #pkts compressed: 0, #pkts decompressed: 0
   #pkts not compressed: 0, #pkts compr. failed: 0
   #pkts not decompressed: 0, #pkts decompress failed: 0
   #send errors 1, #recv errors 0

     local crypto endpt.: 10.1.1.2, remote crypto endpt.:10.2.2.2
     path mtu 1500, ip mtu 1500, ip mtu idb Serial0/0/0
     current outbound spi: 0xAD88AF3A(2911416122)

     inbound esp sas:
      spi: 0x7797A416(2006426646)
```

Die anzahl der verschlüsselten Pakete hat sich nicht erhöht
http://nvs.schreib.at/NVS/5CHIF_20161018_Schreib/