**Router(config)#: license boot module c1900 technology-package securityk9**

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

Router(config)#: %IOS\_LICENSE\_IMAGE\_APPLICATION-6-LICENSE\_LEVEL: Module name = C1900 Next reboot level = securityk9 and License = securityk9

Router(config)#do write

Building configuration...

[OK]

Router(config)#

Router(config)#do reload

Proceed with reload? [confirm]

System Bootstrap, Version 15.1(4)M4, RELEASE SOFTWARE (fc1)

Technical Support: http://www.cisco.com/techsupport

Copyright (c) 2010 by cisco Systems, Inc.

Total memory size = 512 MB - On-board = 512 MB, DIMM0 = 0 MB

CISCO1941/K9 platform with 524288 Kbytes of main memory

Main memory is configured to 64/-1(On-board/DIMM0) bit mode with ECC disabled

Readonly ROMMON initialized

program load complete, entry point: 0x80803000, size: 0x1b340

program load complete, entry point: 0x80803000, size: 0x1b340

IOS Image Load Test

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Digitally Signed Release Software

program load complete, entry point: 0x81000000, size: 0x2bb1c58

Self decompressing the image :

########################################################################## [OK]

Smart Init is enabled

smart init is sizing iomem

TYPE MEMORY\_REQ

HWIC Slot 0 0x00200000 Onboard devices &

buffer pools 0x01E8F000

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

TOTAL: 0x0268F000

Rounded IOMEM up to: 40Mb.

Using 6 percent iomem. [40Mb/512Mb]

Restricted Rights Legend

Use, duplication, or disclosure by the Government is

subject to restrictions as set forth in subparagraph

(c) of the Commercial Computer Software - Restricted

Rights clause at FAR sec. 52.227-19 and subparagraph

(c) (1) (ii) of the Rights in Technical Data and Computer

Software clause at DFARS sec. 252.227-7013.

cisco Systems, Inc.

170 West Tasman Drive

San Jose, California 95134-1706

Cisco IOS Software, C1900 Software (C1900-UNIVERSALK9-M), Version 15.1(4)M4, RELEASE SOFTWARE (fc2)

Technical Support: http://www.cisco.com/techsupport

Copyright (c) 1986-2012 by Cisco Systems, Inc.

Compiled Thurs 5-Jan-12 15:41 by pt\_team

Image text-base: 0x2100F918, data-base: 0x24729040

This product contains cryptographic features and is subject to United

States and local country laws governing import, export, transfer and

use. Delivery of Cisco cryptographic products does not imply

third-party authority to import, export, distribute or use encryption.

Importers, exporters, distributors and users are responsible for

compliance with U.S. and local country laws. By using this product you

agree to comply with applicable laws and regulations. If you are unable

to comply with U.S. and local laws, return this product immediately.

A summary of U.S. laws governing Cisco cryptographic products may be found at:

http://www.cisco.com/wwl/export/crypto/tool/stqrg.html

If you require further assistance please contact us by sending email to

export@cisco.com.

Cisco CISCO1941/K9 (revision 1.0) with 491520K/32768K bytes of memory.

Processor board ID FTX152400KS

2 Gigabit Ethernet interfaces

2 Low-speed serial(sync/async) network interface(s)

DRAM configuration is 64 bits wide with parity disabled.

255K bytes of non-volatile configuration memory.

249856K bytes of ATA System CompactFlash 0 (Read/Write)

Press RETURN to get started!

Router>en

Router#conf t

Enter configuration commands, one per line. End with CNTL/Z.

Router(config)#access-list 110 permit ip 172.16.2.113 0.0.255.255 172.18.2.113 0.0.255.255

Router(config)#crypto isakmp policy 10

Router(config-isakmp)#encryption aes 256

Router(config-isakmp)#authentication pre-share

Router(config-isakmp)#group 5

Router(config-isakmp)#exit

Router(config)#crypto isakmp key ?

WORD The UNENCRYPTED (cleartext) user password

Router(config)#crypto isakmp key VPN1 ?

address define shared key with IP address

Router(config)#crypto isakmp key VPN1 address 10.2.2.2

Router(config)#crypto ipsec transform-set VPN-SET esp-aes esp-sha-hmac

Router(config)#crypto map VPN-MAP ?

<1-65535> Sequence to insert into crypto map entry

client Specify client configuration settings

isakmp Specify isakmp configuration settings

Router(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.

Router(config-crypto-map)#description VPN connectie naar Windows

Router(config-crypto-map)#set peer 10.2.2.2

Router(config-crypto-map)#set transform-set VPN-SET

Router(config-crypto-map)#match address 110

Router(config-crypto-map)#exit

Router(config)#interface s0/0/1

Router(config-if)#crypto map VPN-MAP

\*Jan 3 07:16:26.785: %CRYPTO-6-ISAKMP\_ON\_OFF: ISAKMP is ON

Router(config-if)#exit

Router(config)#

Router#conf t

Enter configuration commands, one per line. End with CNTL/Z.

Router(config)#access-list 110 permit ip 172.18.2.113 0.0.255.255 172.16.2.113 0.0.255.255

Router(config)#crypto isakmp policy 10

Router(config-isakmp)#encryption aes 256

Router(config-isakmp)#authentication pre-share

Router(config-isakmp)#group 5

Router(config-isakmp)#exit

Router(config)#crypto isakmp key VPN1 address 10.1.1.2

Router(config)#crypto ipsec transform-set VPN-SET esp-aes esp-sha-hmac

Router(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.

Router(config-crypto-map)#description VPN connectie naar Linux

Router(config-crypto-map)#set peer 10.1.1.2

Router(config-crypto-map)#set transform-set VPN-SET

Router(config-crypto-map)#match address 110

Router(config-crypto-map)#exit

Router(config)#int s0/0/1

Router(config-if)#crypto map VPN-MAP

\*Jan 3 07:16:26.785: %CRYPTO-6-ISAKMP\_ON\_OFF: ISAKMP is ON

Router(config-if)#

Router#

%SYS-5-CONFIG\_I: Configured from console by console