# R2(config)#do sh start

Using 3142 out of 131072 bytes

!

! Last configuration change at 19:44:00 AWST Tue Apr 21 2015

!

version 15.4

service timestamps debug datetime msec

service timestamps log datetime msec

no service password-encryption

!

hostname R2

!

boot-start-marker

boot-end-marker

!

aqm-register-fnf

!

logging discriminator EXCESS severity drops 6 msg-body drops EXCESSCOLL

logging buffered 50000

logging console discriminator EXCESS

!

no aaa new-model

clock timezone AWST 8 0

mmi polling-interval 60

no mmi auto-configure

no mmi pvc

mmi snmp-timeout 180

no ip icmp rate-limit unreachable

!

!

!

!

!

!

!

!

!

!

!

!

no ip domain lookup

ip domain name candy.com

ip cef

no ipv6 cef

ipv6 multicast rpf use-bgp

!

multilink bundle-name authenticated

!

!

!

!

!

!

!

!

username cisco privilege 0 password 0 cisco

username admin privilege 15 password 0 admin

!

redundancy

!

no cdp log mismatch duplex

!

ip tcp synwait-time 5

!

!

!

!

!

!

!

!

!

!

!

!

!

interface Ethernet0/0

ip address 192.168.2.2 255.255.255.0

ip nat inside

ip virtual-reassembly in

!

interface Ethernet0/1

ip address 192.168.21.2 255.255.255.0

ip nat inside

ip virtual-reassembly in

!

interface Ethernet0/2

no ip address

shutdown

!

interface Ethernet0/3

no ip address

shutdown

!

interface Ethernet1/0

no ip address

shutdown

!

interface Ethernet1/1

no ip address

shutdown

!

interface Ethernet1/2

no ip address

shutdown

!

interface Ethernet1/3

no ip address

shutdown

!

interface Serial2/0

ip address 22.22.22.2 255.255.255.0

ip nat outside

ip virtual-reassembly in

serial restart-delay 0

!

interface Serial2/1

no ip address

shutdown

serial restart-delay 0

!

interface Serial2/2

no ip address

shutdown

serial restart-delay 0

!

interface Serial2/3

no ip address

shutdown

serial restart-delay 0

!

interface Serial3/0

no ip address

shutdown

serial restart-delay 0

!

interface Serial3/1

no ip address

shutdown

serial restart-delay 0

!

interface Serial3/2

no ip address

shutdown

serial restart-delay 0

!

interface Serial3/3

no ip address

shutdown

serial restart-delay 0

!

ip forward-protocol nd

!

!

no ip http server

no ip http secure-server

ip nat pool NAT\_POOL 22.22.22.192 22.22.22.253 prefix-length 24

ip nat inside source route-map NAT\_PROCESS pool NAT\_POOL overload

ip nat inside source static 192.168.21.23 22.22.22.254

ip route 0.0.0.0 0.0.0.0 Serial2/0

!

ip access-list extended R2\_NAT\_ACL

deny ip 192.168.0.0 0.0.255.255 192.168.0.0 0.0.255.255

permit ip 192.168.0.0 0.0.255.255 any

!

!

route-map NAT\_PROCESS permit 10

match ip address R2\_NAT\_ACL

!

!

!

control-plane

!

!

!

!

!

!

!

alias exec srb sh run | beg

alias exec srs sh run | sec

alias exec sri sh run | incl

alias exec siib sh ip int brief

alias exec siibu sh ip int brief | include up

alias exec srint sh run interface

alias exec wrx copy run unix:

alias exec ssha ssh -l admin -c 3des

alias exec sshu ssh -l admin -c 3des

alias exec diff sh archive config diff unix:start.cfg unix:running-config

banner motd ^CC

\*\*\* You are connecting to R2 \*\*\*

^C

!

line con 0

exec-timeout 0 0

logging synchronous

line aux 0

line vty 0 4

exec-timeout 0 5

privilege level 15

login local

transport input telnet ssh

!

!

end

# R2#sh run

Building configuration...

Current configuration : 4400 bytes

!

! Last configuration change at 20:16:04 AWST Wed Apr 22 2015

!

version 15.4

service timestamps debug datetime msec

service timestamps log datetime msec

no service password-encryption

!

hostname R2

!

boot-start-marker

boot-end-marker

!

aqm-register-fnf

!

logging discriminator EXCESS severity drops 6 msg-body drops EXCESSCOLL

logging buffered 50000

logging console discriminator EXCESS

!

no aaa new-model

clock timezone AWST 8 0

mmi polling-interval 60

no mmi auto-configure

no mmi pvc

mmi snmp-timeout 180

no ip icmp rate-limit unreachable

!

!

!

!

!

!

!

!

!

!

!

!

no ip domain lookup

ip domain name candy.com

ip inspect audit-trail

ip inspect name INSIDE\_TO\_OUT icmp timeout 60

ip inspect name INSIDE\_TO\_OUT telnet timeout 60

ip inspect name INSIDE\_TO\_OUT tcp timeout 60

ip inspect name INSIDE\_TO\_OUT udp timeout 60

ip inspect name INTO\_DMZ icmp timeout 60

ip inspect name INTO\_DMZ ssh timeout 60

ip cef

no ipv6 cef

ipv6 multicast rpf use-bgp

!

multilink bundle-name authenticated

!

!

!

!

!

!

!

!

username cisco privilege 0 password 0 cisco

username admin privilege 15 password 0 admin

!

redundancy

!

no cdp log mismatch duplex

!

ip tcp synwait-time 5

!

!

!

!

!

!

!

!

!

!

!

!

!

interface Tunnel1

no ip address

!

interface Ethernet0/0

ip address 192.168.2.2 255.255.255.0

ip access-group 101 in

ip nat inside

ip inspect INSIDE\_TO\_OUT in

ip virtual-reassembly in

!

interface Ethernet0/1

ip address 192.168.21.2 255.255.255.0

ip access-group 103 in

ip nat inside

ip inspect INTO\_DMZ out

ip virtual-reassembly in

!

interface Ethernet0/2

no ip address

shutdown

!

interface Ethernet0/3

no ip address

shutdown

!

interface Ethernet1/0

no ip address

shutdown

!

interface Ethernet1/1

no ip address

shutdown

!

interface Ethernet1/2

no ip address

shutdown

!

interface Ethernet1/3

no ip address

shutdown

!

interface Serial2/0

ip address 22.22.22.2 255.255.255.0

ip access-group 102 in

ip nat outside

ip virtual-reassembly in

serial restart-delay 0

!

interface Serial2/1

no ip address

shutdown

serial restart-delay 0

!

interface Serial2/2

no ip address

shutdown

serial restart-delay 0

!

interface Serial2/3

no ip address

shutdown

serial restart-delay 0

!

interface Serial3/0

no ip address

shutdown

serial restart-delay 0

!

interface Serial3/1

no ip address

shutdown

serial restart-delay 0

!

interface Serial3/2

no ip address

shutdown

serial restart-delay 0

!

interface Serial3/3

no ip address

shutdown

serial restart-delay 0

!

ip forward-protocol nd

!

!

no ip http server

no ip http secure-server

ip nat pool NAT\_POOL 22.22.22.192 22.22.22.253 prefix-length 24

ip nat inside source route-map NAT\_PROCESS pool NAT\_POOL overload

ip nat inside source static 192.168.21.23 22.22.22.254

ip route 0.0.0.0 0.0.0.0 Serial2/0

!

ip access-list extended R2\_NAT\_ACL

deny ip 192.168.0.0 0.0.255.255 192.168.0.0 0.0.255.255

permit ip 192.168.0.0 0.0.255.255 any

!

!

route-map NAT\_PROCESS permit 10

match ip address R2\_NAT\_ACL

!

!

access-list 101 permit icmp 192.168.2.0 0.0.0.15 host 192.168.114.114

access-list 101 permit tcp 192.168.2.0 0.0.0.15 host 192.168.114.114 eq telnet

access-list 101 deny ip 192.168.2.0 0.0.0.15 192.168.0.0 0.0.255.255 log

access-list 101 deny ip 192.168.2.16 0.0.0.3 192.168.0.0 0.0.255.255 log

access-list 101 deny ip host 192.168.2.20 192.168.0.0 0.0.255.255 log

access-list 101 permit ip 192.168.2.0 0.0.0.15 any

access-list 101 permit ip 192.168.2.16 0.0.0.3 any

access-list 101 permit ip host 192.168.2.20 any

access-list 101 deny ip any any log

access-list 101 remark RO req12

access-list 102 permit icmp any host 22.22.22.254 echo

access-list 102 permit tcp any host 22.22.22.254 eq 22

access-list 102 deny ip any any log

access-list 103 deny ip any any log

access-list 103 remark RO req4

!

control-plane

!

!

!

!

!

!

!

alias exec srb sh run | beg

alias exec srs sh run | sec

alias exec sri sh run | incl

alias exec siib sh ip int brief

alias exec siibu sh ip int brief | include up

alias exec srint sh run interface

alias exec wrx copy run unix:

alias exec ssha ssh -l admin -c 3des

alias exec sshu ssh -l admin -c 3des

alias exec diff sh archive config diff unix:start.cfg unix:running-config

banner motd ^CCC

\*\*\* You are connecting to R2 \*\*\*

^C

!

line con 0

exec-timeout 0 0

logging synchronous

line aux 0

line vty 0 4

exec-timeout 0 5

privilege level 15

login local

transport input telnet ssh

!

!

end

# R2#sh run

Building configuration...

Current configuration : 4566 bytes

!

! Last configuration change at 10:30:50 AWST Fri Apr 24 2015

!

version 15.4

service timestamps debug datetime msec

service timestamps log datetime msec

no service password-encryption

!

hostname R2

!

boot-start-marker

boot-end-marker

!

aqm-register-fnf

!

logging discriminator EXCESS severity drops 6 msg-body drops EXCESSCOLL

logging buffered 50000

logging console discriminator EXCESS

!

no aaa new-model

clock timezone AWST 8 0

mmi polling-interval 60

no mmi auto-configure

no mmi pvc

mmi snmp-timeout 180

no ip icmp rate-limit unreachable

!

!

!

!

!

!

!

!

!

!

!

!

no ip domain lookup

ip domain name candy.com

ip inspect audit-trail

ip inspect name INSIDE\_TO\_OUT icmp timeout 60

ip inspect name INSIDE\_TO\_OUT telnet timeout 60

ip inspect name INSIDE\_TO\_OUT tcp timeout 60

ip inspect name INSIDE\_TO\_OUT udp timeout 60

ip inspect name INTO\_DMZ icmp timeout 60

ip inspect name INTO\_DMZ ssh timeout 60

ip inspect name VPN\_TO\_INSIDE icmp timeout 60

ip inspect name VPN\_TO\_INSIDE tcp timeout 60

ip inspect name VPN\_TO\_INSIDE udp timeout 60

ip cef

no ipv6 cef

ipv6 multicast rpf use-bgp

!

multilink bundle-name authenticated

!

!

!

!

!

!

!

!

username cisco privilege 0 password 0 cisco

username admin privilege 15 password 0 admin

!

redundancy

!

no cdp log mismatch duplex

!

ip tcp synwait-time 5

!

!

!

!

!

!

!

!

!

!

!

!

!

interface Tunnel1

no ip address

!

interface Ethernet0/0

ip address 192.168.2.2 255.255.255.0

ip access-group 101 in

ip nat inside

ip inspect INSIDE\_TO\_OUT in

ip inspect VPN\_TO\_INSIDE out

ip virtual-reassembly in

!

interface Ethernet0/1

ip address 192.168.21.2 255.255.255.0

ip access-group 103 in

ip nat inside

ip inspect INTO\_DMZ out

ip virtual-reassembly in

!

interface Ethernet0/2

no ip address

shutdown

!

interface Ethernet0/3

no ip address

shutdown

!

interface Ethernet1/0

no ip address

shutdown

!

interface Ethernet1/1

no ip address

shutdown

!

interface Ethernet1/2

no ip address

shutdown

!

interface Ethernet1/3

no ip address

shutdown

!

interface Serial2/0

ip address 22.22.22.2 255.255.255.0

ip access-group 102 in

ip nat outside

ip virtual-reassembly in

serial restart-delay 0

!

interface Serial2/1

no ip address

shutdown

serial restart-delay 0

!

interface Serial2/2

no ip address

shutdown

serial restart-delay 0

!

interface Serial2/3

no ip address

shutdown

serial restart-delay 0

!

interface Serial3/0

no ip address

shutdown

serial restart-delay 0

!

interface Serial3/1

no ip address

shutdown

serial restart-delay 0

!

interface Serial3/2

no ip address

shutdown

serial restart-delay 0

!

interface Serial3/3

no ip address

shutdown

serial restart-delay 0

!

ip forward-protocol nd

!

!

no ip http server

no ip http secure-server

ip nat pool NAT\_POOL 22.22.22.192 22.22.22.253 prefix-length 24

ip nat inside source route-map NAT\_PROCESS pool NAT\_POOL overload

ip nat inside source static 192.168.21.23 22.22.22.254

ip route 0.0.0.0 0.0.0.0 Serial2/0

!

ip access-list extended R2\_NAT\_ACL

deny ip 192.168.0.0 0.0.255.255 192.168.0.0 0.0.255.255

permit ip 192.168.0.0 0.0.255.255 any

!

!

route-map NAT\_PROCESS permit 10

match ip address R2\_NAT\_ACL

!

!

access-list 101 permit icmp 192.168.2.0 0.0.0.15 host 192.168.114.114

access-list 101 permit tcp 192.168.2.0 0.0.0.15 host 192.168.114.114 eq telnet

access-list 101 deny ip 192.168.2.0 0.0.0.15 192.168.0.0 0.0.255.255 log

access-list 101 deny ip 192.168.2.16 0.0.0.3 192.168.0.0 0.0.255.255 log

access-list 101 deny ip host 192.168.2.20 192.168.0.0 0.0.255.255 log

access-list 101 permit ip 192.168.2.0 0.0.0.15 any

access-list 101 permit ip 192.168.2.16 0.0.0.3 any

access-list 101 permit ip host 192.168.2.20 any

access-list 101 deny ip any any log

access-list 101 remark RO req12

access-list 102 permit icmp any host 22.22.22.254 echo

access-list 102 permit tcp any host 22.22.22.254 eq 22

access-list 102 deny ip any any log

access-list 103 deny ip any any log

access-list 103 remark RO req4

!

control-plane

!

!

!

!

!

!

!

alias exec srb sh run | beg

alias exec srs sh run | sec

alias exec sri sh run | incl

alias exec siib sh ip int brief

alias exec siibu sh ip int brief | include up

alias exec srint sh run interface

alias exec wrx copy run unix:

alias exec ssha ssh -l admin -c 3des

alias exec sshu ssh -l admin -c 3des

alias exec diff sh archive config diff unix:start.cfg unix:running-config

banner motd ^CCC

\*\*\* You are connecting to R2 \*\*\*

^C

!

line con 0

exec-timeout 0 0

logging synchronous

line aux 0

line vty 0 4

exec-timeout 0 5

privilege level 15

login local

transport input telnet ssh

!

!

end

# R2(config-if)#do sh run

Building configuration...

Current configuration : 5719 bytes

!

! Last configuration change at 10:30:50 AWST Fri Apr 24 2015

!

version 15.4

service timestamps debug datetime msec

service timestamps log datetime msec

no service password-encryption

!

hostname R2

!

boot-start-marker

boot-end-marker

!

aqm-register-fnf

!

logging discriminator EXCESS severity drops 6 msg-body drops EXCESSCOLL

logging buffered 50000

logging console discriminator EXCESS

!

no aaa new-model

clock timezone AWST 8 0

mmi polling-interval 60

no mmi auto-configure

no mmi pvc

mmi snmp-timeout 180

no ip icmp rate-limit unreachable

!

!

!

!

!

!

!

!

!

!

!

!

no ip domain lookup

ip domain name candy.com

ip inspect audit-trail

ip inspect name INSIDE\_TO\_OUT icmp timeout 60

ip inspect name INSIDE\_TO\_OUT telnet timeout 60

ip inspect name INSIDE\_TO\_OUT tcp timeout 60

ip inspect name INSIDE\_TO\_OUT udp timeout 60

ip inspect name INTO\_DMZ icmp timeout 60

ip inspect name INTO\_DMZ ssh timeout 60

ip inspect name VPN\_TO\_INSIDE icmp timeout 60

ip inspect name VPN\_TO\_INSIDE tcp timeout 60

ip inspect name VPN\_TO\_INSIDE udp timeout 60

ip cef

no ipv6 cef

ipv6 multicast rpf use-bgp

!

multilink bundle-name authenticated

!

!

!

!

!

!

!

!

username cisco privilege 0 password 0 cisco

username admin privilege 15 password 0 admin

!

redundancy

!

no cdp log mismatch duplex

!

ip tcp synwait-time 5

!

!

!

!

!

crypto isakmp policy 5

authentication pre-share

lifetime 1800

crypto isakmp key cisco12345 address 0.0.0.0

!

crypto ipsec security-association lifetime seconds 1800

!

crypto ipsec transform-set DMVPN\_TRANSFORM ah-md5-hmac esp-des

mode transport

!

crypto ipsec profile DMVPN\_PROFILE

set transform-set DMVPN\_TRANSFORM

!

!

!

!

!

!

!

interface Tunnel1

description \*\*\* Spoke R2 \*\*\*

bandwidth 192

ip address 10.0.1.2 255.255.255.0

no ip redirects

ip mtu 1400

ip nhrp authentication cisco123

ip nhrp map multicast 11.11.11.1

ip nhrp map 10.0.1.1 11.11.11.1

ip nhrp network-id 100001

ip nhrp holdtime 300

ip nhrp nhs 11.11.11.1

ip nhrp nhs 10.0.1.1

ip nhrp registration no-unique

ip nhrp registration timeout 120

ip nhrp shortcut

ip tcp adjust-mss 1360

tunnel source Serial2/0

tunnel mode gre multipoint

tunnel key 100001

tunnel protection ipsec profile DMVPN\_PROFILE

!

interface Ethernet0/0

ip address 192.168.2.2 255.255.255.0

ip access-group 101 in

ip nat inside

ip inspect INSIDE\_TO\_OUT in

ip inspect VPN\_TO\_INSIDE out

ip virtual-reassembly in

!

interface Ethernet0/1

ip address 192.168.21.2 255.255.255.0

ip access-group 103 in

ip nat inside

ip inspect INTO\_DMZ out

ip virtual-reassembly in

!

interface Ethernet0/2

no ip address

shutdown

!

interface Ethernet0/3

no ip address

shutdown

!

interface Ethernet1/0

no ip address

shutdown

!

interface Ethernet1/1

no ip address

shutdown

!

interface Ethernet1/2

no ip address

shutdown

!

interface Ethernet1/3

no ip address

shutdown

!

interface Serial2/0

ip address 22.22.22.2 255.255.255.0

ip access-group 102 in

ip nat outside

ip virtual-reassembly in

serial restart-delay 0

!

interface Serial2/1

no ip address

shutdown

serial restart-delay 0

!

interface Serial2/2

no ip address

shutdown

serial restart-delay 0

!

interface Serial2/3

no ip address

shutdown

serial restart-delay 0

!

interface Serial3/0

no ip address

shutdown

serial restart-delay 0

!

interface Serial3/1

no ip address

shutdown

serial restart-delay 0

!

interface Serial3/2

no ip address

shutdown

serial restart-delay 0

!

interface Serial3/3

no ip address

shutdown

serial restart-delay 0

!

!

router eigrp 1

network 10.0.1.0 0.0.0.255

network 192.168.2.0

passive-interface Ethernet0/1

eigrp stub connected

!

ip forward-protocol nd

!

!

no ip http server

no ip http secure-server

ip nat pool NAT\_POOL 22.22.22.192 22.22.22.253 prefix-length 24

ip nat inside source route-map NAT\_PROCESS pool NAT\_POOL overload

ip nat inside source static 192.168.21.23 22.22.22.254

ip route 0.0.0.0 0.0.0.0 Serial2/0

!

ip access-list extended R2\_NAT\_ACL

deny ip 192.168.0.0 0.0.255.255 192.168.0.0 0.0.255.255

permit ip 192.168.0.0 0.0.255.255 any

!

!

route-map NAT\_PROCESS permit 10

match ip address R2\_NAT\_ACL

!

!

access-list 101 permit icmp 192.168.2.0 0.0.0.15 host 192.168.114.114

access-list 101 permit tcp 192.168.2.0 0.0.0.15 host 192.168.114.114 eq telnet

access-list 101 deny ip 192.168.2.0 0.0.0.15 192.168.0.0 0.0.255.255 log

access-list 101 deny ip 192.168.2.16 0.0.0.3 192.168.0.0 0.0.255.255 log

access-list 101 deny ip host 192.168.2.20 192.168.0.0 0.0.255.255 log

access-list 101 permit ip 192.168.2.0 0.0.0.15 any

access-list 101 permit ip 192.168.2.16 0.0.0.3 any

access-list 101 permit ip host 192.168.2.20 any

access-list 101 deny ip any any log

access-list 101 remark RO req12

access-list 102 permit eigrp any any

access-list 102 permit gre any any

access-list 102 permit ahp any any

access-list 102 permit esp any any

access-list 102 permit udp any any eq isakmp

access-list 102 permit icmp any host 22.22.22.254 echo

access-list 102 permit tcp any host 22.22.22.254 eq 22

access-list 102 deny ip any any log

access-list 103 deny ip any any log

access-list 103 remark RO req4

!

control-plane

!

!

!

!

!

!

!

alias exec srb sh run | beg

alias exec srs sh run | sec

alias exec sri sh run | incl

alias exec siib sh ip int brief

alias exec siibu sh ip int brief | include up

alias exec srint sh run interface

alias exec wrx copy run unix:

alias exec ssha ssh -l admin -c 3des

alias exec sshu ssh -l admin -c 3des

alias exec diff sh archive config diff unix:start.cfg unix:running-config

banner motd ^CCC

\*\*\* You are connecting to R2 \*\*\*

^C

!

line con 0

exec-timeout 0 0

logging synchronous

line aux 0

line vty 0 4

exec-timeout 0 5

privilege level 15

login local

transport input telnet ssh

!

!

end

# R2(config-ext-nacl)#do sh run

Building configuration...

Current configuration : 5643 bytes

!

! Last configuration change at 10:30:50 AWST Fri Apr 24 2015

!

version 15.4

service timestamps debug datetime msec

service timestamps log datetime msec

no service password-encryption

!

hostname R2

!

boot-start-marker

boot-end-marker

!

aqm-register-fnf

!

logging discriminator EXCESS severity drops 6 msg-body drops EXCESSCOLL

logging buffered 50000

logging console discriminator EXCESS

!

no aaa new-model

clock timezone AWST 8 0

mmi polling-interval 60

no mmi auto-configure

no mmi pvc

mmi snmp-timeout 180

no ip icmp rate-limit unreachable

!

!

!

!

!

!

!

!

!

!

!

!

no ip domain lookup

ip domain name candy.com

ip inspect audit-trail

ip inspect name INSIDE\_TO\_OUT icmp timeout 60

ip inspect name INSIDE\_TO\_OUT telnet timeout 60

ip inspect name INSIDE\_TO\_OUT tcp timeout 60

ip inspect name INSIDE\_TO\_OUT udp timeout 60

ip inspect name INTO\_DMZ icmp timeout 60

ip inspect name INTO\_DMZ ssh timeout 60

ip inspect name VPN\_TO\_INSIDE icmp timeout 60

ip inspect name VPN\_TO\_INSIDE tcp timeout 60

ip inspect name VPN\_TO\_INSIDE udp timeout 60

ip cef

no ipv6 cef

ipv6 multicast rpf use-bgp

!

multilink bundle-name authenticated

!

!

!

!

!

!

!

!

username cisco privilege 0 password 0 cisco

username admin privilege 15 password 0 admin

!

redundancy

!

no cdp log mismatch duplex

!

ip tcp synwait-time 5

!

!

!

!

!

crypto isakmp policy 5

authentication pre-share

lifetime 1800

crypto isakmp key cisco12345 address 0.0.0.0

!

crypto ipsec security-association lifetime seconds 1800

!

crypto ipsec transform-set DMVPN\_TRANSFORM ah-md5-hmac esp-des

mode transport

!

crypto ipsec profile DMVPN\_PROFILE

set transform-set DMVPN\_TRANSFORM

!

!

!

!

!

!

!

interface Tunnel1

description \*\*\* Spoke R2 \*\*\*

bandwidth 192

ip address 10.0.1.2 255.255.255.0

no ip redirects

ip mtu 1400

ip nhrp authentication cisco123

ip nhrp map multicast 11.11.11.1

ip nhrp map 10.0.1.1 11.11.11.1

ip nhrp network-id 100001

ip nhrp holdtime 300

ip nhrp nhs 10.0.1.1

ip nhrp registration no-unique

ip nhrp registration timeout 120

ip nhrp shortcut

ip tcp adjust-mss 1360

tunnel source Serial2/0

tunnel mode gre multipoint

tunnel key 100001

tunnel protection ipsec profile DMVPN\_PROFILE

!

interface Ethernet0/0

ip address 192.168.2.2 255.255.255.0

ip access-group 101 in

ip nat inside

ip inspect INSIDE\_TO\_OUT in

ip inspect VPN\_TO\_INSIDE out

ip virtual-reassembly in

!

interface Ethernet0/1

ip address 192.168.21.2 255.255.255.0

ip access-group 103 in

ip nat inside

ip inspect INTO\_DMZ out

ip virtual-reassembly in

!

interface Ethernet0/2

no ip address

shutdown

!

interface Ethernet0/3

no ip address

shutdown

!

interface Ethernet1/0

no ip address

shutdown

!

interface Ethernet1/1

no ip address

shutdown

!

interface Ethernet1/2

no ip address

shutdown

!

interface Ethernet1/3

no ip address

shutdown

!

interface Serial2/0

ip address 22.22.22.2 255.255.255.0

ip access-group 102 in

ip nat outside

ip virtual-reassembly in

serial restart-delay 0

!

interface Serial2/1

no ip address

shutdown

serial restart-delay 0

!

interface Serial2/2

no ip address

shutdown

serial restart-delay 0

!

interface Serial2/3

no ip address

shutdown

serial restart-delay 0

!

interface Serial3/0

no ip address

shutdown

serial restart-delay 0

!

interface Serial3/1

no ip address

shutdown

serial restart-delay 0

!

interface Serial3/2

no ip address

shutdown

serial restart-delay 0

!

interface Serial3/3

no ip address

shutdown

serial restart-delay 0

!

!

router eigrp 1

network 10.0.1.0 0.0.0.255

network 192.168.2.0

passive-interface Ethernet0/1

passive-interface Ethernet0/0

eigrp stub connected

!

ip forward-protocol nd

!

!

no ip http server

no ip http secure-server

ip nat pool NAT\_POOL 22.22.22.192 22.22.22.253 prefix-length 24

ip nat inside source route-map NAT\_PROCESS pool NAT\_POOL overload

ip nat inside source static 192.168.21.23 22.22.22.254

ip route 0.0.0.0 0.0.0.0 Serial2/0

!

ip access-list extended R2\_NAT\_ACL

deny ip 192.168.0.0 0.0.255.255 192.168.0.0 0.0.255.255

permit ip 192.168.0.0 0.0.255.255 any

!

!

route-map NAT\_PROCESS permit 10

match ip address R2\_NAT\_ACL

!

!

access-list 101 permit icmp 192.168.2.0 0.0.0.15 host 192.168.114.114

access-list 101 permit tcp 192.168.2.0 0.0.0.15 host 192.168.114.114 eq telnet

access-list 101 deny ip 192.168.2.0 0.0.0.15 192.168.0.0 0.0.255.255 log

access-list 101 deny ip 192.168.2.16 0.0.0.3 192.168.0.0 0.0.255.255 log

access-list 101 deny ip host 192.168.2.20 192.168.0.0 0.0.255.255 log

access-list 101 permit ip 192.168.2.0 0.0.0.15 any

access-list 101 permit ip 192.168.2.16 0.0.0.3 any

access-list 101 permit ip host 192.168.2.20 any

access-list 101 deny ip any any log

access-list 101 remark RO req12

access-list 102 permit ahp any any

access-list 102 permit udp any any eq isakmp

access-list 102 permit icmp any host 22.22.22.254 echo

access-list 102 permit tcp any host 22.22.22.254 eq 22

access-list 102 deny ip any any log

access-list 103 deny ip any any log

access-list 103 remark RO req4

!

control-plane

!

!

!

!

!

!

!

alias exec srb sh run | beg

alias exec srs sh run | sec

alias exec sri sh run | incl

alias exec siib sh ip int brief

alias exec siibu sh ip int brief | include up

alias exec srint sh run interface

alias exec wrx copy run unix:

alias exec ssha ssh -l admin -c 3des

alias exec sshu ssh -l admin -c 3des

alias exec diff sh archive config diff unix:start.cfg unix:running-config

banner motd ^CCC

\*\*\* You are connecting to R2 \*\*\*

^C

!

line con 0

exec-timeout 0 0

logging synchronous

line aux 0

line vty 0 4

exec-timeout 0 5

privilege level 15

login local

transport input telnet ssh

!

!

end

# R2(config-if)#do sh run

Building configuration...

Current configuration : 5215 bytes

!

version 15.4

service timestamps debug datetime msec

service timestamps log datetime msec

no service password-encryption

!

hostname R2

!

boot-start-marker

boot-end-marker

!

aqm-register-fnf

!

logging discriminator EXCESS severity drops 6 msg-body drops EXCESSCOLL

logging buffered 50000

!

no aaa new-model

clock timezone AWST 8 0

mmi polling-interval 60

no mmi auto-configure

no mmi pvc

mmi snmp-timeout 180

no ip icmp rate-limit unreachable

!

!

!

!

!

!

!

!

!

!

!

!

no ip domain lookup

ip domain name candy.com

ip inspect name INSIDE\_TO\_OUT icmp timeout 60

ip inspect name INSIDE\_TO\_OUT tcp timeout 60

ip inspect name INSIDE\_TO\_OUT udp timeout 60

ip inspect name INTO\_DMZ icmp timeout 60

ip inspect name INTO\_DMZ tcp timeout 60

ip inspect name INTO\_DMZ udp timeout 60

ip inspect name VPN\_TO\_INSIDE icmp timeout 60

ip inspect name VPN\_TO\_INSIDE tcp timeout 60

ip inspect name VPN\_TO\_INSIDE udp timeout 60

ip cef

no ipv6 cef

ipv6 multicast rpf use-bgp

!

multilink bundle-name authenticated

!

!

!

!

!

!

!

!

object-group service ICMP&SSH

icmp echo

tcp eq 22

!

object-group service ICMP&TELNET

icmp

tcp eq telnet

!

username cisco privilege 0 password 0 cisco

username admin privilege 15 password 0 admin

!

redundancy

!

no cdp log mismatch duplex

!

ip tcp synwait-time 5

!

!

!

!

!

crypto isakmp policy 5

authentication pre-share

lifetime 1800

crypto isakmp key cisco12345 address 0.0.0.0

!

crypto ipsec security-association lifetime seconds 1800

!

crypto ipsec transform-set DMVPN\_TRANSFORM ah-md5-hmac esp-des

mode transport

!

crypto ipsec profile DMVPN\_PROFILE

set transform-set DMVPN\_TRANSFORM

!

!

!

!

!

!

!

interface Tunnel1

bandwidth 192

ip address 10.0.1.2 255.255.255.0

no ip redirects

ip nhrp authentication cisco123

ip nhrp map multicast 11.11.11.1

ip nhrp map 10.0.1.1 11.11.11.1

ip nhrp network-id 100001

ip nhrp nhs 10.0.1.1

tunnel source Serial2/0

tunnel mode gre multipoint

tunnel key 100001

tunnel protection ipsec profile DMVPN\_PROFILE

!

interface Ethernet0/0

ip address 192.168.2.2 255.255.255.0

ip access-group 101 in

ip nat inside

ip inspect INSIDE\_TO\_OUT in

ip inspect VPN\_TO\_INSIDE out

ip virtual-reassembly in

!

interface Ethernet0/1

ip address 192.168.21.2 255.255.255.0

ip access-group 103 in

ip nat inside

ip inspect INTO\_DMZ out

ip virtual-reassembly in

!

interface Ethernet0/2

no ip address

shutdown

!

interface Ethernet0/3

no ip address

shutdown

!

interface Ethernet1/0

no ip address

shutdown

!

interface Ethernet1/1

no ip address

shutdown

!

interface Ethernet1/2

no ip address

shutdown

!

interface Ethernet1/3

no ip address

shutdown

!

interface Serial2/0

ip address 22.22.22.2 255.255.255.0

ip access-group 102 in

ip nat outside

ip virtual-reassembly in

serial restart-delay 0

!

interface Serial2/1

no ip address

shutdown

serial restart-delay 0

!

interface Serial2/2

no ip address

shutdown

serial restart-delay 0

!

interface Serial2/3

no ip address

shutdown

serial restart-delay 0

!

interface Serial3/0

no ip address

shutdown

serial restart-delay 0

!

interface Serial3/1

no ip address

shutdown

serial restart-delay 0

!

interface Serial3/2

no ip address

shutdown

serial restart-delay 0

!

interface Serial3/3

no ip address

shutdown

serial restart-delay 0

!

!

router eigrp 1

network 10.0.1.0 0.0.0.255

network 192.168.0.0 0.0.255.255

eigrp stub connected summary

!

ip forward-protocol nd

!

!

no ip http server

no ip http secure-server

ip nat pool R2\_NAT 22.22.22.192 22.22.22.253 prefix-length 24

ip nat inside source route-map NAT\_PROCESS pool R2\_NAT overload

ip nat inside source static 192.168.21.23 22.22.22.254

ip route 0.0.0.0 0.0.0.0 Serial2/0

!

ip access-list extended R2\_NAT\_ACL

deny ip 192.168.0.0 0.0.255.255 192.168.0.0 0.0.255.255

permit ip 192.168.0.0 0.0.255.255 any

!

!

route-map NAT\_PROCESS permit 10

match ip address R2\_NAT\_ACL

!

!

access-list 101 permit object-group ICMP&TELNET 192.168.2.0 0.0.0.15 host 192.168.114.114

access-list 101 deny ip 192.168.2.0 0.0.0.15 192.168.0.0 0.0.255.255 log

access-list 101 deny ip 192.168.2.16 0.0.0.3 192.168.0.0 0.0.255.255 log

access-list 101 deny ip host 192.168.2.20 192.168.0.0 0.0.255.255 log

access-list 101 permit ip 192.168.2.0 0.0.0.15 any

access-list 101 permit ip 192.168.2.16 0.0.0.3 any

access-list 101 permit ip host 192.168.2.20 any

access-list 101 deny ip any any log

access-list 102 permit object-group ICMP&SSH any host 22.22.22.254

access-list 102 permit ahp any any

access-list 102 permit udp any any eq isakmp

access-list 102 deny ip any any log

access-list 103 deny ip any any log

!

control-plane

!

!

!

!

!

!

!

alias exec srb sh run | beg

alias exec srs sh run | sec

alias exec sri sh run | incl

alias exec siib sh ip int brief

alias exec siibu sh ip int brief | include up

alias exec srint sh run interface

alias exec wrx copy run unix:

alias exec ssha ssh -l admin -c 3des

alias exec sshu ssh -l admin -c 3des

alias exec diff sh archive config diff unix:start.cfg unix:running-config

banner motd ^CC

\*\*\* You are connecting to R2 \*\*\*

^C

!

line con 0

exec-timeout 0 0

logging synchronous

line aux 0

line vty 0 4

exec-timeout 0 5

privilege level 15

login local

transport input telnet ssh

!

!

end