# R3#sh run

Building configuration...

Current configuration : 3016 bytes

!

! Last configuration change at 16:52:52 AWST Thu Apr 23 2015

!

version 15.4

service timestamps debug datetime msec

service timestamps log datetime msec

no service password-encryption

!

hostname R3

!

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 admin privilege 15 password 0 admin

username cisco password 0 cisco

!

redundancy

!

no cdp log mismatch duplex

!

ip tcp synwait-time 5

!

!

!

!

!

!

!

!

!

!

!

!

!

interface Ethernet0/0

ip address 192.168.3.3 255.255.255.0

ip nat inside

ip virtual-reassembly in

!

interface Ethernet0/1

no ip address

shutdown

!

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 33.33.33.3 255.255.255.0

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 33.33.33.80 33.33.33.83 prefix-length 24

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

ip route 0.0.0.0 0.0.0.0 Serial2/0

!

ip access-list extended R3\_NAT\_ACL

deny ip 192.168.0.0 0.0.255.255 192.168.0.0 0.0.255.255

permit ip 192.168.3.0 0.0.0.255 any

!

!

route-map NAT\_PROCESS permit 10

match ip address R3\_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 R3 \*\*\*

^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

# R3#sh run

Building configuration...

Current configuration : 4500 bytes

!

! Last configuration change at 17:36:33 AWST Thu Apr 23 2015

!

version 15.4

service timestamps debug datetime msec

service timestamps log datetime msec

no service password-encryption

!

hostname R3

!

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

!

!

!

!

!

!

!

!

object-group network INSIDESRV

host 192.168.114.114

host 192.168.2.22

!

username admin privilege 15 password 0 admin

username cisco password 0 cisco

!

redundancy

!

no cdp log mismatch duplex

!

ip tcp synwait-time 5

!

class-map type inspect match-all INSIDE2OUTSIDE-CL

match access-group 101

class-map type inspect match-any SERVICE

match protocol icmp

match protocol telnet

class-map type inspect match-all INSIDE2VPN-CL

match access-group 102

match class-map SERVICE

!

policy-map type inspect INSIDE2OUTSIDE-PL

class type inspect INSIDE2OUTSIDE-CL

inspect

class class-default

drop log

policy-map type inspect INSIDE2VPN-PL

class type inspect INSIDE2VPN-CL

inspect

class class-default

drop log

!

zone security INSIDE

description 3

zone security OUTSIDE

description s2/0

zone security DMVPN

description 10.0.1.3

zone-pair security INSIDE2OUTSIDE source INSIDE destination OUTSIDE

service-policy type inspect INSIDE2OUTSIDE-PL

zone-pair security INSIDE2VPN source INSIDE destination DMVPN

service-policy type inspect INSIDE2OUTSIDE-PL

!

!

!

!

!

!

!

!

!

!

!

!

!

interface Ethernet0/0

ip address 192.168.3.3 255.255.255.0

ip nat inside

ip virtual-reassembly in

zone-member security INSIDE

!

interface Ethernet0/1

no ip address

shutdown

!

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 33.33.33.3 255.255.255.0

ip nat outside

ip virtual-reassembly in

zone-member security OUTSIDE

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 33.33.33.80 33.33.33.83 prefix-length 24

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

ip route 0.0.0.0 0.0.0.0 Serial2/0

!

ip access-list extended R3\_NAT\_ACL

deny ip 192.168.0.0 0.0.255.255 192.168.0.0 0.0.255.255

permit ip 192.168.3.0 0.0.0.255 any

!

!

route-map NAT\_PROCESS permit 10

match ip address R3\_NAT\_ACL

!

!

access-list 101 deny ip 192.168.3.0 0.0.0.7 192.168.0.0 0.0.255.255

access-list 101 deny ip 192.168.3.8 0.0.0.1 192.168.0.0 0.0.255.255

access-list 101 deny ip host 192.168.3.10 192.168.0.0 0.0.255.255

access-list 101 permit ip 192.168.3.0 0.0.0.7 any

access-list 101 permit ip 192.168.3.8 0.0.0.1 any

access-list 101 permit ip host 192.168.3.10 any

access-list 102 permit icmp host 192.168.3.33 object-group INSIDESRV echo

access-list 102 permit tcp host 192.168.3.33 object-group INSIDESRV eq telnet

!

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 R3 \*\*\*

^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

# R3#sh run

Building configuration...

Current configuration : 4959 bytes

!

! Last configuration change at 10:32:01 AWST Fri Apr 24 2015

!

version 15.4

service timestamps debug datetime msec

service timestamps log datetime msec

no service password-encryption

!

hostname R3

!

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

!

!

!

!

!

!

!

!

object-group network INSIDESRV

host 192.168.114.114

host 192.168.2.22

!

username admin privilege 15 password 0 admin

username cisco password 0 cisco

!

redundancy

!

no cdp log mismatch duplex

!

ip tcp synwait-time 5

!

class-map type inspect match-all VPN2INSIDE-CL

match access-group 103

class-map type inspect match-all INSIDE2OUTSIDE-CL

match access-group 101

class-map type inspect match-any SERVICE

match protocol icmp

match protocol telnet

class-map type inspect match-all INSIDE2VPN-CL

match access-group 102

match class-map SERVICE

!

policy-map type inspect VPN2INSIDE-PL

class type inspect VPN2INSIDE-CL

inspect

class class-default

drop log

policy-map type inspect INSIDE2OUTSIDE-PL

class type inspect INSIDE2OUTSIDE-CL

inspect

class class-default

drop log

policy-map type inspect INSIDE2VPN-PL

class type inspect INSIDE2VPN-CL

inspect

class class-default

drop log

!

zone security INSIDE

description 3

zone security OUTSIDE

description s2/0

zone security DMVPN

description 10.0.1.3

zone-pair security INSIDE2OUTSIDE source INSIDE destination OUTSIDE

service-policy type inspect INSIDE2OUTSIDE-PL

zone-pair security INSIDE2VPN source INSIDE destination DMVPN

service-policy type inspect INSIDE2OUTSIDE-PL

zone-pair security VPN2INSIDE source DMVPN destination INSIDE

service-policy type inspect VPN2INSIDE-PL

!

!

!

!

!

!

!

!

!

!

!

!

!

interface Tunnel1

no ip address

zone-member security DMVPN

!

interface Ethernet0/0

ip address 192.168.3.3 255.255.255.0

ip nat inside

ip virtual-reassembly in

zone-member security INSIDE

!

interface Ethernet0/1

no ip address

shutdown

!

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 33.33.33.3 255.255.255.0

ip nat outside

ip virtual-reassembly in

zone-member security OUTSIDE

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 33.33.33.80 33.33.33.83 prefix-length 24

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

ip route 0.0.0.0 0.0.0.0 Serial2/0

!

ip access-list extended R3\_NAT\_ACL

deny ip 192.168.0.0 0.0.255.255 192.168.0.0 0.0.255.255

permit ip 192.168.3.0 0.0.0.255 any

!

!

route-map NAT\_PROCESS permit 10

match ip address R3\_NAT\_ACL

!

!

access-list 101 deny ip 192.168.3.0 0.0.0.7 192.168.0.0 0.0.255.255

access-list 101 deny ip 192.168.3.8 0.0.0.1 192.168.0.0 0.0.255.255

access-list 101 deny ip host 192.168.3.10 192.168.0.0 0.0.255.255

access-list 101 permit ip 192.168.3.0 0.0.0.7 any

access-list 101 permit ip 192.168.3.8 0.0.0.1 any

access-list 101 permit ip host 192.168.3.10 any

access-list 102 permit icmp host 192.168.3.33 object-group INSIDESRV echo

access-list 102 permit tcp host 192.168.3.33 object-group INSIDESRV eq telnet

access-list 103 permit ip 192.168.0.0 0.0.255.255 192.168.3.0 0.0.0.255

access-list 103 remark VPN2INSIDE

!

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 R3 \*\*\*

^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

# R3(config-sec-zone-pair)#do sh run

Building configuration...

Current configuration : 5890 bytes

!

! Last configuration change at 10:32:01 AWST Fri Apr 24 2015

!

version 15.4

service timestamps debug datetime msec

service timestamps log datetime msec

no service password-encryption

!

hostname R3

!

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

!

!

!

!

!

!

!

!

object-group network INSIDESRV

host 192.168.114.114

host 192.168.2.22

!

username admin privilege 15 password 0 admin

username cisco password 0 cisco

!

redundancy

!

no cdp log mismatch duplex

!

ip tcp synwait-time 5

!

class-map type inspect match-all VPN2INSIDE-CL

match access-group 103

class-map type inspect match-all INSIDE2OUTSIDE-CL

match access-group 101

class-map type inspect match-any SERVICE

match protocol icmp

match protocol telnet

class-map type inspect match-all INSIDE2VPN-CL

match access-group 102

match class-map SERVICE

!

policy-map type inspect VPN2INSIDE-PL

class type inspect VPN2INSIDE-CL

inspect

class class-default

drop log

policy-map type inspect INSIDE2OUTSIDE-PL

class type inspect INSIDE2OUTSIDE-CL

inspect

class class-default

drop log

policy-map type inspect INSIDE2VPN-PL

class type inspect INSIDE2VPN-CL

inspect

class class-default

drop log

!

zone security INSIDE

description 3

zone security OUTSIDE

description s2/0

zone security DMVPN

description 10.0.1.3

zone-pair security INSIDE2OUTSIDE source INSIDE destination OUTSIDE

service-policy type inspect INSIDE2OUTSIDE-PL

zone-pair security INSIDE2VPN source INSIDE destination DMVPN

service-policy type inspect INSIDE2VPN-PL

zone-pair security VPN2INSIDE source DMVPN destination INSIDE

service-policy type inspect VPN2INSIDE-PL

!

!

!

!

!

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 R3 \*\*\*

bandwidth 192

ip address 10.0.1.3 255.255.255.0

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

zone-member security DMVPN

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 192.168.3.3 255.255.255.0

ip nat inside

ip virtual-reassembly in

zone-member security INSIDE

!

interface Ethernet0/1

no ip address

shutdown

!

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 33.33.33.3 255.255.255.0

ip nat outside

ip virtual-reassembly in

zone-member security OUTSIDE

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 192.168.3.0

eigrp stub connected

!

ip forward-protocol nd

!

!

no ip http server

no ip http secure-server

ip nat pool NAT\_POOL 33.33.33.80 33.33.33.83 prefix-length 24

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

ip route 0.0.0.0 0.0.0.0 Serial2/0

!

ip access-list extended R3\_NAT\_ACL

deny ip 192.168.0.0 0.0.255.255 192.168.0.0 0.0.255.255

permit ip 192.168.3.0 0.0.0.255 any

!

!

route-map NAT\_PROCESS permit 10

match ip address R3\_NAT\_ACL

!

!

access-list 101 deny ip 192.168.3.0 0.0.0.7 192.168.0.0 0.0.255.255

access-list 101 deny ip 192.168.3.8 0.0.0.1 192.168.0.0 0.0.255.255

access-list 101 deny ip host 192.168.3.10 192.168.0.0 0.0.255.255

access-list 101 permit ip 192.168.3.0 0.0.0.7 any

access-list 101 permit ip 192.168.3.8 0.0.0.1 any

access-list 101 permit ip host 192.168.3.10 any

access-list 102 permit icmp host 192.168.3.33 object-group INSIDESRV echo

access-list 102 permit tcp host 192.168.3.33 object-group INSIDESRV eq telnet

access-list 103 permit ip 192.168.0.0 0.0.255.255 192.168.3.0 0.0.0.255

access-list 103 remark VPN2INSIDE

!

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 R3 \*\*\*

^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

# R3(config-sec-zone-pair)#do sh run

Building configuration...

Current configuration : 5936 bytes

!

version 15.4

service timestamps debug datetime msec

service timestamps log datetime msec

no service password-encryption

!

hostname R3

!

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

!

!

!

!

!

!

!

!

object-group network INSIDESRV

host 192.168.114.114

host 192.168.2.22

!

username admin privilege 15 password 0 admin

username cisco password 0 cisco

!

redundancy

!

no cdp log mismatch duplex

!

ip tcp synwait-time 5

!

class-map type inspect match-any ANYSERVICE

match protocol icmp

match protocol tcp

match protocol udp

class-map type inspect match-all VPN2INSIDE-CL

match access-group 103

class-map type inspect match-any SERVICE

match protocol icmp

match protocol telnet

class-map type inspect match-all INSIDE2VPN-CL

match access-group 102

match class-map SERVICE

class-map type inspect match-all INSIDE2OUTSIDE-CL

match access-group 101

match class-map ANYSERVICE

!

policy-map type inspect VPN2INSIDE-PL

class type inspect VPN2INSIDE-CL

inspect

class class-default

drop log

policy-map type inspect INSIDE2OUTSIDE-PL

class type inspect INSIDE2OUTSIDE-CL

inspect

class class-default

drop log

policy-map type inspect INSIDE2VPN-PL

class type inspect INSIDE2VPN-CL

inspect

class class-default

drop log

!

zone security INSIDE

description 3

zone security OUTSIDE

description s2/0

zone security DMVPN

description 10.0.1.3

zone-pair security INSIDE2OUTSIDE source INSIDE destination OUTSIDE

service-policy type inspect INSIDE2OUTSIDE-PL

zone-pair security INSIDE2VPN source INSIDE destination DMVPN

service-policy type inspect INSIDE2VPN-PL

zone-pair security VPN2INSIDE source DMVPN destination INSIDE

service-policy type inspect VPN2INSIDE-PL

!

!

!

!

!

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 R3 \*\*\*

bandwidth 192

ip address 10.0.1.3 255.255.255.0

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

zone-member security DMVPN

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 192.168.3.3 255.255.255.0

ip nat inside

ip virtual-reassembly in

zone-member security INSIDE

!

interface Ethernet0/1

no ip address

shutdown

!

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 33.33.33.3 255.255.255.0

ip nat outside

ip virtual-reassembly in

zone-member security OUTSIDE

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 192.168.3.0

eigrp stub connected

!

ip forward-protocol nd

!

!

no ip http server

no ip http secure-server

ip nat pool NAT\_POOL 33.33.33.80 33.33.33.83 prefix-length 24

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

ip route 0.0.0.0 0.0.0.0 Serial2/0

!

ip access-list extended R3\_NAT\_ACL

deny ip 192.168.0.0 0.0.255.255 192.168.0.0 0.0.255.255

permit ip 192.168.3.0 0.0.0.255 any

!

!

route-map NAT\_PROCESS permit 10

match ip address R3\_NAT\_ACL

!

!

access-list 101 deny ip 192.168.3.0 0.0.0.7 192.168.0.0 0.0.255.255

access-list 101 deny ip 192.168.3.8 0.0.0.1 192.168.0.0 0.0.255.255

access-list 101 deny ip host 192.168.3.10 192.168.0.0 0.0.255.255

access-list 101 permit ip 192.168.3.0 0.0.0.7 any

access-list 101 permit ip 192.168.3.8 0.0.0.1 any

access-list 101 permit ip host 192.168.3.10 any

access-list 102 permit icmp host 192.168.3.33 object-group INSIDESRV echo

access-list 102 permit tcp host 192.168.3.33 object-group INSIDESRV eq telnet

access-list 103 permit ip 192.168.0.0 0.0.255.255 192.168.3.0 0.0.0.255

access-list 103 remark VPN2INSIDE

!

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 R3 \*\*\*

^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

# R3(config-sec-zone-pair)#do sh run

Building configuration...

Current configuration : 5413 bytes

!

version 15.4

service timestamps debug datetime msec

service timestamps log datetime msec

no service password-encryption

!

hostname R3

!

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 cef

no ipv6 cef

ipv6 multicast rpf use-bgp

!

multilink bundle-name authenticated

!

!

!

!

!

!

!

!

object-group service ICMP&TELNET

icmp echo

tcp eq telnet

!

object-group network INTERNAL-SERVERS

host 192.168.114.114

host 192.168.2.22

!

username admin privilege 15 password 0 admin

username cisco password 0 cisco

!

redundancy

!

no cdp log mismatch duplex

!

ip tcp synwait-time 5

!

class-map type inspect match-all INSIDE2VPN-CL

match access-group 102

class-map type inspect match-all VPN2INSIDE-CL

match access-group name VPN2INSIDE

class-map type inspect match-all INSIDE2OUTSIDE-CL

match access-group 101

!

policy-map type inspect OUTSIDE-PL

class type inspect VPN2INSIDE-CL

inspect

class class-default

drop log

policy-map type inspect INSIDE-PL

class type inspect INSIDE2OUTSIDE-CL

inspect

class type inspect INSIDE2VPN-CL

inspect

class class-default

drop log

!

zone security INSIDE

description 3.0

zone security OUTSIDE

description S2/0

zone security DMVPN

description T1

zone-pair security INSIDE2OUTSIDE source INSIDE destination OUTSIDE

service-policy type inspect INSIDE-PL

zone-pair security INSIDE2VPN source INSIDE destination DMVPN

service-policy type inspect INSIDE-PL

zone-pair security VPN2INSIDE source DMVPN destination INSIDE

service-policy type inspect OUTSIDE-PL

!

!

!

!

!

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 10.0.1.3 255.255.255.0

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

zone-member security DMVPN

tunnel source Serial2/0

tunnel mode gre multipoint

tunnel key 100001

tunnel protection ipsec profile DMVPN\_PROFILE

!

interface Ethernet0/0

ip address 192.168.3.3 255.255.255.0

ip nat inside

ip virtual-reassembly in

zone-member security INSIDE

!

interface Ethernet0/1

no ip address

shutdown

!

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 33.33.33.3 255.255.255.0

ip nat outside

ip virtual-reassembly in

zone-member security OUTSIDE

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 R3\_NAT 33.33.33.80 33.33.33.83 prefix-length 24

ip nat inside source route-map NAT\_PROCESS pool R3\_NAT overload

ip route 0.0.0.0 0.0.0.0 Serial2/0

!

ip access-list extended R3\_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

ip access-list extended VPN2INSIDE

permit ip 192.168.0.0 0.0.255.255 192.168.3.0 0.0.0.255

!

!

route-map NAT\_PROCESS permit 10

match ip address R3\_NAT\_ACL

!

!

access-list 101 deny ip 192.168.3.0 0.0.0.7 192.168.0.0 0.0.255.255

access-list 101 deny ip 192.168.3.8 0.0.0.1 192.168.0.0 0.0.255.255

access-list 101 deny ip host 192.168.3.10 192.168.0.0 0.0.255.255

access-list 101 permit ip 192.168.3.0 0.0.0.7 any

access-list 101 permit ip 192.168.3.8 0.0.0.1 any

access-list 101 permit ip host 192.168.3.10 any

access-list 102 permit object-group ICMP&TELNET host 192.168.3.33 object-group INTERNAL-SERVERS

!

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 R3 \*\*\*

^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