show route advertising-protocol bgp 220.152.112.73

show route 103.197.250.0/23

run show configuration | match static | display set

#b3dc10

set protocols bgp group iBGP outbound-route-filter

Top >>> exit

root

cli

edit or config

cisco config mode do junus run and mkt \ all

run request system zeroize < system defolt >

set system root-authentication plain-text-password

root> show interfaces terse < int status check >

run show configuration | match inter

run show configuration | match inter | display set

commit confirmed 2 <<< only >>>

configure exclusive

configure private

edit protocols ospf area 0

set interface em0 passive

set interface em1 interface-type p2p

show

"show log messages | match "error | kernel | panic"

monitor traffic interface fxp0.0

show interfaces terse

clear system reboot command

root# show | display set

set protocols ospf area 0.0.0.0 interface em0.0 passive

set protocols ospf area 0.0.0.0 interface em1.0 interface-type p2p

[edit protocols ospf area 0.0.0.0]

exit mane full back

up = one step back up 2 = 2 stape back

top and exit same

=====================================router portt down and up ===

[edit interfaces em0]

root# set disable //// shutdown

[edit interfaces em0]

root# show

disable;

[edit interfaces em0]

root# de

^

'de' is ambiguous.

Possible completions:

deactivate Add the inactive tag to a statement

delete Delete a data element

[edit interfaces em0]

root# delete disable //// no shutdown

[edit interfaces em0]

root# show

[edit interfaces em0]

run show interfaces em0 terse

============================================== exta slot up korle ===

root# run show chassis hardware ?

Possible completions:

<[Enter]> Execute this command

clei-models Display CLEI barcode and model number for orderable FRUs

detail Include RAM and disk information in output

extensive Display ID EEPROM information

models Display serial number and model number for orderable FRUs

| Pipe through a command

[edit interfaces em0]

root# run show chassis hardware fpc 2

ping command

run ping 1.1.1.1 source 5.5.5.5 count 100 rapid size 1000

run show system uptime

root# run show arp

root# show | display set

set routing-options static route 10.0.0.1/32 next-hop 11.0.0.1

commit check

sinha@sinhaFirewaLL# run show configuration | match inter | display set

set system services web-management http interface ge-0/0/0.0

set system services web-management http interface ge-0/0/1.0

set system syslog file interactive-commands interactive-commands error

set interfaces ge-0/0/0 unit 0 family inet address 172.168.0.1/24

set interfaces ge-0/0/1 unit 0 family inet address 103.16.73.253/29

set interfaces lo0 unit 0 family inet address 127.0.0.1/32

set security nat source rule-set internal-to-internet from zone trust

set security nat source rule-set internal-to-internet to zone untrust

set security nat source rule-set internal-to-internet rule internet-access match source-address 0.0.0.0/0

set security nat source rule-set internal-to-internet rule internet-access match destination-address 0.0.0.0/0

set security nat source rule-set internal-to-internet rule internet-access then source-nat interface

set security zones security-zone trust interfaces ge-0/0/0.0 host-inbound-traffic system-services http

set security zones security-zone trust interfaces ge-0/0/0.0 host-inbound-traffic system-services https

set security zones security-zone trust interfaces ge-0/0/0.0 host-inbound-traffic system-services ssh

set security zones security-zone trust interfaces ge-0/0/0.0 host-inbound-traffic system-services telnet

set security zones security-zone trust interfaces ge-0/0/0.0 host-inbound-traffic system-services dhcp

set security zones security-zone trust interfaces ge-0/0/0.0 host-inbound-traffic system-services all

set security zones security-zone untrust interfaces ge-0/0/1.0 host-inbound-traffic system-services all

sinha@sinhaFirewaLL# show | display set

set version 9.5R1.8

set system host-name sinhaFirewaLL

set system root-authentication encrypted-password "$1$6Kgj7GB7$exUgGdgzemxBbosZ73ff9."

set system name-server 8.8.8.8

set system name-server 8.8.4.4

set system name-server 4.2.2.2

set system login user sinha full-name sinha

set system login user sinha uid 2004

set system login user sinha class superuser

set system login user sinha authentication encrypted-password "$1$Clf1Mo/A$sthTOPYb0GZAuUAkcNyW/1"

set system services ssh

set system services xnm-clear-text

set system services web-management http interface ge-0/0/0.0

set system services web-management http interface ge-0/0/1.0

set system syslog user \* any emergency

set system syslog file messages any critical

set system syslog file messages authorization info

set system syslog file interactive-commands interactive-commands error

set system max-configurations-on-flash 5

set system max-configuration-rollbacks 5

set system license autoupdate url https://ae1.juniper.net/junos/key\_retrieval

set interfaces ge-0/0/0 unit 0 family inet address 172.168.0.1/24

set interfaces ge-0/0/1 unit 0 family inet address 103.16.73.253/29

set interfaces lo0 unit 0 family inet address 127.0.0.1/32

set routing-options static route 0.0.0.0/0 next-hop 103.16.73.249

set security nat source rule-set internal-to-internet from zone trust

set security nat source rule-set internal-to-internet to zone untrust

set security nat source rule-set internal-to-internet rule internet-access match source-address 0.0.0.0/0

set security nat source rule-set internal-to-internet rule internet-access match destination-address 0.0.0.0/0

set security nat source rule-set internal-to-internet rule internet-access then source-nat interface

set security screen ids-option untrust-screen icmp ping-death

set security screen ids-option untrust-screen ip source-route-option

set security screen ids-option untrust-screen ip tear-drop

set security screen ids-option untrust-screen tcp syn-flood alarm-threshold 1024

set security screen ids-option untrust-screen tcp syn-flood attack-threshold 200

set security screen ids-option untrust-screen tcp syn-flood source-threshold 1024

set security screen ids-option untrust-screen tcp syn-flood destination-threshold 2048

set security screen ids-option untrust-screen tcp syn-flood queue-size 2000

set security screen ids-option untrust-screen tcp syn-flood timeout 20

set security screen ids-option untrust-screen tcp land

set security zones security-zone trust tcp-rst

set security zones security-zone trust host-inbound-traffic system-services all

set security zones security-zone trust host-inbound-traffic protocols all

set security zones security-zone trust interfaces ge-0/0/0.0 host-inbound-traffic system-services http

set security zones security-zone trust interfaces ge-0/0/0.0 host-inbound-traffic system-services https

set security zones security-zone trust interfaces ge-0/0/0.0 host-inbound-traffic system-services ssh

set security zones security-zone trust interfaces ge-0/0/0.0 host-inbound-traffic system-services telnet

set security zones security-zone trust interfaces ge-0/0/0.0 host-inbound-traffic system-services dhcp

set security zones security-zone trust interfaces ge-0/0/0.0 host-inbound-traffic system-services all

set security zones security-zone untrust screen untrust-screen

set security zones security-zone untrust host-inbound-traffic protocols all

set security zones security-zone untrust interfaces ge-0/0/1.0 host-inbound-traffic system-services all

set security policies from-zone trust to-zone trust policy default-permit match source-address any

set security policies from-zone trust to-zone trust policy default-permit match destination-address any

set security policies from-zone trust to-zone trust policy default-permit match application any

set security policies from-zone trust to-zone trust policy default-permit then permit

set security policies from-zone trust to-zone untrust policy default-permit match source-address any

set security policies from-zone trust to-zone untrust policy default-permit match destination-address any

set security policies from-zone trust to-zone untrust policy default-permit match application any

set security policies from-zone trust to-zone untrust policy default-permit then permit

set security policies from-zone untrust to-zone trust policy default-deny match source-address any

set security policies from-zone untrust to-zone trust policy default-deny match destination-address any

set security policies from-zone untrust to-zone trust policy default-deny match application any

set security policies from-zone untrust to-zone trust policy default-deny then deny

set security policies default-policy deny-all

set security alg dns disable

set security alg ftp disable

set security alg h323 disable

set security alg mgcp disable

set security alg msrpc disable

set security alg sccp disable

set security alg sql disable

set security alg tftp disable

set security alg pptp disable

set security flow tcp-mss all-tcp mss 1300

set security flow tcp-session no-syn-check

set security flow tcp-session no-sequence-check

set firewall family inet filter filter1 term redirect-to-proxy from destination-port 80

set firewall family inet filter filter1 term redirect-to-proxy then routing-instance redirect

set firewall family inet filter filter1 term default then accept

set firewall family inet filter filter2 term 1 from source-port 80

set firewall family inet filter filter2 term 1 then routing-instance redirect

set firewall family inet filter filter2 term 2 then accept

[edit]

sinha@sinhaFirewaLL#