version 10.4R10.7;

## Last changed: 2012-10-02 11:32:49 UTC

version 10.4R10.7;

system {

host-name Juniper;

authentication-order password;

root-authentication {

encrypted-password "$1$ocItWR2P$bHsiDQGq41m0/0vjSD6i11";

}

name-server {

4.2.2.2;

4.2.2.4;

}

login {

user admin {

uid 2000;

class super-user;

authentication {

encrypted-password "$1$Ib75mnA6$ZqLkEPx4ikafwYoKZ7gvU.";

}

}

user operation {

uid 2001;

class read-only;

authentication {

encrypted-password "$1$tHKxLwoi$f24pd5MPP05HarYJ3QzvA.";

}

}

}

services {

ssh;

web-management {

http {

interface [ ge-0/0/0.0 vlan.0 ];

}

}

}

syslog {

user \* {

any emergency;

}

file messages {

any critical;

authorization info;

}

file interactive-commands {

interactive-commands error;

}

}

max-configurations-on-flash 5;

max-configuration-rollbacks 5;

license {

autoupdate {

url https://ae1.juniper.net/junos/key\_retrieval;

}

}

}

interfaces {

ge-0/0/0 {

unit 0 {

family inet {

address 192.168.2.1/24;

}

}

}

ge-0/0/1 {

unit 0 {

family ethernet-switching;

}

}

ge-0/0/2 {

unit 0 {

family ethernet-switching;

}

}

ge-0/0/3 {

unit 0 {

family ethernet-switching;

}

}

ge-0/0/4 {

description "Vodafone-Leased Line-6M";

unit 0 {

family inet {

address a.a.a.130/29;

}

}

}

ge-0/0/5 {

description NOOR-LeasedLine-6M;

unit 0 {

family inet {

address b.b.b.30/29;

}

}

}

ge-0/0/6 {

description Noor-LeasedLine-2M;

unit 0 {

family inet {

address c.c.c.170/29;

}

}

}

ge-0/0/7 {

description Noor-ADSL-4M;

unit 0 {

family inet {

address d.d.d.2/30;

}

}

}

ge-0/0/8 {

description "TEdata-LeasedLine-2M 65";

unit 0 {

family inet {

address e.e.e.66/29;

}

}

}

ge-0/0/9 {

description "TEdata-LeasedLine-2M 73";

unit 0 {

family inet {

address f.f.f.74/29;

}

}

}

lo0 {

unit 0 {

family inet {

address 127.0.0.1/32;

}

}

}

vlan {

description Internal\_Lan;

unit 0 {

description Internal\_LAN;

family inet {

filter {

input Filter1;

}

address 172.20.1.1/32;

}

}

}

}

routing-options {

interface-routes {

rib-group inet IMPORT-PHY;

}

static {

route c.c.c.168/29 next-hop c.c.c.170;

route b.b.b.24/29 next-hop b.b.b.30;

route d.d.d.0/30 next-hop d.d.d.2;

route e.e.e.64/29 next-hop e.e.e.66;

route f.f.f.72/29 next-hop f.f.f.74;

route 0.0.0.0/0 next-hop c.c.c.169;

}

rib-groups {

IMPORT-PHY {

import-rib [ inet.0 ISP1.inet.0 ISP2.inet.0 ISP3.inet.0 ISP4.inet.0 ISP5.inet.0 ISP6.inet.0 ];

}

}

}

protocols {

isis {

rib-group inet IMPORT-PHY;

interface all;

}

}

security {

nat {

source {

rule-set interface-nat {

from zone trust;

to zone untrust;

rule rule1 {

match {

source-address 0.0.0.0/0;

destination-address 0.0.0.0/0;

}

then {

source-nat {

interface;

}

}

}

}

}

destination {

pool server-1 {

address 172.20.1.7/32 port 80;

}

pool server-2 {

address 172.20.1.7/32 port 3399;

}

pool server-3 {

address 172.20.1.7/32 port 1440;

}

rule-set Port-Forwarding {

from zone untrust;

rule WEB {

match {

destination-address c.c.c.168/30;

destination-port 80;

}

then {

destination-nat pool server-1;

}

}

rule RDP {

match {

destination-address c.c.c.171/32;

destination-port 3399;

}

then {

destination-nat pool server-2;

}

}

rule SQL {

match {

destination-address c.c.c.172/32;

destination-port 1440;

}

then {

destination-nat pool server-3;

}

}

}

}

proxy-arp {

interface ge-0/0/6.0 {

address {

c.c.c.171/32;

c.c.c.172/32;

}

}

}

}

screen {

ids-option untrust-screen {

icmp {

ping-death;

}

ip {

source-route-option;

tear-drop;

}

tcp {

syn-flood {

alarm-threshold 1024;

attack-threshold 200;

source-threshold 1024;

destination-threshold 2048;

queue-size 2000;

timeout 20;

}

land;

}

}

}

zones {

security-zone trust {

tcp-rst;

host-inbound-traffic {

system-services {

any-service;

}

protocols {

all;

}

}

interfaces {

ge-0/0/0.0 {

host-inbound-traffic {

system-services {

http;

https;

ssh;

telnet;

dhcp;

ping;

}

}

}

vlan.0 {

host-inbound-traffic {

system-services {

all;

}

protocols {

all;

}

}

}

ge-0/0/1.0;

ge-0/0/2.0;

ge-0/0/3.0;

}

}

security-zone untrust {

screen untrust-screen;

interfaces {

ge-0/0/4.0;

ge-0/0/5.0;

ge-0/0/6.0;

ge-0/0/7.0;

ge-0/0/8.0;

ge-0/0/9.0;

}

}

}

policies {

from-zone trust to-zone trust {

policy default-permit {

match {

source-address any;

destination-address any;

application any;

}

then {

permit;

}

}

}

from-zone trust to-zone untrust {

policy default-permit {

match {

source-address any;

destination-address any;

application any;

}

then {

permit;

}

}

}

from-zone untrust to-zone trust {

policy HTTP {

match {

source-address any;

destination-address any;

application [ junos-https junos-http RDP1 SQL RDP ];

}

then {

permit {

destination-address {

drop-untranslated;

}

}

}

}

policy default-deny {

match {

source-address any;

destination-address any;

application any;

}

then {

deny;

}

}

}

}

utm {

feature-profile {

anti-virus {

type kaspersky-lab-engine;

}

}

utm-policy UTM-Policy {

anti-virus {

http-profile junos-av-defaults;

}

traffic-options {

sessions-per-client {

over-limit log-and-permit;

}

}

}

}

}

firewall {

family inet {

filter Filter1 {

term NOOR-ADSL-4M {

from {

source-address {

172.20.1.4/32;

}

}

then {

routing-instance ISP4;

}

}

term "Noor-Leased Line-2M" {

from {

source-address {

172.20.1.7/32;

}

}

then {

routing-instance ISP3;

}

}

term Noor-LeasedLine-6M {

from {

source-address {

172.20.1.8/32;

172.20.1.9/32;

172.20.1.10/32;

172.20.1.6/32;

}

}

then {

routing-instance ISP2;

}

}

term "TEdata-Leased Line-2M 65" {

from {

source-address {

172.20.1.11/32;

}

}

then {

routing-instance ISP5;

}

}

term "TEdata-LeasedLine-2M 73" {

from {

source-address {

172.20.1.14/32;

172.20.1.15/32;

172.20.1.16/32;

}

}

then {

routing-instance ISP6;

}

}

term Vodafone-LeaseLine-6M {

from {

source-address {

172.20.1.5/32;

}

}

then {

routing-instance ISP1;

}

}

}

}

}

routing-instances {

ISP1 {

instance-type forwarding;

routing-options {

static {

route 0.0.0.0/0 next-hop a.a.a.129;

route c.c.c.168/29 next-hop c.c.c.170;

route b.b.b.24/29 next-hop b.b.b.30;

route d.d.d.0/30 next-hop d.d.d.2;

route e.e.e.64/29 next-hop e.e.e.66;

route f.f.f.72/29 next-hop f.f.f.74;

route a.a.a.128/29 next-hop a.a.a.130;

}

}

}

ISP2 {

description "Noor-Leased Line-6M";

instance-type forwarding;

routing-options {

static {

route 0.0.0.0/0 next-hop c.c.c.25;

route c.c.c.168/29 next-hop c.c.c.170;

route b.b.b.24/29 next-hop b.b.b.30;

route f.f.f.72/29 next-hop f.f.f.74;

route e.e.e.64/29 next-hop e.e.e.66;

route d.d.d.0/30 next-hop d.d.d.2;

}

}

}

ISP3 {

description Noor-LeasedLine-2M;

instance-type forwarding;

routing-options {

static {

route 0.0.0.0/0 next-hop c.c.c.169;

route c.c.c.168/29 next-hop c.c.c.170;

route b.b.b.24/29 next-hop b.b.b.30;

route e.e.e.64/29 next-hop e.e.e.66;

route f.f.f.72/29 next-hop f.f.f.74;

route d.d.d.0/30 next-hop d.d.d.2;

}

}

}

ISP4 {

description Noor-ADSL-4M;

instance-type forwarding;

routing-options {

static {

route 0.0.0.0/0 next-hop d.d.d.1;

route c.c.c.168/29 next-hop c.c.c.170;

route d.d.d.0/30 next-hop d.d.d.2;

route b.b.b.24/29 next-hop b.b.b.30;

route e.e.e.64/29 next-hop e.e.e.66;

route f.f.f.72/29 next-hop f.f.f.74;

}

}

}

ISP5 {

description "TEdata-Leased Line-2M 65";

instance-type forwarding;

routing-options {

static {

route 0.0.0.0/0 next-hop 196.219.224.65;

route c.c.c.168/29 next-hop c.c.c.170;

route b.b.b.24/29 next-hop b.b.b.30;

route e.e.e.64/29 next-hop e.e.e.66;

route f.f.f.72/29 next-hop f.f.f.74;

route d.d.d.0/30 next-hop d.d.d.2;

}

}

}

ISP6 {

description "TEdata-LeasedLine-2M 73";

instance-type forwarding;

routing-options {

static {

route 0.0.0.0/0 next-hop 196.219.224.73;

route c.c.c.168/29 next-hop c.c.c.170;

route b.b.b.24/29 next-hop b.b.b.30;

route d.d.d.0/30 next-hop d.d.d.2;

route e.e.e.64/29 next-hop e.e.e.66;

route f.f.f.72/29 next-hop f.f.f.74;

}

}

}

LAN {

instance-type forwarding;

routing-options {

static {

route 172.20.1.0/24 next-hop 172.20.1.1;

}

}

}

}

applications {

application RDP {

protocol tcp;

destination-port 3389;

inactivity-timeout 86400;

}

application RDP1 {

protocol tcp;

destination-port 3399;

inactivity-timeout 86400;

}

application SQL {

protocol tcp;

destination-port 1440;

inactivity-timeout 86400;

}

}

vlans {

default {

interface {

ge-0/0/1.0;

ge-0/0/2.0;

ge-0/0/3.0;

}

filter {

input Filter1;

}

l3-interface vlan.0;

}

}