## Last changed: 2014-03-03 20:42:09 UTC

version 12.1X45;

system {

root-authentication {

encrypted-password "$1$V9CRtfiV$C34TvQkEAQ5DBexh2epwQ0";

}

name-server {

208.67.222.222;

208.67.220.220;

}

scripts {

commit {

file templates.xsl;

}

}

services {

ssh;

telnet;

xnm-clear-text;

web-management {

http {

interface vlan.0;

}

https {

system-generated-certificate;

interface vlan.0;

}

}

dhcp {

router {

192.168.1.1;

}

pool 192.168.1.0/24 {

address-range low 192.168.1.2 high 192.168.1.254;

}

propagate-settings ge-0/0/0.0;

}

}

syslog {

archive size 100k files 3;

user \* {

any emergency;

}

file messages {

any critical;

authorization info;

}

file interactive-commands {

interactive-commands error;

}

file idp-attack-event.log {

user info;

match IDP\_ATTACK\_LOG\_EVENT;

archive size 1000k world-readable;

structured-data;

}

}

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 ethernet-switching {

port-mode trunk;

vlan {

members all;

}

}

}

}

ge-0/0/1 {

unit 0 {

family ethernet-switching {

vlan {

members vlan-trust;

}

}

}

}

ge-0/0/2 {

unit 0 {

family ethernet-switching {

vlan {

members vlan-trust;

}

}

}

}

ge-0/0/3 {

unit 0 {

family ethernet-switching {

vlan {

members vlan-trust;

}

}

}

}

ge-0/0/4 {

unit 0 {

family ethernet-switching {

vlan {

members vlan-trust;

}

}

}

}

ge-0/0/5 {

unit 0 {

family ethernet-switching {

vlan {

members vlan-trust;

}

}

}

}

ge-0/0/6 {

unit 0 {

family ethernet-switching {

vlan {

members vlan-trust;

}

}

}

}

ge-0/0/7 {

unit 0 {

family ethernet-switching {

vlan {

members vlan-trust;

}

}

}

}

ge-0/0/8 {

unit 0 {

family ethernet-switching {

port-mode access;

vlan {

members vlan-trust;

}

}

}

}

ge-0/0/9 {

unit 0 {

family ethernet-switching {

vlan {

members vlan-trust;

}

}

}

}

ge-0/0/10 {

unit 0 {

family ethernet-switching {

vlan {

members vlan-trust;

}

}

}

}

ge-0/0/11 {

unit 0 {

family ethernet-switching {

vlan {

members vlan-trust;

}

}

}

}

ge-0/0/12 {

unit 0 {

family ethernet-switching {

vlan {

members vlan-trust;

}

}

}

}

ge-0/0/13 {

unit 0 {

family ethernet-switching {

vlan {

members vlan-trust;

}

}

}

}

ge-0/0/14 {

unit 0 {

family ethernet-switching {

vlan {

members vlan-trust;

}

}

}

}

ge-0/0/15 {

unit 0 {

family ethernet-switching {

vlan {

members vlan-trust;

}

}

}

}

vlan {

unit 0 {

family inet {

address 192.168.8.100/24;

}

}

unit 1 {

family inet {

address 192.168.8.115/24;

}

}

}

}

routing-options {

static {

route 0.0.0.0/0 next-hop 192.168.8.1;

}

}

protocols {

stp;

}

security {

idp {

idp-policy Recommended {

/\* This template policy covers the most important vulnerabilities. Use this template as a base line. \*/

rulebase-ips {

rule 1 {

/\* This rule is designed to protect your networks against important TCP/IP attacks. \*/

match {

from-zone any;

source-address any;

to-zone any;

destination-address any;

application default;

attacks {

predefined-attack-groups [ "[Recommended]IP - Critical" "[Recommended]IP - Minor" "[Recommended]IP - Major" "[Recommended]TCP - Critical" "[Recommended]TCP - Minor" "[Recommended]TCP - Major" ];

}

}

then {

action {

recommended;

}

notification {

log-attacks;

}

}

}

rule 2 {

/\* This rule is designed to protect your network against important ICMP attacks. \*/

match {

from-zone any;

source-address any;

to-zone any;

destination-address any;

application default;

attacks {

predefined-attack-groups [ "[Recommended]ICMP - Major" "[Recommended]ICMP - Minor" ];

}

}

then {

action {

recommended;

}

notification {

log-attacks;

}

}

}

rule 3 {

/\* This rule is designed to protect your network against important HTTP attacks. \*/

match {

from-zone any;

source-address any;

to-zone any;

destination-address any;

application default;

attacks {

predefined-attack-groups [ "[Recommended]HTTP - Critical" "[Recommended]HTTP - Major" "[Recommended]HTTP - Minor" ];

}

}

then {

action {

recommended;

}

notification {

log-attacks;

}

}

}

rule 4 {

/\* This rule is designed to protect your network against important SMTP attacks. \*/

match {

from-zone any;

source-address any;

to-zone any;

destination-address any;

application default;

attacks {

predefined-attack-groups [ "[Recommended]SMTP - Critical" "[Recommended]SMTP - Major" "[Recommended]SMTP - Minor" ];

}

}

then {

action {

recommended;

}

notification {

log-attacks;

}

}

}

rule 5 {

/\* This rule is designed to protect your network against important DNS attacks. \*/

match {

from-zone any;

source-address any;

to-zone any;

destination-address any;

application default;

attacks {

predefined-attack-groups [ "[Recommended]DNS - Critical" "[Recommended]DNS - Minor" "[Recommended]DNS - Major" ];

}

}

then {

action {

recommended;

}

notification {

log-attacks;

}

}

}

rule 6 {

/\* This rule is designed to protect your network against important FTP attacks. \*/

match {

from-zone any;

source-address any;

to-zone any;

destination-address any;

application default;

attacks {

predefined-attack-groups [ "[Recommended]FTP - Critical" "[Recommended]FTP - Minor" "[Recommended]FTP - Major" ];

}

}

then {

action {

recommended;

}

notification {

log-attacks;

}

}

}

rule 7 {

/\* This rule is designed to protect your network against important POP3 attacks. \*/

match {

from-zone any;

source-address any;

to-zone any;

destination-address any;

application default;

attacks {

predefined-attack-groups [ "[Recommended]POP3 - Critical" "[Recommended]POP3 - Minor" "[Recommended]POP3 - Major" ];

}

}

then {

action {

recommended;

}

notification {

log-attacks;

}

}

}

rule 8 {

/\* This rule is designed to protect your network against important IMAP attacks. \*/

match {

from-zone any;

source-address any;

to-zone any;

destination-address any;

application default;

attacks {

predefined-attack-groups [ "[Recommended]IMAP - Critical" "[Recommended]IMAP - Major" ];

}

}

then {

action {

recommended;

}

notification {

log-attacks;

}

}

}

rule 9 {

/\* This rule is designed to protect your network against common internet malware. \*/

match {

from-zone any;

source-address any;

to-zone any;

destination-address any;

application default;

attacks {

predefined-attack-groups [ "[Recommended]TROJAN - Critical" "[Recommended]TROJAN - Major" "[Recommended]TROJAN - Minor" "[Recommended]VIRUS - Critical" "[Recommended]VIRUS - Major" "[Recommended]VIRUS - Minor" "[Recommended]WORM - Critical" "[Recommended]WORM - Major" "[Recommended]WORM - Minor" ];

}

}

then {

action {

recommended;

}

notification {

log-attacks;

}

}

}

rule 0 {

match {

from-zone any;

source-address any;

to-zone any;

destination-address any;

application default;

attacks {

custom-attacks test-attack;

}

}

then {

action {

close-client-and-server;

}

severity critical;

}

}

}

}

active-policy Recommended;

custom-attack test-attack {

recommended-action close;

severity critical;

attack-type {

signature {

context ftp-username;

pattern "\[srxidptestattack\]";

direction any;

}

}

}

}

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;

timeout 20;

}

land;

}

}

}

nat {

source {

rule-set trust-to-untrust {

from zone trust;

to zone untrust;

rule source-nat-rule {

match {

source-address 0.0.0.0/0;

}

then {

source-nat {

interface;

}

}

}

}

}

}

policies {

from-zone trust to-zone untrust {

policy trust-to-untrust {

match {

source-address any;

destination-address any;

application any;

}

then {

permit {

application-services {

idp;

}

}

log {

session-init;

session-close;

}

count;

}

}

}

from-zone untrust to-zone trust {

policy untrust-to-trust {

match {

source-address any;

destination-address any;

application any;

}

then {

permit {

application-services {

idp;

}

}

log {

session-init;

session-close;

}

count;

}

}

}

}

zones {

security-zone trust {

host-inbound-traffic {

system-services {

all;

}

protocols {

all;

}

}

interfaces {

vlan.0;

ge-0/0/8.0;

}

}

security-zone untrust {

screen untrust-screen;

host-inbound-traffic {

system-services {

all;

}

protocols {

all;

}

}

interfaces {

ge-0/0/0.0 {

host-inbound-traffic {

system-services {

dhcp;

tftp;

}

}

}

}

}

}

}

vlans {

BEL {

vlan-id 40;

l3-interface vlan.1;

}

vlan-trust {

vlan-id 3;

l3-interface vlan.0;

}

}