## Last changed: 2014-02-19 16:21:30 UTC

version 12.1X45;

system {

root-authentication {

encrypted-password "$1$1iCY6uQZ$YyBf609c.A2PfLq87Edgk.";

}

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;

}

host 192.168.10.110 {

any any;

match RT\_ID;

}

file messages {

any error;

authorization info;

}

file interactive-commands {

interactive-commands error;

}

file traffic-log {

any any;

match RT\_FLOW\_SESSION;

}

file IDP-Log {

any any;

match RT\_ID;

}

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;

}

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 {

port-mode trunk;

vlan {

members all;

}

}

}

}

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 192.168.10.100/24;

}

}

unit 1 {

family inet {

address 192.168.10.115/24;

}

}

}

}

routing-options {

static {

route 0.0.0.0/0 next-hop 192.168.10.1;

}

}

protocols {

stp;

}

security {

log {

utc-timestamp;

mode stream;

source-address 192.168.10.100;

stream build {

format sd-syslog;

host {

192.168.10.110;

}

}

}

idp {

idp-policy Web\_Server {

/\* This template policy is designed to protect commonly used HTTP servers from remote attacks. \*/

rulebase-ips {

rule 1 {

/\* This rule drops all packets that should not occur on a clean network, and can be used by attackers to evade IDSs. This rule is necessary to harden the IDP against evasion attempts. \*/

match {

from-zone any;

source-address any;

to-zone any;

destination-address any;

application default;

attacks {

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

}

}

then {

action {

drop-packet;

}

notification {

log-attacks;

}

}

}

rule 2 {

/\* This rule drops all DNS and DHCP packets that contain critical severity attacks and logs them as alarms. Enable this rule if you are running your IDP in "in-line" mode, and wish to protect your network against critical DNS and DHCP attacks. \*/

match {

from-zone any;

source-address any;

to-zone any;

destination-address any;

application default;

attacks {

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

}

}

then {

action {

drop-packet;

}

notification {

log-attacks;

}

}

}

rule 3 {

/\* This rule drops critical and high severity attacks against common web and IIS services and logs them as alarms. Enable this rule if you are running your IDP in "in-line" mode, and wish to protect your network against critical and high severity attacks. \*/

match {

from-zone any;

source-address any;

to-zone any;

destination-address any;

application default;

attacks {

predefined-attack-groups [ "FINGER - Critical" "FINGER - Major" "GOPHER - Critical" "GOPHER - Major" "FTP - Critical" "FTP - Major" "HTTP - Critical" "HTTP - Major" "SHELLCODE - Major" "SHELLCODE - Critical" "NNTP - Critical" "NNTP - Major" ];

}

}

then {

action {

drop-packet;

}

notification {

log-attacks;

}

}

}

rule 4 {

/\* This rule logs medium severity attacks. Enable this rule if you are running your IDP in "in-line" mode, and wish to monitor your network for attacks and IDS evasion attempts. \*/

match {

from-zone any;

source-address any;

to-zone any;

destination-address any;

application default;

attacks {

predefined-attack-groups [ "DNS - Minor" "FINGER - Minor" "FTP - Minor" "GOPHER - Minor" "HTTP - Minor" "NNTP - Minor" "SHELLCODE - Minor" ];

}

}

then {

action {

no-action;

}

notification {

log-attacks;

}

}

}

inactive: rule 5 {

/\* This rule logs low severity attacks. The rule is disabled by default, as some networks contain many low severity events, which results in many logs. \*/

match {

from-zone any;

source-address any;

to-zone any;

destination-address any;

application default;

attacks {

predefined-attack-groups [ "Anomaly - Warning" "Signature - Warning" ];

}

}

then {

action {

no-action;

}

notification {

log-attacks;

}

}

}

inactive: rule 6 {

/\* This rule logs informational events. This rule is disabled by default as it generates many logs. Informational signatures are included not to necessarily detect attacks, but to provide additional understanding of your network's traffic. \*/

match {

from-zone any;

source-address any;

to-zone any;

destination-address any;

application default;

attacks {

predefined-attack-groups [ "Anomaly - Info" "Signature - Info" ];

}

}

then {

action {

no-action;

}

notification {

log-attacks;

}

}

}

}

}

idp-policy DMZ\_Services {

/\* This template policy is designed to be used to protect a typical DMZ environment. \*/

rulebase-ips {

rule 1 {

/\* This rule drops all packets that should not occur on a clean network, and can be used by attackers to evade IDSs. This rule is necessary to harden the IDP against evasion attempts. \*/

match {

from-zone any;

source-address any;

to-zone any;

destination-address any;

application default;

attacks {

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

}

}

then {

action {

drop-packet;

}

notification {

log-attacks {

alert;

}

}

}

}

rule 2 {

/\* This rule drops all DNS and DHCP packets that contain critical severity attacks and logs them as alarms. Enable this rule if you are running your IDP in \"in-line\" mode, and wish to protect your network against critical DNS and DHCP attacks. \*/

match {

from-zone any;

source-address any;

to-zone any;

destination-address any;

application default;

attacks {

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

}

}

then {

action {

drop-packet;

}

notification {

log-attacks {

alert;

}

}

}

}

rule 3 {

/\* This rule drops critical and high severity attacks against common DMZ services and logs them as alarms. Enable this rule if you are running your IDP in \"in-line\" mode, and wish to protect your network against critical and high severity attacks. \*/

match {

from-zone any;

source-address any;

to-zone any;

destination-address any;

application default;

attacks {

predefined-attack-groups [ "FINGER - Critical" "FINGER - Major" "GOPHER - Critical" "GOPHER - Major" "FTP - Critical" "FTP - Major" "HTTP - Critical" "HTTP - Major" "SHELLCODE - Major" "SHELLCODE - Critical" "NNTP - Critical" "NNTP - Major" "IMAP - Critical" "IMAP - Major" "POP3 - Critical" "POP3 - Major" "SMTP - Critical" "SMTP - Major" "SSH - Critical" "SSH - Major" ];

}

}

then {

action {

drop-packet;

}

notification {

log-attacks {

alert;

}

}

}

}

rule 4 {

/\* This rule logs medium severity attacks. Enable this rule if you are running your IDP in "in-line" mode, and wish to monitor your network for attacks and IDS evasion attempts. \*/

match {

from-zone any;

source-address any;

to-zone any;

destination-address any;

application default;

attacks {

predefined-attack-groups [ "FINGER - Minor" "FTP - Minor" "GOPHER - Minor" "HTTP - Minor" "IMAP - Minor" "NNTP - Minor" "POP3 - Minor" "SHELLCODE - Minor" "SMTP - Minor" "SSH - Minor" ];

}

}

then {

action {

no-action;

}

notification {

log-attacks;

}

}

}

inactive: rule 5 {

/\* This rule logs low severity attacks. The rule is disabled by default, as some networks contain many low severity events, which results in many logs. \*/

match {

from-zone any;

source-address any;

to-zone any;

destination-address any;

application default;

attacks {

predefined-attack-groups [ "Anomaly - Warning" "Signature - Warning" ];

}

}

then {

action {

no-action;

}

notification {

log-attacks;

}

}

}

inactive: rule 6 {

/\* This rule logs informational events. This rule is disabled by default as it generates many logs. Informational signatures are included not to necessarily detect attacks, but to provide additional understanding of your network's traffic. \*/

match {

from-zone any;

source-address any;

to-zone any;

destination-address any;

application default;

attacks {

predefined-attack-groups [ "Anomaly - Info" "Signature - Info" ];

}

}

then {

action {

no-action;

}

notification {

log-attacks;

}

}

}

}

}

idp-policy DNS\_Service {

/\* This template policy is designed to protect DNS services. Use this template as a starting point to customize your desired level of protection. \*/

rulebase-ips {

rule 1 {

/\* This rule drops all packets that should not occur on a clean network, and can be used by attackers to evade IDSs. This rule is necessary to harden the IDP against evasion attempts. \*/

match {

from-zone any;

source-address any;

to-zone any;

destination-address any;

application default;

attacks {

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

}

}

then {

action {

drop-packet;

}

notification {

log-attacks {

alert;

}

}

}

}

rule 2 {

/\* This rule drops all DNS and DHCP packets that contain critical severity attacks and logs them as alarms. Enable this rule if you are running your IDP in "in-line" mode, and wish to protect your network against critical DNS and DHCP attacks. \*/

match {

from-zone any;

source-address any;

to-zone any;

destination-address any;

application default;

attacks {

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

}

}

then {

action {

drop-packet;

}

notification {

log-attacks {

alert;

}

}

}

}

rule 3 {

/\* This rule logs medium severity DNS attacks. Enable this rule to investigate possible threats against Domain Name Services. \*/

match {

from-zone any;

source-address any;

to-zone any;

destination-address any;

application default;

attacks {

predefined-attack-groups "DNS - Minor";

}

}

then {

action {

no-action;

}

notification {

log-attacks;

}

}

}

inactive: rule 4 {

/\* This rule logs low severity attacks. The rule is disabled by default, as some networks contain many low severity events, which results in many logs. \*/

match {

from-zone any;

source-address any;

to-zone any;

destination-address any;

application default;

attacks {

predefined-attack-groups [ "Anomaly - Warning" "Signature - Warning" ];

}

}

then {

action {

no-action;

}

notification {

log-attacks;

}

}

}

inactive: rule 5 {

/\* This rule logs informational events. This rule is disabled by default as it generates many logs. Informational signatures are included not to necessarily detect attacks, but to provide additional understanding of your network's traffic. \*/

match {

from-zone any;

source-address any;

to-zone any;

destination-address any;

application default;

attacks {

predefined-attack-groups [ "Anomaly - Info" "Signature - Info" ];

}

}

then {

action {

no-action;

}

notification {

log-attacks;

}

}

}

}

}

idp-policy File\_Server {

/\* This template policy is designed to provide protection to various file sharing services such as AMB, NFS, FTP, and others. \*/

rulebase-ips {

rule 1 {

/\* This rule drops all packets that should not occur on a clean network, and can be used by attackers to evade IDSs. This rule is necessary to harden the IDP against evasion attempts. \*/

match {

from-zone any;

source-address any;

to-zone any;

destination-address any;

application default;

attacks {

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

}

}

then {

action {

drop-packet;

}

notification {

log-attacks {

alert;

}

}

}

}

rule 2 {

/\* This rule drops all DNS and DHCP packets that contain critical severity attacks and logs them as alarms. Enable this rule if you are running your IDP in \"in-line\" mode, and wish to protect your network against critical DNS and DHCP attacks. \*/

match {

from-zone any;

source-address any;

to-zone any;

destination-address any;

application default;

attacks {

predefined-attack-groups [ "DNS - Critical" "DNS - Major" "DHCP - Critical" "DHCP - Major" "SHELLCODE - Critical" "SHELLCODE - Major" ];

}

}

then {

action {

drop-packet;

}

notification {

log-attacks {

alert;

}

}

}

}

rule 3 {

/\* This rule drops critical and high severity attacks against common DMZ services and logs them as alarms. Enable this rule if you are running your IDP in "in-line" mode, and wish to protect your network against critical and high severity attacks. \*/

match {

from-zone any;

source-address any;

to-zone any;

destination-address any;

application default;

attacks {

predefined-attack-groups [ "FTP - Critical" "FTP - Major" "SSH - Critical" "SSH - Major" "NFS - Critical" "NFS - Major" "PORTMAPPER - Critical" "PORTMAPPER - Major" "RPC - Critical" "RPC - Major" "SMB - Critical" "SMB - Major" "MS-RPC - Critical" "MS-RPC - Major" "NETBIOS - Critical" "NETBIOS - Major" "TFTP - Critical" "TFTP - Major" ];

}

}

then {

action {

drop-packet;

}

notification {

log-attacks {

alert;

}

}

}

}

rule 4 {

/\* This rule logs medium severity file service attacks. Enable this rule to investigate possible threats against file sharing services. \*/

match {

from-zone any;

source-address any;

to-zone any;

destination-address any;

application default;

attacks {

predefined-attack-groups [ "FTP - Minor" "SSH - Minor" "MS-RPC - Minor" "NETBIOS - Minor" "NFS - Minor" "PORTMAPPER - Minor" "RPC - Minor" "SMB - Minor" "TFTP - Minor" ];

}

}

then {

action {

no-action;

}

notification {

log-attacks;

}

}

}

inactive: rule 5 {

/\* This rule logs low severity attacks. The rule is disabled by default, as some networks contain many low severity events, which results in many logs. \*/

match {

from-zone any;

source-address any;

to-zone any;

destination-address any;

application default;

attacks {

predefined-attack-groups [ "Anomaly - Warning" "Signature - Warning" ];

}

}

then {

action {

no-action;

}

notification {

log-attacks;

}

}

}

inactive: rule 6 {

/\* This rule logs informational events. This rule is disabled by default as it generates many logs. Informational signatures are included not to necessarily detect attacks, but to provide additional understanding of your network's traffic. \*/

match {

from-zone any;

source-address any;

to-zone any;

destination-address any;

application default;

attacks {

predefined-attack-groups [ "Anomaly - Info" "Signature - Info" ];

}

}

then {

action {

no-action;

}

notification {

log-attacks;

}

}

}

}

}

idp-policy Getting\_Started {

/\* This template is a good starting point for learning how to create IDP policies. \*/

rulebase-ips {

rule 10 {

match {

from-zone any;

source-address any;

to-zone any;

destination-address any;

application default;

attacks {

predefined-attacks [ ICMP:INFO:ECHO-REPLY ICMP:INFO:ECHO-REQUEST ];

}

}

then {

action {

drop-packet;

}

notification {

log-attacks {

alert;

}

}

severity critical;

}

}

rule 1 {

match {

from-zone any;

source-address any;

to-zone any;

destination-address any;

application default;

attacks {

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

}

}

then {

action {

no-action;

}

notification {

log-attacks;

}

}

}

rule 2 {

match {

from-zone any;

source-address any;

to-zone any;

destination-address any;

application default;

attacks {

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

}

}

then {

action {

no-action;

}

notification {

log-attacks;

}

}

}

rule 3 {

match {

from-zone any;

source-address any;

to-zone any;

destination-address any;

application default;

attacks {

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

}

}

then {

action {

no-action;

}

notification {

log-attacks;

}

}

}

rule 4 {

match {

from-zone any;

source-address any;

to-zone any;

destination-address any;

application default;

attacks {

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

}

}

then {

action {

no-action;

}

notification {

log-attacks;

}

}

}

rule 5 {

match {

from-zone any;

source-address any;

to-zone any;

destination-address any;

application default;

attacks {

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

}

}

then {

action {

no-action;

}

notification {

log-attacks;

}

}

}

rule 6 {

match {

from-zone any;

source-address any;

to-zone any;

destination-address any;

application default;

attacks {

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

}

}

then {

action {

no-action;

}

notification {

log-attacks;

}

}

}

rule 7 {

match {

from-zone any;

source-address any;

to-zone any;

destination-address any;

application default;

attacks {

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

}

}

then {

action {

no-action;

}

notification {

log-attacks;

}

}

}

rule 8 {

match {

from-zone any;

source-address any;

to-zone any;

destination-address any;

application default;

attacks {

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

}

}

then {

action {

no-action;

}

notification {

log-attacks;

}

}

}

rule 9 {

match {

from-zone any;

source-address any;

to-zone any;

destination-address any;

application default;

attacks {

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

}

}

then {

action {

no-action;

}

notification {

log-attacks;

}

}

}

}

}

idp-policy IDP\_Default {

/\* This template policy represents a good blend od security and performance. Use this template for "in-line" mode. \*/

rulebase-ips {

rule 1 {

/\* This rule drops all packets that should not occur on a clean network, and can be used by attackers to evade IDSs. This rule is necessary to harden the IDP against evasion attempts. \*/

match {

from-zone any;

source-address any;

to-zone any;

destination-address any;

application default;

attacks {

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

}

}

then {

action {

drop-packet;

}

notification {

log-attacks {

alert;

}

}

severity info;

}

}

rule 2 {

/\* This rule drops high severity attacks and logs them as alarms. Enable this rule if you are running your IDP in "in-line" mode, and wish to protect your network against critical attacks and IDS evasion attempts. \*/

match {

from-zone any;

source-address any;

to-zone any;

destination-address any;

application default;

attacks {

predefined-attack-groups [ "DB - Critical" "DB - Major" "DDOS - Critical" "DDOS - Major" "DHCP - Critical" "DHCP - Major" "DNS - Critical" "DNS - Major" "DOS - Critical" "DOS - Major" "FTP - Critical" "FTP - Major" "HTTP - Critical" "HTTP - Major" "ICMP - Critical" "ICMP - Major" "IMAP - Critical" "IMAP - Major" "NETBIOS - Critical" "NETBIOS - Major" "MS-RPC - Critical" "MS-RPC - Major" "NFS - Critical" "NFS - Major" "POP3 - Critical" "POP3 - Major" "PORTMAPPER - Critical" "PORTMAPPER - Major" "RPC - Critical"

"RPC - Major" "SCAN - Critical" "SCAN - Major" "SHELLCODE - Critical" "SHELLCODE - Major" "SMB - Critical" "SMB - Major" "SMTP - Critical" "SMTP - Major" "SSH - Critical" "SSH - Major" "TELNET - Critical" "TELNET - Major" "TROJAN - Critical" "TROJAN - Major" "WORM - Critical" "WORM - Major" "APP - Critical" "APP - Major" ];

}

}

then {

action {

drop-packet;

}

notification {

log-attacks {

alert;

}

}

severity info;

}

}

rule 3 {

/\* This rule logs medium severity attacks. Enable this rule if you are running your IDP in "in-line" mode, and wish to monitor your network for attacks and IDS evasion attempts. \*/

match {

from-zone any;

source-address any;

to-zone any;

destination-address any;

application default;

attacks {

predefined-attack-groups [ "DB - Minor" "DDOS - Minor" "DHCP - Minor" "DNS - Minor" "DOS - Minor" "FTP - Minor" "HTTP - Minor" "ICMP - Minor" "IMAP - Minor" "NETBIOS - Minor" "MS-RPC - Minor" "NFS - Minor" "POP3 - Minor" "PORTMAPPER - Minor" "RPC - Minor" "SCAN - Minor" "SHELLCODE - Minor" "SMB - Minor" "SMTP - Minor" "SSH - Minor" "TELNET - Minor" "TROJAN - Minor" "WORM - Minor" "APP - Minor" ];

}

}

then {

action {

no-action;

}

notification {

log-attacks;

}

severity info;

}

}

inactive: rule 4 {

/\* This rule logs low severity attacks. The rule is disabled by default, as some networks contain many low severity events, which results in many logs. \*/

match {

from-zone any;

source-address any;

to-zone any;

destination-address any;

application default;

attacks {

predefined-attack-groups [ "Anomaly - Warning" "Signature - Warning" ];

}

}

then {

action {

no-action;

}

notification {

log-attacks;

}

}

}

inactive: rule 5 {

/\* This rule logs informational events. This rule is disabled by default as it generates many logs. Informational signatures are included not to necessarily detect attacks, but to provide additional understanding of your network's traffic. \*/

match {

from-zone any;

source-address any;

to-zone any;

destination-address any;

application default;

attacks {

predefined-attack-groups [ "Anomaly - Info" "Signature - Info" ];

}

}

then {

action {

no-action;

}

notification {

log-attacks;

}

}

}

}

}

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;

}

}

}

}

}

idp-policy ICMP-TEST {

rulebase-ips {

rule 2 {

match {

from-zone any;

source-address any;

to-zone any;

destination-address any;

application any;

}

then {

action {

drop-packet;

}

notification {

log-attacks {

alert;

}

}

severity critical;

}

}

}

}

idp-policy PING {

rulebase-ips {

rule 10 {

match {

from-zone any;

source-address any;

to-zone any;

destination-address any;

application default;

attacks {

predefined-attacks [ ICMP:INFO:ECHO-REPLY ICMP:INFO:ECHO-REQUEST ];

}

}

then {

action {

drop-packet;

}

notification {

log-attacks {

alert;

}

}

severity critical;

}

}

}

}

active-policy ICMP-TEST;

}

application-tracking;

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 new\_trust-to-untrust {

match {

source-address any;

destination-address any;

application junos-icmp-all;

}

then {

deny;

log {

session-init;

session-close;

}

count;

}

}

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 comms to-zone lan {

policy new\_pol1 {

match {

source-address any;

destination-address any;

application junos-icmp-all;

}

then {

deny;

log {

session-init;

session-close;

}

count;

}

}

policy pol1 {

match {

source-address any;

destination-address any;

application any;

}

then {

permit {

application-services {

idp;

}

}

log {

session-init;

session-close;

}

count;

}

}

}

from-zone lan to-zone comms {

policy new\_pol2 {

match {

source-address any;

destination-address any;

application junos-icmp-all;

}

then {

deny;

log {

session-init;

session-close;

}

count;

}

}

policy pol2 {

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;

}

application-tracking;

}

security-zone untrust {

screen untrust-screen;

interfaces {

ge-0/0/0.0 {

host-inbound-traffic {

system-services {

dhcp;

tftp;

}

}

}

}

application-tracking;

}

security-zone comms {

screen untrust-screen;

host-inbound-traffic {

system-services {

all;

ping {

except;

}

}

protocols {

all;

}

}

interfaces {

ge-0/0/7.0;

}

application-tracking;

}

security-zone lan {

host-inbound-traffic {

system-services {

all;

ping {

except;

}

}

protocols {

all;

}

}

interfaces {

ge-0/0/8.0;

}

application-tracking;

}

}

}

vlans {

bel {

vlan-id 40;

l3-interface vlan.1;

}

vlan-trust {

vlan-id 3;

l3-interface vlan.0;

}

}