---------------------------------------------------------------------------

-- Snort++ configuration

---------------------------------------------------------------------------

-- there are over 200 modules available to tune your policy.

-- many can be used with defaults w/o any explicit configuration.

-- use this conf as a template for your specific configuration.

-- 1. configure defaults

-- 2. configure inspection

-- 3. configure bindings

-- 4. configure performance

-- 5. configure detection

-- 6. configure filters

-- 7. configure outputs

-- 8. configure tweaks

---------------------------------------------------------------------------

-- 1. configure defaults

---------------------------------------------------------------------------

-- HOME\_NET and EXTERNAL\_NET must be set now

-- setup the network addresses you are protecting

HOME\_NET = 'Replace with your network' / ‘any’ –was eth0 in my case

-- set up the external network addresses.

-- (leave as "any" in most situations)

EXTERNAL\_NET = 'any'

include 'snort\_defaults.lua'

---------------------------------------------------------------------------

-- 2. configure inspection

---------------------------------------------------------------------------

-- mod = { } uses internal defaults

-- you can see them with snort --help-module mod

-- mod = default\_mod uses external defaults

-- you can see them in snort\_defaults.lua

-- the following are quite capable with defaults:

stream = { }

stream\_ip = { }

stream\_icmp = { }

stream\_tcp = { }

stream\_udp = { }

stream\_user = { }

stream\_file = { }

arp\_spoof = { }

back\_orifice = { }

dns = { }

imap = { }

netflow = {}

normalizer = { }

pop = { }

rpc\_decode = { }

sip = { }

ssh = { }

ssl = { }

telnet = { }

cip = { }

dnp3 = { }

iec104 = { }

mms = { }

modbus = { }

s7commplus = { }

dce\_smb = { }

dce\_tcp = { }

dce\_udp = { }

dce\_http\_proxy = { }

dce\_http\_server = { }

-- see snort\_defaults.lua for default\_\*

gtp\_inspect = default\_gtp

port\_scan = default\_med\_port\_scan

smtp = default\_smtp

ftp\_server = default\_ftp\_server

ftp\_client = { }

ftp\_data = { }

http\_inspect = { }

http2\_inspect = { }

-- see file\_magic.rules for file id rules

file\_id = { rules\_file = 'file\_magic.rules' }

file\_policy = { }

js\_norm = default\_js\_norm

-- the following require additional configuration to be fully effective:

appid =

{

-- appid requires this to use appids in rules

--app\_detector\_dir = 'directory to load appid detectors from'

}

--[[

reputation =

{

-- configure one or both of these, then uncomment reputation

-- (see also related path vars at the top of snort\_defaults.lua)

--blacklist = 'blacklist file name with ip lists'

--whitelist = 'whitelist file name with ip lists'

}

--]]

---------------------------------------------------------------------------

-- 3. configure bindings

---------------------------------------------------------------------------

wizard = default\_wizard

binder =

{

-- port bindings required for protocols without wizard support

{ when = { proto = 'udp', ports = '53', role='server' }, use = { type = 'dns' } },

{ when = { proto = 'tcp', ports = '53', role='server' }, use = { type = 'dns' } },

{ when = { proto = 'tcp', ports = '111', role='server' }, use = { type = 'rpc\_decode' } },

{ when = { proto = 'tcp', ports = '502', role='server' }, use = { type = 'modbus' } },

{ when = { proto = 'tcp', ports = '2123 2152 3386', role='server' }, use = { type = 'gtp\_inspect' } },

{ when = { proto = 'tcp', ports = '2404', role='server' }, use = { type = 'iec104' } },

{ when = { proto = 'udp', ports = '2222', role = 'server' }, use = { type = 'cip' } },

{ when = { proto = 'tcp', ports = '44818', role = 'server' }, use = { type = 'cip' } },

{ when = { proto = 'tcp', service = 'dcerpc' }, use = { type = 'dce\_tcp' } },

{ when = { proto = 'udp', service = 'dcerpc' }, use = { type = 'dce\_udp' } },

{ when = { proto = 'udp', service = 'netflow' }, use = { type = 'netflow' } },

{ when = { service = 'netbios-ssn' }, use = { type = 'dce\_smb' } },

{ when = { service = 'dce\_http\_server' }, use = { type = 'dce\_http\_server' } },

{ when = { service = 'dce\_http\_proxy' }, use = { type = 'dce\_http\_proxy' } },

{ when = { service = 'cip' }, use = { type = 'cip' } },

{ when = { service = 'dnp3' }, use = { type = 'dnp3' } },

{ when = { service = 'dns' }, use = { type = 'dns' } },

{ when = { service = 'ftp' }, use = { type = 'ftp\_server' } },

{ when = { service = 'ftp-data' }, use = { type = 'ftp\_data' } },

{ when = { service = 'gtp' }, use = { type = 'gtp\_inspect' } },

{ when = { service = 'imap' }, use = { type = 'imap' } },

{ when = { service = 'http' }, use = { type = 'http\_inspect' } },

{ when = { service = 'http2' }, use = { type = 'http2\_inspect' } },

{ when = { service = 'iec104' }, use = { type = 'iec104' } },

{ when = { service = 'mms' }, use = { type = 'mms' } },

{ when = { service = 'modbus' }, use = { type = 'modbus' } },

{ when = { service = 'pop3' }, use = { type = 'pop' } },

{ when = { service = 'ssh' }, use = { type = 'ssh' } },

{ when = { service = 'sip' }, use = { type = 'sip' } },

{ when = { service = 'smtp' }, use = { type = 'smtp' } },

{ when = { service = 'ssl' }, use = { type = 'ssl' } },

{ when = { service = 'sunrpc' }, use = { type = 'rpc\_decode' } },

{ when = { service = 's7commplus' }, use = { type = 's7commplus' } },

{ when = { service = 'telnet' }, use = { type = 'telnet' } },

{ use = { type = 'wizard' } }

}

---------------------------------------------------------------------------

-- 4. configure performance

---------------------------------------------------------------------------

-- use latency to monitor / enforce packet and rule thresholds

--latency = { }

-- use these to capture perf data for analysis and tuning

--profiler = { }

--perf\_monitor = { }

---------------------------------------------------------------------------

-- 5. configure detection

---------------------------------------------------------------------------

references = default\_references

classifications = default\_classifications

ips =

{

enable\_builtin\_rules = true,

-- use this to enable decoder and inspector alerts

--enable\_builtin\_rules = true,

-- use include for rules files; be sure to set your path

-- note that rules files can include other rules files

-- (see also related path vars at the top of snort\_defaults.lua)

rules = [[

include /etc/snort/rules/local.rules

]],

variables = default\_variables

}

-- use these to configure additional rule actions

-- react = { }

-- reject = { }

-- use this to enable payload injection utility

-- payload\_injector = { }

---------------------------------------------------------------------------

-- 6. configure filters

---------------------------------------------------------------------------

-- below are examples of filters

-- each table is a list of records

--[[

suppress =

{

-- don't want to any of see these

{ gid = 1, sid = 1 },

-- don't want to see anything for a given host

{ track = 'by\_dst', ip = '1.2.3.4' }

-- don't want to see these for a given host

{ gid = 1, sid = 2, track = 'by\_dst', ip = '1.2.3.4' },

}

--]]

--[[

event\_filter =

{

-- reduce the number of events logged for some rules

{ gid = 1, sid = 1, type = 'limit', track = 'by\_src', count = 2, seconds = 10 },

{ gid = 1, sid = 2, type = 'both', track = 'by\_dst', count = 5, seconds = 60 },

}

--]]

--[[

rate\_filter =

{

-- alert on connection attempts from clients in SOME\_NET

{ gid = 135, sid = 1, track = 'by\_src', count = 5, seconds = 1,

new\_action = 'alert', timeout = 4, apply\_to = '[$SOME\_NET]' },

-- alert on connections to servers over threshold

{ gid = 135, sid = 2, track = 'by\_dst', count = 29, seconds = 3,

new\_action = 'alert', timeout = 1 },

}

--]]

---------------------------------------------------------------------------

-- 7. configure outputs

---------------------------------------------------------------------------

-- event logging

-- you can enable with defaults from the command line with -A <alert\_type>

-- uncomment below to set non-default configs

--alert\_csv = { }

alert\_fast = {

file = true,

}

--alert\_full = { }

--alert\_sfsocket = { }

--alert\_syslog = { }

--unified2 = { }

-- packet logging

-- you can enable with defaults from the command line with -L <log\_type>

--log\_codecs = { }

--log\_hext = { }

--log\_pcap = { }

-- additional logs

--packet\_capture = { }

--file\_log = { }

---------------------------------------------------------------------------

-- 8. configure tweaks

---------------------------------------------------------------------------

if ( tweaks ~= nil ) then

include(tweaks .. '.lua')

end