Snort Rule Guide

header example:

alert	tcp	any	any	->	192.168.1.1	8080
<rule action>	**<protocol>**	**<1st IP>**	**<1st port>**	**<directional operator>**	**<2nd IP>**	**<2nd port>**
pass	tcp	any	any (use any for icmp traffic)	->		
alert	udp	1.1.1.1/##	22	<> ok but too broad		
log	icmp	!1.1.1.1/##	8000:9000	-> invalid, not needed		
activate \/ p. 2.124	ip	[1.1.1.1, 2.2.2.2]	!22			
dynamic ^	future:	variables defined in config file	:22 (gt)			
drop (also logs)	arp	* $EXTERNAL	22: (lt)			
reject (resets sent)	http	* $DNS_SERVER				
sdrop (silent - no log)	802.11	config syntax: var DMZ 1.1.1.1/24				
define your own in config file						
more header examples:						
log	udp	any	any	->	[1.2.2.2, 2.2.2.2]	21974
alert	tcp	$EXTERNAL	any	->	$INTERNAL	79

rule options:

general/metadata	**payload**	**nonpayload**	**post-detection**
sid: 123;	content: "string to match"; //Boyer-Moore	flags: +SA; //match if both SYN/ACK	resp: rst_rcv; //_snd, _all
rev: 23;	content: "|de ad be ef|"; //binary in HEX	flags: !F; // match if not FIN	resp: icmp_all; //_net, _port, _host
msg: "some text";	offset: 32; //where to start	flags: *SAFP; //match if any	react: block
reference: id_system, id; //knows id URLs	depth: 256; //how far to go	flags: *SA, F; //match S or A, ignore F	logto: outputfile.txt;
classtype: attempted-dos;	within: 32; //matches must be this close	fragoffset: < 120;	session: all; //captures tcp stream
priority: ##;	distance: 32; //matches must be apart	fragbits: +M; //match if more frag set	session: printable; //captures ASCII
	nocase;	fragbits: -; //match if any bits set	tag: session, 23, packets; //logs 23 packets of session
	rawbytes;	fragbits: !; //match if no bits set	tag: host, 32, seconds; //logs 32 seconds worth of host packets
	uricontent: pattern; //normalizes URI then		
	searches for pattern	ip_proto: <name or num>;	threshold: type, track, count, seconds
	isdataat: ##; //true/false	ttl: >64; // or =, <, 1-10	
	flow: to_server,established;	tos: <num>;	
	pcre: "/regex/";	id: 32233; //ip id field	
		ipopts: nop; //many on p. 2.134	
		ack: 22;	
		seq: 22;	
		dsize: 22 <> 54; \\range or just < or >	
		icode: < 5; \\or range, icmp field	
		icmp_id: 123;	
		icmp_seq: 123;	
		sameip; \\if src and dst ip same (LAND)	

Snort Rule Guide

Examples with options:

1) alert icmp 1.1.1.1/24 any -> 2.2.2.2 any (msg:"ICMP traffic"; classtype:misc-attack; sid:100;rev:1;)

2) alert tcp 1.1.1.1/24 23 <> 1.1.1.1/24 23 (msg:"Using Telnet"; classtype:misc-attack; sid:100; rev:1;)

3) log tcp any any -> 1.1.1.1 80 (msg:"HTTP Request"; content:"index.htm";classtype:misc-attack;sid:101;rev:1;)

4) alert tcp 1.1.1.1/24 any -> 2.2.2.2 80 (msg:"adobe reader malicious URL null byte"; flow: to_server,established; uricontent:".pdf|00|"; nocase; reference:url,idefense.com/application/poi/display?id=126&type=vulnerabilities; reference:cve,2004-0629; classtype:attempted-admin; sid:2001217; rev:7;)

5) alert tcp any any -> 1.1.1.1 80 (msg:"HTTP bad word request"; flow: from_server,established; content:"hacking";nocase; classtype:policy-violation;sid:100;rev:1;)

6) alert tcp 1.1.1.1/24 any -> any 139 (msg:"BugBear@MM worm copied to startup folder"; flow: established; content:"|77 00 69 00 6B 00 2E 00 65 00 78 00 65 00 00 00|"; reference:url,www.symantec.com/avcenter/venc/data/w32.bugbear@mm.html; classtype:misc-activity; sid: 2001766;rev:4;)

7) alert tcp 1.1.1.1/24 any -> any 80 (msg:"Outlook Exploit Detected"; flow: from_server,established; content:"mailto:"; content:"&quote";nocase;classtype:misc-attack;sid:101;rev:1;)

8) log ip [1.1.1.1, 2.2.2.2] any -> 3.3.3.3/24 any (msg:"Detected a known bad host"; sid:100;rev:1;)

9a) activate tcp 1.1.1.1/24 any -> 1.1.1.1/24 143 (msg:"IMAP buffer overflow"; flags:PA; content:"\E8C0FFFFFF|/bin"; activates:1;)

9b) dynamic tcp 1.1.1.1/24 any -> 1.1.1.1/24 143 (activated_by:1; count:64;)

10) alert tcp 1.1.1.1/24 any -> any 6000: (msg:"X-Windows sessions"; flow: from_server,established; nocase; classtype:misc-attack;sid:101;rev;1;)

11) alert tcp any any -> 1.1.1.1/24 110 (msg:"Rapid POP3 connections - poss brute force attack";flags:S,12;threshold: type both, track by_src, count 10, seconds 120; classtype: misc-activity;sid:2002992;rev:2;)

12) alert tcp any any -> any any (msg:"Zipped DOC in transit"; flow: established; content:"|50 4B 03 04|"; content:"|00|"; content:".doc"; nocase; classtype:not-suspicious; sid:2001402;rev:3;)

13) alert tcp any any -> any any (msg:"HTTP - Password"; flow:to_server,established; pcre:"/\W[p][a4@][sz5]{0,2}[w]([oO][r])?[d]\W/ism"; classtype:policy-violation; sid:2002567; rev:2;)

14) alert tcp any 53 -> any any (msg:"DNS-rebinding attack 192.168.x.x/16 (local IP from remote DNS Server)"; flow:established, from_server; content:"|c0 0c 00 01 00 01|"; content:"|00 04 c0 a8|"; within:4; distance:4; reference:url,crypto.stanford.edu/dns/; classtype:misc-attack; sid:2006917;rev:5;)

15) alert tcp any any -> any any (msg:"P2P limewire P2P traffic";flow:established; content:"User-Agent\:LimeWire"; nocase;classtype:policy-violation;reference:url,www.limewire.com;sid:2001808;rev:3;)

16) log tcp any any -> any 445 (msg:"HTTP download over a SMB connection"; flow:established; content:"|FF 53 4D 42 72|"; content:"HTTP"; nocase; classtype:policy-violation; reference:url,www.linklogger.com/TCP445Scan3.htm; sid:10000; rev:1;)

17) log udp any any -> any 5060 (msg:"VOIP Messages";classtype:misc-attack;sid:100000;rev:1;)

18) log tcp any any -> any 12345 (reference: CVE, CAN-2002-1010);