FortiNDR Cloud

BPF Reference Guide

SYNTAX					
[Protocol] [Direction] [Type] {ip/subnet/port/portrange}					
PROTOCOL		DIRECTION		TYPE	
Limit the match to a specific protocol. If no protocol is supplied, all protocols consistent with the type are assumed.		*Transfer direction to and/or from the type. If no direction is supplied, 'src or dst' is assumed.*		*Type of entity, port, or range of ports. If no type is supplied, host is assumed.*	
ether	*ethernet*	src or dst (default)	*source or destination*	host (default)	*ip address*
fddi	*alias for ether*	src and dst	*source and destination*	net	*ip address or subnet*
icmp	*internet control message protocol*	src	*source only*	port	*tcp/udp port number*
wlan	*wireless lan; alias for ether*	dst	*destination only*	portrange	*range of tcp/udp ports (xxxx-xxxx)*
ip	*ipv4*	[proto] broadcast	proto must be ip or ether		
ip6	*ipv6*	OPERATORS			
arp	*address resolution protocol*	'='	*equal to*	'||' 'or'	*logical or*
tcp	*transmission control protocol*	'!' or 'not'	*not equal to*	'<' 'less'	*less than*
udp	*user datagram protocol*	'&&' 'and'	*logical and*	'>' 'greater'	*greater than*

COMMON EXPRESSIONS	
host xxx.xxx.xxx.xxx	*all packets to/from a host*
src host xxx.xxx.xxx.xxx && dst host xxx.xxx.xxx.xxx	*all packets from a source host to a destination host*
dst port 23	*all packets to port 23 (telnet)*
udp src net xxx.xxx.xxx && dst host xxx.xxx.xxx.xxx	*only udp packets from a dotted pair subnet to destination host*
ip6 && not net xxx.xxx.xxx	*only IPv6 packets outside of a dotted triple subnet*
src host xxx.xxx.xxx.xxx && (dst portrange xxxx-xxxx && dst net xxx.xxx.xxx)	*all packets from a source host to a destination port range in a dotted triple subnet*
dst portrange 49152-65535 && gateway xxx.xxx.xxx.xxx	*all packets to non-standard ports on a gateway*
host xxx.xxx.xxx.xxx || host xxx.xxx.xxx.xxx	*all packets to/from host A or host B*

BYTE LEVEL FILTERING	
ip[9]!=47	*all packets where IP protocol field is GRE (tunnel)*
ip[8]<64	*all packets where IP time-to-live (TTL) is less than 64*
icmp[0]=3	*all packets with ICMP message type 3 (destination unreachable)*
tcp[13]=32 || tcp[13]=8	*all packets with TCP flags set to PSH or URG*

HOW TO READ PACKET HEADERS

Word 0																													
Byte Offset 0								Byte Offset 1								Byte Offset 2								Byte Offset 3							
Nibble 0				Nibble 1				Nibble 2				Nibble 3				Nibble 4				Nibble 5				Nibble 6				Nibble 7			
BIT 0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31

TCP HEADER – RFC 793

0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31
Offset 0								Offset 1								Offset 2								Offset 3							
Source Port Number																Destination Port Number															
Offset 4								Offset 5								Offset 6								Offset 7							
Sequence Number																															
Offset 8								Offset 9								Offset 10								Offset 11							
Acknowledgement Number																															
Offset 12								Offset 13								Offset 14								Offset 15							
Hacker Length				Reserved				CWR			ECE			URG		ACK			PSH			RST			SYN			FIN			
Window Size																															
Offset 16								Offset 17								Offset 18								Offset 19							
Checksum																Urgent Pointer															
Offset 20								Offset 21								Offset 22								Offset 23							
TCP Options																															
Data																															

20 BYTES

VARIABLE

UDP HEADER – RFC 768

0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31
Offset 0								Offset 1								Offset 2								Offset 3							
Source Port Number																Destination Port Number															
Offset 4								Offset 5								Offset 6								Offset 7							
Length																Checksum															
Offset 8								Offset 9								Offset 10								Offset 11							
Data																															

8 BYTES

VAR

ICMP HEADER – RFC 792

0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31
Offset 0								Offset 1								Offset 2								Offset 3							
Message Type								Message Code								Checksum															
Offset 4								Offset 5								Offset 6								Offset 7							
(Variable Contents Depending on Type and Code)																															

4 BYTES

VAR

IPv4 HEADER – RFC 791

0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31
Offset 0								Offset 1								Offset 2								Offset 3							
Version				IP Header Length				Type of Service								Total Length (in Offsets)															
Offset 4								Offset 5								Offset 6								Offset 7							
IP Identification Number																x	D	M	Fragment Offset											
Offset 8								Offset 9								Offset 10								Offset 11							
Time to Live (TTL)								Protocol								Header Checksum															
Offset 12								Offset 13								Offset 14								Offset 15							
Source IP Address																															
Offset 16								Offset 17								Offset 18								Offset 19							
Destination IP Address																															
Offset 20								Offset 21								Offset 22								Offset 23							
IP Options																															
Data																															

20 BYTES

FLAGS
x = Reserved D = Do Not Fragment M = More Fragments Follow

IPv6 HEADER – RFC 2460

0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31
Offset 0								Offset 1								Offset 2								Offset 3							
Version				Traffic Class								Flow Label																			
Offset 4								Offset 5								Offset 6								Offset 7							
Payload Length																Next Header								Hop Limit							
Offset 8								Offset 9								Offset 10								Offset 11							
Source IP Address																															
Offset 12								Offset 13								Offset 14								Offset 15							
Source IP Address (continued)																															
Offset 16								Offset 17								Offset 18								Offset 19							
Source IP Address (continued)																															
Offset 20								Offset 21								Offset 22								Offset 23							
Source IP Address (continued)																															
Offset 24								Offset 25								Offset 26								Offset 27							
Destination IP Address																															
Offset 28								Offset 29								Offset 30								Offset 31							
Destination IP Address (continued)																															
Offset 32								Offset 33								Offset 34								Offset 35							
Destination IP Address (continued)																															
Offset 36								Offset 37								Offset 38								Offset 39							
Destination IP Address (continued)																															
Offset 40								Offset 41								Offset 42								Offset 43							
Net Header								Extension Header Information																							
Extension Header																															
Data																															

40 BYTES

VARIABLE