

HALTDOS CANARY TECHSPECS

HD-CAN-1100

HD-CAN-550

Base Models

MITIGATION PERFORMANCE

100 GE Ports

1 GE (RJ-45) Ports Console (RS232/RJ45) Ports HA Ports (RJ-45/SFP/SFP+)

OUT OF BAND PORTS

HD-CAN-4100

HD-CAN-4600

MILIOATION I EN ONMANOL				
L4 Throughput	upto 500 Mbps	upto 1 Gbps	upto 5 Gbps	upto 24 Gbps
L7 Throughput	upto 500 Mbps	upto 1 Gbps	upto 4 Gbps	upto 25 Gbps
SSL Throughput	500 Mbps	1 Gbps	4 Gbps	20 Gbps
Compression Throughput	500 Mbps	1 Gbps	4 Gbps	20 Gbps
Decompression Throughput	500 Mbps	1 Gbps	5 Gbps	20 Gbps
becompression infoughput			· ·	•
SSL/TLS Connections per Second	10K (RSA 2K)	22K (RSA 2K)	22K (RSA 2K)	40K (RSA 2K)
· · · · · · · · · · · · · · · · · · ·	5K (ECC)	15K (ECC)	15K (ECC)	25K (ECC)
L4 Connection per Second	320 K	400 K	600 K	1.5 M
L7 Request per Second	250 K	500 K	1 M	3 M
Max Concurrent Connections	7 M	12 M	24 M	32 M
Induced Latency		<1	ms	
HARDWARE SPECS				
Processor	Intel Xeon	Intel Xeon	Intel Xeon	Intel Xeon
CPU Cores	6	8	8	20
	8 GB	16 GB	16 GB	32 GB
Memory				
Hard Disk	128 GB SSD	128 GB SSD	256 GB SSD	256 GB SSD
		· · · · · · · · · · · · · · · · · · ·	RAID or dual partition	
Additional Space	Built-in TPM Chip and Hardware HSM fo	or SSL offloading & compression optin	nization Option	
Additional Specs	available for FIPS-140-2 (additional cha	rge) or Non-FIPS compliant HSM		
Form Factor	1U/2U Rack Mount Server (19 inch mou			
Power Supply	Redundant Power Supply (Hot Swappa			
Operating Temperature	0° – 40° C	,		
Humidity	8% - 95% (non-condensing)	A	l No.	
Virtual ADC Supported	NA	NA	NA	upto 15
		Hard Disk and Memory can be o	customized over the base mode	<u> </u>
INSPECTION PORTS				
1 GE Ports	4	8	8	8
10 GE Ports	-	-	-	2
25 GE Ports	-	-	-	
40 GE Ports	_		_	
100 GE Ports	-	-	-	<u>-</u>
		No. of ports can be custor	nized over the base model	
OUT OF BAND PORTS				
1 GE (RJ-45) Ports	1	2	2	2
Console (RS232/RJ45) Ports	-	1	1	1
HA Ports (RJ-45/SFP/SFP+)	1	1	1	1
11/1 013 (10-45/511/5111)	<u> </u>	1	1	1
Input/Output (USB)	2	2	2	2
				LID CAN STOR
Rasa Models	HD-CAN-5100	HD_CAN_5400	HD-CVN-6300	
Base Models	HD-CAN-5100	HD-CAN-5400	HD-CAN-6200	HD-CAN-6700
MITIGATION PERFORMANCE				
MITIGATION PERFORMANCE L4 Throughput	upto 48 Gbps	upto 72 Gbps	upto 120 Gbps	upto 150 Gbps
MITIGATION PERFORMANCE L4 Throughput L7 Throughput	upto 48 Gbps upto 40 Gbps	upto 72 Gbps upto 60 Gbps	upto 120 Gbps upto 100 Gbps	upto 150 Gbps upto 120 Gbps
MITIGATION PERFORMANCE L4 Throughput	upto 48 Gbps	upto 72 Gbps	upto 120 Gbps	upto 150 Gbps
MITIGATION PERFORMANCE L4 Throughput L7 Throughput	upto 48 Gbps upto 40 Gbps	upto 72 Gbps upto 60 Gbps	upto 120 Gbps upto 100 Gbps	upto 150 Gbps upto 120 Gbps
MITIGATION PERFORMANCE L4 Throughput L7 Throughput SSL Throughput	upto 48 Gbps upto 40 Gbps 40 Gbps	upto 72 Gbps upto 60 Gbps 50 Gbps	upto 120 Gbps upto 100 Gbps 100 Gbps	upto 150 Gbps upto 120 Gbps 200 Gbps
MITIGATION PERFORMANCE L4 Throughput L7 Throughput SSL Throughput Compression Throughput Decompression Throughput	upto 48 Gbps upto 40 Gbps 40 Gbps 24 Gbps 30 Gbps	upto 72 Gbps upto 60 Gbps 50 Gbps 37 Gbps 54 Gbps	upto 120 Gbps upto 100 Gbps 100 Gbps 66 Gbps 120 Gbps	upto 150 Gbps upto 120 Gbps 200 Gbps 132 Gbps 240 Gbps
MITIGATION PERFORMANCE L4 Throughput L7 Throughput SSL Throughput Compression Throughput	upto 48 Gbps upto 40 Gbps 40 Gbps 24 Gbps 30 Gbps 40K (RSA 2K)	upto 72 Gbps upto 60 Gbps 50 Gbps 37 Gbps 54 Gbps 95K (RSA 2K)	upto 120 Gbps upto 100 Gbps 100 Gbps 66 Gbps 120 Gbps 95K (RSA 2K)	upto 150 Gbps upto 120 Gbps 200 Gbps 132 Gbps 240 Gbps 190K (RSA 2K)
MITIGATION PERFORMANCE L4 Throughput L7 Throughput SSL Throughput Compression Throughput Decompression Throughput SSL/TLS Connections per Second	upto 48 Gbps upto 40 Gbps 40 Gbps 24 Gbps 30 Gbps 40K (RSA 2K) 25K (ECC)	upto 72 Gbps upto 60 Gbps 50 Gbps 37 Gbps 54 Gbps 95K (RSA 2K) 48K (ECC)	upto 120 Gbps upto 100 Gbps 100 Gbps 66 Gbps 120 Gbps 95K (RSA 2K) 48K (ECC)	upto 150 Gbps upto 120 Gbps 200 Gbps 132 Gbps 240 Gbps 190K (RSA 2K) 96K (ECC)
MITIGATION PERFORMANCE L4 Throughput L7 Throughput SSL Throughput Compression Throughput Decompression Throughput SSL/TLS Connections per Second L4 Connection per Second	upto 48 Gbps upto 40 Gbps 40 Gbps 24 Gbps 30 Gbps 40K (RSA 2K) 25K (ECC)	upto 72 Gbps upto 60 Gbps 50 Gbps 37 Gbps 54 Gbps 95K (RSA 2K) 48K (ECC) 2 M	upto 120 Gbps upto 100 Gbps 100 Gbps 66 Gbps 120 Gbps 95K (RSA 2K) 48K (ECC)	upto 150 Gbps upto 120 Gbps 200 Gbps 132 Gbps 240 Gbps 190K (RSA 2K) 96K (ECC) 4.2 M
MITIGATION PERFORMANCE L4 Throughput L7 Throughput SSL Throughput Compression Throughput Decompression Throughput SSL/TLS Connections per Second L4 Connection per Second L7 Request per Second	upto 48 Gbps upto 40 Gbps 40 Gbps 24 Gbps 30 Gbps 40K (RSA 2K) 25K (ECC) 1.5 M	upto 72 Gbps upto 60 Gbps 50 Gbps 37 Gbps 54 Gbps 95K (RSA 2K) 48K (ECC) 2 M 10 M	upto 120 Gbps upto 100 Gbps 100 Gbps 66 Gbps 120 Gbps 95K (RSA 2K) 48K (ECC) 4 M 15 M	upto 150 Gbps upto 120 Gbps 200 Gbps 132 Gbps 240 Gbps 190K (RSA 2K) 96K (ECC) 4.2 M 18 M
MITIGATION PERFORMANCE L4 Throughput L7 Throughput SSL Throughput Compression Throughput Decompression Throughput SSL/TLS Connections per Second L4 Connection per Second L7 Request per Second Max Concurrent Connections	upto 48 Gbps upto 40 Gbps 40 Gbps 24 Gbps 30 Gbps 40K (RSA 2K) 25K (ECC)	upto 72 Gbps upto 60 Gbps 50 Gbps 37 Gbps 54 Gbps 95K (RSA 2K) 48K (ECC) 2 M 10 M 96 M	upto 120 Gbps upto 100 Gbps 100 Gbps 66 Gbps 120 Gbps 95K (RSA 2K) 48K (ECC) 4 M 15 M 160 M	upto 150 Gbps upto 120 Gbps 200 Gbps 132 Gbps 240 Gbps 190K (RSA 2K) 96K (ECC) 4.2 M
MITIGATION PERFORMANCE L4 Throughput L7 Throughput SSL Throughput Compression Throughput Decompression Throughput SSL/TLS Connections per Second L4 Connection per Second L7 Request per Second Max Concurrent Connections Induced Latency	upto 48 Gbps upto 40 Gbps 40 Gbps 24 Gbps 30 Gbps 40K (RSA 2K) 25K (ECC) 1.5 M	upto 72 Gbps upto 60 Gbps 50 Gbps 37 Gbps 54 Gbps 95K (RSA 2K) 48K (ECC) 2 M 10 M 96 M	upto 120 Gbps upto 100 Gbps 100 Gbps 66 Gbps 120 Gbps 95K (RSA 2K) 48K (ECC) 4 M 15 M	upto 150 Gbps upto 120 Gbps 200 Gbps 132 Gbps 240 Gbps 190K (RSA 2K) 96K (ECC) 4.2 M 18 M
MITIGATION PERFORMANCE L4 Throughput L7 Throughput SSL Throughput Compression Throughput Decompression Throughput SSL/TLS Connections per Second L4 Connection per Second L7 Request per Second Max Concurrent Connections	upto 48 Gbps upto 40 Gbps 40 Gbps 24 Gbps 30 Gbps 40K (RSA 2K) 25K (ECC) 1.5 M	upto 72 Gbps upto 60 Gbps 50 Gbps 37 Gbps 54 Gbps 95K (RSA 2K) 48K (ECC) 2 M 10 M 96 M	upto 120 Gbps upto 100 Gbps 100 Gbps 66 Gbps 120 Gbps 95K (RSA 2K) 48K (ECC) 4 M 15 M 160 M	upto 150 Gbps upto 120 Gbps 200 Gbps 132 Gbps 240 Gbps 190K (RSA 2K) 96K (ECC) 4.2 M 18 M
MITIGATION PERFORMANCE L4 Throughput L7 Throughput SSL Throughput Compression Throughput Decompression Throughput SSL/TLS Connections per Second L4 Connection per Second L7 Request per Second Max Concurrent Connections Induced Latency HARDWARE SPECS	upto 48 Gbps upto 40 Gbps 40 Gbps 24 Gbps 30 Gbps 40K (RSA 2K) 25K (ECC) 1.5 M	upto 72 Gbps upto 60 Gbps 50 Gbps 37 Gbps 54 Gbps 95K (RSA 2K) 48K (ECC) 2 M 10 M 96 M	upto 120 Gbps upto 100 Gbps 100 Gbps 66 Gbps 120 Gbps 95K (RSA 2K) 48K (ECC) 4 M 15 M 160 M	upto 150 Gbps upto 120 Gbps 200 Gbps 132 Gbps 240 Gbps 190K (RSA 2K) 96K (ECC) 4.2 M 18 M
MITIGATION PERFORMANCE L4 Throughput L7 Throughput SSL Throughput Compression Throughput Decompression Throughput SSL/TLS Connections per Second L4 Connection per Second L7 Request per Second Max Concurrent Connections Induced Latency HARDWARE SPECS Processor	upto 48 Gbps upto 40 Gbps 40 Gbps 24 Gbps 30 Gbps 40K (RSA 2K) 25K (ECC) 1.5 M 7 M 56 M	upto 72 Gbps upto 60 Gbps 50 Gbps 37 Gbps 54 Gbps 95K (RSA 2K) 48K (ECC) 2 M 10 M 96 M <1	upto 120 Gbps upto 100 Gbps 100 Gbps 66 Gbps 120 Gbps 95K (RSA 2K) 48K (ECC) 4 M 15 M 160 M ms	upto 150 Gbps upto 120 Gbps 200 Gbps 132 Gbps 240 Gbps 190K (RSA 2K) 96K (ECC) 4.2 M 18 M 192 M
MITIGATION PERFORMANCE L4 Throughput L7 Throughput SSL Throughput Compression Throughput Decompression Throughput SSL/TLS Connections per Second L4 Connection per Second L7 Request per Second Max Concurrent Connections Induced Latency HARDWARE SPECS Processor CPU Cores	upto 48 Gbps upto 40 Gbps 40 Gbps 24 Gbps 30 Gbps 40K (RSA 2K) 25K (ECC) 1.5 M 7 M 56 M	upto 72 Gbps upto 60 Gbps 50 Gbps 37 Gbps 54 Gbps 95K (RSA 2K) 48K (ECC) 2 M 10 M 96 M <1	upto 120 Gbps upto 100 Gbps 100 Gbps 66 Gbps 120 Gbps 95K (RSA 2K) 48K (ECC) 4 M 15 M 160 M ms	upto 150 Gbps upto 120 Gbps 200 Gbps 132 Gbps 240 Gbps 190K (RSA 2K) 96K (ECC) 4.2 M 18 M 192 M
MITIGATION PERFORMANCE L4 Throughput L7 Throughput SSL Throughput Compression Throughput Decompression Throughput L4 Connections per Second L7 Request per Second L7 Request per Second Max Concurrent Connections Induced Latency HARDWARE SPECS Processor CPU Cores Memory	upto 48 Gbps upto 40 Gbps 40 Gbps 24 Gbps 30 Gbps 40K (RSA 2K) 25K (ECC) 1.5 M 7 M 56 M	upto 72 Gbps upto 60 Gbps 50 Gbps 37 Gbps 54 Gbps 95K (RSA 2K) 48K (ECC) 2 M 10 M 96 M <1	upto 120 Gbps upto 100 Gbps 100 Gbps 66 Gbps 120 Gbps 95K (RSA 2K) 48K (ECC) 4 MM 15 M 160 M ms	upto 150 Gbps upto 120 Gbps 200 Gbps 132 Gbps 240 Gbps 190K (RSA 2K) 96K (ECC) 4.2 M 18 M 192 M
MITIGATION PERFORMANCE L4 Throughput L7 Throughput SSL Throughput SSL Throughput Decompression Throughput SSL/TLS Connections per Second L4 Connection per Second L7 Request per Second Max Concurrent Connections Induced Latency HARDWARE SPECS Processor CPU Cores	upto 48 Gbps upto 40 Gbps 40 Gbps 24 Gbps 30 Gbps 40K (RSA 2K) 25K (ECC) 1.5 M 7 M 56 M Intel Xeon 32 64 GB 512 GB SSD	upto 72 Gbps upto 60 Gbps 50 Gbps 37 Gbps 54 Gbps 95K (RSA 2K) 48K (ECC) 2 M 10 M 96 M <1 Intel Xeon 40 128 GB 1 TB SSD	upto 120 Gbps upto 100 Gbps 100 Gbps 66 Gbps 120 Gbps 95K (RSA 2K) 48K (ECC) 4 M 15 M 160 M ms	upto 150 Gbps upto 120 Gbps 200 Gbps 132 Gbps 240 Gbps 190K (RSA 2K) 96K (ECC) 4.2 M 18 M 192 M
MITIGATION PERFORMANCE L4 Throughput L7 Throughput SSL Throughput Compression Throughput Decompression Throughput L4 Connections per Second L7 Request per Second L7 Request per Second Max Concurrent Connections Induced Latency HARDWARE SPECS Processor CPU Cores Memory	upto 48 Gbps upto 40 Gbps 40 Gbps 24 Gbps 30 Gbps 40K (RSA 2K) 25K (ECC) 1.5 M 7 M 56 M	upto 72 Gbps upto 60 Gbps 50 Gbps 37 Gbps 54 Gbps 95K (RSA 2K) 48K (ECC) 2 M 10 M 96 M <1 Intel Xeon 40 128 GB 1 TB SSD	upto 120 Gbps upto 100 Gbps 100 Gbps 66 Gbps 120 Gbps 95K (RSA 2K) 48K (ECC) 4 MM 15 M 160 M ms	upto 150 Gbps upto 120 Gbps 200 Gbps 132 Gbps 240 Gbps 190K (RSA 2K) 96K (ECC) 4.2 M 18 M 192 M
MITIGATION PERFORMANCE L4 Throughput L7 Throughput SSL Throughput Compression Throughput Decompression Throughput SSL/TLS Connections per Second L4 Connection per Second L7 Request per Second Max Concurrent Connections Induced Latency HARDWARE SPECS Processor CPU Cores Memory Hard Disk	upto 48 Gbps upto 40 Gbps 40 Gbps 24 Gbps 30 Gbps 40K (RSA 2K) 25K (ECC) 1.5 M 7 M 56 M Intel Xeon 32 64 GB 512 GB SSD	upto 72 Gbps upto 60 Gbps 50 Gbps 37 Gbps 54 Gbps 95K (RSA 2K) 48K (ECC) 2 M 10 M 96 M <1 Intel Xeon 40 128 GB 1 TB SSD	upto 120 Gbps upto 100 Gbps 100 Gbps 66 Gbps 120 Gbps 95K (RSA 2K) 48K (ECC) 4 M 15 M 160 M ms Intel Xeon 64 256 GB 2 TB SSD	upto 150 Gbps upto 120 Gbps 200 Gbps 132 Gbps 240 Gbps 190K (RSA 2K) 96K (ECC) 4.2 M 18 M 192 M Intel Xeon 64 512 GB 2 TB SSD
MITIGATION PERFORMANCE L4 Throughput L7 Throughput SSL Throughput Compression Throughput Decompression Throughput L4 Connections per Second L7 Request per Second L7 Request per Second Max Concurrent Connections Induced Latency HARDWARE SPECS Processor CPU Cores Memory	upto 48 Gbps upto 40 Gbps 40 Gbps 24 Gbps 30 Gbps 40K (RSA 2K) 25K (ECC) 1.5 M 7 M 56 M Intel Xeon 32 64 GB 512 GB SSD Option available for RAID or dual partitio	upto 72 Gbps upto 60 Gbps 50 Gbps 37 Gbps 54 Gbps 95K (RSA 2K) 48K (ECC) 2 M 10 M 96 M <1 Intel Xeon 40 128 GB 1 TB SSD	upto 120 Gbps upto 100 Gbps 100 Gbps 66 Gbps 120 Gbps 95K (RSA 2K) 48K (ECC) 4 M 15 M 160 M ms Intel Xeon 64 256 GB 2 TB SSD	upto 150 Gbps upto 120 Gbps 200 Gbps 132 Gbps 240 Gbps 190K (RSA 2K) 96K (ECC) 4.2 M 18 M 192 M Intel Xeon 64 512 GB 2 TB SSD
MITIGATION PERFORMANCE L4 Throughput L7 Throughput SSL Throughput Compression Throughput Decompression Throughput SSL/TLS Connections per Second L4 Connection per Second L7 Request per Second Max Concurrent Connections Induced Latency HARDWARE SPECS Processor CPU Cores Memory Hard Disk	upto 48 Gbps upto 40 Gbps 40 Gbps 24 Gbps 30 Gbps 40K (RSA 2K) 25K (ECC) 1.5 M 7 M 56 M Intel Xeon 32 64 GB 512 GB SSD Option available for RAID or dual partitio	upto 72 Gbps upto 60 Gbps 50 Gbps 37 Gbps 54 Gbps 95K (RSA 2K) 48K (ECC) 2 M 10 M 96 M <1 Intel Xeon 40 128 GB 1 TB SSD n or SSL offloading & compression optin	upto 120 Gbps upto 100 Gbps 100 Gbps 66 Gbps 120 Gbps 95K (RSA 2K) 48K (ECC) 4 M 15 M 160 M ms Intel Xeon 64 256 GB 2 TB SSD	upto 150 Gbps upto 120 Gbps 200 Gbps 132 Gbps 240 Gbps 190K (RSA 2K) 96K (ECC) 4.2 M 18 M 192 M Intel Xeon 64 512 GB 2 TB SSD
MITIGATION PERFORMANCE L4 Throughput L7 Throughput SSL Throughput Compression Throughput Decompression Throughput SSL/TLS Connections per Second L4 Connection per Second L7 Request per Second Max Concurrent Connections Induced Latency HARDWARE SPECS Processor CPU Cores Memory Hard Disk Additional Specs Form Factor	upto 48 Gbps upto 40 Gbps 40 Gbps 24 Gbps 30 Gbps 40K (RSA 2K) 25K (ECC) 1.5 M 7 M 56 M Intel Xeon 32 64 GB 512 GB SSD Option available for RAID or dual partitio Built-in TPM Chip and Hardware HSM fc compliant HSM 1U/2U/4U Rack Mount Server (19- inch	upto 72 Gbps upto 60 Gbps 50 Gbps 37 Gbps 54 Gbps 95K (RSA 2K) 48K (ECC) 2 M 10 M 96 M <1 Intel Xeon 40 128 GB 1 TB SSD n or SSL offloading & compression optin	upto 120 Gbps upto 100 Gbps 100 Gbps 66 Gbps 120 Gbps 95K (RSA 2K) 48K (ECC) 4 M 15 M 160 M ms Intel Xeon 64 256 GB 2 TB SSD	upto 150 Gbps upto 120 Gbps 200 Gbps 132 Gbps 240 Gbps 190K (RSA 2K) 96K (ECC) 4.2 M 18 M 192 M Intel Xeon 64 512 GB 2 TB SSD
MITIGATION PERFORMANCE L4 Throughput L7 Throughput SSL Throughput Decompression Throughput SSL/TLS Connections per Second L4 Connection per Second L7 Request per Second Max Concurrent Connections Induced Latency HARDWARE SPECS Processor CPU Cores Memory Hard Disk Additional Specs Form Factor Power Supply	upto 48 Gbps upto 40 Gbps 40 Gbps 24 Gbps 30 Gbps 40K (RSA 2K) 25K (ECC) 1.5 M 7 M 56 M Intel Xeon 32 64 GB 512 GB SSD Option available for RAID or dual partitio Built-in TPM Chip and Hardware HSM fc compliant HSM 1U/2U/4U Rack Mount Server (19- inch Redundant Power Supply (Hot Swappa)	upto 72 Gbps upto 60 Gbps 50 Gbps 37 Gbps 54 Gbps 95K (RSA 2K) 48K (ECC) 2 M 10 M 96 M <1 Intel Xeon 40 128 GB 1 TB SSD n or SSL offloading & compression optin	upto 120 Gbps upto 100 Gbps 100 Gbps 66 Gbps 120 Gbps 95K (RSA 2K) 48K (ECC) 4 M 15 M 160 M ms Intel Xeon 64 256 GB 2 TB SSD	upto 150 Gbps upto 120 Gbps 200 Gbps 132 Gbps 240 Gbps 190K (RSA 2K) 96K (ECC) 4.2 M 18 M 192 M Intel Xeon 64 512 GB 2 TB SSD
MITIGATION PERFORMANCE L4 Throughput L7 Throughput SSL Throughput Compression Throughput Decompression Throughput SSL/TLS Connections per Second L4 Connection per Second L7 Request per Second Max Concurrent Connections Induced Latency HARDWARE SPECS Processor CPU Cores Memory Hard Disk Additional Specs Form Factor Power Supply Operating Temperature	upto 48 Gbps upto 40 Gbps 40 Gbps 24 Gbps 30 Gbps 40K (RSA 2K) 25K (ECC) 1.5 M 7 M 56 M Intel Xeon 32 64 GB 512 GB SSD Option available for RAID or dual partitio Built-in TPM Chip and Hardware HSM for compliant HSM 1U/2U/4U Rack Mount Server (19- inch Redundant Power Supply (Hot Swappal 0° - 40° C	upto 72 Gbps upto 60 Gbps 50 Gbps 37 Gbps 54 Gbps 95K (RSA 2K) 48K (ECC) 2 M 10 M 96 M <1 Intel Xeon 40 128 GB 1 TB SSD n or SSL offloading & compression optin	upto 120 Gbps upto 100 Gbps 100 Gbps 66 Gbps 120 Gbps 95K (RSA 2K) 48K (ECC) 4 M 15 M 160 M ms Intel Xeon 64 256 GB 2 TB SSD	upto 150 Gbps upto 120 Gbps 200 Gbps 132 Gbps 240 Gbps 190K (RSA 2K) 96K (ECC) 4.2 M 18 M 192 M Intel Xeon 64 512 GB 2 TB SSD
MITIGATION PERFORMANCE L4 Throughput L7 Throughput SSL Throughput Compression Throughput Decompression Throughput SSL/TLS Connections per Second L4 Connection per Second L7 Request per Second Max Concurrent Connections Induced Latency HARDWARE SPECS Processor CPU Cores Memory Hard Disk Additional Specs Form Factor Power Supply Operating Temperature Humidity	upto 48 Gbps upto 40 Gbps 40 Gbps 24 Gbps 30 Gbps 40K (RSA 2K) 25K (ECC) 1.5 M 7 M 56 M Intel Xeon 32 64 GB 512 GB SSD Option available for RAID or dual partitio Built-in TPM Chip and Hardware HSM fc compliant HSM 1U/2U/4U Rack Mount Server (19- inch Redundant Power Supply (Hot Swappal 0° – 40° C 8% - 95% (non-condensing)	upto 72 Gbps upto 60 Gbps 50 Gbps 37 Gbps 54 Gbps 95K (RSA 2K) 48K (ECC) 2 M 10 M 96 M <1 Intel Xeon 40 128 GB 1 TB SSD n or SSL offloading & compression optin mounting) with panel indicators ole) AC 170-240V, 50 Hz	upto 120 Gbps upto 100 Gbps 100 Gbps 66 Gbps 120 Gbps 95K (RSA 2K) 48K (ECC) 4 MM 15 M 160 M ms Intel Xeon 64 256 GB 2 TB SSD	upto 150 Gbps upto 120 Gbps 200 Gbps 132 Gbps 240 Gbps 190K (RSA 2K) 96K (ECC) 4.2 M 18 M 192 M Intel Xeon 64 512 GB 2 TB SSD 0-2 (additional charge) or Non-FIPS
MITIGATION PERFORMANCE L4 Throughput L7 Throughput SSL Throughput Compression Throughput Decompression Throughput SSL/TLS Connections per Second L4 Connection per Second L7 Request per Second Max Concurrent Connections Induced Latency HARDWARE SPECS Processor CPU Cores Memory Hard Disk Additional Specs Form Factor Power Supply Operating Temperature	upto 48 Gbps upto 40 Gbps 40 Gbps 24 Gbps 30 Gbps 40K (RSA 2K) 25K (ECC) 1.5 M 7 M 56 M Intel Xeon 32 64 GB 512 GB SSD Option available for RAID or dual partitio Built-in TPM Chip and Hardware HSM fc compliant HSM 1U/2U/4U Rack Mount Server (19- inch Redundant Power Supply (Hot Swappal 0° – 40° C 8% - 95% (non-condensing) upto 25	upto 72 Gbps upto 60 Gbps 50 Gbps 37 Gbps 54 Gbps 95K (RSA 2K) 48K (ECC) 2 M 10 M 96 M <1 Intel Xeon 40 128 GB 1 TB SSD n or SSL offloading & compression optin mounting) with panel indicators ole) AC 170-240V, 50 Hz upto 30	upto 120 Gbps upto 100 Gbps 100 Gbps 66 Gbps 120 Gbps 95K (RSA 2K) 48K (ECC) 4 M 15 M 160 M ms Intel Xeon 64 256 GB 2 TB SSD	upto 150 Gbps upto 120 Gbps 200 Gbps 132 Gbps 240 Gbps 190K (RSA 2K) 96K (ECC) 4.2 M 18 M 192 M Intel Xeon 64 512 GB 2 TB SSD 0-2 (additional charge) or Non-FIPS
MITIGATION PERFORMANCE L4 Throughput L7 Throughput SSL Throughput Compression Throughput Decompression Throughput SSL/TLS Connections per Second L4 Connection per Second L7 Request per Second Max Concurrent Connections Induced Latency HARDWARE SPECS Processor CPU Cores Memory Hard Disk Additional Specs Form Factor Power Supply Operating Temperature Humidity	upto 48 Gbps upto 40 Gbps 40 Gbps 24 Gbps 30 Gbps 40K (RSA 2K) 25K (ECC) 1.5 M 7 M 56 M Intel Xeon 32 64 GB 512 GB SSD Option available for RAID or dual partitio Built-in TPM Chip and Hardware HSM fc compliant HSM 1U/2U/4U Rack Mount Server (19- inch Redundant Power Supply (Hot Swappal 0° – 40° C 8% - 95% (non-condensing) upto 25	upto 72 Gbps upto 60 Gbps 50 Gbps 37 Gbps 54 Gbps 95K (RSA 2K) 48K (ECC) 2 M 10 M 96 M <1 Intel Xeon 40 128 GB 1 TB SSD n or SSL offloading & compression optin mounting) with panel indicators ole) AC 170-240V, 50 Hz upto 30	upto 120 Gbps upto 100 Gbps 100 Gbps 66 Gbps 120 Gbps 95K (RSA 2K) 48K (ECC) 4 MM 15 M 160 M ms Intel Xeon 64 256 GB 2 TB SSD	upto 150 Gbps upto 120 Gbps 200 Gbps 132 Gbps 240 Gbps 190K (RSA 2K) 96K (ECC) 4.2 M 18 M 192 M Intel Xeon 64 512 GB 2 TB SSD 0-2 (additional charge) or Non-FIPS
MITIGATION PERFORMANCE L4 Throughput L7 Throughput SSL Throughput Compression Throughput Decompression Throughput SSL/TLS Connections per Second L4 Connection per Second L7 Request per Second Max Concurrent Connections Induced Latency HARDWARE SPECS Processor CPU Cores Memory Hard Disk Additional Specs Form Factor Power Supply Operating Temperature Humidity	upto 48 Gbps upto 40 Gbps 40 Gbps 24 Gbps 30 Gbps 40K (RSA 2K) 25K (ECC) 1.5 M 7 M 56 M Intel Xeon 32 64 GB 512 GB SSD Option available for RAID or dual partitio Built-in TPM Chip and Hardware HSM fc compliant HSM 1U/2U/4U Rack Mount Server (19- inch Redundant Power Supply (Hot Swappal 0° – 40° C 8% - 95% (non-condensing) upto 25	upto 72 Gbps upto 60 Gbps 50 Gbps 37 Gbps 54 Gbps 95K (RSA 2K) 48K (ECC) 2 M 10 M 96 M <1 Intel Xeon 40 128 GB 1 TB SSD n or SSL offloading & compression optin mounting) with panel indicators ole) AC 170-240V, 50 Hz upto 30	upto 120 Gbps upto 100 Gbps 100 Gbps 66 Gbps 120 Gbps 95K (RSA 2K) 48K (ECC) 4 M 15 M 160 M ms Intel Xeon 64 256 GB 2 TB SSD	upto 150 Gbps upto 120 Gbps 200 Gbps 132 Gbps 240 Gbps 190K (RSA 2K) 96K (ECC) 4.2 M 18 M 192 M Intel Xeon 64 512 GB 2 TB SSD 0-2 (additional charge) or Non-FIPS
MITIGATION PERFORMANCE L4 Throughput L7 Throughput SSL Throughput Decompression Throughput SSL/TLS Connections per Second L4 Connection per Second L7 Request per Second Max Concurrent Connections Induced Latency HARDWARE SPECS Processor CPU Cores Memory Hard Disk Additional Specs Form Factor Power Supply Operating Temperature Humidity Virtual ADC Supported	upto 48 Gbps upto 40 Gbps 40 Gbps 24 Gbps 30 Gbps 40K (RSA 2K) 25K (ECC) 1.5 M 7 M 56 M Intel Xeon 32 64 GB 512 GB SSD Option available for RAID or dual partitio Built-in TPM Chip and Hardware HSM fc compliant HSM 1U/2U/4U Rack Mount Server (19- inch Redundant Power Supply (Hot Swappal 0° – 40° C 8% - 95% (non-condensing) upto 25	upto 72 Gbps upto 60 Gbps 50 Gbps 37 Gbps 54 Gbps 95K (RSA 2K) 48K (ECC) 2 M 10 M 96 M <1 Intel Xeon 40 128 GB 1 TB SSD n or SSL offloading & compression optin mounting) with panel indicators ole) AC 170-240V, 50 Hz upto 30	upto 120 Gbps upto 100 Gbps 100 Gbps 66 Gbps 120 Gbps 95K (RSA 2K) 48K (ECC) 4 M 15 M 160 M ms Intel Xeon 64 256 GB 2 TB SSD	upto 150 Gbps upto 120 Gbps 200 Gbps 132 Gbps 240 Gbps 190K (RSA 2K) 96K (ECC) 4.2 M 18 M 192 M Intel Xeon 64 512 GB 2 TB SSD 0-2 (additional charge) or Non-FIPS
MITIGATION PERFORMANCE L4 Throughput L7 Throughput SSL Throughput Compression Throughput Decompression Throughput SSL/TLS Connections per Second L4 Connection per Second L7 Request per Second Max Concurrent Connections Induced Latency HARDWARE SPECS Processor CPU Cores Memory Hard Disk Additional Specs Form Factor Power Supply Operating Temperature Humidity Virtual ADC Supported	upto 48 Gbps upto 40 Gbps 40 Gbps 24 Gbps 30 Gbps 40K (RSA 2K) 25K (ECC) 1.5 M 7 M 56 M Intel Xeon 32 64 GB 512 GB SSD Option available for RAID or dual partitio Built-in TPM Chip and Hardware HSM for compliant HSM 1U/2U/4U Rack Mount Server (19- inch Redundant Power Supply (Hot Swappai 0° – 40° C 8% - 95% (non-condensing) upto 25	upto 72 Gbps upto 60 Gbps 50 Gbps 37 Gbps 54 Gbps 95K (RSA 2K) 48K (ECC) 2 M 10 M 96 M <1 Intel Xeon 40 128 GB 1 TB SSD n or SSL offloading & compression optin mounting) with panel indicators on AC 170-240V, 50 Hz upto 30 Hard Disk and Memory can be of	upto 120 Gbps upto 100 Gbps 100 Gbps 66 Gbps 120 Gbps 95K (RSA 2K) 48K (ECC) 4 M 15 M 160 M ms Intel Xeon 64 256 GB 2 TB SSD nization. Option available for FIPS-140	upto 150 Gbps upto 120 Gbps 200 Gbps 132 Gbps 240 Gbps 190K (RSA 2K) 96K (ECC) 4.2 M 18 M 192 M Intel Xeon 64 512 GB 2 TB SSD D-2 (additional charge) or Non-FIPS
MITIGATION PERFORMANCE L4 Throughput L7 Throughput SSL Throughput Compression Throughput Decompression Throughput SSL/TLS Connections per Second L4 Connection per Second Max Concurrent Connections Induced Latency HARDWARE SPECS Processor CPU Cores Memory Hard Disk Additional Specs Form Factor Power Supply Operating Temperature Humidity Virtual ADC Supported INSPECTION PORTS 1 GE Ports 1 0 GE Ports	upto 48 Gbps upto 40 Gbps 40 Gbps 24 Gbps 30 Gbps 40K (RSA 2K) 25K (ECC) 1.5 M 7 M 56 M Intel Xeon 32 64 GB 512 GB SSD Option available for RAID or dual partitio Built-in TPM Chip and Hardware HSM for compliant HSM 1U/2U/4U Rack Mount Server (19- inch Redundant Power Supply (Hot Swappal 0° - 40° C 8% - 95% (non-condensing) upto 25	upto 72 Gbps	upto 120 Gbps upto 100 Gbps 100 Gbps 66 Gbps 120 Gbps 95K (RSA 2K) 48K (ECC) 4 M 15 M 160 M ms Intel Xeon 64 256 GB 2 TB SSD nization. Option available for FIPS-140 upto 50 customized over the base mode	upto 150 Gbps upto 120 Gbps 200 Gbps 132 Gbps 240 Gbps 190K (RSA 2K) 96K (ECC) 4.2 M 18 M 192 M Intel Xeon 64 512 GB 2 TB SSD 0-2 (additional charge) or Non-FIPS upto 50
MITIGATION PERFORMANCE L4 Throughput L7 Throughput SSL Throughput Compression Throughput Decompression Throughput SSL/TLS Connections per Second L4 Connection per Second L7 Request per Second Max Concurrent Connections Induced Latency HARDWARE SPECS Processor CPU Cores Memory Hard Disk Additional Specs Form Factor Power Supply Operating Temperature Humidity Virtual ADC Supported INSPECTION PORTS L6 E Ports 10 GE Ports 10 GE Ports	upto 48 Gbps upto 40 Gbps 40 Gbps 24 Gbps 30 Gbps 40K (RSA 2K) 25K (ECC) 1.5 M 7 M 56 M Intel Xeon 32 64 GB 512 GB SSD Option available for RAID or dual partitlo Built-in TPM Chip and Hardware HSM fcompliant HSM 1U/2U/4U Rack Mount Server (19- inch Redundant Power Supply (Hot Swappai 0° – 40° C 8% - 95% (non-condensing) upto 25	upto 72 Gbps upto 60 Gbps 50 Gbps 37 Gbps 54 Gbps 95K (RSA 2K) 48K (ECC) 2 M 10 M 96 M <1 Intel Xeon 40 128 GB 1 TB SSD n or SSL offloading & compression optin mounting) with panel indicators ole) AC 170-240V, 50 Hz upto 30 Hard Disk and Memory can be of 8 - 8	upto 120 Gbps upto 100 Gbps 100 Gbps 66 Gbps 120 Gbps 95K (RSA 2K) 48K (ECC) 4 MM 15 M 160 M ms Intel Xeon 64 256 GB 2 TB SSD nization. Option available for FIPS-14C	upto 150 Gbps upto 120 Gbps 200 Gbps 132 Gbps 240 Gbps 190K (RSA 2K) 96K (ECC) 4.2 M 18 M 192 M Intel Xeon 64 512 GB 2 TB SSD D-2 (additional charge) or Non-FIPS
MITIGATION PERFORMANCE L4 Throughput L7 Throughput SSL Throughput Compression Throughput Decompression Throughput Decompression Throughput SSL/TLS Connections per Second L4 Connections per Second Max Concurrent Connections Induced Latency HARDWARE SPECS Processor CPU Cores Memory Hard Disk Additional Specs Form Factor Power Supply Operating Temperature Humidity Virtual ADC Supported INSPECTION PORTS 1 GE Ports 1 0 GE Ports	upto 48 Gbps upto 40 Gbps 40 Gbps 24 Gbps 30 Gbps 40K (RSA 2K) 25K (ECC) 1.5 M 7 M 56 M Intel Xeon 32 64 GB 512 GB SSD Option available for RAID or dual partitio Built-in TPM Chip and Hardware HSM for compliant HSM 1U/2U/4U Rack Mount Server (19- inch Redundant Power Supply (Hot Swappal 0° - 40° C 8% - 95% (non-condensing) upto 25	upto 72 Gbps	upto 120 Gbps upto 100 Gbps 100 Gbps 66 Gbps 120 Gbps 95K (RSA 2K) 48K (ECC) 4 M 15 M 160 M ms Intel Xeon 64 256 GB 2 TB SSD nization. Option available for FIPS-140 upto 50 customized over the base mode	upto 150 Gbps upto 120 Gbps 200 Gbps 132 Gbps 240 Gbps 190K (RSA 2K) 96K (ECC) 4.2 M 18 M 192 M Intel Xeon 64 512 GB 2 TB SSD 0-2 (additional charge) or Non-FIPS upto 50

No. of ports can be customized over the base model

TECHNOLOGY, CERTIFICATION & SUPPO	hrt
Platform	Haltdos Platform – hdPlatform (EAL 2+ Certified)
Technology	Signature with Threat Intelligence, Machine Learning
License	Unlimited applications. Bandwidth capping on provided license. Upgrade possible without hardware replacement upto max supported bandwidth on
Additional Licenses	hardware Optional license for LLB & DNS Firewall
Certification	FCC, ROHS, CE compliant, Common Criteria EAL 2+
Support	24x7 Support with dedicated Account Manager
Warranty	1-year software and hardware maintenance. Additional changes for extended warranty
TAC Support OPERATION MODE	TAC support in India
Network Operations	Inline Reverse Proxy, Inline Forward Proxy, Inline Bridge, Inline Router Mode, Inline L2 Transparent, Offline
Inline Modes	Proxy or Direct Server Return
Deployment Modes	1-Arm or n-Arm
Binding IP Stack	Immediate or Delayed binding Dual IPv4 & IPv6 stack
HTTP Protocols	HTTP 0.9/1.0/1.1/2.0/3.0 (QUIC) with translation
Port Mirroring	Mirror traffic / specific traffic to another NIC port
Web Socket Support	Yes
Virtual Matrix Architecture	Yes
Direct Access Mode Mitigation Modes	Yes Bypass, Record (Report Only), Learning, Mitigation (Block and Report)
Dynamic Routing Protocols	BGP, OSFP, RIP v1, RIP v2
Networking	Support for VLAN, Link Aggregation & Trunking (LACP). ARP Table, multiple Routing Tables, etc
Block Actions	Drop Request, Terminate Connection or Session, Blacklist (temporary or permanent), Send Challenge (Captcha, JavaScript), Rate Limiting
	or Tarpit
HIGH AVAILABILITY Multiple Appliances	N+1 Active - Active or Active – Passive (VRRP) with floating MAC
Management Modes	Standalone / Centralized Management (VM or appliance) with Haltdos Hawk
Secure Communication	Secure communication between centralized management and HA appliances for full state synchronization
INTEGRATION FEATURES	
Custom Threat Intel	Integration with 3 rd party Threat Intelligence (TI) feeds
Storage and Export NIMS Integration	Local retention of logs, reports and events. Support for export to 3 rd party storage Support for SNMP, NTP / SNTP, DNS, Web Proxy integration
3 rd Party Integration	Notification & Logging via SNMP, SMTP, SMS Gateway and 3 rd party integration via API hooks, CI/CD, Kubernetes
SIEM Integration	Support for integration with SIEM and Syslog services
AAA Integration	Support for integration via RADIUS and TACACS+
Identity Management	Inbuilt with support for integration with AD / SAML / LDAP
Security Tools Integration Export IOCs	Support for integration with SAST/DAST/IAST tools Support for exporting attacking IOCs via STIX / TAXII
MANAGEMENT FEATURES	supported unporting secondary was some and secondary was
Graphical User Interface (GUI)	Secure web interface over HTTPs with support for all modern browsers
Command Line Interface (CLI)	Command Line Interface over SSH or console port
API Integration	Yes (XML or JSON)
System Management Audit Trail, Logging & Recovery	IPMI 2.0 Compliant Centralized logging of system, services, MIS, incidents. Built-in MIS with policy recovery
Dashboards	Real-Time & historical dashboards with custom duration. Support for custom dashboards
System Status Dashboard	Status dashboard for 1-click health check
Reporting	Periodic daily, weekly or monthly reports in PDF or Excel
RBAC Administration Backup & Restore	Configurable user profiles with role-based access control Automatic or manual backup and restore. CLI tool for pushing current snapshot to Haltdos Cloud for diagnostics
Snapshots & Cloud Sync	Automatic and/or manual policy snapshot for diagnosis, policy creation & enforcement using AI/ML via Haltdos cloud
Policy Management	On the fly configuration updates on mitigation appliances
Certificate Management	SSL certificate management with support for Let's Encrypt certificate generation
Events / Alerts	Detailed event and alert reporting on attack, health, etc.
Network Forensic Attack Forensic	Network forensic with packet capture and traceroute Built-in utilities for investigating attackers, attack payloads and identifying false positives.
Haltdos Threat Stream	
	Definition threat intel updates (Signatures, Geo IP, Bad IP, TOR IP, Anon Proxy, etc.) from Haltdos
Updates	
ADC FEATURES	Periodic threat intel updates (Signatures, Geo IP, Bad IP, TOR IP, Anon Proxy, etc.) from Haltdos Update and upgrade management on version releases and patch updates from Haltdos. Support for multiple OS Templates
ADC FEATURES Enforce RFC Compliance	Periodic threat intel updates (Signatures, Geo IP, Bad IP, TOR IP, Anon Proxy, etc.) from Haltdos Update and upgrade management on version releases and patch updates from Haltdos. Support for multiple OS Templates Protection against invalid HTTP requests
ADC FEATURES Enforce RFC Compliance NAT & Routing	Periodic threat intel updates (Signatures, Geo IP, Bad IP, TOR IP, Anon Proxy, etc.) from Haltdos Update and upgrade management on version releases and patch updates from Haltdos. Support for multiple OS Templates Protection against invalid HTTP requests Support for client, server or full NAT, static routing for IPv4 & IPv6
ADC FEATURES Enforce RFC Compliance NAT & Routing SSL/TLS Management	Periodic threat intel updates (Signatures, Geo IP, Bad IP, TOR IP, Anon Proxy, etc.) from Haltdos Update and upgrade management on version releases and patch updates from Haltdos. Support for multiple OS Templates Protection against invalid HTTP requests Support for client, server or full NAT, static routing for IPv4 & IPv6 Support for SSL v2/v3, TLS 1.0/1.1/1.2/1.3 offloading (and re-encryption) with custom cipher suites. Client certificate-based authentication also supported, proxy SSL/TLS connections. Conditional SSL offloading by SRC, DST, SNI etc.
ADC FEATURES Enforce RFC Compliance NAT & Routing SSL/TLS Management Load Balancing	Periodic threat intel updates (Signatures, Geo IP, Bad IP, TOR IP, Anon Proxy, etc.) from Haltdos Update and upgrade management on version releases and patch updates from Haltdos. Support for multiple OS Templates Protection against invalid HTTP requests Support for client, server or full NAT, static routing for IPv4 & IPv6 Support for SSL v2/v3, TLS 1.0/1.1/1.2/1.3 offloading (and re-encryption) with custom cipher suites. Client certificate-based authentication also supported, proxy SSL/TLS connections. Conditional SSL offloading by SRC, DST, SNI etc. Layer 4 (TCP, UDP, Mail, etc.) and Layer 7 (HTTP, DNS, etc.) supported
ADC FEATURES Enforce RFC Compliance NAT & Routing SSL/TLS Management	Periodic threat intel updates (Signatures, Geo IP, Bad IP, TOR IP, Anon Proxy, etc.) from Haltdos Update and upgrade management on version releases and patch updates from Haltdos. Support for multiple OS Templates Protection against invalid HTTP requests Support for client, server or full NAT, static routing for IPv4 & IPv6 Support for SSL v2/v3, TLS 1.0/1.1/1.2/1.3 offloading (and re-encryption) with custom cipher suites. Client certificate-based authentication also supported, proxy SSL/TLS connections. Conditional SSL offloading by SRC, DST, SNI etc. Layer 4 (TCP, UDP, Mail, etc.) and Layer 7 (HTTP, DNS, etc.) supported Content based load balancing with upstream rules
ADC FEATURES Enforce RFC Compliance NAT & Routing SSL/TLS Management Load Balancing	Periodic threat intel updates (Signatures, Geo IP, Bad IP, TOR IP, Anon Proxy, etc.) from Haltdos Update and upgrade management on version releases and patch updates from Haltdos. Support for multiple OS Templates Protection against invalid HTTP requests Support for client, server or full NAT, static routing for IPv4 & IPv6 Support for SSL v2/v3, TLS 1.0/1.1/1.2/1.3 offloading (and re-encryption) with custom cipher suites. Client certificate-based authentication also supported, proxy SSL/TLS connections. Conditional SSL offloading by SRC, DST, SNI etc. Layer 4 (TCP, UDP, Mail, etc.) and Layer 7 (HTTP, DNS, etc.) supported Content based load balancing with upstream rules Round robin (RR), weighted round robin, minimum misses, persistent hash, tuneable hash, least connections, least response time, least bandwidth, SNMP
ADC FEATURES Enforce RFC Compliance NAT & Routing SSL/TLS Management Load Balancing Advanced Load Balancing	Periodic threat intel updates (Signatures, Geo IP, Bad IP, TOR IP, Anon Proxy, etc.) from Haltdos Update and upgrade management on version releases and patch updates from Haltdos. Support for multiple OS Templates Protection against invalid HTTP requests Support for client, server or full NAT, static routing for IPv4 & IPv6 Support for SSL v2/v3, TLS 1.0/1.1/1.2/1.3 offloading (and re-encryption) with custom cipher suites. Client certificate-based authentication also supported, proxy SSL/TLS connections. Conditional SSL offloading by SRC, DST, SNI etc. Layer 4 (TCP, UDP, Mail, etc.) and Layer 7 (HTTP, DNS, etc.) supported Content based load balancing with upstream rules
ADC FEATURES Enforce RFC Compliance NAT & Routing SSL/TLS Management Load Balancing Advanced Load Balancing Load Balancing Algorithms Network Optimization HTTP Optimization	Periodic threat intel updates (Signatures, Geo IP, Bad IP, TOR IP, Anon Proxy, etc.) from Haltdos Update and upgrade management on version releases and patch updates from Haltdos. Support for multiple OS Templates Protection against invalid HTTP requests Support for client, server or full NAT, static routing for IPv4 & IPv6 Support for SSL v2/v3, TLS 1.0/1.1/1.2/1.3 offloading (and re-encryption) with custom cipher suites. Client certificate-based authentication also supported, proxy SSL/TLS connections. Conditional SSL offloading by SRC, DST, SNI etc. Layer 4 (TCP, UDP, Mail, etc.) and Layer 7 (HTTP, DNS, etc.) supported Content based load balancing with upstream rules Round robin (RR), weighted round robin, minimum misses, persistent hash, tuneable hash, least connections, least response time, least bandwidth, SNMP metrics such as CPU, RAM, etc. Support for TCP buffering, multiplexing & optimization, connection pools, TCP keep alive & timeouts Support for content compression (gzip or brotili) and caching. Content minification and acceleration for mobile clients
ADC FEATURES Enforce RFC Compliance NAT & Routing SSL/TLS Management Load Balancing Advanced Load Balancing Load Balancing Algorithms Network Optimization HTTP Optimization Virtual Contexts	Periodic threat intel updates (Signatures, Geo IP, Bad IP, TOR IP, Anon Proxy, etc.) from Haltdos Update and upgrade management on version releases and patch updates from Haltdos. Support for multiple OS Templates Protection against invalid HTTP requests Support for client, server or full NAT, static routing for IPv4 & IPv6 Support for SSL v2/v3, TLS 1.0/1.1/1.2/1.3 offloading (and re-encryption) with custom cipher suites. Client certificate-based authentication also supported, proxy SSL/TLS connections. Conditional SSL offloading by SRC, DST, SNI etc. Layer 4 (TCP, UDP, Mail, etc.) and Layer 7 (HTTP, DNS, etc.) supported Content based load balancing with upstream rules Round robin (RR), weighted round robin, minimum misses, persistent hash, tuneable hash, least connections, least response time, least bandwidth, SNMP metrics such as CPU, RAM, etc. Support for TCP buffering, multiplexing & optimization, connection pools, TCP keep alive & timeouts Support for content compression (gzip or brotili) and caching. Content minification and acceleration for mobile clients Support for multiple virtual contexts along with resource allocation
ADC FEATURES Enforce RFC Compliance NAT & Routing SSL/TLS Management Load Balancing Advanced Load Balancing Load Balancing Algorithms Network Optimization HTTP Optimization Virtual Contexts Failover Management	Periodic threat intel updates (Signatures, Geo IP, Bad IP, TOR IP, Anon Proxy, etc.) from Haltdos Update and upgrade management on version releases and patch updates from Haltdos. Support for multiple OS Templates Protection against invalid HTTP requests Support for client, server or full NAT, static routing for IPv4 & IPv6 Support for SSL v2/v3, TLS 1.0/1.1/1.2/1.3 offloading (and re-encryption) with custom cipher suites. Client certificate-based authentication also supported, proxy SSL/TLS connections. Conditional SSL offloading by SRC, DST, SNI etc. Layer 4 (TCP, UDP, Mail, etc.) and Layer 7 (HTTP, DNS, etc.) supported Content based load balancing with upstream rules Round robin (RR), weighted round robin, minimum misses, persistent hash, tuneable hash, least connections, least response time, least bandwidth, SNMP metrics such as CPU, RAM, etc. Support for TCP buffering, multiplexing & optimization, connection pools, TCP keep alive & timeouts Support for content compression (gzip or brottil) and caching. Content minification and acceleration for mobile clients Support for multiple virtual contexts along with resource allocation Automatic failover & recovery. Support for marking servers up / down / backup
ADC FEATURES Enforce RFC Compliance NAT & Routing SSL/TLS Management Load Balancing Advanced Load Balancing Load Balancing Algorithms Network Optimization HTTP Optimization Virtual Contexts	Periodic threat intel updates (Signatures, Geo IP, Bad IP, TOR IP, Anon Proxy, etc.) from Haltdos Update and upgrade management on version releases and patch updates from Haltdos. Support for multiple OS Templates Protection against invalid HTTP requests Support for client, server or full NAT, static routing for IPv4 & IPv6 Support for SSL v2/v3, TLS 1.0/1.1/1.2/1.3 offloading (and re-encryption) with custom cipher suites. Client certificate-based authentication also supported, proxy SSL/TLS connections. Conditional SSL offloading by SRC, DST, SNI etc. Layer 4 (TCP, UDP, Mail, etc.) and Layer 7 (HTTP, DNS, etc.) supported Content based load balancing with upstream rules Round robin (RR), weighted round robin, minimum misses, persistent hash, tuneable hash, least connections, least response time, least bandwidth, SNMP metrics such as CPU, RAM, etc. Support for TCP buffering, multiplexing & optimization, connection pools, TCP keep alive & timeouts Support for content compression (gzip or brotili) and caching. Content minification and acceleration for mobile clients Support for multiple virtual contexts along with resource allocation
ADC FEATURES Enforce RFC Compliance NAT & Routing SSL/TLS Management Load Balancing Advanced Load Balancing Load Balancing Algorithms Network Optimization HTTP Optimization Virtual Contexts Failover Management Health Check Client Visibility Redirection Rules	Periodic threat intel updates (Signatures, Geo IP, Bad IP, TOR IP, Anon Proxy, etc.) from Haltdos Update and upgrade management on version releases and patch updates from Haltdos. Support for multiple OS Templates Protection against invalid HTTP requests Support for client, server or full NAT, static routing for IPv4 & IPv6 Support for SSL v2/v3, TLS 1.0/1.1/1.2/1.3 offloading (and re-encryption) with custom cipher suites. Client certificate-based authentication also supported, proxy SSL/TLS connections. Conditional SSL offloading by SRC, DST, SNI etc. Layer 4 (TCP, UDP, Mail, etc.) and Layer 7 (HTTP, DNS, etc.) supported Content based load balancing with upstream rules Round robin (RR), weighted round robin, minimum misses, persistent hash, tuneable hash, least connections, least response time, least bandwidth, SNMP metrics such as CPU, RAM, etc. Support for TCP buffering, multiplexing & optimization, connection pools, TCP keep alive & timeouts Support for content compression (gzip or brotili) and caching. Content minification and acceleration for mobile clients Support for multiple virtual contexts along with resource allocation Automatic failover & recovery. Support for marking servers up / down / backup Periodic server or server group health check and alerting via TCP, SSL, ICMP, SNMP, HTTP, DNS or custom script Embedding Real IP information in X-* headers, client cert information, etc REGEX based redirection rules to rewrite URLs
ADC FEATURES Enforce RFC Compliance NAT & Routing SSL/TLS Management Load Balancing Advanced Load Balancing Load Balancing Algorithms Network Optimization HTTP Optimization Virtual Contexts Failover Management Health Check Client Visibility Redirection Rules Variable Rules	Periodic threat intel updates (Signatures, Geo IP, Bad IP, TOR IP, Anon Proxy, etc.) from Haltdos Update and upgrade management on version releases and patch updates from Haltdos. Support for multiple OS Templates Protection against invalid HTTP requests Support for client, server or full NAT, static routing for IPv4 & IPv6 Support for client, server or full NAT, static routing for IPv4 & IPv6 Support for SSL v2/v3, TLS 1.0/1.1/1.2/1.3 offloading (and re-encryption) with custom cipher suites. Client certificate-based authentication also supported, proxy SSL/TLS connections. Conditional SSL offloading by SRC, DST, SNI etc. Layer 4 (TCP, UDP, Mail, etc.) and Layer 7 (HTTP, DNS, etc.) supported Content based load balancing with upstream rules Round robin (RR), weighted round robin, minimum misses, persistent hash, tuneable hash, least connections, least response time, least bandwidth, SNMP metrics such as CPU, RAM, etc. Support for TCP buffering, multiplexing & optimization, connection pools, TCP keep alive & timeouts Support for content compression (gzip or brotili) and caching. Content minification and acceleration for mobile clients Support for multiple virtual contexts along with resource allocation Automatic failover & recovery. Support for marking servers up / down / backup Periodic server or server group health check and alerting via TCP, SSL, ICMP, SNMP, HTTP, DNS or custom script Embedding Real IP information in X-* headers, client cert information, etc REGEX based redirection rules to rewrite URLs Support for embedding and using variables for A/B testing or custom load balancing
ADC FEATURES Enforce RFC Compliance NAT & Routing SSL/TLS Management Load Balancing Advanced Load Balancing Load Balancing Algorithms Network Optimization HTTP Optimization Virtual Contexts Failover Management Health Check Client Visibility Redirection Rules Variable Rules Script Rules	Periodic threat intel updates (Signatures, Geo IP, Bad IP, TOR IP, Anon Proxy, etc.) from Haltdos Update and upgrade management on version releases and patch updates from Haltdos. Support for multiple OS Templates Protection against invalid HTTP requests Support for client, server or full NAT, static routing for IPv4 & IPv6 Support for client, server or full NAT, static routing for IPv4 & IPv6 Support for SSL v2/v3, TLS 1.0/1.1/1.2/1.3 offloading (and re-encryption) with custom cipher suites. Client certificate-based authentication also supported, proxy SSL/TLS connections. Conditional SSL offloading by SRC, DST, SNI etc. Layer 4 (TCP, UDP, Mail, etc.) and Layer 7 (HTTP, DNS, etc.) supported Content based load balancing with upstream rules Round robin (RR), weighted round robin, minimum misses, persistent hash, tuneable hash, least connections, least response time, least bandwidth, SNMP metrics such as CPU, RAM, etc. Support for TCP buffering, multiplexing & optimization, connection pools, TCP keep alive & timeouts Support for content compression (gzip or brotili) and caching. Content minification and acceleration for mobile clients Support for multiple virtual contexts along with resource allocation Automatic failover & recovery. Support for marking servers up / down / backup Periodic server or server group health check and alerting via TCP, SSL, ICMP, SNMP, HTTP, DNS or custom script Embedding Real IP information in X-* headers, client cert information, etc REGEX based redirection rules to rewrite URLS Support for embedding and using variables for A/B testing or custom load balancing Embedding user defined custom code for advanced routing
ADC FEATURES Enforce RFC Compliance NAT & Routing SSL/TLS Management Load Balancing Advanced Load Balancing Load Balancing Algorithms Network Optimization HTTP Optimization Virtual Contexts Failover Management Health Check Client Visibility Redirection Rules Variable Rules Script Rules Error Handling	Periodic threat intel updates (Signatures, Geo IP, Bad IP, TOR IP, Anon Proxy, etc.) from Haltdos Update and upgrade management on version releases and patch updates from Haltdos. Support for multiple OS Templates Protection against invalid HTTP requests Support for client, server or full NAT, static routing for IPv4 & IPv6 Support for SSL v2/v3, TLS 1.0/1.1/1.2/1.3 offloading (and re-encryption) with custom cipher suites. Client certificate-based authentication also supported, proxy SSL/TLS connections. Conditional SSL offloading by SRC, DST, SNI etc. Layer 4 (TCP, UDP, Mail, etc.) and Layer 7 (HTTP, DNS, etc.) supported Content based load balancing with upstream rules Round robin (RR), weighted round robin, minimum misses, persistent hash, tuneable hash, least connections, least response time, least bandwidth, SNMP metrics such as CPU, RAM, etc. Support for TCP buffering, multiplexing & optimization, connection pools, TCP keep allive & timeouts Support for multiple virtual contexts along with resource allocation Automatic failover & recovery. Support for marking servers up / down / backup Periodic server or server group health check and alerting via TCP, SSL, ICMP, SNMP, HTTP, DNS or custom script Embedding Real IP information in X-* headers, client cert information, etc REGEX based redirection rules to rewrite URLs Support for embedding and using variables for A/B testing or custom load balancing Embedding user defined custom code for advanced routing Error rules for custom error handling
ADC FEATURES Enforce RFC Compliance NAT & Routing SSL/TLS Management Load Balancing Advanced Load Balancing Load Balancing Algorithms Network Optimization HTTP Optimization Virtual Contexts Failover Management Health Check Client Visibility Redirection Rules Variable Rules Script Rules	Periodic threat intel updates (Signatures, Geo IP, Bad IP, TOR IP, Anon Proxy, etc.) from Haltdos Update and upgrade management on version releases and patch updates from Haltdos. Support for multiple OS Templates Protection against invalid HTTP requests Support for client, server or full NAT, static routing for IPv4 & IPv6 Support for client, server or full NAT, static routing for IPv4 & IPv6 Support for SSL v2/v3, TLS 1.0/1.1/1.2/1.3 offloading (and re-encryption) with custom cipher suites. Client certificate-based authentication also supported, proxy SSL/TLS connections. Conditional SSL offloading by SRC, DST, SNI etc. Layer 4 (TCP, UDP, Mail, etc.) and Layer 7 (HTTP, DNS, etc.) supported Content based load balancing with upstream rules Round robin (RR), weighted round robin, minimum misses, persistent hash, tuneable hash, least connections, least response time, least bandwidth, SNMP metrics such as CPU, RAM, etc. Support for TCP buffering, multiplexing & optimization, connection pools, TCP keep alive & timeouts Support for content compression (gzip or brotili) and caching. Content minification and acceleration for mobile clients Support for multiple virtual contexts along with resource allocation Automatic failover & recovery. Support for marking servers up / down / backup Periodic server or server group health check and alerting via TCP, SSL, ICMP, SNMP, HTTP, DNS or custom script Embedding Real IP information in X-* headers, client cert information, etc REGEX based redirection rules to rewrite URLS Support for embedding and using variables for A/B testing or custom load balancing Embedding user defined custom code for advanced routing
ADC FEATURES Enforce RFC Compliance NAT & Routing SSL/TLS Management Load Balancing Advanced Load Balancing Load Balancing Algorithms Network Optimization HTTP Optimization Virtual Contexts Failover Management Health Check Client Visibility Redirection Rules Variable Rules Script Rules Error Handling Content Transformation End-User Fingerprinting & Monitoring DDoS Protection	Periodic threat intel updates (Signatures, Geo IP, Bad IP, TOR IP, Anon Proxy, etc.) from Haltdos Update and upgrade management on version releases and patch updates from Haltdos. Support for multiple OS Templates Protection against invalid HTTP requests Support for client, server or full NAT, static routing for IPv4 & IPv6 Support for SSL v2/v3, TLS 1.0/1.1/1.2/1.3 offloading (and re-encryption) with custom cipher suites. Client certificate-based authentication also supported, proxy SSL/TLS connections. Conditional SSL offloading by SRC, DST, SNI etc. Layer 4 (TCP, UDP, Mail, etc.) and Layer 7 (HTTP, DNS, etc.) supported Content based load balancing with upstream rules Round robin (RR), weighted round robin, minimum misses, persistent hash, tuneable hash, least connections, least response time, least bandwidth, SNMP metrics such as CPU, RAM, etc. Support for TCP buffering, multiplexing & optimization, connection pools, TCP keep alive & timeouts Support for multiple virtual contexts along with resource allocation Automatic failover & recovery. Support for marking servers up / down / backup Periodic server or server group health check and alerting via TCP, SSL, ICMP, SNMP, HTTP, DNS or custom script Embedding Real IP information in X-* headers, client cert information, etc REGEX based redirection rules to rewrite URLS Support for embedding and using variables for A/B testing or custom load balancing Embedding user defined custom code for advanced routing Error rules for custom error handling Transformation rules for data manipulation and Header rules for add / edit or delete headers in request or response Advanced user and device fingerprinting for user profiling and Real User Metrics (RUM) for performance monitoring Protection against volumetric and low & slow DDoS attacks. Support for rate limiting based on connections and requests
ADC FEATURES Enforce RFC Compliance NAT & Routing SSL/TLS Management Load Balancing Advanced Load Balancing Load Balancing Algorithms Network Optimization HTTP Optimization Virtual Contexts Failover Management Health Check Client Visibility Redirection Rules Variable Rules Script Rules Error Handling Content Transformation End-User Fingerprinting & Monitoring DDoS Protection Compliance	Periodic threat intel updates (Signatures, Geo IP, Bad IP, TOR IP, Anon Proxy, etc.) from Haltdos Update and upgrade management on version releases and patch updates from Haltdos. Support for multiple OS Templates Protection against invalid HTTP requests Support for client, server or full NAT, static routing for IPv4 & IPv6 Support for SSL v2/v3, TLS 1.0/1.1/1.2/1.3 offloading (and re-encryption) with custom cipher suites. Client certificate-based authentication also supported, proxy SSL/TLS connections. Conditional SSL offloading by SRC, DST, SNI etc. Layer 4 (TCP, UPP, Mail, etc.) and Layer 7 (HTTP, DNS, etc.) supported Content based load balancing with upstream rules Round robin (RR), weighted round robin, minimum misses, persistent hash, tuneable hash, least connections, least response time, least bandwidth, SNMP metrics such as CPU, RAM, etc. Support for TCP buffering, multiplexing & optimization, connection pools, TCP keep alive & timeouts Support for content compression (gzip or brotili) and caching. Content minification and acceleration for mobile clients Support for multiple virtual contexts along with resource allocation Automatic failover & recovery. Support for marking servers up / down / backup Periodic server or server group health check and alerting via TCP, SSL, ICMP, SNMP, HTTP, DNS or custom script Embedding Real IP information in X-* headers, client cert information, etc. REGEX based redirection rules to rewrite URLs Support for embedding and using variables for A/B testing or custom load balancing Ermbedding user defined custom code for advanced routing Error rules for custom error handling Transformation rules for data manipulation and Header rules for add / edit or delete headers in request or response Advanced user and device fingerprinting for user profiling and Real User Metrics (RUM) for performance monitoring Protection against volumetric and low & slow DDOS attacks. Support for rate limiting based on connections and requests PCI-DSS 2.0 section 6.6, HIPAA, SOC2,
ADC FEATURES Enforce RFC Compliance NAT & Routing SSL/TLS Management Load Balancing Advanced Load Balancing Load Balancing Algorithms Network Optimization HTTP Optimization Virtual Contexts Failover Management Health Check Client Visibility Redirection Rules Variable Rules Script Rules Error Handling Content Transformation End-User Fingerprinting & Monitoring DDOS Protection Compliance API Security	Periodic threat intel updates (Signatures, Geo IP, Bad IP, TOR IP, Anon Proxy, etc.) from Haltdos Update and upgrade management on version releases and patch updates from Haltdos. Support for multiple OS Templates Protection against invalid HTTP requests Support for client, server or full NAT, static routing for IPv4 & IPv6 Support for SSL v2/v3, TLS 1.0/1.1/1.2/1.3 offloading (and re-encryption) with custom cipher suites. Client certificate-based authentication also supported, proxy SSL/TLS connections. Conditional SSL offloading by SRC, DST, SNI etc. Layer 4 (TCP, UDP, Mail, etc.) and Layer 7 (HTTP, DNS, etc.) supported Content based load balancing with upstream rules Round robin (RR), weighted round robin, minimum misses, persistent hash, tuneable hash, least connections, least response time, least bandwidth, SNMP metrics such as CPU, RAM, etc. Support for TCP buffering, multiplexing & optimization, connection pools, TCP keep alive & timeouts Support for content compression (gzip or brotili) and caching. Content minification and acceleration for mobile clients Support for multiple virtual contexts along with resource allocation Automatic failover & recovery. Support for marking servers up / down / backup Periodic server or server group health check and alerting via TCP, SSL, ICMP, SNMP, HTTP, DNS or custom script Embedding Real IP information in X* headers, client cert information, etc REGEX based redirection rules to rewrite URLs Support for embedding and using variables for A/B testing or custom load balancing Embedding user defined custom code for advanced routing Error rules for custom error handling Transformation rules for data manipulation and Header rules for add / edit or delete headers in request or response Advanced user and device fingerprinting for user profiling and Real User Metrics (RUM) for performance monitoring Protection against volumetric and low & slow DDoS attacks. Support for rate limiting based on connections and requests PCI-DSS 2.0 section 6.6, HIPAA, SOC2, GDP
ADC FEATURES Enforce RFC Compliance NAT & Routing SSL/TLS Management Load Balancing Advanced Load Balancing Load Balancing Algorithms Network Optimization HTTP Optimization Virtual Contexts Failover Management Health Check Client Visibility Redirection Rules Variable Rules Script Rules Error Handling Content Transformation End-User Fingerprinting & Monitoring DDoS Protection Compliance	Periodic threat intel updates (Signatures, Geo IP, Bad IP, TOR IP, Anon Proxy, etc.) from Haltdos Update and upgrade management on version releases and patch updates from Haltdos. Support for multiple OS Templates Protection against invalid HTTP requests Support for client, server or full NAT, static routing for IPv4 & IPv6 Support for SSL v2/v3, TLS 1.0/1.1/1.2/1.3 offloading (and re-encryption) with custom cipher suites. Client certificate-based authentication also supported, proxy SSL/TLS connections. Conditional SSL offloading by SRC, DST, SNI etc. Layer 4 (TCP, UPP, Mail, etc.) and Layer 7 (HTTP, DNS, etc.) supported Content based load balancing with upstream rules Round robin (RR), weighted round robin, minimum misses, persistent hash, tuneable hash, least connections, least response time, least bandwidth, SNMP metrics such as CPU, RAM, etc. Support for TCP buffering, multiplexing & optimization, connection pools, TCP keep alive & timeouts Support for content compression (gzip or brotili) and caching. Content minification and acceleration for mobile clients Support for multiple virtual contexts along with resource allocation Automatic failover & recovery. Support for marking servers up / down / backup Periodic server or server group health check and alerting via TCP, SSL, ICMP, SNMP, HTTP, DNS or custom script Embedding Real IP information in X-* headers, client cert information, etc REGEX based redirection rules to rewrite URLs Support for embedding and using variables for A/B testing or custom load balancing Ermbedding user defined custom code for advanced routing Error rules for custom error handling Transformation rules for data manipulation and Header rules for add / edit or delete headers in request or response Advanced user and device fingerprinting for user profiling and Real User Metrics (RUM) for performance monitoring Protection against volumetric and love & slow DDOS attacks. Support for rate limiting based on connections and requests PCI-DSS 2.0 section 6.6, HIPAA, SOC2,
ADC FEATURES Enforce RFC Compliance NAT & Routing SSL/TLS Management Load Balancing Advanced Load Balancing Load Balancing Algorithms Network Optimization HTTP Optimization Virtual Contexts Failover Management Health Check Client Visibility Redirection Rules Variable Rules Script Rules Error Handling Content Transformation End-User Fingerprinting & Monitoring DDOS Protection Compliance API Security Authentication	Periodic threat intel updates (Signatures, Geo IP, Bad IP, TOR IP, Anon Proxy, etc.) from Haltdos Update and upgrade management on version releases and patch updates from Haltdos. Support for multiple OS Templates Protection against invalid HTTP requests Support for client, server or full NAT, static routing for IPv4 & IPv6 Support for SSL v2/v3, TLS 1.0/1.1/1.2/1.3 offloading (and re-encryption) with custom cipher suites. Client certificate-based authentication also supported, proxy SSL/TLS connections. Conditional SSL offloading by SRC, DST, SNI etc. Layer 4(TCP, UDP, Mail, etc.) and Layer 7 (HTTP, DNS, etc.) supported Content based load balancing with upstream rules Round robin (RR), weighted round robin, minimum misses, persistent hash, tuneable hash, least connections, least response time, least bandwidth, SNMP metrics such as CPU, RAM, etc. Support for TCP buffering, multiplexing & optimization, connection pools, TCP keep alive & timeouts Support for content compression (gzip or brotili) and caching. Content minification and acceleration for mobile clients Support for multiple virtual contexts along with resource allocation Automatic failover & recovery. Support for marking servers up / down / backup Periodic server or server group health check and alerting via TCP, SSL, ICMP, SNMP, HTTP, DNS or custom script Embedding Real IP information in X* headers, client cert information, etc REGEX based redirection rules to rewrite URLs Support for embedding and using variables for A/B testing or custom load balancing Embedding user defined custom code for advanced routing Error rules for custom error handling Transformation rules for data manipulation and Header rules for add / edit or delete headers in request or response Advanced user and device fingerprinting for user profiling and Real User Metrics (RUM) for performance monitoring Protection against volumetric and low & slow DDoS attacks. Support for rate limiting based on connections and requests PCI-DSS 2.0 section 6.6, HIPAA, SOC2, GDPR
ADC FEATURES Enforce RFC Compliance NAT & Routing SSL/TLS Management Load Balancing Advanced Load Balancing Load Balancing Algorithms Network Optimization HTTP Optimization Virtual Contexts Failover Management Health Check Client Visibility Redirection Rules Variable Rules Script Rules Error Handling Content Transformation End-User Fingerprinting & Monitoring DDOS Protection Compliance API Security Authentication Forwarding Rule WAF FEATURES Comprehensive Security	Periodic threat intel updates (Signatures, Geo IP, Bad IP, TOR IP, Anon Proxy, etc.) from Haltdos Update and upgrade management on version releases and patch updates from Haltdos. Support for multiple OS Templates Protection against invalid HTTP requests Support for Client, server or full NAT, static routing for IPv4 & IPv6 Support for Sts. vz/v3, TLS 1.0/1.1/1.2/1.3 offloading (and re-encryption) with custom cipher suites. Client certificate-based authentication also supported, proxy SSL/TLS connections. Conditional SSL offloading by SRC, DST, SNI etc. Layer 4 (TCP, UDP, Mail, etc.) and Layer 7 (HTTP, DNS, etc.) supported Content based load balancing with upstream rules Round robin (RR), weighted round robin, minimum misses, persistent hash, tuneable hash, least connections, least response time, least bandwidth, SNMP metrics such as CPU, RAM, etc. Support for TCP buffering, multiplexing & optimization, connection pools, TCP keep alive & timeouts Support for content compression (gzip or brotili) and caching. Content minification and acceleration for mobile clients Support for multiple virtual contexts along with resource allocation Automatic failover & recovery. Support for marking servers up / down / backup Periodic server or server group health check and alerting via TCP, SSL, ICMP, SNMP, HTTP, DNS or custom script Embedding Real IP information in X-* headers, client cert information, etc REGEX based redirection rules to rewrite URLs Support for multed for data manipulation and Header rules for add / edit or delete headers in request or response Advanced user and device fingerprinting for user profiling and Real User Metrics (RUM) for performance monitoring Protection against volumetric and low & slow DDoS attacks. Support for rate limiting based on connections and requests PCI-DSS 2.0 section 6.6, HIPAA, SOC2, GDPR, enforcement Sulptor for Single SignOn with multiple Auth type like Basic Auth, Form Auth, NTLM, LDAP, SAML, etc. Support for Single SignOn with multiple auth type like Basic A
ADC FEATURES Enforce RFC Compliance NAT & Routing SSL/TLS Management Load Balancing Advanced Load Balancing Load Balancing Algorithms Network Optimization HTTP Optimization Virtual Contexts Failover Management Health Check Client Visibility Redirection Rules Variable Rules Script Rules Error Handling Content Transformation End-User Fingerprinting & Monitoring DDOS Protection Compliance API Security Authentication Forwarding Rule WAF FEATURES Comprehensive Security Security Profiles	Periodic threat intel updates (Signatures, Geo IP, Bad IP, TOR IP, Anon Proxy, etc.) from Haltdos Update and upgrade management on version releases and patch updates from Haltdos. Support for multiple OS Templates Protection against invalid HTTP requests Support for client, server or full NAT, static routing for IPv4 & IPv6 Support for Sts. Vz/v3, TLS (10/1.1/2.1/3.) offloading (and re-encryption) with custom cipher suites. Client certificate-based authentication also supported, proxy SSL/TLS connections. Conditional SSL offloading by SRC, DST, SNI etc. Layer 4 (TCP, UDP, Mail, etc.) and Layer 7 (HTTP, DNS, etc.) supported Content based load balancing with upstream rules Round robin (RR), weighted round robin, minimum misses, persistent hash, tuneable hash, least connections, least response time, least bandwidth, SNMP metrics such as CPU, RAM, etc. Support for TCP buffering, multiplexing & optimization, connection pools, TCP keep alive & timeouts Support for content compression (gzip or brotili) and caching. Content minification and acceleration for mobile clients Support for multiple virtual contexts along with resource allocation Automatic failower & recovery. Support for marking servers up / down / backup Periodic server or server group health check and alerting via TCP, SSL, ICMP, SNMP, HTTP, DNS or custom script Embedding Real IP information in X-* headers, client cert information, etc REGEX based redirection rules to rewrite URLs Support for embedding and using variables for A/B testing or custom load balancing Embedding user defined custom code for advanced routing Error rules for custom error handling Transformation rules for data manipulation and Header rules for add / edit or delete headers in request or response Advanced user and device fingerprinting for user profiling and Real User Metrics (RUM) for performance monitoring Protection against volumeric and low & Slow DDoS attacks. Support for rate limiting based on connections and requests PCI-DSS 2.0 section 6.6, HIPAA, SOC2, GD
ADC FEATURES Enforce RFC Compliance NAT & Routing SSL/TLS Management Load Balancing Advanced Load Balancing Load Balancing Algorithms Network Optimization HTTP Optimization Virtual Contexts Failover Management Health Check Client Visibility Redirection Rules Variable Rules Script Rules Error Handling Content Transformation End-User Fingerprinting & Monitoring DDOS Protection Compliance API Security Authentication Forwarding Rule WAF FEATURES Comprehensive Security	Periodic threat intel updates (Signatures, Geo IP, Bad IP, TOR IP, Anon Proxy, etc.) from Haltdos Update and upgrade management on version releases and patch updates from Haltdos. Support for multiple OS Templates Protection against invalid HTTP requests Support for Client, server or full NAT, static routing for IPv4 & IPv6 Support for Sts. vz/v3, TLS 1.0/1.1/1.2/1.3 offloading (and re-encryption) with custom cipher suites. Client certificate-based authentication also supported, proxy SSL/TLS connections. Conditional SSL offloading by SRC, DST, SNI etc. Layer 4 (TCP, UDP, Mail, etc.) and Layer 7 (HTTP, DNS, etc.) supported Content based load balancing with upstream rules Round robin (RR), weighted round robin, minimum misses, persistent hash, tuneable hash, least connections, least response time, least bandwidth, SNMP metrics such as CPU, RAM, etc. Support for TCP buffering, multiplexing & optimization, connection pools, TCP keep alive & timeouts Support for content compression (gzip or brotili) and caching. Content minification and acceleration for mobile clients Support for multiple virtual contexts along with resource allocation Automatic failover & recovery. Support for marking servers up / down / backup Periodic server or server group health check and alerting via TCP, SSL, ICMP, SNMP, HTTP, DNS or custom script Embedding Real IP information in X-* headers, client cert information, etc REGEX based redirection rules to rewrite URLs Support for multed for data manipulation and Header rules for add / edit or delete headers in request or response Advanced user and device fingerprinting for user profiling and Real User Metrics (RUM) for performance monitoring Protection against volumetric and low & slow DDoS attacks. Support for rate limiting based on connections and requests PCI-DSS 2.0 section 6.6, HIPAA, SOC2, GDPR, enforcement Sulptor for Single SignOn with multiple Auth type like Basic Auth, Form Auth, NTLM, LDAP, SAML, etc. Support for Single SignOn with multiple auth type like Basic A

Micros Services Policy Protection Policy Protecti	10. 10.11	The second secon
Column Concernition Concernitio	Virtual Patching	Support for virtual patching through built-in web security scanner or upload of 3 rd party SAST / DAST / IAST scan results
Ministros Source Protection Bit Management An Activation Bit Management An Activation Ministro falls Publishe Protection agent belows and Daily does, account belower attemption, town from thempti, course, proceedings of the Activation Ministro falls Publishe Ministro	Built-in Signatures	Over 4000+ built-in signatures on various technologies, platforms and frameworks with pre-defined templates.
Bett Management Michael Agent Principion Michael Agent Michael Michael Michael	0-day Protection	Automatic learning and profiling application structure. Threat scoring and baseline creation for AI driven 0-day attack protection
Bett Management Michael Agent Principion Michael Agent Michael Michael Michael	Malicious Source Protection	Protection against TOR IP, Bad Reputation IP, dark IP, known Bots, proxies, spammers provided by Haltdos or user defined threat intel
And Austreadins Protection Notice page Protection Notice page Protection Notice page Protection Make In Page 10 Control (1997) Make In Page 10 Control (1		
Mobile top Protection A Scientify Billion of Year Scientify Billion of		
Minimize False Publics Minimize False False Recording False Minimize False Minimize False False Minimize False False Minimize False Minimize False False Minimize False Minimize False False Minimize False False Minimize False Minimize False False Minimize Fa	Anti-Automation Protection	Protection against known and 0-day bots, account takeover attempts, brute force attempts, scraping, reconnaissance, cloaking, etc
Minimier Febr Powlets HIPFVoldations Protect validations receives menutation totation & automate signature about packed the southers Relay injuried. Capital or Calman. Relay injuried. Rel	Mobile App Protection	Anti-Bot mobile SDK for Android & iOS for protecting mobile apps and communication between apps and web APIs
Minimier Febr Powlets HIPFVoldations Protect validations receives menutation totation & automate signature about packed the southers Relay injuried. Capital or Calman. Relay injuried. Rel	AV Scanning	Built-in AV scanner for malicious file upload. Support for ICAP integration for 3rd party scanners
Intervolvations and Processor solutions, recent remonitation (excelling & assort techniques) all prior impaction, managing sectorly account on the Modern Account of the Processor (Inspect of the Inspect o		1 11 11 11 11 11 11 11 11 11 11 11 11 1
Policy impection Booksist / Promised Support for foreignory or permanent bacedings and withinstelling based on p. P. prefix, uir, country, etc. Support for foreignory Support for foreignory or permanent bacedings and withinstelling based on p. P. prefix, uir, country, etc. Support for foreignory Support for foreignory Booksist / Promised Booksist / Bo		
Backet / Whiteled Caption Challenge Support for Ser caption ballings on source content of the co	HTTP Validations	Protocol validations, request normalization (encoding & evasion techniques) before inspection, managing security headers and cookies etc.
Residency Trailing Seption (1975) or capable challenger on suspicious user activity or traversor trailing ser prouse. Per our are defined paley MPL Webfoods in Proceedings of the Committee of t	Policy Inspection	Policy validation such as HTTP methods, file extension, request size, etc
Residency Trailing Seption (1975) or capable challenger on suspicious user activity or traversor trailing ser prouse. Per our are defined paley MPL Webfoods in Proceedings of the Committee of t	Blacklist / Whitelist	Support for temporary or permanent Blacklisting and Whitelisting based on IP, IP prefix, url, country, etc
Risk Umility API & Wedschark Procedure Security Neon Provention Ballin 19MA, Il Insert (auditation 19MA) (20M, 50M/50M/50M/50M) (20M, 20M, 20M/50M) (auditation 19MA) (20M, 50M/50M/50M/50M) (20M, 20M, 20M/50M/50M/50M/50M) Provided the provided of the security of the security personal committed information. Provided the Scription (20M, 20M, 20M, 20M, 20M, 20M, 20M, 20M,	· · · · · · · · · · · · · · · · · · ·	
Security Record Prevention Security Record Prevention Security Record Prevention Balli to Support for did as is prevention record and as in prevention record as in the security of the data last prevention records and as in the security of the data last prevention records and as in the security of count of the prevention of the prev		
Scourly Preced Prevention Tamper labor Life Jungsoner for data loss prevention, response filtering for sentitive personal identificative information. Tamper labor Life Jung Framer labor protection, veitable descripent, and protection, cooks legiting and encryption, etc. Variables & Scriptor Variables & Varia	- _	
Temper Proofing Condition Engineer visits for URE / presented tamper protection, website determents, folder from fined protections, cooler spings and encryption, etc. Condition Engineer visits of the process of the proofing visits of surface process of the proofing visits of	API & WebSocket Protection	Built-in XML firewall, validation of XML / JSON /SOAP/GraphQL/ Ajax /REST API requests and WebSocket requests
Tamper Proofing Connection Engine Abstraction of the Confession Engine Abstraction of the Confession Engine Abstraction Confession Engine Abstraction Confession Engine Abstraction Confession Engine Abstraction Confession Engine Conception Technology Social Vision Engineering Conception Technology Social Vision Engineering Conception Technology Social Vision Engineering Conception Engineering Engi	Security Breach Prevention	Built-in support for data leak prevention, response filtering for sensitive personal identifiable information
Consistion Expline Variables & Scriptor Variables & Variable	Tamper Proofing	Tamper rules for URL / parameter tamper protection, website defacement, hidden form field protection, cookie signing and encryption, etc.
Description Technology (appeared for user defined variables and scripts for habiding custom applications specific security policy (implement descript with metal applications) and provided the state of the part of the state of		
Sestive Data Modern Service (and the sestion of the		
Sensive Dist Making finding de Power of the Sensite of Power of the Sensite of Power of the Sensite of Power of the Sensite Office of Power of the Sensite Office O	Variables & Scripting	Support for user defined variables and scripts for building custom application specific security policy
Sensive Dist Making finding de Power of the Sensite of Power of the Sensite of Power of the Sensite of Power of the Sensite Office of Power of the Sensite Office O	Deception Technology	Implement decoys in web application to protect against advanced bots, profile attacks and trap attackers
Enforced Stowning Micro Protection Micro Protection Micro Protection Another Prote		Support for Log Rules for masking sensitive information such as passwords in logs and events
Melic Protection Molic Protection Support for protection against buffer overflow attack, man-in-the-midde attacks, sloosing malware payload, buffer overflow, SQL, SSL, LDAP injection, control of the protection protection protection against buffer overflow, specification and control of the protection protection and control of the pro		
Mice Potention 1.09 FEATURES (ADDITIONAL LICENSINO) 1.00 Relationing & Parth Selection No. Table No. Table Round robin (R.R.) weighted round trobs, minimum packet loss, persistent hash, tuneable hash, least connections, least response time, least bandwidth, etc. Path selection based on jittor, packet loss, latency, etc. Support for rotal K.N.P. (Park R.N.) AMIL (PARK P.N.) FAIR PARK P.N. (Park R.N.) AMIL (PARK P.N.) AMIL	Enforced Browsing	
Load Balancing & Path Selection NAT Bules Support for state NAT, General Selection (Control of the Control of t		authentication (2FA)
Load Balancing & Path Selection NAT Bules Support for state NAT, General Selection (Control of the Control of t	Mica Drotastias	Support for protection against buffer overflow attacks, man-in-the-middle attacks, blocking malware payload, buffer overflow, SQL, SSI, LDAP injection,
Load Balancing & Part Selection	IVIISC. Protection	
Loud Balancing & Path Selection NAT Ruises Harath Montante (Per 2 State Care) (Per 2 St	LLB FEATURES (ADDITIONAL LICENSING	
Bandwidth, etc. Parts election based on pitter, packet loss, latency, etc. NATE May be Support for State NAT, Sympan NAT, PAT, Pall NAT Limited Packet State NAT, Sympan NAT, PAT, Pall NAT Limited Packet State NAT, Sympan NAT, PAT, Pall NAT Limited Packet State State State NAT, Sympan NAT, PAT, Pall NAT Limited Packet State Stat	EED TEATOREO (ADDITIONAE EIGENGING	
MAT Rules Support to static NAT, Gyant MAT, SMC, DMAT, PAT, Fail INAT Health Monitoring Routine Rules South Mark Support to Static NAT, Gyant MAT, SMC, DMAT, PAT, Fail INAT Unknowntoring with instant failbove (1.5). Support for TCP, HTTP, DKS, CMP or script-based monitoring. Multiple monitors with AND / OR combination Dual Stark Lite Support for NAT 86 / 64 and DNS 46 / 64 with DNS Proxy Traffit Shaping Traffic Support for NAT 86 / 64 and DNS 46 / 64 with DNS Proxy Traffit Shaping Traffic Support for NAT 86 / 64 and DNS 46 / 64 with DNS Proxy Traffit Shaping Traffic American Support for NAT 86 / 64 and DNS 46 / 64 with DNS Proxy Traffit Shaping Traffic American Support for NAT 86 / 64 and DNS 46 / 64 with DNS Proxy Traffit Shaping Traffic American Support for NAT 86 / 64 and DNS 46 / 64 with DNS Proxy Traffit Shaping And Dos on Industry and Dos On Industry and Shaping And Dos On Industry	Load Balancing & Path Selection	
Health Monitoring Routing Rules Routing Rules Dual Stack LEP Dual Stack LEP		
Health Monitoring Routing Rules Routing Rules Dual Stack LEP Dual Stack LEP	NAT Rules	Support for static NAT, dynamic NAT, SNAT, DNAT, PAT, Full NAT
Reuting Rules Dual Stack Lite Support for North 76/ 6/4 and DNS 46/ 6/4 with DNS Proxy Traffic Shaping GSLB FEATURES (ADDITIONAL LICENSING) GSLB FEATURES (ADDITIONAL LICENSING) Until Salarining Cuttouring WARF in selection based on in lisk health Cuttouring WARF in selection based on link health was support for pattern, selfs, domain, etc. DOSS FEATURES (ADDITIONAL LICENSING) Cuttouring WARF in selection applied for anomaly detection and packet to company to remain was selected in the selection of the selection of the selection of the se		
Dual Stack Lies Traffic Shaping Traffic Shapin	Health Monitoring	and a section of the
Dual Stack Lies Traffic Shaping Traffic Shapin	B. H. B.	Custom rules for Static and Policy based routing
Traffice Shapings SISB FEATURES (ADDITIONAL STATE) SISB FEATURES (ADDITIONAL STATE of shaping and dos on inbound and outbound links WAN Load Balancing, WAN Load Balancing, Load Balancing, All Control of the state		
Global Load Balancing, Routing fraffic across multiple data centers based on health checks WAN Load Balancing, Routing fraffic across multiple data centers based on health checks WAN Load Balancing, Routing fraffic across multiple data centers based on health checks Operation Mode Operation Mode Operation Mode Option for Authoritative or Recursive operational modes with support for various DNS record types such as A, AAAA, MM, TXT, PTR, etc. Custom Signatures Support DNS over HTTP, UDP, TCP, 8 SSI as well as DNSSEC ONS Firewall Post Post Fewall Post Fewall Post Fewall Blacklist / Whitelist Custom Signatures Support for pure remained Balakishing and Whitelisting based on IP, IP prefix, domain, country, etc. Custom Signatures DOSS FEATURES (ADDITIONAL LICENSING) Comprehensive Protection DOSD bettom 8 Mitigation Attack detection 8 mitigation in less than 188 and 10s respectively BlackActions Dos Beak Mitigation Attack detection 8 mitigation in less than 188 and 10s respectively BlockActions BlockActions Block Actions Block Complance Benefit Protectional Benefit Protectional Specific Traffic Companies Protection applicate Specific Traffic (based on proto, src, dst, etc.) Protectional Specific Traffic Companies Protection applicate Specific Traffic Companies Protection applicate Specific Traffic Companies, responses, ecolopses, etc. Beladiary Whitelist Multiple Security Profiles Port Milroring Retal Limit & Op Shangement Retal Limit & Op Shangement Beladiary Milroring Retal Limit & Op Shangement Beladiary Milroring Automatic detection against Took Page Repea	Dual Stack Lite	Support for NAT 46 / 64 and DNS 46 / 64 with DNS Proxy
Global Load Balancing WAN Load Balancing Load Balancing Operation Mode Operation	Traffic Shaping	Traffic shaping and QoS on inbound and outbound links
Global Load Balancing WAN Load Balancing Load Balancing Operation Mode Operation	GSLB FEATURES (ADDITIONAL LICENS)	NG)
Used Balancing (Agorthms Support for Least common C		
Load Balancing Algorithms	- _	
Operation Mode Routing Rules Routi	WAN Load Balancing	Outbound WAN link selection based on link health
Returning Kulles Network Mode Network Mode Network Mode DNS Firewall Blackidt, Withtelist Custom Signatures Support For premate Blackidting and withtelisting based on IP, Perfeth, Onania, country, etc. Support For premate Blackidting and withtelisting based on IP, Perfeth, Onania, country, etc. DDOS FEATURES (ADDITIONAL LIGENSNO) Comprehensive Protection Dos Detection & Mitigation Attack detection & mitigation in less than 18s and 10s respectively Blackidt, Mithelist Comprehensive Protection Dos Detection & Mitigation Attack detection & mitigation in less than 18s and 10s respectively Blackidt, Mithelist Attack detection & mitigation in less than 18s and 10s respectively Black Actions Block Actions Block Actions Block Actions Block Actions Block Actions Support for integration with Haltdos Cloud Scrubbing or ISP clean pipe services Block Protection Deep Packet Inspection Protection against mainformed packets (TCP, UDP, ICMP, Ping of death, DNS, HTTP, SIP, SIMMP, IPv4, IPv6, Fragmented packets, etc.) Fortection against mainformed packets (TCP, UDP, ICMP, Ping of death, DNS, HTTP, SIP, SIMMP, IPv4, IPv6, Fragmented packets, etc.) Behavior Analysis Multiple Security Profiles Port Mirroring Rate Limit & QoS Management Blackidts / Wilhelist Support for multiple security profiles for enforcing different policy for different sub-networks (Src, Dst IP Prefix, VLANI). Default Global security profile Rate Limit & QoS Management Blackidts / Wilhelist Support for tour indended and ada of Samagement with option for rate limit of specific traffic (based on proto, src, dst, etc.) Protection against main spils for anomaly detection and packets corring technology Support for multiple security profiles for enforcing different policy for different sub-networks (Src, Dst IP Prefix, VLANI). Default Global security profile Rate Limit & QoS Management Blackidts / Wilhelist Support for tour defined custom rules with support for Refex and byte matching Tour Samagement Signatures for Known Vu	Load Balancing Algorithms	Support for Least connection, Proximity, Round Robin, Weighted RR, Persistent Hash, Geo, etc.
Returning Kulles Network Mode Network Mode Network Mode DNS Firewall Blackidt, Withtelist Custom Signatures Support For premate Blackidting and withtelisting based on IP, Perfeth, Onania, country, etc. Support For premate Blackidting and withtelisting based on IP, Perfeth, Onania, country, etc. DDOS FEATURES (ADDITIONAL LIGENSNO) Comprehensive Protection Dos Detection & Mitigation Attack detection & mitigation in less than 18s and 10s respectively Blackidt, Mithelist Comprehensive Protection Dos Detection & Mitigation Attack detection & mitigation in less than 18s and 10s respectively Blackidt, Mithelist Attack detection & mitigation in less than 18s and 10s respectively Black Actions Block Actions Block Actions Block Actions Block Actions Block Actions Support for integration with Haltdos Cloud Scrubbing or ISP clean pipe services Block Protection Deep Packet Inspection Protection against mainformed packets (TCP, UDP, ICMP, Ping of death, DNS, HTTP, SIP, SIMMP, IPv4, IPv6, Fragmented packets, etc.) Fortection against mainformed packets (TCP, UDP, ICMP, Ping of death, DNS, HTTP, SIP, SIMMP, IPv4, IPv6, Fragmented packets, etc.) Behavior Analysis Multiple Security Profiles Port Mirroring Rate Limit & QoS Management Blackidts / Wilhelist Support for multiple security profiles for enforcing different policy for different sub-networks (Src, Dst IP Prefix, VLANI). Default Global security profile Rate Limit & QoS Management Blackidts / Wilhelist Support for tour indended and ada of Samagement with option for rate limit of specific traffic (based on proto, src, dst, etc.) Protection against main spils for anomaly detection and packets corring technology Support for multiple security profiles for enforcing different policy for different sub-networks (Src, Dst IP Prefix, VLANI). Default Global security profile Rate Limit & QoS Management Blackidts / Wilhelist Support for tour defined custom rules with support for Refex and byte matching Tour Samagement Signatures for Known Vu	Operation Mode	Option for Authoritative or Recursive operational modes with support for various DNS record types such as A AAAA MX TXT PTR etc
Network Mode DNS Freewall DNS Free Free Free Free Free Free Free Fre	<u>-</u>	
Blackist / Whitelets Blackist / Blackist / Whitelets Blackist / Whitelest / Bla	Pouting Pulos	
Bucklist / Whitelets (Cutom Signatures Support for permanent Blacklisting and Whiteletting based on IP, IP prefix, domain, country, etc. DDOS FEATURES (ADDITIONAL LICENSING) Comprehensive Protection DDOS Detection & Mitigation DDOS Detection & Mitigation DDOS Detection & Mitigation DDOS Detection & Mitigation DDOS Integration Attack detection & Mitigation in less than 18s and 105 respectively DDOS Integration Block Actions DDOS Integration DDOS Integration DDOS Integration Blovinetional DDOS Integration Blovinetional DDOS Integration DDOS Inte		
DOS FEATURES (ADDITIONAL LICERSING) DOS PEATURES (ADDITIONAL LICERSING) Comprehensive Protection DOS Detection & Mitigation Attack detection & mitigation in less than 18s and 10s respectively Block Actions Dos Detection & Mitigation Attack detection & mitigation in less than 18s and 10s respectively Block Actions Dos Detection & Mitigation Attack detection & mitigation in less than 18s and 10s respectively Block Actions Deep Packet Inspection Bet Protection against malformed packets (TCP, UDP, ICMP, Ping of death, DNS, HTTP, SIP, SNMP, IPv4, IPv6, Fragmented packets, etc.) Enforce RC Compliance Bet Protection Bethaviour Analysis Multiple Security Profiles Port Mirroring Rate Limit & QoS Management Balkisity Whitelist Support for wind lipit security profiles Port Mirroring Rate Limit & QoS Management Balkisity Whitelist Support for male Backlisting and Whitelisting based on IP, IP prefix, Onania, country, etc. Malicious Source Protection All Malicious Source Protection Signatures Support for Tro Interperative proteins Syn Flood Protection Connection Based Protection DNS Protection Signatures Connection Based Protection DNS Protection All Malicious Source Protection DNS Protection Signatures Connection Based Protection DNS Protection Note Protection against TOR IP, Bad Reputation IP / domain, dark ip, malicious Bots, proxies, resolvers, etc Support for Tro IPTP, DNS challenge and response for validation of traffic from suspicious sources Connection Based Protection DNS Protection Signatures Connection Based Protection Note Street Connection Based Protection Note Street Connection Based Protection DNS Protection Ballist in Use for Amount of the Connection Against Connection Agains		
DOS FEATURES (ADDITIONAL LICERSING) DOS PEATURES (ADDITIONAL LICERSING) Comprehensive Protection DOS Detection & Mitigation Attack detection & mitigation in less than 18s and 10s respectively Block Actions Dos Detection & Mitigation Attack detection & mitigation in less than 18s and 10s respectively Block Actions Dos Detection & Mitigation Attack detection & mitigation in less than 18s and 10s respectively Block Actions Deep Packet Inspection Bet Protection against malformed packets (TCP, UDP, ICMP, Ping of death, DNS, HTTP, SIP, SNMP, IPv4, IPv6, Fragmented packets, etc.) Enforce RC Compliance Bet Protection Bethaviour Analysis Multiple Security Profiles Port Mirroring Rate Limit & QoS Management Balkisity Whitelist Support for wind lipit security profiles Port Mirroring Rate Limit & QoS Management Balkisity Whitelist Support for male Backlisting and Whitelisting based on IP, IP prefix, Onania, country, etc. Malicious Source Protection All Malicious Source Protection Signatures Support for Tro Interperative proteins Syn Flood Protection Connection Based Protection DNS Protection Signatures Connection Based Protection DNS Protection All Malicious Source Protection DNS Protection Signatures Connection Based Protection DNS Protection Note Protection against TOR IP, Bad Reputation IP / domain, dark ip, malicious Bots, proxies, resolvers, etc Support for Tro IPTP, DNS challenge and response for validation of traffic from suspicious sources Connection Based Protection DNS Protection Signatures Connection Based Protection Note Street Connection Based Protection Note Street Connection Based Protection DNS Protection Ballist in Use for Amount of the Connection Against Connection Agains	Network Mode	Support DNS over HTTP, UDP, TCP & SSL as well as DNSSEC
DOS FEATURES (ADDITIONAL LICENSING) Comprehensive Protection Dos Detection & Mitigation Attack detection & mitigation in less than 18s and 10s respectively Block Actions Block Actions Blob Integration Bl	Network Mode DNS Firewall	Support DNS over HTTP, UDP, TCP & SSL as well as DNSSEC Protecting DNS infrastructure from bot attacks, data exfiltration attacks, RPZ policy
Comprehensive Protection DoSo Detection & Mitigation Block Actions Block Actions Block Actions Block Actions Block Actions Block Actions Block Actions Block Actions Block Actions Block Actions Block Actions Block Actions Block Actions Block Actions Block Action	Network Mode DNS Firewall Blacklist / Whitelist	Support DNS over HTTP, UDP, TCP & SSL as well as DNSSEC Protecting DNS infrastructure from bot attacks, data exfiltration attacks, RPZ policy Support for permanent Blacklisting and Whitelisting based on IP, IP prefix, domain, country, etc.
DDOS Detection & Mitigation Block Actions Block Action Block Block Action Block Block Action Block Block Action Block Action Block Action Block Block Action Block Block Action Block Block Action Block Block	Network Mode DNS Firewall Blacklist / Whitelist Custom Signatures	Support DNS over HTTP, UDP, TCP & SSL as well as DNSSEC Protecting DNS infrastructure from bot attacks, data exfiltration attacks, RPZ policy Support for permanent Blacklisting and Whitelisting based on IP, IP prefix, domain, country, etc. Support for user defined custom rules with support for pattern, suffix, domain, etc.
Block Actions Drop Packet, Terminate Connection (RST), Blacklist (temporary or permanent), Send Challenge (TCP, HTTP, DNS), Rate Limiting Hybrid DDos Integration Support for integration with Haltdos Cloud Scrubbing or ISP clean pipe services Bi-Directional Support for integration with Haltdos Cloud Scrubbing or ISP clean pipe services Bi-Directional Support for integration with Haltdos Cloud Scrubbing or ISP clean pipe services Broth Protection against misbehaving cleints sending in misdle or unto 15 atta packets Bot Protection against misbehaving cleints sending limital or unto 15 atta packets Bot Protection against misbehaving cleints sending limital or unto 15 atta packets Bot Protection against misbehaving cleints sending limital or unto 15 atta packets Automatic detection and blocking of bot traffic with support for manual bot policy Behaviour Analysis Protection and plocking of bot traffic with support for manual bot policy Both Military Support for mittiglie security profiles for enforcing different policy for different sub-networks (Src, Dst IP Prefix, VLAN). Default Global security profile Port Mirroring Mirror traffic / specific traffic to another NIC port Rate Limit & QoS Management Malicious Source Protection Protection against TOR IP, Bad Reputation IP / domain, dark IP, malicious Bots, proxies, resolvers, etc Support for user defined custom rules with support for REGK and byte matching Challenge & Response Connection Based Protection TCP SYM Rood protection with SYM Proxy and connection aging Challenge & Response Connection Based Protection Signatures for Known Vulnerabilities Built-in NS Riewall capability for protecting Disk infrastructure against DNS Dobs attacks (Water Torture, NXDomain, etc.) Protection against TOR IP, Bad Reputation IP / Sym Analysis and Protection against DNS Dobs attacks (Water Torture, NXDomain, etc.) Protection against Vide Protection Protection Protection Symbor	Network Mode DNS Firewall Blacklist / Whitelist Custom Signatures DDOS FEATURES (ADDITIONAL LICENSI	Support DNS over HTTP, UDP, TCP & SSL as well as DNSSEC Protecting DNS infrastructure from bot attacks, data exfiltration attacks, RPZ policy Support for permanent Blacklisting and Whitelisting based on IP, IP prefix, domain, country, etc. Support for user defined custom rules with support for pattern, suffix, domain, etc. NG)
Hybrid DDoS Integration Bi-Directional Bi-Directional Deep Packet Inspection Protection against misformed packets (TPC, UDP, ICMP, Ping of death, DNS, HTTP, SIP, SNMP, IPv4, IPv6, Fragmented packets, etc.) Enforce RFC Compliance Bot Protection against misformed packets (TPC, UDP, ICMP, Ping of death, DNS, HTTP, SIP, SNMP, IPv4, IPv6, Fragmented packets, etc.) Behaviour Analysis Network behaviour analysis for anomaly detection and packet scoring technology Support for multiple security profiles Port Mirroring Port Mirroring Mirror traffic / specific traffic to another NIC port Rate Limit & Qos Management Blacklist / Whitelist Support for temporary or permanent Blacklisting and Whitelisting based on IP, IP prefix, domain, country, etc. Malicious Source Protection Custom Signatures Syn Flood Protection Custom Signatures TCP Syn flood protection with Syn Proxy and connection aging Challenge & Response Connection Based Protection Bullici DNS firewall capability for protecting DNS infrastructure against TOR protection against TOR including about a slow slow attacks such as Sockstress, connection / src, zombie flood, SSL renegotiations, etc DNS Protection Signatures for Known Vulnerabilities VPN FEATURES (ADDITIONAL LICENSING) HTTP Protocols Mark Routing Support for reminer measures and dynamic signature creation upon attack detection Support for reminer measures and dynamic signature creation upon attack detection Support for reminer measures and dynamic signature creation upon attack detection Support for reminer measures and dynamic signature creation upon attack detection Support for reminer measures and dynamic signature creation upon attack detection Support for reminer measures and dynamic signature creation upon attack detection Support for reminer measures and dynamic signature creation upon attack detection Support for St. V2/V3, TIS 1.0/1.1/1.2/13 offloading (and re-encryption) with custom cipher suites. Client certificate-base d authentication Authentication Password,	Network Mode DNS Firewall Blacklist / Whitelist Custom Signatures DDOS FEATURES (ADDITIONAL LICENSI	Support DNS over HTTP, UDP, TCP & SSL as well as DNSSEC Protecting DNS infrastructure from bot attacks, data exfiltration attacks, RPZ policy Support for permanent Blacklisting and Whitelisting based on IP, IP prefix, domain, country, etc. Support for user defined custom rules with support for pattern, suffix, domain, etc. NG)
Hybrid DDoS Integration Bi-Directional Bi-Directional Deep Packet Inspection Protection against misformed packets (TPC, UDP, ICMP, Ping of death, DNS, HTTP, SIP, SNMP, IPv4, IPv6, Fragmented packets, etc.) Enforce RFC Compliance Bot Protection against misformed packets (TPC, UDP, ICMP, Ping of death, DNS, HTTP, SIP, SNMP, IPv4, IPv6, Fragmented packets, etc.) Behaviour Analysis Network behaviour analysis for anomaly detection and packet scoring technology Support for multiple security profiles Port Mirroring Port Mirroring Mirror traffic / specific traffic to another NIC port Rate Limit & Qos Management Blacklist / Whitelist Support for temporary or permanent Blacklisting and Whitelisting based on IP, IP prefix, domain, country, etc. Malicious Source Protection Custom Signatures Syn Flood Protection Custom Signatures TCP Syn flood protection with Syn Proxy and connection aging Challenge & Response Connection Based Protection Bullici DNS firewall capability for protecting DNS infrastructure against TOR protection against TOR including about a slow slow attacks such as Sockstress, connection / src, zombie flood, SSL renegotiations, etc DNS Protection Signatures for Known Vulnerabilities VPN FEATURES (ADDITIONAL LICENSING) HTTP Protocols Mark Routing Support for reminer measures and dynamic signature creation upon attack detection Support for reminer measures and dynamic signature creation upon attack detection Support for reminer measures and dynamic signature creation upon attack detection Support for reminer measures and dynamic signature creation upon attack detection Support for reminer measures and dynamic signature creation upon attack detection Support for reminer measures and dynamic signature creation upon attack detection Support for reminer measures and dynamic signature creation upon attack detection Support for St. V2/V3, TIS 1.0/1.1/1.2/13 offloading (and re-encryption) with custom cipher suites. Client certificate-base d authentication Authentication Password,	Network Mode DNS Firewall Blacklist / Whitelist Custom Signatures DDOS FEATURES (ADDITIONAL LICENS) Comprehensive Protection	Support DNS over HTTP, UDP, TCP & SSL as well as DNSSEC Protecting DNS infrastructure from bot attacks, data exfiltration attacks, RPZ policy Support for permanent Blacklisting and Whitelisting based on IP, IP prefix, domain, country, etc. Support for user defined custom rules with support for pattern, suffix, domain, etc. NG) Layer 3 to Layer 7 protection covering Network, Protocol, Application, Reflection / Amplification and 0-day DDoS attacks
Be-Directional Support for both inbound and outbound traffic protection Deep Packet Inspection Protection against malformed packets (TCP, UDP, ICMP, Ping of death, DNS, HTTP, SIP, SNMP, IPv4, IPv6, Fragmented packets, etc.) Enforce RFC Compliance Bot Protection Behaviour Analysis Behaviour Analysis Network behaviour analysis Multiple Security Profiles Port Mirroring Rate Limit & QoS Management Bakkist / Whitelst Bakkist / Whitelst Bakkist / Whitelst Support for temporary or permanent Blackisting and Whitelsting and Support for real limit of specific traffic (based on proto, src, dst, etc.) Malicious Source Protection Custom Signatures SYN Flood Protection Challenge & Response Connection Based Protection DNS Protection L7D DNS Protection L7D DNS Protection DNS Protection Signatures for Known Vulnerabilities Built-in DNS firewall capability for protecting DNS infrastructure against DNS DDOS attacks (Water Torture, NXDomain, etc.) Protection against TOR DN, Alanch Signatures for Known Vulnerabilities SUPP FEATURES (ADDITIONAL LICENSING) Client Support Or VLAN, Link Aggregation & Trunking (LACP) Support for reasons and support for retenting Protection Authentic Learning contection Dynamic Routing Protocols NAT& Routing Support for VLAN, Link Aggregation & Trunking (LACP) Support for retenting mile of creating multiple users or groups with fine grained access to different part of network and/or services	Network Mode DNS Firewall Blacklist / Whitelist Custom Signatures DDOS FEATURES (ADDITIONAL LICENS) Comprehensive Protection DDOS Detection & Mitigation	Support DNS over HTTP, UDP, TCP & SSL as well as DNSSEC Protecting DNS infrastructure from bot attacks, data exfiltration attacks, RPZ policy Support for permanent Blacklisting and Whitelisting based on IP, IP prefix, domain, country, etc. Support for user defined custom rules with support for pattern, suffix, domain, etc. NG) Layer 3 to Layer 7 protection covering Network, Protocol, Application, Reflection / Amplification and 0-day DDoS attacks Attack detection & mitigation in less than 18s and 10s respectively
Deep Packet Inspection Enforce RFC Compliance Bot Protection against malformed packets (TCP, UDP, ICMP, Ping of death, DNS, HTTP, SIP, SNMP, IPv4, IPv6, Fragmented packets, etc.) Protection against misbehaving clients sending invalid or out of state packets Bot Protection Behaviour Analysis Multiple Security Profiles Port Mirroring Mirror traffic Vibracy Profiles Port Mirroring Mirror traffic Vibracy Profiles Port Mirroring Mirror traffic Vibracy Profiles Blacklist / Whitelist Blacklist / Whitelist Malicious Source Protection Custom Signatures SYN Flood Protection Challenge & Response Connection Based Protection DNS Protection DNS Protection Bull-in DNS firewall capability for protection against TOR IP, Bad Reputation IP / domain, dark IP, malicious Bots, proxies, resolvers, etc Support for custom rules with Support for REGEX and byte matching Signatures for known Vulnerabilities Protection against TOR Doos attacks such as sockstress, connection / src, zombie flood, SSL renegotiations, etc Machine Learning Protection Signatures for known Vulnerabilities Protection against Not Solven Automatic learning counter measures and dynamic signature creation upon attack detection Dynamic Routing Protocols SIJ/TLS Management Dynamic Routing Protocols Automatic learning Protection Dynamic Routing Protocols Signatures for known Vulnerabilities Protection Seep Cyll Syll Syll Syll Syll Syll Syll Syll	Network Mode DNS Firewall Blacklist / Whitelist Custom Signatures DDOS FEATURES (ADDITIONAL LICENS) Comprehensive Protection DDOS Detection & Mitigation Block Actions	Support DNS over HTTP, UDP, TCP & SSL as well as DNSSEC Protecting DNS infrastructure from bot attacks, data exfiltration attacks, RPZ policy Support for permanent Blacklisting and Whitelisting based on IP, IP prefix, domain, country, etc. Support for user defined custom rules with support for pattern, suffix, domain, etc. NG) Layer 3 to Layer 7 protection covering Network, Protocol, Application, Reflection / Amplification and 0-day DDoS attacks Attack detection & mitigation in less than 18s and 10s respectively Drop Packet, Terminate Connection (RST), Blacklist (temporary or permanent), Send Challenge (TCP, HTTP, DNS), Rate Limiting
Enforce RFC Compliance Bor Protection Bor Protection Behaviour Analysis Network behaviour analysis Multiple Security Profiles Port Mirroring Retal Imit & QoS Management Blacklist / Whitelist Support for multiple security profile profile Retal Imit & QoS Management Blacklist / Whitelist Support for multiple security profile profile Rate Limit & QoS Management Blacklist / Whitelist Support for temporary or permanent Blacklisting and Whitelisting based on IP, IP prefix, domain, country, etc. Protection against TOR IP, Bad Reputation IP / domain, dark IP, malicious Bots, proxies, resolvers, etc Support for user defined custom rules with support for REGEX and byte matching TCP SYN flood protection Challenge & Response Connection Based Protection DNS Protection DNS Protection DNS Protection Machine Learning Protection Machine Learning Protection Signatures for Room vulnerabilities Built-in rules for known vulnerabilities (server, web, mail, FTP, SIP, SQL, DNS, IPS Signatures etc.) VPN FEATURES (ADDITIONAL LICENSING) HTTP Protocols SUPPort for VAIN, Link Aggregation & Trunking (LACP) Client Support Support for VAIN, Link Aggregation & Support for VAIN, Link Aggregation & Trunking (LACP) Support for valid Routing Protection NATE Routing Support for viewind was public land, Raggregation & Trunking (LACP) Support for VICAN, Link Aggregation & Trunking (LACP) Support for VICAN, Link Aggregation & Support for VICAN, Link Aggregation & Trunking (LACP) Support for vication multiple users, user groups with fine grained access to different policy of other protectics Support for vication against to was publicable users, user groups with fine grained access to different part of network and/or services	Network Mode DNS Firewall Blacklist / Whitelist Custom Signatures DDOS FEATURES (ADDITIONAL LICENSI Comprehensive Protection DDOS Detection & Mitigation Block Actions Hybrid DDOS Integration	Support DNS over HTTP, UDP, TCP & SSL as well as DNSSEC Protecting DNS infrastructure from bot attacks, data exfiltration attacks, RPZ policy Support for permanent Blacklisting and Whitelisting based on IP, IP prefix, domain, country, etc. Support for user defined custom rules with support for pattern, suffix, domain, etc. NG) Layer 3 to Layer 7 protection covering Network, Protocol, Application, Reflection / Amplification and 0-day DDoS attacks Attack detection & mitigation in less than 18s and 10s respectively Drop Packet, Terminate Connection (RST), Blacklist (temporary or permanent), Send Challenge (TCP, HTTP, DNS), Rate Limiting Support for integration with Haltdos Cloud Scrubbing or ISP clean pipe services
Bot Protection Behaviour Analysis Multiple Security Profiles Multiple Security Profiles Port Mirroring Rate Limit & QoS Management Blacklist / Whitelist Malicious Source Protection Custom Signatures SYN Flood Protection Challenge & Respons SYN Flood Protection Challenge & Respons Connection Based Protection DNS Protection DNS Protection Machine Learning Protection Machine Learning Protection Signatures for Known Vulnerabilities Protection against TOR Is solowal translation SL/TLS Management SL/TLS Management SL/TLS Management Machine Learning Protection Slyn Food Protection Slyn Food Protection Slyn Food Protection Machine Learning Protection Slyn Food Protection Slyn Food Protection Machine Learning Protection Slyn Food Protection Slyn Food Protection Machine Learning Protection Slyn Food Protection Slyn Food Protection Machine Learning Protection Slyn Food Protection Slyn Food Protection Signatures for Known Vulnerabilities SL/TLS Management Dynamic Routing Protocols Begin Tor SL v2/V3, TLS 1.0/1.1/2.0 with translation Dynamic Routing Protocols Dynamic Routing Protocols Dynamic Routing Protocols Support for SL v2/V3, TLS 1.0/1.1/1.2/1.3 offloading (and re-encryption) with custom cipher suites. Client certificate-based authentication Support for VLAN, Link Aggregation & Trunking (LACP) Support for Client, sever or full NAT, static rore full NAT, static rore for fine protection NAT & Routing Support for Client, sever or full NAT, static rore for for protection or full NAT, static rore for fine protection NAT & Routing Support for Client, sever or full NAT, static rore for for fine protection Nat Routing Support for Client, sever or full NAT, static rore for fine for protection and for protection or for fine for protection or for fill NAT, static rore for f	Network Mode DNS Firewall Blacklist / Whitelist Custom Signatures DDOS FEATURES (ADDITIONAL LICENSI Comprehensive Protection DDOS Detection & Mitigation Block Actions Hybrid DDOS Integration	Support DNS over HTTP, UDP, TCP & SSL as well as DNSSEC Protecting DNS infrastructure from bot attacks, data exfiltration attacks, RPZ policy Support for permanent Blacklisting and Whitelisting based on IP, IP prefix, domain, country, etc. Support for user defined custom rules with support for pattern, suffix, domain, etc. NG) Layer 3 to Layer 7 protection covering Network, Protocol, Application, Reflection / Amplification and 0-day DDoS attacks Attack detection & mitigation in less than 18s and 10s respectively Drop Packet, Terminate Connection (RST), Blacklist (temporary or permanent), Send Challenge (TCP, HTTP, DNS), Rate Limiting Support for integration with Haltdos Cloud Scrubbing or ISP clean pipe services
Bot Protection Behaviour Analysis Multiple Security Profiles Multiple Security Profiles Port Mirroring Rate Limit & QoS Management Blacklist / Whitelist Malicious Source Protection Custom Signatures SYN Flood Protection Challenge & Respons SYN Flood Protection Challenge & Respons Connection Based Protection DNS Protection DNS Protection Machine Learning Protection Machine Learning Protection Signatures for Known Vulnerabilities Protection against TOR Is solowal translation SL/TLS Management SL/TLS Management SL/TLS Management Machine Learning Protection Slyn Food Protection Slyn Food Protection Slyn Food Protection Machine Learning Protection Slyn Food Protection Slyn Food Protection Machine Learning Protection Slyn Food Protection Slyn Food Protection Machine Learning Protection Slyn Food Protection Slyn Food Protection Machine Learning Protection Slyn Food Protection Slyn Food Protection Signatures for Known Vulnerabilities SL/TLS Management Dynamic Routing Protocols Begin Tor SL v2/V3, TLS 1.0/1.1/2.0 with translation Dynamic Routing Protocols Dynamic Routing Protocols Dynamic Routing Protocols Support for SL v2/V3, TLS 1.0/1.1/1.2/1.3 offloading (and re-encryption) with custom cipher suites. Client certificate-based authentication Support for VLAN, Link Aggregation & Trunking (LACP) Support for Client, sever or full NAT, static rore full NAT, static rore for fine protection NAT & Routing Support for Client, sever or full NAT, static rore for for protection or full NAT, static rore for fine protection NAT & Routing Support for Client, sever or full NAT, static rore for for fine protection Nat Routing Support for Client, sever or full NAT, static rore for fine for protection and for protection or for fine for protection or for fill NAT, static rore for f	Network Mode DNS Firewall Blacklist / Whitelist Custom Signatures DDOS FEATURES (ADDITIONAL LICENSI Comprehensive Protection DDOS Detection & Mitigation Block Actions Hybrid DDOS Integration Bi-Directional	Support DNS over HTTP, UDP, TCP & SSL as well as DNSSEC Protecting DNS infrastructure from bot attacks, data exfiltration attacks, RPZ policy Support for permanent Blacklisting and Whitelisting based on IP, IP prefix, domain, country, etc. Support for user defined custom rules with support for pattern, suffix, domain, etc. NG) Layer 3 to Layer 7 protection covering Network, Protocol, Application, Reflection / Amplification and 0-day DDoS attacks Attack detection & mitigation in less than 18s and 10s respectively Drop Packet, Terminate Connection (RST), Blacklist (temporary or permanent), Send Challenge (TCP, HTTP, DNS), Rate Limiting Support for integration with Haltdos Cloud Scrubbing or ISP clean pipe services Support for both inbound and outbound traffic protection
Behaviour Analysis Multiple Security Profiles Multiple Security Profiles Port Mirroring Mirror traffic / specific traffic to another NIC port Rate Limit & QoS Management Blacklist / Whitelist Blacklist / Whitelist support for REGEX and byte matching Blacklist / Whitelist blacklist management Blacklist / Whitelist support for REGEX and byte matching Blacklist / Whitelist support for REGEX and byte matching Blacklist / Whitelist support for REGEX and byte matching Blacklist / Whitelist support for REGEX and byte matching Blacklist / Whitelist support for REGEX and byte matching	Network Mode DNS Firewall Blacklist / Whitelist Custom Signatures DDOS FEATURES (ADDITIONAL LICENSI Comprehensive Protection DDOS Detection & Mitigation Block Actions Hybrid DDOS Integration Bi-Directional Deep Packet Inspection	Support DNS over HTTP, UDP, TCP & SSL as well as DNSSEC Protecting DNS infrastructure from bot attacks, data exfiltration attacks, RPZ policy Support for permanent Blacklisting and Whitelisting based on IP, IP prefix, domain, country, etc. Support for user defined custom rules with support for pattern, suffix, domain, etc. NG) Layer 3 to Layer 7 protection covering Network, Protocol, Application, Reflection / Amplification and 0-day DDoS attacks Attack detection & mitigation in less than 18s and 10s respectively Drop Packet, Terminate Connection (RST), Blacklist (temporary or permanent), Send Challenge (TCP, HTTP, DNS), Rate Limiting Support for integration with Haltdos Cloud Scrubbing or ISP clean pipe services Support for both inbound and outbound traffic protection Protection against malformed packets (TCP, UDP, ICMP, Ping of death, DNS, HTTP, SIP, SNMP, IPv4, IPv6, Fragmented packets, etc.)
Multiple Security Profiles Port Mirroring Port Mirroring Rate Limit & QoS Management Blacklist / Whitelist Support for temporary or permanent Blacklisting and Whitelisting based on IP, IP prefix, domain, country, etc. Malicious Source Protection Custom Signatures Syn Flood Protection Challenge & Response Connection Based Protection IT PDDS Protection Machine Learning Protection Signatures for Known Vulnerabilities Machine Learning Protection Signatures for Known Vulnerabilities Stal/TLS Management Stal/TLS Management Support for St. v2/v3, TLS 1.0/1.1/1.2/1.3 offloading (and re-encryption) with custom cipher suites. Client certificate- b as ed authentication Dynamic Routing Protocols Nate Routing Protocols Support for VLAN, Link Aggregation & Trunking (LACP) Client Support Support for Width (Apr Land) Support for St. v2/v3, TLS 1.00 / LDA / SSO, AAA, OAuth, MDM parameters (CPU, HDD, MAC, etc.). 3rd Party (via Webhooks) NAT & Routing Support for Centering multiple users, user groups with fine grained access to different part of inferent sub-networks (Src. Dst IP Perfix, VLAN). Default Global party (profile profile Mitror traffic / specific traffic to another NIC port Matchine Learning Protection Signatures for Known Vulnerabilities Support for User All Capability for protecting DNS infrastructure against DNS profile flood, SSL renegotiations, etc Built-in rules for known vulnerabilities (server, web, mail, FTP, SIP, SQL, DNS, IPS Signatures etc.) VPN FEATURES (ADDITIONAL LICENSING) Built-in rules for known vulnerabilities (server, web, mail, FTP, SIP, SQL, DNS, IPS Signatures etc.) VPN FEATURES (ADDITIONAL LICENSING) Support for SSL v2/v3, TLS 1.0/1.1/1.2/1.3 offloading (and re-encryption) with custom cipher suites. Client certificate- b as ed authentication also supported, proxy SSL/TLS connections Support for VLAN, Link Aggregation & Trunking (LACP) Support for VLAN, Link Aggregation & Trunking (LACP) Support for VLAN, Link Aggregation & Trunking (LACP) Support for Creating multiple users, user groups wit	Network Mode DNS Firewall Blacklist / Whitelist Custom Signatures DDOS FEATURES (ADDITIONAL LICENS) Comprehensive Protection DDOS Detection & Mitigation Block Actions Hybrid DDOS Integration Bi-Directional Deep Packet Inspection Enforce RFC Compliance	Support DNS over HTTP, UDP, TCP & SSL as well as DNSSEC Protecting DNS infrastructure from bot attacks, data exfiltration attacks, RPZ policy Support for permanent Blacklisting and Whitelisting based on IP, IP prefix, domain, country, etc. Support for user defined custom rules with support for pattern, suffix, domain, etc. NG) Layer 3 to Layer 7 protection covering Network, Protocol, Application, Reflection / Amplification and 0-day DDoS attacks Attack detection & mitigation in less than 18s and 10s respectively Drop Packet, Terminate Connection (RST), Blacklist (temporary or permanent), Send Challenge (TCP, HTTP, DNS), Rate Limiting Support for integration with Haltdos Cloud Scrubbing or ISP clean pipe services Support for both inbound and outbound traffic protection Protection against malformed packets (TCP, UDP, ICMP, Ping of death, DNS, HTTP, SIP, SNMP, IPv4, IPv6, Fragmented packets, etc.) Protection against misbehaving clients sending invalid or out of state packets
Port Mirroring Rate Limit & QoS Management Rate Limit & QoS Management Rate Limit & QoS Management Blacklist / Whitelist Blacklist / Whitelist Support for temporary or permanent Blacklisting and Whitelisting based on IP, IP prefix, domain, country, etc. Protection against TOR IP, Bad Reputation IP / domain, dark IP, maliclous Bots, proxies, resolvers, etc Custom Signatures SYN Flood Protection Challenge & Response Connection Based Protection DNS Protection DNS Protection LT DOS Protection Machine Learning Protection Machine Learning Protection Signatures for Known Vulnerabilities VPN FEATURES (ADDITIONAL LICENSING) HTTP Protocols SUpport for St. V2/V3, TLS 1.0/1.1/1.2./1.3 offloading (and re-encryption) with custom cipher suites. Client certificate-based authentication Dynamic Routing Protocols Networking Client Support Authentication Nate Routing Support for Vicinal, server or full NAT, static routing for IPA & IPVO Support for circular Super or permanent blacklisting and Whitelisting based on IP, IP prefix, domain, country, etc. Protection against TOR IP, Bad Reputation IP / domain, dark IP, maliclous Bots, proxies, resolvers, etc Protection against TOR IP, Bad Reputation IP / domain, dark IP, maliclous Bots, proxies, resolvers, etc Support for TCP, HTTP, DNS challenge and response for validation of traffic from suspicious sources Connection Based Protection DNS rotection against TCP connection DDOs attacks und as conscious of traffic from suspicious sources Connection Based Protection against TCP connection DDOs attacks und as sockstress, connection of traffic from suspicious sources Connection Based Protection of TCP, HTTP, DNS challenge and response for validation of traffic from suspicious sources Connection Based Protection of TCP, HTTP, DNS challenge and response for validation of traffic from suspicious sources Connection Based Protection of TCP, HTTP, DNS challenge and response for Validation of traffic from suspicious sources Connection Based Protection and suspic	Network Mode DNS Firewall Blacklist / Whitelist Custom Signatures DDOS FEATURES (ADDITIONAL LICENS) Comprehensive Protection DDOS Detection & Mitigation Block Actions Hybrid DDOS Integration Bi-Directional Deep Packet Inspection Enforce RFC Compliance Bot Protection	Support DNS over HTTP, UDP, TCP & SSL as well as DNSSEC Protecting DNS infrastructure from bot attacks, data exfiltration attacks, RPZ policy Support for permanent Blacklisting and Whitelisting based on IP, IP prefix, domain, country, etc. Support for user defined custom rules with support for pattern, suffix, domain, etc. NG) Layer 3 to Layer 7 protection covering Network, Protocol, Application, Reflection / Amplification and 0-day DDoS attacks Attack detection & mitigation in less than 18s and 10s respectively Drop Packet, Terminate Connection (RST), Blacklist (temporary or permanent), Send Challenge (TCP, HTTP, DNS), Rate Limiting Support for integration with Haltdos Cloud Scrubbing or ISP clean pipe services Support for both inbound and outbound traffic protection Protection against malformed packets (TCP, UDP, ICMP, Ping of death, DNS, HTTP, SIP, SNMP, IPv4, IPv6, Fragmented packets, etc.) Protection against misbehaving clients sending invalid or out of state packets Automatic detection and blocking of bot traffic with support for manual bot policy
Port Mirroring Rate Limit & QoS Management Rate Limit & QoS Management Rate Limit & QoS Management Blacklist / Whitelist Blacklist / Whitelist Support for temporary or permanent Blacklisting and Whitelisting based on IP, IP prefix, domain, country, etc. Protection against TOR IP, Bad Reputation IP / domain, dark IP, maliclous Bots, proxies, resolvers, etc Custom Signatures SYN Flood Protection Challenge & Response Connection Based Protection DNS Protection DNS Protection LT DOS Protection Machine Learning Protection Machine Learning Protection Signatures for Known Vulnerabilities VPN FEATURES (ADDITIONAL LICENSING) HTTP Protocols SUpport for St. V2/V3, TLS 1.0/1.1/1.2./1.3 offloading (and re-encryption) with custom cipher suites. Client certificate-based authentication Dynamic Routing Protocols Networking Client Support Authentication Nate Routing Support for Vicinal, server or full NAT, static routing for IPA & IPVO Support for circular Super or permanent blacklisting and Whitelisting based on IP, IP prefix, domain, country, etc. Protection against TOR IP, Bad Reputation IP / domain, dark IP, maliclous Bots, proxies, resolvers, etc Protection against TOR IP, Bad Reputation IP / domain, dark IP, maliclous Bots, proxies, resolvers, etc Support for TCP, HTTP, DNS challenge and response for validation of traffic from suspicious sources Connection Based Protection DNS rotection against TCP connection DDOs attacks und as conscious of traffic from suspicious sources Connection Based Protection against TCP connection DDOs attacks und as sockstress, connection of traffic from suspicious sources Connection Based Protection of TCP, HTTP, DNS challenge and response for validation of traffic from suspicious sources Connection Based Protection of TCP, HTTP, DNS challenge and response for validation of traffic from suspicious sources Connection Based Protection of TCP, HTTP, DNS challenge and response for Validation of traffic from suspicious sources Connection Based Protection and suspic	Network Mode DNS Firewall Blacklist / Whitelist Custom Signatures DDOS FEATURES (ADDITIONAL LICENS) Comprehensive Protection DDOS Detection & Mitigation Block Actions Hybrid DDOS Integration Bi-Directional Deep Packet Inspection Enforce RFC Compliance Bot Protection	Support DNS over HTTP, UDP, TCP & SSL as well as DNSSEC Protecting DNS infrastructure from bot attacks, data exfiltration attacks, RPZ policy Support for permanent Blacklisting and Whitelisting based on IP, IP prefix, domain, country, etc. Support for user defined custom rules with support for pattern, suffix, domain, etc. NG) Layer 3 to Layer 7 protection covering Network, Protocol, Application, Reflection / Amplification and 0-day DDOS attacks Attack detection & mitigation in less than 18s and 10s respectively Drop Packet, Terminate Connection (RST), Blacklist (temporary or permanent), Send Challenge (TCP, HTTP, DNS), Rate Limiting Support for integration with Haltdos Cloud Scrubbing or ISP clean pipe services Support for bin inbound and outbound traffic protection Protection against malformed packets (TCP, UDP, ICMP, Ping of death, DNS, HTTP, SIP, SNMP, IPv4, IPv6, Fragmented packets, etc.) Protection against misbehaving clients sending invalid or out of state packets Automatic detection and blocking of bot traffic with support for manual bot policy Network behaviour analysis for anomaly detection and packet scoring technology
Port Mirroring Rate Limit & QoS Management Rate limit (apability for bandwidth and QoS management with option for rate limit of specific traffic (based on proto, src, dst, etc.) Rate limit (apability for bandwidth and QoS management with option for rate limit of specific traffic (based on proto, src, dst, etc.) Rate limit (apability for bandwidth and QoS management with option for rate limit of specific traffic (based on proto, src, dst, etc.) Rate limit (apability for bandwidth and QoS management with option for rate limit of specific traffic (based on proto, src, dst, etc.) Rate limit (apability for bandwidth and QoS management with option for rate limit of specific traffic (based on proto, src, dst, etc.) Rate limit (apability for Protection apainst TOP IP) Rad Reputation IP / domain, dark IP, malicious Bots, proxies, resolvers, etc Support for user defined custom rules with support for REGEX and byte matching TCP SYN flood protection with SYN Proxy and connection aging TCP SYN flood protection with SYN Proxy and connection aging TCP SYN flood protection with SYN Proxy and connection aging TCP SYN flood protection with SYN Proxy and connection aging TCP SYN flood protection with SYN Proxy and connection of traffic from suspicious sources Connection Based Protection DN Protection against TCP connection DDOS attacks such as sockstress, connection / src, zombie flood, SSL renegotiations, etc Built-in DNS firewall capability for protecting DNS infrastructure against DNS DDOS attacks (Water Torture, NXDomain, etc.) Protection against ION S flowall stacks such as value as sockstress, connection / src, zombie flood, SSL renegotiations, etc Machine Learning Protection Signatures for Known Vulnerabilities National Protection Signatures for Known Vulnerabilities (server, web, mail, FTP, SIP, SQL, DNS, IPS Signatures etc.) WPN FEATURES (ADDITIONAL LICENSING) HTTP Protocols HTTP Protocols BGP, OSFP, RIP VI, RIP V2 Networking Support for SSL v2/v3, TLS 1.0/1.1/1.2/1.3 offloading (and re-encryptio	Network Mode DNS Firewall Blacklist / Whitelist Custom Signatures DDOS FEATURES (ADDITIONAL LICENS) Comprehensive Protection DDOS Detection & Mitigation Block Actions Hybrid DDOS Integration Bi-Directional Deep Packet Inspection Enforce RFC Compliance Bot Protection Behaviour Analysis	Support DNS over HTTP, UDP, TCP & SSL as well as DNSSEC Protecting DNS infrastructure from bot attacks, data exfiltration attacks, RPZ policy Support for permanent Blacklisting and Whitelisting based on IP, IP prefix, domain, country, etc. Support for user defined custom rules with support for pattern, suffix, domain, etc. NG) Layer 3 to Layer 7 protection covering Network, Protocol, Application, Reflection / Amplification and 0-day DDOS attacks Attack detection & mitigation in less than 18s and 10s respectively Drop Packet, Terminate Connection (RST), Blacklist (temporary or permanent), Send Challenge (TCP, HTTP, DNS), Rate Limiting Support for integration with Haltdos Cloud Scrubbing or ISP clean pipe services Support for bin inbound and outbound traffic protection Protection against malformed packets (TCP, UDP, ICMP, Ping of death, DNS, HTTP, SIP, SNMP, IPv4, IPv6, Fragmented packets, etc.) Protection against misbehaving clients sending invalid or out of state packets Automatic detection and blocking of bot traffic with support for manual bot policy Network behaviour analysis for anomaly detection and packet scoring technology
Rate Limit & QoS Management Blacklist / Whitelist Blacklist / Whitelist Support for temporary or permanent Blacklisting and Whitelisting based on IP, IP prefix, domain, country, etc. Malicious Source Protection Custom Signatures Support for user defined custom rules with support for REGEX and byte matching SYN Flood Protection Challenge & Response Connection Based Protection DNS Protection Built-in DNS friewall capability for protecting DNS infrastructure against DNS DDOS attacks (Water Torture, NXDomain, etc.) L7 DDOS Protection Signatures for known Vulnerabilities VPN FEATURES (ADDITIONAL LICENSING) HTTP Protocols SSL/TLS Management Dynamic Routing Protectols Bosed Protection Signatures for Study Sylva, 1st 1.0/1.1/1.2/1.3 offloading (and re-encryption) with custom cipher suites. Client certificate-based authentication Dynamic Routing Protocols Support for VLAN, Link Aggregation & Trunking (LACP) Client Support Support for Windows, Linux, Mobile Apps (Android or 10S), Web (Java Applet) Authentication NAT& Routing Support for creating multiple users, user groups with fine grained access to different part of network and/or services	Network Mode DNS Firewall Blacklist / Whitelist Custom Signatures DDOS FEATURES (ADDITIONAL LICENS) Comprehensive Protection DDOS Detection & Mitigation Block Actions Hybrid DDOS Integration Bi-Directional Deep Packet Inspection Enforce RFC Compliance Bot Protection Behaviour Analysis	Support DNS over HTTP, UDP, TCP & SSL as well as DNSSEC Protecting DNS infrastructure from bot attacks, data exfiltration attacks, RPZ policy Support for permanent Blacklisting and Whitelisting based on IP, IP prefix, domain, country, etc. Support for user defined custom rules with support for pattern, suffix, domain, etc. NG) Layer 3 to Layer 7 protection covering Network, Protocol, Application, Reflection / Amplification and 0-day DDOS attacks Attack detection & mitigation in less than 18s and 10s respectively Drop Packet, Terminate Connection (RST), Blacklist (temporary or permanent), Send Challenge (TCP, HTTP, DNS), Rate Limiting Support for integration with Haltdos Cloud Scrubbing or ISP clean pipe services Support for both inbound and outbound traffic protection Protection against malformed packets (TCP, UDP, ICMP, Ping of death, DNS, HTTP, SIP, SNMP, IPv4, IPv6, Fragmented packets, etc.) Protection against misbehaving clients sending invalid or out of state packets Automatic detection and blocking of bot traffic with support for manual bot policy Network behaviour analysis for anomaly detection and packet scoring technology Support for multiple security profiles for enforcing different policy for different sub-networks (Src, Dst IP Prefix, VLAN). Default Global security
Blacklist / Whitelist Malicious Source Protection Protection against TOR IP, Bad Reputation IP / domain, dark IP, malicious Bots, proxies, resolvers, etc Custom Signatures Syn Flood Protection Challenge & Response Challenge & Response Connection Based Protection DNS protectio	Network Mode DNS Firewall Blacklist / Whitelist Custom Signatures DDOS FEATURES (ADDITIONAL LICENS) Comprehensive Protection DDOS Detection & Mitigation Block Actions Hybrid DDOS Integration Bi-Directional Deep Packet Inspection Enforce RFC Compliance Bot Protection Behaviour Analysis Multiple Security Profiles	Support DNS over HTTP, UDP, TCP & SSL as well as DNSSEC Protecting DNS infrastructure from bot attacks, data exfiltration attacks, RPZ policy Support for permanent Blacklisting and Whitelisting based on IP, IP prefix, domain, country, etc. Support for user defined custom rules with support for pattern, suffix, domain, etc. NG) Layer 3 to Layer 7 protection covering Network, Protocol, Application, Reflection / Amplification and 0-day DDoS attacks Attack detection & mitigation in less than 18s and 10s respectively Drop Packet, Terminate Connection (RST), Blacklist (temporary or permanent), Send Challenge (TCP, HTTP, DNS), Rate Limiting Support for integration with Haltdos Cloud Scrubbing or ISP clean pipe services Support for both inbound and outbound traffic protection Protection against malformed packets (TCP, UDP, ICMP, Ping of death, DNS, HTTP, SIP, SNMP, IPv4, IPv6, Fragmented packets, etc.) Protection against misbehaving clients sending invalid or out of state packets Automatic detection and blocking of bot traffic with support for manual bot policy Network behaviour analysis for anomaly detection and packet scoring technology Support for multiple security profiles for enforcing different policy for different sub-networks (Src, Dst IP Prefix, VLAN). Default Global security profile
Malicious Source Protection Custom Signatures Support for user defined custom rules with support for REGEX and byte matching SYN Flood Protection Challenge & Response Challenge & Response Support for TCP, HTTP, DNS challenge and response for validation of traffic from suspicious sources Connection Based Protection DNS Protection Built-in DNS firewall capability for protecting DNS infrastructure against DNS DDOS attacks (Water Torture, NXDomain, etc.) L7 DDOS Protection Machine Learning Protection Signatures for Known Vulnerabilities Built-in rules for known vulnerabilities (server, web, mail, FTP, SIP, SQL, DNS, IPS Signatures etc.) VPN FEATURES (ADDITIONAL LICENSING) HTTP Protocols BURN-TO-STAIL-ALD-STAIL	Network Mode DNS Firewall Blacklist / Whitelist Custom Signatures DDOS FEATURES (ADDITIONAL LICENS) Comprehensive Protection DDOS Detection & Mitigation Block Actions Hybrid DDOS Integration Bi-Directional Deep Packet Inspection Enforce RFC Compliance Bot Protection Behaviour Analysis Multiple Security Profiles Port Mirroring	Support DNS over HTTP, UDP, TCP & SSL as well as DNSSEC Protecting DNS infrastructure from bot attacks, data exfiltration attacks, RPZ policy Support for permanent Blacklisting and Whitelisting based on IP, IP prefix, domain, country, etc. Support for user defined custom rules with support for pattern, suffix, domain, etc. NG) Layer 3 to Layer 7 protection covering Network, Protocol, Application, Reflection / Amplification and 0-day DDoS attacks Attack detection & mitigation in less than 18s and 10s respectively Drop Packet, Terminate Connection (RST), Blacklist (temporary or permanent), Send Challenge (TCP, HTTP, DNS), Rate Limiting Support for integration with Haltdos Cloud Scrubbing or ISP clean pipe services Support for both inbound and outbound traffic protection Protection against malformed packets (TCP, UDP, ICMP, Ping of death, DNS, HTTP, SIP, SNMP, IPv4, IPv6, Fragmented packets, etc.) Protection against misbehaving clients sending invalid or out of state packets Automatic detection and blocking of bot traffic with support for manual bot policy Network behaviour analysis for anomaly detection and packet scoring technology Support for multiple security profiles for enforcing different policy for different sub-networks (Src, Dst IP Prefix, VLAN). Default Global security profile Mirror traffic / specific traffic to another NIC port
Custom Signatures Support for user defined custom rules with support for REGEX and byte matching SYN Flood Protection Challenge & Response Connection Based Protection DNS frotection DNS frotection Built-in DNS firewall capability for protecting DNS infrastructure against DNS DDOS attacks (Water Torture, NXDomain, etc.) L7 DDOS Protection Machine Learning Protection Signatures for Known Vulnerabilities VPN FEATURES (ADDITIONAL LICENSING HTTP Protocols DYnamic Routing Protectos Bujport for VLAN, Link Aggregation & Trunking (LACP) Client Support for VLAN, Link Aggregation & Trunking (LACP) Client Support for Creating multiple users, user groups with fine grained access to different part of network and/or services Support for creating multiple users, user groups with fine grained access to different part of network and/or services	Network Mode DNS Firewall Blacklist / Whitelist Custom Signatures DDOS FEATURES (ADDITIONAL LICENS) Comprehensive Protection DDOS Detection & Mitigation Block Actions Hybrid DDOS Integration Bi-Directional Deep Packet Inspection Enforce RFC Compliance Bot Protection Behaviour Analysis Multiple Security Profiles Port Mirroring Rate Limit & QoS Management	Support DNS over HTTP, UDP, TCP & SSL as well as DNSSEC Protecting DNS infrastructure from bot attacks, data exfiltration attacks, RPZ policy Support for permanent Blacklisting and Whitelisting based on IP, IP prefix, domain, country, etc. Support for user defined custom rules with support for pattern, suffix, domain, etc. NG) Layer 3 to Layer 7 protection covering Network, Protocol, Application, Reflection / Amplification and 0-day DDoS attacks Attack detection & mitigation in less than 18s and 10s respectively Drop Packet, Terminate Connection (RST), Blacklist (temporary or permanent), Send Challenge (TCP, HTTP, DNS), Rate Limiting Support for integration with Haltdos Cloud Scrubbing or ISP clean pipe services Support for both inbound and outbound traffic protection Protection against malformed packets (TCP, UDP, ICMP, Ping of death, DNS, HTTP, SIP, SNMP, IPv4, IPv6, Fragmented packets, etc.) Protection against misbehaving clients sending invalid or out of state packets Automatic detection and blocking of bot traffic with support for manual bot policy Network behaviour analysis for anomaly detection and packet scoring technology Support for multiple security profiles for enforcing different policy for different sub-networks (Src, Dst IP Prefix, VLAN). Default Global security profile Mirror traffic / specific traffic to another NIC port Rate limit capability for bandwidth and QoS management with option for rate limit of specific traffic (based on proto, src, dst, etc.)
SYN Flood Protection Challenge & Response Connection Based Protection Description Descript	Network Mode DNS Firewall Blacklist / Whitelist Custom Signatures Custom Signatures DDOS FEATURES (ADDITIONAL LICENS) Comprehensive Protection DDOS Detection & Mitigation Block Actions Hybrid DDOS Integration Bi-Directional Deep Packet Inspection Enforce RFC Compliance Bot Protection Behaviour Analysis Multiple Security Profiles Port Mirroring Rate Limit & QoS Management Blacklist / Whitelist	Support DNS over HTTP, UDP, TCP & SSL as well as DNSSEC Protecting DNS infrastructure from bot attacks, data exfiltration attacks, RPZ policy Support for permanent Blacklisting and Whitelisting based on IP, IP prefix, domain, country, etc. Support for user defined custom rules with support for pattern, suffix, domain, etc. NG) Layer 3 to Layer 7 protection covering Network, Protocol, Application, Reflection / Amplification and 0-day DDOS attacks Attack detection & mitigation in less than 18s and 10s respectively Drop Packet, Terminate Connection (RST), Blacklist (temporary or permanent), Send Challenge (TCP, HTTP, DNS), Rate Limiting Support for integration with Haltdos Cloud Scrubbing or ISP clean pipe services Support for integration with and outbound traffic protection Protection against malformed packets (TCP, UDP, ICMP, Ping of death, DNS, HTTP, SIP, SNMP, IPv4, IPv6, Fragmented packets, etc.) Protection against misbehaving clients sending invalid or out of state packets Automatic detection and blocking of bot traffic with support for manual bot policy Network behaviour analysis for anomaly detection and packet scoring technology Support for multiple security profiles for enforcing different policy for different sub-networks (Src, Dst IP Prefix, VLAN). Default Global security profile Mirror traffic / specific traffic to another NIC port Rate limit capability for bandwidth and QoS management with option for rate limit of specific traffic (based on proto, src, dst, etc.) Support for temporary or permanent Blacklisting and Whitelisting based on IP, IP prefix, domain, country, etc.
SYN Flood Protection Challenge & Response Connection Based Protection Description Descript	Network Mode DNS Firewall Blacklist / Whitelist Custom Signatures Custom Signatures DDOS FEATURES (ADDITIONAL LICENS) Comprehensive Protection DDOS Detection & Mitigation Block Actions Hybrid DDOS Integration Bi-Directional Deep Packet Inspection Enforce RFC Compliance Bot Protection Behaviour Analysis Multiple Security Profiles Port Mirroring Rate Limit & QoS Management Blacklist / Whitelist	Support DNS over HTTP, UDP, TCP & SSL as well as DNSSEC Protecting DNS infrastructure from bot attacks, data exfiltration attacks, RPZ policy Support for permanent Blacklisting and Whitelisting based on IP, IP prefix, domain, country, etc. Support for user defined custom rules with support for pattern, suffix, domain, etc. NG) Layer 3 to Layer 7 protection covering Network, Protocol, Application, Reflection / Amplification and 0-day DDOS attacks Attack detection & mitigation in less than 18s and 10s respectively Drop Packet, Terminate Connection (RST), Blacklist (temporary or permanent), Send Challenge (TCP, HTTP, DNS), Rate Limiting Support for integration with Haltdos Cloud Scrubbing or ISP clean pipe services Support for integration with and outbound traffic protection Protection against malformed packets (TCP, UDP, ICMP, Ping of death, DNS, HTTP, SIP, SNMP, IPv4, IPv6, Fragmented packets, etc.) Protection against misbehaving clients sending invalid or out of state packets Automatic detection and blocking of bot traffic with support for manual bot policy Network behaviour analysis for anomaly detection and packet scoring technology Support for multiple security profiles for enforcing different policy for different sub-networks (Src, Dst IP Prefix, VLAN). Default Global security profile Mirror traffic / specific traffic to another NIC port Rate limit capability for bandwidth and QoS management with option for rate limit of specific traffic (based on proto, src, dst, etc.) Support for temporary or permanent Blacklisting and Whitelisting based on IP, IP prefix, domain, country, etc.
Challenge & Response Connection Based Protection DNS Protection against TCP connection DDS attacks such as sockstress, connection / src, zombie flood, SSL renegotiations, etc DNS Protection Built-in DNS firewall capability for protecting DNS infrastructure against DNS DDOS attacks (Water Torture, NXDomain, etc.) L7 DDOS Protection Protection against low & slow attacks such as Slowloris, R.U.D.Y., slow HTTP GET / POST, etc Machine Learning Protection Signatures for Known Vulnerabilities Built-in rules for known vulnerabilities Built-in rules for known vulnerabilities (server, web, mail, FTP, SIP, SQL, DNS, IPS Signatures etc.) VPN FEATURES (ADDITIONAL LICENSING) HTTP Protocols SSL/TLS Management SSL/TLS Management Dynamic Routing Protocols BGP, OSFP, RIP v1, RIP v2 Networking Support for VLAN, Link Aggregation & Trunking (LACP) Client Support Authentication Password, SAML / AD / LDAP / SSO, AAA, OAuth, MDM parameters (CPU, HDD, MAC, etc.), 3 rd Party (via Webhooks) NAT & Routing User Grouping Support for creating multiple users, user groups with fine grained access to different part of network and/or services	Network Mode DNS Firewall Blacklist / Whitelist Custom Signatures Custom Signatures DDOS FEATURES (ADDITIONAL LICENS) Comprehensive Protection DDOS Detection & Mitigation Block Actions Hybrid DDOS Integration Bi-Directional Deep Packet Inspection Enforce RFC Compliance Bot Protection Behaviour Analysis Multiple Security Profiles Port Mirroring Rate Limit & QoS Management Blacklist / Whitelist Malicious Source Protection	Support DNS over HTTP, UDP, TCP & SSL as well as DNSSEC Protecting DNS infrastructure from bot attacks, data exfiltration attacks, RPZ policy Support for permanent Blacklisting and Whitelisting based on IP, IP prefix, domain, country, etc. Support for user defined custom rules with support for pattern, suffix, domain, etc. NG) Layer 3 to Layer 7 protection covering Network, Protocol, Application, Reflection / Amplification and 0-day DDoS attacks Attack detection & mitigation in less than 18s and 10s respectively Drop Packet, Terminate Connection (RST), Blacklist (temporary or permanent), Send Challenge (TCP, HTTP, DNS), Rate Limiting Support for integration with Haltdos Cloud Scrubbing or ISP clean pipe services Support for both inbound and outbound traffic protection Protection against malformed packets (TCP, UDP, ICMP, Ping of death, DNS, HTTP, SIP, SNMP, IPv4, IPv6, Fragmented packets, etc.) Protection against misbehaving clients sending invalid or out of state packets Automatic detection and blocking of bot traffic with support for manual bot policy Network behaviour analysis for anomaly detection and packet scoring technology Support for multiple security profiles for enforcing different policy for different sub-networks (Src, Dst IP Prefix, VLAN). Default Global security profile Mirror traffic / specific traffic to another NIC port Rate limit capability for bandwidth and QoS management with option for rate limit of specific traffic (based on proto, src, dst, etc.) Support for temporary or permanent Blacklisting and Whitelisting based on IP, IP prefix, domain, country, etc. Protection against TOR IP, Bad Reputation IP / domain, dark IP, malicious Bots, proxies, resolvers, etc
Connection Based Protection DNS Protection Built-in DNS firewall capability for protecting DNS infrastructure against DNS DDOS attacks (Water Torture, NXDomain, etc.) L7 DDOS Protection Automatic learning counter measures and dynamic signature creation upon attack detection Signatures for Known Vulnerabilities VPN FEATURES (ADDITIONAL LICENSING) HTTP Protocols Automatic learning counter measures and dynamic signature creation upon attack detection Built-in rules for known vulnerabilities (server, web, mail, FTP, SIP, SQL, DNS, IPS Signatures etc.) VPN FEATURES (ADDITIONAL LICENSING) HTTP Protocols SSL/TLS Management SUpport for SSL v2/v3, TLS 1.0/1.1/1.2/1.3 offloading (and re-encryption) with custom cipher suites. Client certificate- b a s e d authentication also supported, proxy SSL/TLS connections Dynamic Routing Protocols BCP, OSFP, RIP v1, RIP v2 Support for VLAN, Link Aggregation & Trunking (LACP) Client Support Client Support Authentication Password, SAML/ AD / LDAP / SSO, AAA, OAuth, MDM parameters (CPU, HDD, MAC, etc.), 3 rd Party (via Webhooks) NAT & Routing Support for creating multiple users, user groups with fine grained access to different part of network and/or services	Network Mode DNS Firewall Blacklist / Whitelist Custom Signatures DDOS FEATURES (ADDITIONAL LICENS) Comprehensive Protection DDoS Detection & Mitigation Block Actions Hybrid DDOS Integration Bi-Directional Deep Packet Inspection Enforce RFC Compliance Bot Protection Behaviour Analysis Multiple Security Profiles Port Mirroring Rate Limit & QoS Management Blacklist / Whitelist Malicious Source Protection Custom Signatures	Support DNS over HTTP, UDP, TCP & SSL as well as DNSSEC Protecting DNS infrastructure from bot attacks, data exfiltration attacks, RPZ policy Support for permanent Blacklisting and Whitelisting based on IP, IP prefix, domain, country, etc. Support for user defined custom rules with support for pattern, suffix, domain, etc. NG) Layer 3 to Layer 7 protection covering Network, Protocol, Application, Reflection / Amplification and 0-day DDoS attacks Attack detection & mitigation in less than 18s and 10s respectively Drop Packet, Terminate Connection (RST), Blacklist (temporary or permanent), Send Challenge (TCP, HTTP, DNS), Rate Limiting Support for integration with Haltdos Cloud Scrubbing or ISP clean pipe services Support for both inbound and outbound traffic protection Protection against malformed packets (TCP, UDP, ICMP, Ping of death, DNS, HTTP, SIP, SNMP, IPv4, IPv6, Fragmented packets, etc.) Protection against misbehaving clients sending invalid or out of state packets Automatic detection and blocking of bot traffic with support for manual bot policy Network behaviour analysis for anomaly detection and packet scoring technology Support for multiple security profiles for enforcing different policy for different sub-networks (Src, Dst IP Prefix, VLAN). Default Global security profile Mirror traffic / specific traffic to another NIC port Rate limit capability for bandwidth and QoS management with option for rate limit of specific traffic (based on proto, src, dst, etc.) Support for temporary or permanent Blacklisting and Whitelisting based on IP, IP prefix, domain, country, etc. Protection against TOR IP, Bad Reputation IP / domain, dark IP, malicious Bots, proxies, resolvers, etc Support for user defined custom rules with support for REGEX and byte matching
DNS Protection L7 DDOS Protection L7 DDOS Protection Machine Learning Protection Signatures for Known Vulnerabilities VPN FEATURES (ADDITIONAL LICENSING) HTTP Protocols SULTLS Management Systylts Management Dynamic Routing Protocols Dynamic Routing Protocols Dynamic Routing Protocols Client Support Dynamic Routing Protocols Authentication Dynamic Routing Protocols Authentication Support for VLAN, Link Aggregation & Trunking (LACP) Client Support Authentication Password, SAML/ AD / LDAP / SSO, AAA, OAuth, MDM parameters (CPU, HDD, MAC, etc), 3 rd Party (via Webhooks) NAT & Routing Support for creating multiple users, user groups with fine grained access to different part of network and/or services	Network Mode DNS Firewall Blacklist / Whitelist Custom Signatures DDOS FEATURES (ADDITIONAL LICENS) Comprehensive Protection DDOS Detection & Mitigation Block Actions Hybrid DDOS Integration Bi-Directional Deep Packet Inspection Enforce RFC Compliance Bot Protection Behaviour Analysis Multiple Security Profiles Port Mirroring Rate Limit & QoS Management Blacklist / Whitelist Malicious Source Protection Custom Signatures SYN Flood Protection	Support DNS over HTTP, UDP, TCP & SSL as well as DNSSEC Protecting DNS infrastructure from bot attacks, data exfiltration attacks, RPZ policy Support for permanent Blacklisting and Whitelisting based on IP, IP prefix, domain, country, etc. Support for user defined custom rules with support for pattern, suffix, domain, etc. NG) Layer 3 to Layer 7 protection covering Network, Protocol, Application, Reflection / Amplification and 0-day DDoS attacks Attack detection & mitigation in less than 18s and 10s respectively Drop Packet, Terminate Connection (RST), Blacklist (temporary or permanent), Send Challenge (TCP, HTTP, DNS), Rate Limiting Support for integration with Haltdos Cloud Scrubbing or ISP clean pipe services Support for both inbound and outbound traffic protection Protection against malformed packets (TCP, UDP, ICMP, Ping of death, DNS, HTTP, SIP, SNMP, IPv4, IPv6, Fragmented packets, etc.) Protection against misbehaving clients sending invalid or out of state packets Automatic detection and blocking of bot traffic with support for manual bot policy Network behaviour analysis for anomaly detection and packet scoring technology Support for multiple security profiles for enforcing different policy for different sub-networks (Src, Dst IP Prefix, VLAN). Default Global security profile Mirror traffic / specific traffic to another NIC port Rate limit capability for bandwidth and QoS management with option for rate limit of specific traffic (based on proto, src, dst, etc.) Support for temporary or permanent Blacklisting and Whitelisting based on IP, IP prefix, domain, country, etc. Protection against TOR IP, Bad Reputation IP / domain, dark IP, malicious Bots, proxies, resolvers, etc Support for user defined custom rules with support for REGEX and byte matching TCP SYN flood protection with SYN Proxy and connection aging
L7 DDoS Protection Machine Learning Protection Machine Learning Protection Signatures for Known Vulnerabilities WPN FEATURES (ADDITIONAL LICENSING) HTTP Protocols HTTP Protocols SSL/TLS Management Dynamic Routing Protocols Dynamic Routing Protocols Dynamic Routing Protocols Okeroprical Support for VLAN, Link Aggregation & Trunking (LACP) Client Support Authentication Authentication Protection against low & slow attacks such as Slowloris, R.U.D.Y., slow HTTP GET / POST, etc Automatic learning counter measures and dynamic signature creation upon attack detection Bull-in rules for known vulnerabilities (server, web, mail, FTP, SIP, SQL, DNS, IPS Signatures etc.) HTTP Protocols HTTP Protocols Support for SSL V2/V3, TLS 1.0/1.1/1.2/1.3 offloading (and re-encryption) with custom cipher suites. Client certificate-based authentication also supported, proxy SSL/TLS connections BGP, OSFP, RIP v1, RIP v2 Support for VLAN, Link Aggregation & Trunking (LACP) Support for Windows, Linux, Mobile Apps (Android or iOS), Web (Java Applet) Password, SAML / AD / LDAP / SSO, AAA, OAuth, MDM parameters (CPU, HDD, MAC, etc), 3 rd Party (via Webhooks) NAT & Routing Support for client, server or full NAT, static routing for IPv4 & IPv6 User Grouping Support for creating multiple users, user groups with fine grained access to different part of network and/or services	Network Mode DNS Firewall Blacklist / Whitelist Custom Signatures DDOS FEATURES (ADDITIONAL LICENSI Comprehensive Protection DDOS Detection & Mitigation Block Actions Hybrid DDOS Integration Bi-Directional Deep Packet Inspection Enforce RFC Compliance Bot Protection Behaviour Analysis Multiple Security Profiles Port Mirroring Rate Limit & QoS Management Blacklist / Whitelist Malicious Source Protection Custom Signatures SYN Flood Protection Challenge & Response	Support DNS over HTTP, UDP, TCP & SSL as well as DNSSEC Protecting DNS infrastructure from bot attacks, data exfiltration attacks, RPZ policy Support for permanent Blacklisting and Whitelisting based on IP, IP prefix, domain, country, etc. Support for user defined custom rules with support for pattern, suffix, domain, etc. NG Layer 3 to Layer 7 protection covering Network, Protocol, Application, Reflection / Amplification and 0-day DDoS attacks Attack detection & mitigation in less than 18s and 10s respectively Drop Packet, Terminate Connection (RST), Blacklist (temporary or permanent), Send Challenge (TCP, HTTP, DNS), Rate Limiting Support for integration with Haltdos Cloud Scrubbing or ISP clean pipe services Support for both inbound and outbound traffic protection Protection against misformed packets (TCP, UDP, ICMP, Ping of death, DNS, HTTP, SIP, SNMP, IPv4, IPv6, Fragmented packets, etc.) Protection against misbehaving clients sending invalid or out of state packets Automatic detection and blocking of bot traffic with support for manual bot policy Network behaviour analysis for anomaly detection and packet scoring technology Support for multiple security profiles for enforcing different policy for different sub-networks (Src, Dst IP Prefix, VLAN). Default Global security profile Mirror traffic / specific traffic to another NIC port Rate limit capability for bandwidth and QoS management with option for rate limit of specific traffic (based on proto, src, dst, etc.) Support for temporary or permanent Blacklisting and Whitelisting based on IP, IP prefix, domain, country, etc. Protection against TOR IP, Bad Reputation IP / domain, dark IP, malicious Bots, proxies, resolvers, etc Support for user defined custom rules with support for REGEX and byte matching TCP SYN flood protection with SYN Proxy and connection aging Support for TCP, HTTP, DNS challenge and response for validation of traffic from suspicious sources
L7 DDoS Protection Machine Learning Protection Signatures for Known Vulnerabilities Bullt-in rules for known vulnerabilities (server, web, mail, FTP, SIP, SQL, DNS, IPS Signatures etc.) VPN FEATURES (ADDITIONAL LICENSING) HTTP Protocols HTTP Protocols SSL/TLS Management SSL/TLS Management Dynamic Routing Protocols Dynamic Routing Protocols Dynamic Routing Protocols Client Support Support for VLAN, Link Aggregation & Trunking (LACP) Client Support Authentication Password, SAML / AD / LDAP / SSO, AAA, OAuth, MDM parameters (CPU, HDD, MAC, etc.), 3 rd Party (via Webhooks) NAT & Routing Support for creating multiple users, user groups with fine grained access to different part of network and/or services	Network Mode DNS Firewall Blacklist / Whitelist Custom Signatures DDOS FEATURES (ADDITIONAL LICENS) Comprehensive Protection DDOS Detection & Mitigation Block Actions Hybrid DDOS Integration Bi-Directional Deep Packet Inspection Enforce RFC Compliance Bot Protection Behaviour Analysis Multiple Security Profiles Port Mirroring Rate Limit & QoS Management Blacklist / Whitelist Malicious Source Protection Custom Signatures SYN Flood Protection Challenge & Response Connection Based Protection	Support DNS over HTTP, UDP, TCP & SSL as well as DNSSEC Protecting DNS infrastructure from bot attacks, data exfiltration attacks, RPZ policy Support for permanent Blacklisting and Whitelisting based on IP, IP prefix, domain, country, etc. Support for user defined custom rules with support for pattern, suffix, domain, etc. NG Layer 3 to Layer 7 protection covering Network, Protocol, Application, Reflection / Amplification and 0-day DDoS attacks Attack detection & mitigation in less than 18s and 10s respectively Drop Packet, Terminate Connection (RST), Blacklist (temporary or permanent), Send Challenge (TCP, HTTP, DNS), Rate Limiting Support for integration with Haltdos Cloud Scrubbing or ISP clean pipe services Support for both inbound and outbound traffic protection Protection against misformed packets (TCP, UDP, ICMP, Ping of death, DNS, HTTP, SIP, SNMP, IPv4, IPv6, Fragmented packets, etc.) Protection against misbehaving clients sending invalid or out of state packets Automatic detection and blocking of bot traffic with support for manual bot policy Network behaviour analysis for anomaly detection and packet scoring technology Support for multiple security profiles for enforcing different policy for different sub-networks (Src, Dst IP Prefix, VLAN). Default Global security profile Mirror traffic / specific traffic to another NIC port Rate limit capability for bandwidth and QoS management with option for rate limit of specific traffic (based on proto, src, dst, etc.) Support for temporary or permanent Blacklisting and Whitelisting based on IP, IP prefix, domain, country, etc. Protection against TOR IP, Bad Reputation IP / domain, dark IP, malicious Bots, proxies, resolvers, etc Support for user defined custom rules with support for REGEX and byte matching TCP SYN flood protection with SYN Proxy and connection aging Support for TCP, HTTP, DNS challenge and response for validation of traffic from suspicious sources
Machine Learning Protection Signatures for Known Vulnerabilities Built-in rules for known vulnerabilities FYPN FEATURES (ADDITIONAL LICENSING) HTTP Protocols SSL/TLS Management SSL/TLS Management Dynamic Routing Protocols BGP, OSFP, RIP v1, RIP v2 Networking Support for VLAN, Link Aggregation & Trunking (LACP) Client Support Authentication Password, SAML / AD / LDAP / SSO, AAA, OAuth, MDM parameters (CPU, HDD, MAC, etc), 3 rd Party (via Webhooks) NAT & Routing Support for Client, server or full NAT, static routing for IPv4 & IPv6 User Grouping Support for recating multiple users, user groups with fine grained access to different part of network and/or services	Network Mode DNS Firewall Blacklist / Whitelist Custom Signatures DDOS FEATURES (ADDITIONAL LICENS) Comprehensive Protection DDOS Detection & Mitigation Block Actions Hybrid DDOS Integration Bi-Directional Deep Packet Inspection Enforce RFC Compliance Bot Protection Behaviour Analysis Multiple Security Profiles Port Mirroring Rate Limit & QoS Management Blacklist / Whitelist Malicious Source Protection Custom Signatures SYN Flood Protection Challenge & Response Connection Based Protection	Support DNS over HTTP, UDP, TCP & SSL as well as DNSSEC Protecting DNS infrastructure from bot attacks, data exfiltration attacks, RPZ policy Support for permanent Blacklisting and Whitelisting based on IP, IP prefix, domain, country, etc. Support for user defined custom rules with support for pattern, suffix, domain, etc. NG Layer 3 to Layer 7 protection covering Network, Protocol, Application, Reflection / Amplification and 0-day DDoS attacks Attack detection & mitigation in less than 18s and 10s respectively Drop Packet, Terminate Connection (RST), Blacklist (temporary or permanent), Send Challenge (TCP, HTTP, DNS), Rate Limiting Support for integration with Haltdos Cloud Scrubbing or ISP clean pipe services Support for both inbound and outbound traffic protection Protection against malformed packets (TCP, UDP, ICMP, Ping of death, DNS, HTTP, SIP, SNMP, IPv4, IPv6, Fragmented packets, etc.) Protection against misbehaving clients sending invalid or out of state packets Automatic detection and blocking of bot traffic with support for manual bot policy Network behaviour analysis for anomaly detection and packet scoring technology Support for multiple security profiles for enforcing different policy for different sub-networks (Src, Dst IP Prefix, VLAN). Default Global security profile Mirror traffic / specific traffic to another NIC port Rate limit capability for bandwidth and QoS management with option for rate limit of specific traffic (based on proto, src, dst, etc.) Support for temporary or permanent Blacklisting and Whitelisting based on IP, IP prefix, domain, country, etc. Protection against TOR IP, Bad Reputation IP / domain, dark IP, malicious Bots, proxies, resolvers, etc Support for USP, HTTP, DNS challenge and response for validation of traffic from suspicious sources Protection against TCP connection DDoS attacks such as sockstress, connection / src, zombie flood, SSL renegotiations, etc
Signatures for Known Vulnerabilities WPN FEATURES (ADDITIONAL LICENSING) HTTP Protocols SSL/TLS Management Dynamic Routing Protocols Networking Olient Support Authentication Authentication Authentication NAT & Routing User Grouping Support for VLAN Link Aggregation & Trunking (LACP) Authentication Support for VLAN Link Aggregation & Trunking (LACP) Authentication Support for VLAN Link Aggregation & Trunking (LACP) Authentication Support for Windows, Linux, Mobile Apps (Android or iOS), Web (Java Applet) Password, SAML / AD / LDAP / SSO, AAA, OAuth, MDM parameters (CPU, HDD, MAC, etc), 3 rd Party (via Webhooks) Support for creating multiple users, user groups with fine grained access to different part of network and/or services	Network Mode DNS Firewall Blacklist / Whitelist Custom Signatures DDOS FEATURES (ADDITIONAL LICENSI Comprehensive Protection DDOS Detection & Mitigation Block Actions Hybrid DDOS Integration Bi-Directional Deep Packet Inspection Enforce RFC Compliance Bot Protection Behaviour Analysis Multiple Security Profiles Port Mirroring Rate Limit & QoS Management Blacklist / Whitelist Malicious Source Protection Custom Signatures SYN Flood Protection Challenge & Response Connection Based Protection	Support DNS over HTTP, UDP, TCP & SSL as well as DNSSEC Protecting DNS infrastructure from bot attacks, data exfiltration attacks, RPZ policy Support for permanent Blacklisting and Whitelisting based on IP, IP prefix, domain, country, etc. Support for user defined custom rules with support for pattern, suffix, domain, etc. NG) Layer 3 to Layer 7 protection covering Network, Protocol, Application, Reflection / Amplification and 0-day DDoS attacks Attack detection & mitigation in less than 18s and 10s respectively Drop Packet, Terminate Connection (RST), Blacklist (temporary or permanent), Send Challenge (TCP, HTTP, DNS), Rate Limiting Support for integration with Haltdos Cloud Scrubbing or ISP clean pipe services Support for both inbound and outbound traffic protection Protection against malformed packets (TCP, UDP, ICMP, Ping of death, DNS, HTTP, SIP, SNMP, IPv4, IPv6, Fragmented packets, etc.) Protection against misbehaving clients sending invalid or out of state packets Automatic detection and blocking of bot traffic with support for manual bot policy Network behaviour analysis for anomaly detection and packet scoring technology Support for multiple security profiles for enforcing different policy for different sub-networks (Src, Dst IP Prefix, VLAN). Default Global security profile Mirror traffic / specific traffic to another NIC port Rate limit capability for bandwidth and QoS management with option for rate limit of specific traffic (based on proto, src, dst, etc.) Support for user defined custom rules with support for REGEX and byte matching TCP SYN flood protection with SYN Proxy and connection aging Support for TCP, HTTP, DNS challenge and response for validation of traffic from suspicious sources Protection against TCP connection DDoS attacks such as sockstress, connection / src, zombie flood, SSL renegotiations, etc.
PATTURES (ADDITIONAL LICENSING) HTTP Protocols HTTP 0.9/1.0/1.1/2.0 with translation SUpport for SSL v2/v3, TLS 1.0/1.1/1.2/1.3 offloading (and re-encryption) with custom cipher suites. Client certificate-based authentication also supported, proxy SSL/TLS connections Dynamic Routing Protocols BGP, OSFP, RIP v1, RIP v2 Support for VLAN, Link Aggregation & Trunking (LACP) Client Support Glient Support Authentication Password, SAML / AD / LDAP / SSO, AAA, OAuth, MDM parameters (CPU, HDD, MAC, etc), 3 rd Party (via Webhooks) NAT & Routing Support for creating multiple users, user groups with fine grained access to different part of network and/or services	Network Mode DNS Firewall Blacklist / Whitelist Custom Signatures DDOS FEATURES (ADDITIONAL LICENSI Comprehensive Protection DDOS Detection & Mitigation Block Actions Hybrid DDOS Integration Bi-Directional Deep Packet Inspection Enforce RFC Compliance Bot Protection Behaviour Analysis Multiple Security Profiles Port Mirroring Rate Limit & QoS Management Blacklist / Whitelist Malicious Source Protection Custom Signatures SYN Flood Protection Challenge & Response Connection Based Protection DNS Protection DNS Protection	Support DNS over HTTP, UDP, TCP & SSL as well as DNSSEC Protecting DNS infrastructure from bot attacks, data exfiltration attacks, RPZ policy Support for permanent Blacklisting and Whitelisting based on IP, IP prefix, domain, country, etc. Support for user defined custom rules with support for pattern, suffix, domain, etc. NG) Layer 3 to Layer 7 protection covering Network, Protocol, Application, Reflection / Amplification and 0-day DDoS attacks Attack detection & mitigation in less than 18s and 10s respectively Drop Packet, Terminate Connection (RST), Blacklist (temporary or permanent), Send Challenge (TCP, HTTP, DNS), Rate Limiting Support for integration with Haltdos Cloud Scrubbing or ISP clean pipe services Support for both inbound and outbound traffic protection Protection against maliformed packets (TCP, UDP, ICMP, Ping of death, DNS, HTTP, SIP, SNMP, IPv4, IPv6, Fragmented packets, etc.) Protection against misbehaving clients sending invalid or out of state packets Automatic detection and blocking of bot traffic with support for manual bot policy Network behaviour analysis for anomaly detection and packet scoring technology Support for multiple security profiles for enforcing different policy for different sub-networks (Src, Dst IP Prefix, VLAN). Default Global security profile Mirror traffic / specific traffic to another NIC port Rate limit capability for bandwidth and QoS management with option for rate limit of specific traffic (based on proto, src, dst, etc.) Support for temporary or permanent Blacklisting and Whitelisting based on IP, IP prefix, domain, country, etc. Protection against TOR IP, Bad Reputation IP / domain, dark IP, malicious Bots, proxies, resolvers, etc Support for temporary or permanent Blacklisting and Whitelisting based on IP, IP prefix, domain, country, etc. Protection against TOR IP, Bad Reputation IP / domain, dark IP, malicious Bots, proxies, resolvers, etc Support for TCP, HTTP, DNS challenge and response for validation of traffic from suspicious sources Protection again
HTTP Protocols HTTP 0.9/1.0/1.1/2.0 with translation SSL/TLS Management Support for SSL v2/v3, TLS 1.0/1.1/1.2/1.3 offloading (and re-encryption) with custom cipher suites. Client certificate-based authentication also supported, proxy SSL/TLS connections Dynamic Routing Protocols BGP, OSFP, RIP v1, RIP v2 Networking Support for VLAN, Link Aggregation & Trunking (LACP) Client Support Support Support for Windows, Linux, Mobile Apps (Android or iOS), Web (Java Applet) Authentication Password, SAML / AD / LDAP / SSO, AAA, OAuth, MDM parameters (CPU, HDD, MAC, etc), 3 rd Party (via Webhooks) NAT & Routing Support for client, server or full NAT, static routing for IPv4 & IPv6 User Grouping Support for creating multiple users, user groups with fine grained access to different part of network and/or services	Network Mode DNS Firewall Blacklist / Whitelist Custom Signatures DDOS FEATURES (ADDITIONAL LICENS) Comprehensive Protection DDoS Detection & Mitigation Block Actions Hybrid DDOS Integration Bi-Directional Deep Packet Inspection Enforce RFC Compliance Bot Protection Behaviour Analysis Multiple Security Profiles Port Mirroring Rate Limit & QoS Management Blacklist / Whitelist Malicious Source Protection Custom Signatures SYN Flood Protection Challenge & Response Connection Based Protection DNS Protection LT DDoS Protection LT DDoS Protection Machine Learning Protection	Support DNS over HTTP, UDP, TCP & SSL as well as DNSSEC Protecting DNS infrastructure from bot attacks, data exfiltration attacks, RPZ policy Support for permanent Blacklisting and Whitelisting based on IP, IP prefix, domain, country, etc. Support for user defined custom rules with support for pattern, suffix, domain, etc. NG) Layer 3 to Layer 7 protection covering Network, Protocol, Application, Reflection / Amplification and 0-day DDoS attacks Attack detection & mitigation in less than 18s and 10s respectively Drop Packet, Terminate Connection (RST), Blacklist (temporary or permanent), Send Challenge (TCP, HTTP, DNS), Rate Limiting Support for integration with Haltdos Cloud Scrubbing or ISP clean pipe services Support for both inbound and outbound traffic protection Protection against misbehaving clients sending invalid or out of state packets Automatic detection and blocking of bot traffic with support for manual bot policy Network behaviour analysis for anomaly detection and packet scoring technology Support for multiple security profiles for enforcing different policy for different sub-networks (Src, Dst IP Prefix, VLAN). Default Global security profile Mirror traffic / specific traffic to another NIC port Rate limit capability for bandwidth and QoS management with option for rate limit of specific traffic (based on proto, src, dst, etc.) Support for user defined custom rules with support for REGEX and byte matching TCP SYN flood protection with SYN Proxy and connection aging Support for TCP, HTTP, DNS challenge and response for validation of traffic from suspicious sources Protection against TCP connection DDoS attacks such as sockstress, connection / src, zombie flood, SSL renegotiations, etc Built-in DNS firewall capability for protecting DNS infrastructure against DNS DDoS attacks (Water Torture, NXDomain, etc.) Protection against low & slow attacks such as Slowloris, R.U.D.Y., slow HTTP GET / POST, etc Automatic learning counter measures and dynamic signature creation upon attack detection
SSL/TLS Management Support for SSL v2/v3, TLS 1.0/1.1/1.2/1.3 offloading (and re-encryption) with custom cipher suites. Client certificate-based authentication also supported, proxy SSL/TLS connections Dynamic Routing Protocols BGP, OSFP, RIP v1, RIP v2 Support for VLAN, Link Aggregation & Trunking (LACP) Client Support Support for Windows, Linux, Mobile Apps (Android or iOS), Web (Java Applet) Authentication Password, SAML/AD/LDAP/SSO, AAA, OAuth, MDM parameters (CPU, HDD, MAC, etc), 3 rd Party (via Webhooks) NAT & Routing Support for client, server or full NAT, static routing for IPv4 & IPv6 User Grouping Support for creating multiple users, user groups with fine grained access to different part of network and/or services	Network Mode DNS Firewall Blacklist / Whitelist Custom Signatures DDOS FEATURES (ADDITIONAL LICENSI Comprehensive Protection DDoS Detection & Mitigation Block Actions Hybrid DDOS Integration Bi-Directional Deep Packet Inspection Enforce RFC Compliance Bot Protection Behaviour Analysis Multiple Security Profiles Port Mirroring Rate Limit & QoS Management Blacklist / Whitelist Malicious Source Protection Custom Signatures SYN Flood Protection Challenge & Response Connection Based Protection DNS Protection LT DDoS Protection Machine Learning Protection Signatures for Known Vulnerabilities	Support DNS over HTTP, UDP, TCP & SSL as well as DNSSEC Protecting DNS infrastructure from bot attacks, data exfiltration attacks, RPZ policy Support for permanent Blacklisting and Whitelisting based on IP, IP prefix, domain, country, etc. Support for user defined custom rules with support for pattern, suffix, domain, etc. NG) Layer 3 to Layer 7 protection covering Network, Protocol, Application, Reflection / Amplification and 0-day DDoS attacks Attack detection & mitigation in less than 18s and 10s respectively Drop Packet, Terminate Connection (RST), Blacklist (temporary or permanent), Send Challenge (TCP, HTTP, DNS), Rate Limiting Support for integration with Haltdos Cloud Scrubbing or ISP clean pipe services Support for both inbound and outbound traffic protection Protection against malformed packets (TCP, UDP, ICMP, Ping of death, DNS, HTTP, SIP, SNMP, IPv4, IPv6, Fragmented packets, etc.) Protection against misbehaving clients sending invalid or out of state packets Automatic detection and blocking of bot traffic with support for manual bot policy Network behaviour analysis for anomaly detection and packet scoring technology Support for multiple security profiles for enforcing different policy for different sub-networks (Src, Dst IP Prefix, VLAN). Default Global security profile Mirror traffic / specific traffic to another NIC port Rate limit capability for bandwidth and QoS management with option for rate limit of specific traffic (based on proto, src, dst, etc.) Support for temporary or permanent Blacklisting and Whitelisting based on IP, IP prefix, domain, country, etc. Protection against TOR IP, Bad Reputation IP / domain, dark IP, malicious Bots, proxies, resolvers, etc Support for user defined custom rules with support for REGEX and byte matching TCP SVN flood protection with SVN Proxy and connection aging Support for user defined custom rules with support for ReGEX and byte matching TCP SVN flood protection with SVN Proxy and connection aging Support for Repainst TCP connection DDoS attacks such
SSL/TLS Management Support for SSL v2/v3, TLS 1.0/1.1/1.2/1.3 offloading (and re-encryption) with custom cipher suites. Client certificate-based authentication also supported, proxy SSL/TLS connections Dynamic Routing Protocols BGP, OSFP, RIP v1, RIP v2 Support for VLAN, Link Aggregation & Trunking (LACP) Client Support Support for Windows, Linux, Mobile Apps (Android or iOS), Web (Java Applet) Authentication Password, SAML/AD/LDAP/SSO, AAA, OAuth, MDM parameters (CPU, HDD, MAC, etc), 3 rd Party (via Webhooks) NAT & Routing Support for client, server or full NAT, static routing for IPv4 & IPv6 User Grouping Support for creating multiple users, user groups with fine grained access to different part of network and/or services	Network Mode DNS Firewall Blacklist / Whitelist Custom Signatures DDOS FEATURES (ADDITIONAL LICENSI Comprehensive Protection DDoS Detection & Mitigation Block Actions Hybrid DDOS Integration Bi-Directional Deep Packet Inspection Enforce RFC Compliance Bot Protection Behaviour Analysis Multiple Security Profiles Port Mirroring Rate Limit & QoS Management Blacklist / Whitelist Malicious Source Protection Custom Signatures SYN Flood Protection Challenge & Response Connection Based Protection DNS Protection LT DDoS Protection Machine Learning Protection Signatures for Known Vulnerabilities	Support DNS over HTTP, UDP, TCP & SSL as well as DNSSEC Protecting DNS infrastructure from bot attacks, data exfiltration attacks, RPZ policy Support for permanent Blacklisting and Whitelisting based on IP, IP prefix, domain, country, etc. Support for user defined custom rules with support for pattern, suffix, domain, etc. NG) Layer 3 to Layer 7 protection covering Network, Protocol, Application, Reflection / Amplification and 0-day DDoS attacks Attack detection & mitigation in less than 18s and 10s respectively Drop Packet, Terminate Connection (RST), Blacklist (temporary or permanent), Send Challenge (TCP, HTTP, DNS), Rate Limiting Support for integration with Haltdos Cloud Scrubbing or ISP clean pipe services Support for both inbound and outbound traffic protection Protection against malformed packets (TCP, UDP, ICMP, Ping of death, DNS, HTTP, SIP, SNMP, IPv4, IPv6, Fragmented packets, etc.) Protection against misbehaving clients sending invalid or out of state packets Automatic detection and blocking of bot traffic with support for manual bot policy Network behaviour analysis for anomaly detection and packet scoring technology Support for multiple security profiles for enforcing different policy for different sub-networks (Src, Dst IP Prefix, VLAN). Default Global security profile Mirror traffic / specific traffic to another NIC port Rate limit capability for bandwidth and QoS management with option for rate limit of specific traffic (based on proto, src, dst, etc.) Support for temporary or permanent Blacklisting and Whitelisting based on IP, IP prefix, domain, country, etc. Protection against TOR IP, Bad Reputation IP / domain, dark IP, malicious Bots, proxies, resolvers, etc Support for user defined custom rules with support for REGEX and byte matching TCP SVN flood protection with SVN Proxy and connection aging Support for user defined custom rules with support for ReGEX and byte matching TCP SVN flood protection with SVN Proxy and connection aging Support for Repainst TCP connection DDoS attacks such
also supported, proxy SSL/TLS connections Dynamic Routing Protocols BGP, OSFP, RIP v1, RIP v2 Networking Support for VLAN, Link Aggregation & Trunking (LACP) Support for Windows, Linux, Mobile Apps (Android or iOS), Web (Java Applet) Authentication Password, SAML / AD / LDAP / SSO, AAA, OAuth, MDM parameters (CPU, HDD, MAC, etc), 3 rd Party (via Webhooks) NAT & Routing Support for client, server or full NAT, static routing for IPv4 & IPv6 User Grouping Support for creating multiple users, user groups with fine grained access to different part of network and/or services	Network Mode DNS Firewall Blacklist / Whitelist Custom Signatures DDOS FEATURES (ADDITIONAL LICENSI Comprehensive Protection DDOS Detection & Mitigation Block Actions Hybrid DDOS Integration Bi-Directional Deep Packet Inspection Enforce RFC Compliance Bot Protection Behaviour Analysis Multiple Security Profiles Port Mirroring Rate Limit & QoS Management Blacklist / Whitelist Malicious Source Protection Custom Signatures SYN Flood Protection Challenge & Response Connection Based Protection DNS Protection LT DDOS Protection Machine Learning Protection Signatures for Known Vulnerabilities VPN FEATURES (ADDITIONAL LICENSING	Support DNS over HTTP, UDP, TCP & SSL as well as DNSSEC Protecting DNS infrastructure from bot attacks, data exfiltration attacks, RPZ policy Support for permanent Blacklisting and Whitelisting based on IP, IP prefix, domain, country, etc. Support for user defined custom rules with support for pattern, suffix, domain, etc. NG) Layer 3 to Layer 7 protection covering Network, Protocol, Application, Reflection / Amplification and 0-day DDoS attacks Attack detection & mitigation in less than 18s and 10s respectively Drop Packet, Terminate Connection (RST), Blacklist (temporary or permanent), Send Challenge (TCP, HTTP, DNS), Rate Limiting Support for integration with Haltdos Cloud Scrubbing or ISP clean pipe services Support for both inbound and outbound traffic protection Protection against malformed packets (TCP, UDP, ICMP, Ping of death, DNS, HTTP, SIP, SNMP, IPv4, IPv6, Fragmented packets, etc.) Protection against misbehaving clients sending invalid or out of state packets Automatic detection and blocking of bot traffic with support for manual bot policy Network behaviour analysis for anomaly detection and packet scoring technology Support for multiple security profiles for enforcing different policy for different sub-networks (Src, Dst IP Prefix, VLAN). Default Global security profile Mirror traffic / specific traffic to another NIC port Rate limit capability for bandwidth and QoS management with option for rate limit of specific traffic (based on proto, src, dst, etc.) Support for temporary or permanent Blacklisting and Whitelisting based on IP, IP prefix, domain, country, etc. Protection against TOR IP, Bad Reputation IP / domain, dark IP, malicious Bots, proxies, resolvers, etc Support for user defined custom rules with support for REGEX and byte matching TCP SYN flood protection with SYN Proxy and connection aging Support for TCP, HTTP, DNS challenge and response for validation of traffic from suspicious sources Protection against TCP connection DDoS attacks such as Solvokoris, R.U.D.V., slow HTTP GET / P
Dynamic Routing Protocols BGP, OSFP, RIP v1, RIP v2 Networking Support for VLAN, Link Aggregation & Trunking (LACP) Client Support Support for Windows, Linux, Mobile Apps (Android or iOS), Web (Java Applet) Authentication Password, SAML / AD / LDAP / SSO, AAA, OAuth, MDM parameters (CPU, HDD, MAC, etc), 3 rd Party (via Webhooks) NAT & Routing Support for client, server or full NAT, static routing for IPv4 & IPv6 User Grouping Support for creating multiple users, user groups with fine grained access to different part of network and/or services	Network Mode DNS Firewall Blacklist / Whitelist Custom Signatures DDOS FEATURES (ADDITIONAL LICENSI Comprehensive Protection DDOS Detection & Mitigation Block Actions Hybrid DDOS Integration Bi-Directional Deep Packet Inspection Enforce RFC Compliance Bot Protection Behaviour Analysis Multiple Security Profiles Port Mirroring Rate Limit & QoS Management Blacklist / Whitelist Malicious Source Protection Custom Signatures SYN Flood Protection Challenge & Response Connection Based Protection DNS Protection LT DDOS Protection Machine Learning Protection Signatures for Known Vulnerabilities VPN FEATURES (ADDITIONAL LICENSING	Support DNS over HTTP, UDP, TCP & SSL as well as DNSSEC Protecting DNS infrastructure from bot attacks, data exfiltration attacks, RPZ policy Support for permanent Blacklisting and Whitelisting based on IP, IP prefix, domain, country, etc. Support for user defined custom rules with support for pattern, suffix, domain, etc. NOS Layer 3 to Layer 7 protection covering Network, Protocol, Application, Reflection / Amplification and 0-day DDoS attacks Attack detection & mitigation in less than 18s and 10s respectively Drop Packet, Terminate Connection (RST), Blacklist (temporary or permanent), Send Challenge (TCP, HTTP, DNS), Rate Limiting Support for integration with Haltdos Cloud Scrubbing or ISP clean pipe services Support for both inbound and outbound traffic protection Protection against malformed packets (TCP, UDP, ICMP, Ping of death, DNS, HTTP, SIP, SNMP, IPv4, IPv6, Fragmented packets, etc.) Protection against misbehaving clients sending invalid or out of state packets Automatic detection and blocking of bot traffic with support for manual bot policy Network behaviour analysis for anomaly detection and packet scoring technology Support for multiple security profiles for enforcing different policy for different sub-networks (Src, Dst IP Prefix, VLAN). Default Global security profile Mirror traffic / specific traffic to another NIC port Rate limit capability for bandwidth and QoS management with option for rate limit of specific traffic (based on proto, src, dst, etc.) Support for temporary or permanent Blacklisting and Whitelisting based on IP, IP prefix, domain, country, etc. Protection against TOR IP, Bad Reputation IP / domain, dark IP, malicious Bots, proxies, resolvers, etc Support for TCP, HTTP, DNS challenge and response for validation of traffic from suspicious sources Protection against TOP connection DDoS attacks such as Slowborns, R.U.D.Y., slow HTTP GET7 POST, etc Automatic learning counter measures and dynamic signature creation upon attack detection Built-in rules for known vul
Networking Support for VLAN, Link Aggregation & Trunking (LACP) Client Support Support for Windows, Linux, Mobile Apps (Android or iOS), Web (Java Applet) Authentication Password, SAML / AD / LDAP / SSO, AAA, OAuth, MDM parameters (CPU, HDD, MAC, etc.), 3 rd Party (via Webhooks) NAT & Routing Support for client, server or full NAT, static routing for IPv4 & IPv6 User Grouping Support for creating multiple users, user groups with fine grained access to different part of network and/or services	Network Mode DNS Firewall Blacklist / Whitelist Custom Signatures DDOS FEATURES (ADDITIONAL LICENSI Comprehensive Protection DDoS Detection & Mitigation Block Actions Hybrid DDOS Integration Bi-Directional Deep Packet Inspection Enforce RFC Compliance Bot Protection Behaviour Analysis Multiple Security Profiles Port Mirroring Rate Limit & QoS Management Blacklist / Whitelist Malicious Source Protection Custom Signatures SYN Flood Protection Challenge & Response Connection Based Protection DNS Protection L7 DDOS Protection Machine Learning Protection Signatures for Known Vulnerabilities VPN FEATURES (ADDITIONAL LICENSIN) HTTP Protocols	Support DNS over HTTP, UDP, TCP & SSL as well as DNSSEC Protecting DNS infrastructure from bot attacks, data exfiltration attacks, RPZ policy Support for permanent Blacklisting and Whitelisting based on IP, IP prefix, domain, country, etc. Support for user defined custom rules with support for pattern, suffix, domain, etc. NOS Layer 7 protection covering Network, Protocol, Application, Reflection / Amplification and 0-day DDOS attacks Attack detection & mitigation in less than 18s and 10s respectively Drop Packet, Terminate Connection (RST), Blacklist (temporary or permanent), Send Challenge (TCP, HTTP, DNS), Rate Limiting Support for integration with Haltdos Cloud Scrubbing or ISP clean pipe services Support for both inbound and outbound traffic protection Protection against malformed packets (TCP, UDP, ICMP, Ping of death, DNS, HTTP, SIP, SNMP, IPv4, IPv6, Fragmented packets, etc.) Protection against misbehaving clients sending invalid or out of state packets Automatic detection and blocking of bot traffic with support for manual bot policy Network behaviour analysis for anomaly detection and packet scoring technology Support for multiple security profiles for enforcing different policy for different sub-networks (Src, Dst IP Prefix, VLAN). Default Global security profile Mirror traffic / specific traffic to another NIC port Rate limit capability for bandwidth and QoS management with option for rate limit of specific traffic (based on proto, src, dst, etc.) Support for temporary or permanent Blacklisting and Whitelisting based on IP, IP prefix, domain, country, etc. Protection against TOR IP, Bad Reputation IP / domain, dark IP, malicious Bots, proxies, resolvers, etc Support for User defined custom rules with support for REGEX and byte matching TCP SYN flood protection with SYN Proxy and connection aging Support for TCP, HTTP, DNS challenge and response for validation of traffic from suspicious sources Protection against TOR ton Protection DDOS attacks such as sockstress, connection / src, zombie flood, S
Networking Support for VLAN, Link Aggregation & Trunking (LACP) Client Support Support for Windows, Linux, Mobile Apps (Android or iOS), Web (Java Applet) Authentication Password, SAML / AD / LDAP / SSO, AAA, OAuth, MDM parameters (CPU, HDD, MAC, etc.), 3 rd Party (via Webhooks) NAT & Routing Support for client, server or full NAT, static routing for IPv4 & IPv6 User Grouping Support for creating multiple users, user groups with fine grained access to different part of network and/or services	Network Mode DNS Firewall Blacklist / Whitelist Custom Signatures DDOS FEATURES (ADDITIONAL LICENSI Comprehensive Protection DDoS Detection & Mitigation Block Actions Hybrid DDOS Integration Bi-Directional Deep Packet Inspection Enforce RFC Compliance Bot Protection Behaviour Analysis Multiple Security Profiles Port Mirroring Rate Limit & QoS Management Blacklist / Whitelist Malicious Source Protection Custom Signatures SYN Flood Protection Challenge & Response Connection Based Protection DNS Protection L7 DDOS Protection Machine Learning Protection Signatures for Known Vulnerabilities VPN FEATURES (ADDITIONAL LICENSIN) HTTP Protocols	Support DNS over HTTP, UDP, TCP & SSL as well as DNSSEC Protecting DNS infrastructure from bot attacks, data extilitation attacks, RPZ policy Support for permanent Blacklisting and Whitelisting based on IP, IP prefix, domain, country, etc. Support for user defined custom rules with support for pattern, suffix, domain, etc. NOS Layer 3 to Layer 7 protection covering Network, Protocol, Application, Reflection / Amplification and 0-day DDoS attacks Attack detection & mitigation in less than 18s and 10s respectively Drop Packet, Terminate Connection (RST), Blacklist (temporary or permanent), Send Challenge (TCP, HTTP, DNS), Rate Limiting Support for integration with Haltdos Cloud Scrubbing or ISP clean pipe services Support for both inbound and outbound traffic protection Protection against maiformed packets (TCP, UDP, ICMP, Ping of death, DNS, HTTP, SIP, SNMP, IPv4, IPv6, Fragmented packets, etc.) Protection against misbehaving clients sending invalid or out of state packets Automatic detection and blocking of bot traffic with support for manual bot policy Network behaviour analysis for anomaly detection and packet scoring technology Support for multiple security profiles for enforcing different policy for different sub-networks (Src, Dst IP Prefix, VLAN). Default Global security profile Mirror traffic / specific traffic to another NIC port Rate limit capability for bandwidth and QoS management with option for rate limit of specific traffic (based on proto, src, dst, etc.) Support for temporary or permanent Blacklisting and Whitelisting based on IP, IP prefix, domain, country, etc. Protection against TOR IP, Bad Reputation IP / domain, dark IP, malicious Bots, proxies, resolvers, etc Support for TCP, HTTP, DNS challenge and response for validation of traffic from suspicious sources Protection against TCP connection DDoS attacks such as sockstress, connection / src, zombie flood, SSL renegotiations, etc Built-in DNS frewall capability for protecting DNS infrastructure against DNS DDoS attacks (Water Torture, NXD
Client Support Support for Windows, Linux, Mobile Apps (Android or iOS), Web (Java Applet) Authentication Password, SAML / AD / LDAP / SSO, AAA, OAuth, MDM parameters (CPU, HDD, MAC, etc.), 3 rd Party (via Webhooks) NAT & Routing Support for client, server or full NAT, static routing for IPv4 & IPv6 User Grouping Support for creating multiple users, user groups with fine grained access to different part of network and/or services	Network Mode DNS Firewall Blacklist / Whitelist Custom Signatures DDOS FEATURES (ADDITIONAL LICENSI Comprehensive Protection DDoS Detection & Mitigation Block Actions Hybrid DDOS Integration Bi-Directional Deep Packet Inspection Enforce RFC Compliance Bot Protection Behaviour Analysis Multiple Security Profiles Port Mirroring Rate Limit & QoS Management Blacklist / Whitelist Malicious Source Protection Custom Signatures SYN Flood Protection Challenge & Response Connection Based Protection DNS Protection DNS Protection Signatures for Known Vulnerabilities VPN FEATURES (ADDITIONAL LICENSING HTTP Protocols SSL/TLS Management	Support DNS over HTTP, UDP, TCP & SSL as well as DNSSEC Protecting DNS infrastructure from bot attacks, data extilitation attacks, RPZ policy Support for permanent Blacklisting and Whitelisting based on IP, IP prefix, domain, country, etc. Support for user defined custom rules with support for pattern, suffix, domain, etc. NOS Layer 3 to Layer 7 protection covering Network, Protocol, Application, Reflection / Amplification and 0-day DDoS attacks Attack detection & mitigation in less than 18s and 10s respectively Drop Packet, Terminate Connection (RST), Blacklist (temporary or permanent), Send Challenge (TCP, HTTP, DNS), Rate Limiting Support for integration with Haltdos Cloud Scrubbing or ISP clean pipe services Support for both inbound and outbound traffic protection Protection against maiformed packets (TCP, UDP, ICMP, Ping of death, DNS, HTTP, SIP, SNMP, IPv4, IPv6, Fragmented packets, etc.) Protection against misbehaving clients sending invalid or out of state packets Automatic detection and blocking of bot traffic with support for manual bot policy Network behaviour analysis for anomaly detection and packet scoring technology Support for multiple security profiles for enforcing different policy for different sub-networks (Src, Dst IP Prefix, VLAN). Default Global security profile Mirror traffic / specific traffic to another NIC port Rate limit capability for bandwidth and QoS management with option for rate limit of specific traffic (based on proto, src, dst, etc.) Support for temporary or permanent Blacklisting and Whitelisting based on IP, IP prefix, domain, country, etc. Protection against TOR IP, Bad Reputation IP / domain, dark IP, malicious Bots, proxies, resolvers, etc Support for TCP, HTTP, DNS challenge and response for validation of traffic from suspicious sources Protection against TCP connection DDoS attacks such as sockstress, connection / src, zombie flood, SSL renegotiations, etc Built-in DNS frewall capability for protecting DNS infrastructure against DNS DDoS attacks (Water Torture, NXD
Authentication Password, SAML/AD/LDAP/SSO, AAA, OAuth, MDM parameters (CPU, HDD, MAC, etc), 3 rd Party (via Webhooks) NAT & Routing Support for client, server or full NAT, static routing for IPv4 & IPv6 User Grouping Support for creating multiple users, user groups with fine grained access to different part of network and/or services	Network Mode DNS Firewall Blacklist / Whitelist Custom Signatures DDOS FEATURES (ADDITIONAL LICENSI Comprehensive Protection DDOS Detection & Mitigation Block Actions Hybrid DDOS Integration Bi-Directional Deep Packet Inspection Enforce RFC Compliance Bot Protection Behaviour Analysis Multiple Security Profiles Port Mirroring Rate Limit & QoS Management Blacklist / Whitelist Malicious Source Protection Custom Signatures SYN Flood Protection Challenge & Response Connection Based Protection IT DDOS Protection Machine Learning Protection Signatures for Known Vulnerabilities VPN FEATURES (ADDITIONAL LICENSING HTTP Protocols SSL/TLS Management Dynamic Routing Protocols	Support DNS over HTTP, UDP, TCP & SSL as well as DNSSEC Protecting DNS infrastructure from bot attacks, data exfilitration attacks, RPZ policy Support for permanent Blacklisting and Whitelisting based on IP, IP prefix, domain, country, etc. Support for user defined custom rules with support for pattern, suffix, domain, etc. NG) Layer 3 to Layer 7 protection covering Network, Protocol, Application, Reflection / Amplification and 0-day DDoS attacks Attack detection & mitigation in less than 18s and 10s respectively Drop Packet, Terminate Connection (RST), Blacklist (temporary or permanent), Send Challenge (TCP, HTTP, DNS), Rate Limiting Support for integration with Haltdos Cloud Scrubbing or ISP clean pipe services Support for both inbound and outbound traffic protection Protection against misbehaving clients sending invalid or out of state packets Automatic detection and blocking of bot traffic with support for manual bot policy Network behaviour analysis for anomaly detection and packet scoring technology Support for multiple security profiles for enforcing different policy for different sub-networks (Src, Dst IP Prefix, VLAN). Default Global security profile Mirror traffic / specific traffic to another NIC port Rate limit capability for bandwidth and QoS management with option for rate limit of specific traffic (based on proto, src, dst, etc.) Support for temporary or permanent Blacklisting and Whitelisting based on IP, IP prefix, domain, country, etc. Protection against TOR IP, Bad Reputation IP / domain, dark IP, malicious Bots, proxies, resolvers, etc Support for user defined custom rules with support for REGEX and byte matching TCP SYN flood protection with SYN Proxy and connection aging Support for User defined custom rules with support for REGEX and byte matching TCP SYN flood protection with SYN Proxy and connection aging Support for Ster Protection against TOR connection DoS attacks such as sockstress, connection / src, zombie flood, SSL renegotiations, etc Built-in DNS firewall capability for protect
NAT & Routing Support for client, server or full NAT, static routing for IPv4 & IPv6 User Grouping Support for creating multiple users, user groups with fine grained access to different part of network and/or services	Network Mode DNS Firewall Blacklist / Whitelist Custom Signatures DDOS FEATURES (ADDITIONAL LICENSI Comprehensive Protection DDoS Detection & Mitigation Block Actions Hybrid DDOS Integration Bi-Directional Deep Packet Inspection Enforce RFC Compliance Bot Protection Behaviour Analysis Multiple Security Profiles Port Mirroring Rate Limit & QoS Management Blacklist / Whitelist Malicious Source Protection Custom Signatures SYN Flood Protection Challenge & Response Connection Based Protection DNS Protection LT DDOS Protection Machine Learning Protection Signatures for Known Vulnerabilities VPN FEATURES (ADDITIONAL LICENSIN) HTTP Protocols SSL/TLS Management Dynamic Routing Protocols Networking	Support DNS over HTTP, UDP, TCP & SSL as well as DNSSEC Protecting DNS infrastructure from bot attacks, data exfiltration attacks, RPZ policy Support for permanent Blacklisting and Whitelisting based on IP, IP prefix, domain, country, etc. Support for user defined custom rules with support for pattern, suffix, domain, etc. NOS Layer 3 to Layer 7 protection covering Network, Protocol, Application, Reflection / Amplification and 0-day DDOS attacks Attack detection & mitigation in less than 18s and 10s respectively Drop Packet, Terminate Connection (RST), Blacklist (temporary or permanent), Send Challenge (TCP, HTTP, DNS), Rate Limiting Support for integration with Haltdos Cloud Scrubbing or 15P clean pipe services Support for both inbound and outbound traffic protection Protection against mislohaming clients sending invalid or out of state packets Automatic detection and blocking of bot traffic with support for manual bot policy Network behaviour analysis for anomaly detection and packet scoring technology Support for multiple security profiles for enforcing different policy for different sub-networks (Src, Dst IP Prefix, VLAN). Default Global security profile Mirror traffic / specific traffic to another NIC port Rate limit capability for bandwidth and QoS management with option for rate limit of specific traffic (based on proto, src, dst, etc.) Support for temporary or permanent Blacklisting and Whitelisting based on IP, IP prefix, domain, country, etc. Protection against TiDe honection Dots and the IP / domain, dark IP, malicious Bots, prowies, resolvers, etc Support for TCP, HTTP, DNS challenge and response for validation of traffic from suspicious sources Protection against TOP connection DOS attacks such as Slowlovins, R.U.D.V., slow HTTP GET / POST, etc Automatic learning counter measures and dynamic signature against DNS DDOS attacks (Water Torture, NXDomain, etc.) Protection against TOP connection DOS attacks such as Slowlovins, R.U.D.V., slow HTTP GET / POST, etc Automatic learning co
User Grouping Support for creating multiple users, user groups with fine grained access to different part of network and/or services	Network Mode DNS Firewall Blacklist / Whitelist Custom Signatures DDOS FEATURES (ADDITIONAL LICENSI Comprehensive Protection DDOS Detection & Mitigation Block Actions Hybrid DDOS Integration Bi-Directional Deep Packet Inspection Enforce RFC Compliance Bot Protection Behaviour Analysis Multiple Security Profiles Port Mirroring Rate Limit & QoS Management Blacklist / Whitelist Malicious Source Protection Custom Signatures SYN Flood Protection Challenge & Response Connection Based Protection DNS Protection DNS Protection LT DDOS Protection Machine Learning Protection Signatures for Known Vulnerabilities VPN FEATURES (ADDITIONAL LICENSING HTTP Protocols SSL/TLS Management Dynamic Routing Protocols Networking Client Support	Support DNS over HTTP, UDP, TCP & SSL as well as DNSSEC Protecting DNS infrastructure from bot attacks, data exfiltration attacks, RPZ policy Support for permanent Blackilsting and Whitelisting based on IP, IP prefix, domain, country, etc. Support for user defined custom rules with support for pattern, suffix, domain, etc. NG) Layer 3 to Layer 7 protection covering Network, Protocol, Application, Reflection / Amplification and 0-day DDoS attacks Attack detection & mitigation in less than 18s and 10s respectively Drop Packet, Terminate Connection (RST), Blackilst (temporary or permanent), Send Challenge (TCP, HTTP, DNS), Rate Limiting Support for both inbound and outbound traffic protection Protection against malformed packets (TCP, UDP, ICMP, Ping of death, DNS, HTTP, SIP, SNMP, IPv4, IPv6, Fragmented packets, etc.) Protection against misbehaving clients sending invalid or out of state packets Automatic detection and blocking of bot traffic with support for manual bot policy Network behaviour analysis for anomaly detection and packet scoring technology Support for multiple security profiles for enforcing different policy for different sub-networks (Src, Dst IP Prefix, VLAN). Default Global security profile Mirror traffic / specific traffic to another NIC port Rate limit capability for bandwidth and QoS management with option for rate limit of specific traffic (based on proto, src, dst, etc.) Support for temporary or permanent Blackilsting and Whitelisting based on IP, IP prefix, domain, country, etc. Protection against TOR IP, Bad Reputation IP / domain, dark IP, mallicious Bots, proxies, resolvers, etc Support for user defined custom rules with support for REGEX and byte matching TCP SYN flood protection with SYN Proxy and connection against TOR, Pla Aga Reputation IP / domain, dark IP, mallicious Bots, proxies, resolvers, etc Support for User defined custom rules with support for REGEX and byte matching TCP SYN flood protection with SYN Proxy and connection against DNS DoS attacks (Water Torture, NXDomain, e
User Grouping Support for creating multiple users, user groups with fine grained access to different part of network and/or services	Network Mode DNS Firewall Blacklist / Whitelist Custom Signatures DDOS FEATURES (ADDITIONAL LICENSI Comprehensive Protection DDOS Detection & Mitigation Block Actions Hybrid DDOS Integration Bi-Directional Deep Packet Inspection Enforce RFC Compliance Bot Protection Behaviour Analysis Multiple Security Profiles Port Mirroring Rate Limit & QoS Management Blacklist / Whitelist Malicious Source Protection Custom Signatures SYN Flood Protection Challenge & Response Connection Based Protection DNS Protection DNS Protection LT DDOS Protection Machine Learning Protection Signatures for Known Vulnerabilities VPN FEATURES (ADDITIONAL LICENSING HTTP Protocols SSL/TLS Management Dynamic Routing Protocols Networking Client Support	Support DNS over HTTP, UDP, TCP & SSL as well as DNSSEC Protecting DNS infrastructure from bot attacks, data exfiltration attacks, RPZ policy Support for permanent Blackilsting and Whitelisting based on IP, IP prefix, domain, country, etc. Support for user defined custom rules with support for pattern, suffix, domain, etc. NG) Layer 3 to Layer 7 protection covering Network, Protocol, Application, Reflection / Amplification and 0-day DDoS attacks Attack detection & mitigation in less than 18s and 10s respectively Drop Packet, Terminate Connection (RST), Blackilst (temporary or permanent), Send Challenge (TCP, HTTP, DNS), Rate Limiting Support for both inbound and outbound traffic protection Protection against malformed packets (TCP, UDP, ICMP, Ping of death, DNS, HTTP, SIP, SNMP, IPv4, IPv6, Fragmented packets, etc.) Protection against misbehaving clients sending invalid or out of state packets Automatic detection and blocking of bot traffic with support for manual bot policy Network behaviour analysis for anomaly detection and packet scoring technology Support for multiple security profiles for enforcing different policy for different sub-networks (Src, Dst IP Prefix, VLAN). Default Global security profile Mirror traffic / specific traffic to another NIC port Rate limit capability for bandwidth and QoS management with option for rate limit of specific traffic (based on proto, src, dst, etc.) Support for temporary or permanent Blackilsting and Whitelisting based on IP, IP prefix, domain, country, etc. Protection against TOR IP, Bad Reputation IP / domain, dark IP, mallicious Bots, proxies, resolvers, etc Support for user defined custom rules with support for REGEX and byte matching TCP SYN flood protection with SYN Proxy and connection against TOR, Pla Aga Reputation IP / domain, dark IP, mallicious Bots, proxies, resolvers, etc Support for User defined custom rules with support for REGEX and byte matching TCP SYN flood protection with SYN Proxy and connection against DNS DoS attacks (Water Torture, NXDomain, e
	Network Mode DNS Firewall Blacklist / Whitelist Custom Signatures DDOS FEATURES (ADDITIONAL LICENSI Comprehensive Protection DDOS Detection & Mitigation Block Actions Hybrid DDOS Integration Bi-Directional Deep Packet Inspection Enforce RFC Compliance Bot Protection Behaviour Analysis Multiple Security Profiles Port Mirroring Rate Limit & QoS Management Blacklist / Whitelist Malicious Source Protection Custom Signatures SYN Flood Protection Custom Signatures SYN Flood Protection Challenge & Response Connection Based Protection DNS Protection L7 DDOS Protection Machine Learning Protection Signatures for Known Vulnerabilities VPN FEATURES (ADDITIONAL LICENSIN) HTTP Protocols SSL/TLS Management Dynamic Routing Protocols Networking Client Support Authentication	Support DNS over HTTP, UDP, TCP & SSL as well as DNSSEC Protecting DNS infrastructure from bot attacks, data exfiltration attacks, RPZ policy Support for user defined custom rules with support for pattern, suffix, domain, country, etc. Support for user defined custom rules with support for pattern, suffix, domain, etc. NO Layer 3 to Layer 7 protection covering Network, Protocol, Application, Reflection / Amplification and 0-day DDoS attacks Attack detection 8 mitigation in less than 18s and 10s respectively Drop Packet, Terminate Connection (RST), Backlist (temporary or permanent), Send Challenge (TCP, HTTP, DNS), Rate Limiting Support for integration with Haltdos Cloud Scrubbing or ISP clean pipe services Support for both inbound and outbound traffic protection Protection against malformed packets (TCP, UDP, ICMP, Ping of death, DNS, HTTP, SIP, SNMP, IPv4, IPv6, Fragmented packets, etc.) Protection against malformed packets (TCP, UDP, ICMP, Ping of death, DNS, HTTP, SIP, SNMP, IPv4, IPv6, Fragmented packets, etc.) Protection against malformed packets (TCP, UDP, ICMP, Ping of death, DNS, HTTP, SIP, SNMP, IPv4, IPv6, Fragmented packets, etc.) Protection against malformed packets (TCP, UDP, ICMP, Ping of death, DNS, HTTP, SIP, SNMP, IPv4, IPv6, Fragmented packets, etc.) Protection against malformed packets (TCP, UDP, ICMP, Ping of death, DNS, HTTP, SIP, SNMP, IPv4, IPv6, Fragmented packets, etc.) Network behaviour analysis for anomaly detection and packet scoring technology Support for multiple security profiles for enforcing different policy for different sub-networks (Src, Dst IP Prefix, VLAN). Default Global security profile Mirror traffic / specific traffic to another NIC port Rate limit capability for bandwidth and QoS management with option for rate limit of specific traffic (based on proto, src, dst, etc.) Support for tremporary or permanent Blacklisting and Whitelisting based on IP, IP prefix, domain, country, etc. Protection against TOR onnoction DDoS attacks uch as Silvaloria, dark IP, malicious Bo
Dual Stack Life T Support for NAT 46 / 64 and DNS 46 / 64 with DNS Proxy	Network Mode DNS Firewall Blacklist / Whitelist Custom Signatures DDOS FEATURES (ADDITIONAL LICENS) Comprehensive Protection DDoS Detection & Mitigation Block Actions Hybrid DDOS Integration Bi-Directional Deep Packet Inspection Enforce RFC Compliance Bot Protection Behaviour Analysis Multiple Security Profiles Port Mirroring Rate Limit & QoS Management Blacklist / Whitelist Malicious Source Protection Custom Signatures SYN Flood Protection Custom Signatures SYN Flood Protection Challenge & Response Connection Based Protection DNS Protection L7 DDoS Protection Machine Learning Protection Signatures for Known Vulnerabilities VPN FEATURES (ADDITIONAL LICENSING HTTP Protocols SSL/TLS Management Dynamic Routing Protocols Networking Client Support Authentication NAT & Routing	Support DNS over HTTP, UDP, TCP & SSL as well as DNSSEC Protecting DNS infrastructure from bot attacks, data exfiltration attacks, RPZ policy Support for permanent Blacklisting and Whitelisting based on IP, IP prefix, domain, country, etc. Support for user defined custom rules with support for pattern, suffix, domain, etc. NGI Layer 3 to Layer 7 protection covering Network, Protocol, Application, Reflection / Amplification and 0-day DDoS attacks Attack detection & mitigation in less than 18s and 10s respectively Drop Packet, Terminate Connection (RST), Blacklist (temporary or permanent), Send Challenge (TCP, HTTP, DNS), Rate Limiting Support for integration with Haltdos Cloud Scrubbing or ISP clean pipe services Support for both inbound and outbound traffic protection Protection against malformed packets (TCP, UDP, ICMP, Ping of death, DNS, HTTP, SIP, SNMP, IPv4, IPv6, Fragmented packets, etc.) Protection against misbehaving clients sending invalid or out of state packets Automatic detection and blocking of bot traffic with support for manual bot policy Network behaviour analysis for anomaly detection and packet scoring technology Support for multiple security profiles for enforcing different policy for different sub-networks (Src, Dst IP Prefix, VLAN). Default Global security profile Mirror traffic / specific traffic to another NIC port Rate limit capability for bandwidth and QoS management with option for rate limit of specific traffic (based on proto, src, dst, etc.) Support for user defined custom rules with support for REGEX and byte matching TCP SYM flood protection with SYM Proxy and Connection aging Support for USA, ISA (Base Protection against TOR IP, Bad Reputation IP / domain, dark IP, malicious bots, proxies, resolvers, etc Support for USA, Pitt Province of the p
Substitution and Composition to Control of C	Network Mode DNS Firewall Blacklist / Whitelist Custom Signatures DDOS FEATURES (ADDITIONAL LICENSI Comprehensive Protection DDoS Detection & Mitigation Block Actions Hybrid DDOS Integration Bi-Directional Deep Packet Inspection Enforce RFC Compliance Bot Protection Behaviour Analysis Multiple Security Profiles Port Mirroring Rate Limit & QoS Management Blacklist / Whitelist Malicious Source Protection Custom Signatures SYN Flood Protection Challenge & Response Connection Based Protection DNS Protection L7 DDOS Protection Machine Learning Protection Signatures for Known Vulnerabilities VPN FEATURES (ADDITIONAL LICENSIN HTTP Protocols SSL/TLS Management Dynamic Routing Protocols Networking Client Support Authentication NAT & Routing User Grouping	Support ONS over HTTP, UDP, TCP & SSL as well as DNSSEC Protecting DNS infrastructure from bot attacks, data exfiltration attacks, RPZ policy Support for permanent Blacklisting and Whitelisting based on IP, IP prefix, domain, country, etc. Support for user defined custom rules with support for pattern, suffix, domain, etc. NOS Layer 3 to Layer 7 protection covering Network, Protocol, Application, Reflection / Amplification and 0-day DDoS attacks Attack detection & mitigation in less than 18s and 10s respectively Drop Packet, Terminate Connection (RST), Blacklist (temporary or permanent), Send Challenge (TCP, HTTP, DNS), Rate Limiting Support for integration with Haltdos Cloud Scrubbing or ISP clean pipe services Support for both inbound and outbound traffic protection Protection against malformed packets (TCP, UDP, ICMP, Ping of death, DNS, HTTP, SIP, SNMP, IPv4, IPv6, Fragmented packets, etc.) Protection against malformed packets (TCP, UDP, ICMP, Ping of death, DNS, HTTP, SIP, SNMP, IPv4, IPv6, Fragmented packets, etc.) Protection against malformed packets (TCP, UDP, ICMP, Ping of death, DNS, HTTP, SIP, SNMP, IPv4, IPv6, Fragmented packets, etc.) Protection against malformed packets (TCP, UDP, ICMP, Ping of death, DNS, HTTP, SIP, SNMP, IPv4, IPv6, Fragmented packets, etc.) Wetwork behaviour analysis for anomaly detection and packet scoring technology Support for multiple security profiles for enforcing different policy for different sub-networks (Src, Dst IP Prefix, VLAN). Default Global security profile Mirror traffic / specific traffic to another NIC port. Rate limit capability for bandwidth and QoS management with option for rate limit of specific traffic (based on proto, src, dst, etc.) Support for temporary or permanent Blacklisting and Whitelisting based on IP, IP prefix, domain, country, etc. Protection against TOR P, Bad Reputation IP / domain, dark IP, mallicious Bots, proxies, resolvers, etc Support for Nindow provide and

HARDWARE FLEXIBILITY

Haltdos appliances are built on a common hardware platform with flexibility in mind. The appliances can be extended to provide remote, out-of-band management and monitoring, performance acceleration, and more with expansion modules Expansion Module includes:

- Network Cards (copper or optical)
 Hardware Security Module (HSM) (non-FIPS and FIPS-140-2)
- SSL acceleration card
- Hard Disk & RAM

NIC Cards			
Part Code	Description	Copper/Fiber	Hardware Bypass
HD-NIC-1x4C	Quad Port 1 Gbps	Copper	No
HD-NIC-1x4CB	Quad Port 1 Gbps	Copper	Yes
HD-NIC-1x4F	Quad Port 1 Gbps	Fiber (Single / Multi-Mode)	No
HD-NIC-10x2C	Dual Port 10 Gbps	Copper	No
HD-NIC-10x2CB	Dual Port 10 Gbps	Copper	Yes
HD-NIC-10x2F	Dual Port 10 Gbps	Fiber (Single / Multi-Mode)	No
HD-NIC-10x2FB	Dual Port 10 Gbps	Fiber (Single / Multi-Mode)	Yes
HD-NIC-10x4F	Quad Port 10 Gbps	Fiber (Single / Multi-Mode)	No
HD-NIC-10x4FB	Quad Port 10 Gbps	Fiber (Single / Multi-Mode)	Yes
HD-NIC-25x2F	Dual Port 25 Gbps	Fiber (Single / Multi-Mode)	No
HD-NIC-25x2FB	Dual Port 25 Gbps	Fiber (Single / Multi-Mode)	Yes
HD-NIC-25x4F	Quad Port 25 Gbps	Fiber (Single / Multi-Mode)	No
HD-NIC-25x4FB	Quad Port 25 Gbps	Fiber (Single / Multi-Mode)	Yes
HD-NIC-40x2F	Dual Port 40 Gbps	Fiber (Single / Multi-Mode)	No
HD-NIC-40x2FB	Dual Port 40 Gbps	Fiber (Single / Multi-Mode)	Yes
HD-NIC-40x4F	Quad Port 40 Gbps	Fiber (Single / Multi-Mode)	No
HD-NIC-40x4FB	Quad Port 40 Gbps	Fiber (Single / Multi-Mode)	Yes
HD-NIC-100x2F	Dual Port 100 Gbps	Fiber (Single / Multi-Mode)	No
HD-NIC-100x2FB	Dual Port 100 Gbps	Fiber (Single / Multi-Mode)	Yes
HD-NIC-100x4F	Quad Port 100 Gbps	Fiber (Single / Multi-Mode)	No
HD-NIC-100x4FB	Quad Port 100 Gbps	Fiber (Single / Multi-Mode)	Yes

SSL Cards				
Part Code	Throughput		SSL TPS	
HD-SSL-25G	SSL	25 Gbps	RSA	40
115 332 233	Compression	20 Gbps	ECC	25K
HD-SSL-50G	SSL	50 Gbps	RSA	95K
	Compression	37 Gbps	ECC	48K

RAM		
HD-RAM-8G	8 GB DDR4 RAM	
HD-RAM-16G	16 GB DDR4 RAM	
HD-RAM-32G	32 GB DDR4 RAM	
HD-RAM-64G	64 GB DDR4 RAM	

Hard Disk		
HD-DSK-128G-SSD	128 GB SSD Hard Disk	
HD-DSK-256G-SSD	256 GB SSD Hard Disk	
HD-DSK-512G-SSD	512 GB SSD Hard Disk	
HD-DSK-1T-SSD	1 TB SSD Hard Disk	
HD-DSK-1T-HDD	1 TB HDD Hard Disk	
HD-DSK-2T-HDD	2 TB HDD Hard Disk	
HD-DSK-4T-HDD	4 TBHDD Hard Disk	