Service Providers all agree that DDoS attacks are more frequent, complex, and destructive than ever. Providers all report an increase in DDoS attacks against their customers, and have experience attacks that impacted their infrastructures as well. Providers of all sizes agree that DDoS defenses deployed in their networks are no longer an option — they're becoming a requirement to maintain consistent levels of service.

At the heart of the NSFOCUS On-Premises DDoS Defenses is the ADS. It provides comprehensive, multi-layered protection from today’s advanced DDoS attacks. When deployed out-of-path, traffic streams for the IP addresses under attack are “diverted” to the ADS. It surgically mitigates DDoS attack traffic, while allowing all legitimate traffic to continue to pass downstream. When deployed in-line, the ADS detects attacks, and mitigates DDoS traffic. Both deployment modes provide extremely low latency and reliable detection and mitigation of attacks; while ensuring service provider’s customers and services are protected from the impact of DDoS.

**MONITOR**
The ADS is easily deployed in any providers network and can scale to support hundreds of Gbps of inspected traffic. When deployed in-line, it monitors the incoming traffic for signs of DDoS. When deployed out-of-path, the NSFOCUS Network Traffic Analyzer (NTA) performs the monitoring and detection function by consuming xFlow data from border, core, or edge routers. Either method provides reliable monitoring and detection of DDoS.

**DETECT**
At the core of the ADS are innovative, multi-stage detection engines. All packets are subjected to a series of analyses, checks, and validations to accurately identify both legitimate and attack traffic. These include RFC Checks, Protocol Analysis, Access Control Lists, IP Reputation, Anti-spoofing, L4-L7 Algorithmic Analysis, User Behavior Analysis, Regular Expressions, Fragmentation Controls, Connection and Rate Limiting. Together they provide industry-leading accuracy that protects against all DDoS attacks. The detection engine is optimized frequently, so providers always have the most accurate protection available.

**MITIGATE**
Regardless of the deployment scenario, once attack traffic has been identified by the ADS, it immediately removes this traffic from the traffic streams it’s inspecting. The ADS then forwards only legitimate traffic to its intended destination. Also, the ADS can integrate with NSFOCUS Threat Intelligence (NTI) to remove the traffic from known botnets immediately, and uploads the attack data to NTI for contributing to intelligence. The ADS supports DDoS attack reporting in real-time to provide valuable information such as attack types, source/destination IPs, protocols, and more. An integrated web services API can also be used to assist with automated configuration, post-incident reporting, and billing operations.

**PERFORMANCE. QUALITY. VALUE.**
The ADS is the ideal solution for service providers to mitigate DDoS attacks against their customers, and their services. Providers who deploy ADS no longer need to rely on null routes to defeat attacks. Available in a range of cost and performance optimized appliances, the ADS has been purpose-built to deliver high quality, scalable mitigation of DDoS attack traffic.
## SOFTWARE SPECIFICATIONS

### DDoS Protection
- Comprehensive, multi-layered protection against volumetric, application, and web application attacks
- Multi-protocol support and advanced inspection including TCP/UDP/ICMP/HTTP/HTTPS/DNS/SIP floods, Amplification attacks (NTP/SSDP/SNMP/DNS/CHARGEN/Memcached/NetBIOS), fragments floods, connection exhaustion, header manipulation and more
- Integrated with NSFOCUS Cloud Security Platform
- Integrated with NSFOCUS Threat Intelligence

### DDoS Mitigation Algorithms
- RFC Checks
- Black Filter Lists
- NTI Black Filter Lists
- White Filter Lists
- GEOIP Filter Lists
- Access Control Lists Filtering
- TCP Regular Expression Filtering
- UDP Regular Expression Filtering
- SYN Check
- ACK Check
- Reflection Amplification Rules
- Port Check
- Connection Exhaustion
- URL-ACK Filter Lists
- Anti-spoofing
- TCP SYN Source IP Rate Limit
- TCP SYN Source Bandwidth Limit
- TCP SYN Time Sequence Check
- TCP Fragment Control
- ICMP Fragment Control
- ICMP Traffic Control
- DNS Keyword Checking
- DNS Rate-Limiting
- DNS TCP-BIT Check
- DNS CNAME Check
- DNS Retransmission
- HTTP Keyword Checking
- HTTP Authentication
- HTTP Dynamic Script
- HTTP FCS Check
- HTTP Pattern Matching Check
- HTTP Slow Attack Check
- IP Behavior Analysis
- Trusted Source IP Control
- Empty Connection Check
- HTTPS SSL Connection Control
- HTTPS Authentication
- SIP Authentication
- UDP Payload Check
- UDP Fragment Control
- UDP Packet Length Check
- UDP Traffic Control
- TCP Watermark Check
- UDP Watermark Check
- TCP Pattern Matching
- UDP Pattern Matching
- Protocol ID Check

### Management
- Protocols: HTTP, SNMP, Email, Syslog
- Authentication: Local database, Radius, TACACS+
- API: web services for reporting and automated configuration

### IP Protocols
- Addressing: IPv4/6
- Routing: BGP, OSPF, RIP, IS-IS, static routing and PBR
- Data link and network layer: MPLS, GRE, VLAN (802.1q)

### Reporting
- Real-time and historical reporting of attack types, source/destination IP
- Formatting: XML, PDF, HTML, and Microsoft Word
- Web Service API to support automated configuration and reporting functions

---

**DDoS Attack Trend**

- **640,000 TBytes of attack traffic in total, 79.4% increase over 2016**
- **14.1 Gbps of average peak traffic of individual attacks, 39.1% increase over 2016**
- **1.4 Tbps of maximum peak traffic among individual attacks, nearly 100% over 2016**

To download the latest report, go to: https://nsfocusglobal.com/company-overview/resources
### DEPLOYMENT OPTIONS

#### Inline Mode

![Inline Mode Diagram](inline_mode.png)

#### Out-of-path Traffic Diversion

![Out-of-path Traffic Diversion Diagram](out_of_path.png)

#### Network Traffic Analyzer

![Network Traffic Analyzer Diagram](network_traffic_analyzer.png)

#### Anti-DDoS System Manager

![Anti-DDoS System Manager Diagram](anti_ddos_manager.png)

<table>
<thead>
<tr>
<th>Hardware</th>
<th>ADSNX5-10000</th>
<th>ADSNX5-8000</th>
<th>ADSNX5-6025E</th>
<th>ADSNX5-4020E</th>
<th>ADSNX3-2020E</th>
</tr>
</thead>
<tbody>
<tr>
<td>Mitigation Capacity</td>
<td>240Gbps</td>
<td>40Gbps</td>
<td>20Gbps</td>
<td>12Gbps</td>
<td>4Gbps</td>
</tr>
<tr>
<td></td>
<td>149,942,000pps</td>
<td>29,760,000pps</td>
<td>14,880,000pps</td>
<td>8,928,000pps</td>
<td>2,976,000pps</td>
</tr>
<tr>
<td>Interfaces</td>
<td>1<em>IPMI, 1</em>Rj45 Serial, 1*USB</td>
<td>1<em>IPMI, 2</em>GE Copper, 1<em>Rj45 Serial, 2</em>USB</td>
<td>2<em>GE Copper, 1</em>Rj45 Serial, 2*USB</td>
<td>2<em>GE Copper, 1</em>Rj45 Serial, 2*USB</td>
<td>2<em>GE Copper, 1</em>Rj45 Serial, 2*USB</td>
</tr>
<tr>
<td></td>
<td>Optional Interface Card: 2<em>100GE CXP and 20</em>10GE SFP+</td>
<td>Up to: 8<em>10GE SFP+ Or 4</em>10GE SFP+ and 16*GE port (copper, SFP-GE-SX, and SFP-GE-LX available)</td>
<td>Up to: 8<em>10GE SFP+ Or 32</em>GE port (copper, SFP-GE-SX, SFP-GE-SX and SFP-GE-LX and bypass module available)</td>
<td>Up to: 8<em>10GE SFP+ Or 32</em>GE port (copper, SFP-GE-SX, SFP-GE-SX and SFP-GE-LX and bypass module available)</td>
<td>Up to: 4<em>GE and 4</em>SFP Or 8*SFP (copper, SFP-GE-SX, SFP-GE-SX and SFP-GE-LX and bypass module available)</td>
</tr>
<tr>
<td>Dimensions (WxDxH)</td>
<td>19&quot;x27&quot;x10.5&quot; 6 RU</td>
<td>17.4&quot;x24.6&quot;x3.5&quot; 2 RU</td>
<td>17.3&quot;x22.2&quot;x3.5&quot; 2RU</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Weight</td>
<td>121.25 lbs (55 kg)</td>
<td>36.38 lbs (16.5 kg)</td>
<td>26.46 lbs (12 kg)</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Environmental</td>
<td>Operating: 32-113° F (0-45° C) Storage: -40-158° F (-40-70° C)</td>
<td>Operating: 41-104° F (5-40° C) Storage: -4-176° F (-20-80° C)</td>
<td>Operating: 32-113° F (0-45° C) Storage: -4-158° F (-20-80° C)</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Power</td>
<td>AC/DC Five Power Supply (1200W total)</td>
<td>AC/DC Dual Power Supply (500W total)</td>
<td>AC/DC Dual Power Supply (450W total)</td>
<td></td>
<td></td>
</tr>
<tr>
<td>MTBF</td>
<td>52,879 hours</td>
<td>45,000 hours</td>
<td>60,000 hours</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>