ON-PREMISES DDoS DEFENSES

COMPREHENSIVE, MULTI-LAYERED DDoS PROTECTION

Today, Service Providers understand that a significant percentage of DDoS attacks targeting their customers can be defeated by anti-DDoS technology deployed within the providers network itself. Statistics demonstrate that nearly 50 percent of DDoS attacks observed are under 10Gbps in size, and last less than 30 minutes in duration. These attacks can easily be defended or mitigated by NSFOCUS On-Premises DDoS Defenses.

In order to defeat a DDoS attack against their customers, providers of all sizes must “detect” a DDoS attack first. Time-and-time again providers have been notified of DDoS attacks against their customers; however, without the proper detection technology in place, they had no ability to see the attack while in progress. DDoS defenses always begin with detection first. The most economical and effective way to detect DDoS attack traffic is to monitor xFlow data coming from the provider’s border, core, and/or edge routers.

Once a DDoS attack is detected by the provider, the most economical and effective way to protect customers is to divert both good and bad traffic for the IP address(s) under attack. DDoS defenses always begin with detection first. The most economical and effective way to detect DDoS traffic is to monitor xFlow data coming from the provider’s border, core, and/or edge routers.

Once a DDoS attack is detected by the provider, the most economical and effective way to protect customers is to divert both good and bad traffic for the IP address(s) under attack. DDoS defenses always begin with detection first. The most economical and effective way to detect DDoS traffic is to monitor xFlow data coming from the provider’s border, core, and/or edge routers.

Once DDoS detection and mitigation have been addressed, a centralized management system is needed to control the overall solution. This system must allow service providers to implement multi-tenant configurations that control customer policies and rule sets, while providing real-time alerting, reporting, and analytics to the provider.

NSFOCUS provides a complete, on-premises anti-DDoS solution that provides detection, mitigation, and management as follows:

**NETWORK TRAFFIC ANALYZER (NTA) - DETECTS DDoS ATTACKS**
NTA is a DDoS detection appliance that identifies attacks via traffic flow monitoring

**ANTI-DDOS SYSTEM (ADS) - MITIGATES DDoS ATTACKS**
ADS is a DDoS mitigation appliance that removes unwanted, malicious traffic

**ANTI-DDOS SYSTEM MANAGER (ADS-M) - MANAGES COMPLETE SOLUTION**
ADS-M is a multi-tenant management system designed for providers. It provides centralized management of the ADS and NTA appliances as well as support for multiple, separate configuration and reporting domains for each customer. A web-based customer portal is also included.

The network traffic analyzer activity by receiving and analyzing xFlow data from border, core and/or edge routers. It uses an innovative, multi-stage DDoS detection engine made up of several algorithms and other mechanisms to accurately identify DDoS traffic from other traffic streams. User can customize NTA alert plugins with specific signatures, in order to extend NTA detection capability. Also, NTA auto-learning feature provides machine learning threshold baseline, which can be adopted in different scenarios. In addition, the NTA can integrate with NSFOCUS Threat Intelligence (NTI) to query the reputation of the suspicious source IP. On the deployment, the NTA can be deployed as a stand-alone system that provides DDoS detection only and supports Remotely Triggered Black Hole (RTBH) functionality. Under large network traffic scenarios, NTA-FLB can manage and collect flow data from multiple detect points, thus implement high performance detection and flow reuse.

**BENEFITS**
Complete service provider ready solution
Defend attacks against your customers
Lowest total cost of ownership (TCO)
Quick and easy install into your network
Deploy as much mitigation capacity as needed
Automatic hand-off with NSFOCUS Cloud Centers
Shorten time to redirection and cloud mitigation
Increased visibility and traffic threshold monitoring
Versatility of deployment options

**KEY FEATURES**
Automated or manual BGP redirection
GRE, VLAN, MPLS, PBR traffic re-injection
All-in-one solution, multi-tenancy enabled
Low false positives, high performance
Easy to integrate and cohabitate
Automated and reliable DDoS mitigation
Efficient and intelligent protection from the botnet-based attacks with NTI

**Out-of-path Traffic Diversion**

**Network Traffic Analyzer**
**Anti-DDoS System Manager**
**Anti-DDoS System**
**Protected Network**
**INTERNET**

Notification to ADS
Flow Data
Attacker Detection
BGP Advertisement

Defend attacks against your customers
Lowest total cost of ownership (TCO)
Quick and easy install into your network
Deploy as much mitigation capacity as needed
Automatic hand-off with NSFOCUS Cloud Centers
Shorten time to redirection and cloud mitigation
Increased visibility and traffic threshold monitoring
Versatility of deployment options

**KEY FEATURES**
Automated or manual BGP redirection
GRE, VLAN, MPLS, PBR traffic re-injection
All-in-one solution, multi-tenancy enabled
Low false positives, high performance
Easy to integrate and cohabitate
Automated and reliable DDoS mitigation
Efficient and intelligent protection from the botnet-based attacks with NTI
When an ADS is added to the deployment, the ADS then comes under the direction of the NTA. The NTA communicates with the ADS, alerting it to the IP address(es) that are under DDoS attack. The ADS next announces the border routers to divert traffic via BGP to the ADS where malicious traffic is discarded. It then re-injects legitimate traffic back into your network with extremely low latency and high accuracy. Also, the ADS can integrate with NSFOCUS Threat Intelligence (NTI) to discard the traffic from known botnets immediately, and uploads the attack data to NTI for contributing to intelligence.

The ADS-M real-time views are highly optimized for traffic monitoring, reporting, ease of use, and improved user experience.

The ADS-M is used for central configuration, management, and reporting. It can be configured in a multi-tenant mode of operation to provide separate administrative domains on a per-customer basis. The ADS-M includes a flexible, web services API to automate provisioning and reporting for your specific environment. Network operators can use the ADS-M to direct and collect packet captures from co-resident ADS systems to shorten problem resolution and incident response times. Extensive reporting options include information on attack types, attack targets, protocols, ports, network status, alert information, device logs, and more.

The ADS-M also supports a customizable “customer portal” designed for providers who desire to offer Managed DDoS Services. This portal allows providers to offer web-based access to their customers for traffic analysis, reporting, and analytics on a case-by-case basis.

INDUSTRY-LEADING ACCURACY AND FASTEST TIME TO MITIGATION
NSFOCUS On-Premises DDoS Defenses incorporate the latest from our internationally-recognized research labs and is developed with over 16 years of experience protecting the world’s largest banks, telecommunications, gaming, and streaming media companies. The NSFOCUS Security Labs is a cyber security threat research lab at the forefront of vulnerability assessment, threat detection, and mitigation research. Their work, combined with world-class engineering, has resulted in a solution with industry leading accuracy capable of automatically defeating advanced, multi-layer DDoS attacks in as little as 20 seconds.

SCALABILITY
The ADS series of appliances includes models that range from 1Gbps to 40Gbps of DDoS mitigation capacity that support flexible licensing, so providers can deploy as much mitigation capacity as needed. When deployed with an ADS-M appliance, the ADS systems can be clustered to withstand the most extreme volumetric and application-layer DDoS attacks.

MULTI-TENANT, CENTRALIZED MANAGEMENT
The ADS-M provides a multi-tenant configuration interface that simplifies the administration and monitoring of Managed DDoS Services. It enables service providers to create and configure customer specific security policies and reports, including daily/weekly/monthly/yearly intervals with pie charts, bar graphs, line graphs, and more. It also provides real-time traffic monitoring, log information, and detailed attack history for post-incident forensic analysis.

EASY TO DEPLOY AND INTEGRATE
The ADS is typically deployed at the ingress points to your network, while the NTA and ADS-M appliances can be installed at any location in your network. The ADS uses industry standard routing protocols to communicate with other routers in order to redirect suspicious traffic and forward legitimate traffic back into your network. A flexible web services API in the ADS-M further simplifies integration of the system into your network by providing a programmatic interface that can be used to automate labor intensive tasks.
NSFOCUS HYBRID DDoS DEFENSES

Many service providers utilize a hybrid approach to defeat the damaging effects of DDoS attacks. The approach combines NSFOCUS On-Premises Defenses (designed to defeat attacks against your customers) with NSFOCUS Cloud DDoS Protection Service (designed to defeat attacks that impact your infrastructure).

Working in unison, this Complete Service Provider DDoS Mitigation Solution eliminates smaller attacks on-premises, while defending infrastructures from larger attacks using the NSFOCUS Cloud. Both defenses are integrated, resulting in increased bandwidth visibility, reduced cloud redirect times for mitigation, and coverage for all L3-L7 DDoS attacks.

SOFTWARE SPECIFICATIONS

**ADS SERIES**

**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/SMTP/CHARGEN/Memcached), fragments/flooding, 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, NIT Black Filter Lists, White Filter Lists, GEOIP Filter Lists, Access Control Lists Filtering
- TCP Regular Expression Filtering, TCP SYN Source IP Rate Limit, TCP SYN Source Bandwidth Limit, TCP SYN Time Sequence Check, TCP Fragment Control, TCP Watermark Check, TCP Pattern Matching
- SYN Check, ACK Check, Port Check, Connection Exhaustion, URL-ACK Filter Lists, Anti-spoofing, Protocol ID Check
- ICMP Fragment Control, ICMP Traffic Control
- UDP Regular Expression Filtering, UDP Payload Check, UDP Fragment Control, UDP Packet Length Check, UDP Traffic Control, UDP Watermark Check, UDP Pattern Matching, Reflection Amplification Rules

**NTA**

**Flow Monitoring**
- sFlow-v4/v5, Netflow-v5/v9, NetStream-v5, Flexible Netflow, IPFIX

**DDoS Attack Detection**
- False source IP detection
- Integrate with NSFOCUS Threat Intelligence

**ADS-M**

**Centralized Management and Configuration**
- Devices: add, delete and configure
- Multi-tenant
- Security policies
- High availability
- ADS clustering
- NTA Clustering

FOR SERVICE PROVIDERS OF ALL SIZES

NSFOCUS On-Premises Defenses is the ideal solution for today’s service providers to defeat DDoS attacks against their customers. It is highly scalable and is performance optimized to meet the current and future needs of service provider environments. It is also easy to deploy, flexible, and provides a multi-tenant configuration interface to simplify the configuration and administration of large-scale Managed DDoS Services.
# HARDWARE SPECIFICATIONS

## ADS SERIES

<table>
<thead>
<tr>
<th>Hardware</th>
<th>ADSNX-10000</th>
<th>ADSNX-8000</th>
<th>ADSNX-6025E</th>
<th>ADSNX-4020E</th>
<th>ADSNX3-2020E</th>
</tr>
</thead>
<tbody>
<tr>
<td>Mitigation Capacity</td>
<td>240Gbps, 145,942,000pps</td>
<td>40Gbps, 29,760,000pps</td>
<td>20Gbps, 14,880,000pps</td>
<td>120Gbps, 8,938,000pps</td>
<td>4Gbps, 2,976,000pps</td>
</tr>
<tr>
<td>Interfaces</td>
<td>1<em>10GPM, 1</em>RJ45 Serial, 1*USB</td>
<td>1<em>10GPM, 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>Operating System</td>
<td>CentOS</td>
<td>Linux</td>
<td>QEMU KVM 1.5.3</td>
<td>QEMU KVM 1.5.3</td>
<td>QEMU KVM 1.5.3</td>
</tr>
<tr>
<td>Hard disk</td>
<td>1TB (at least 10GB free space)</td>
<td>128G at least 32GB free space</td>
<td>120G at least 32GB free space</td>
<td>120G at least 32GB free space</td>
<td>120G at least 32GB free space</td>
</tr>
<tr>
<td>Memory</td>
<td>128G at least 32GB free space</td>
<td>32GB at least</td>
<td>32GB at least</td>
<td>32GB at least</td>
<td>32GB at least</td>
</tr>
<tr>
<td>CPU</td>
<td>Intel(R) Xeon(R) CPU E5-2687vW @ 3.00GHz</td>
<td>Intel(R) Xeon(R) Processor E5-2620 v4 @ 2.10GHz</td>
<td>Intel(R) Xeon(R) Processor E5-2687vW @ 3.00GHz</td>
<td>Intel(R) Xeon(R) Processor E5-2687vW @ 3.00GHz</td>
<td>Intel(R) Xeon(R) Processor E5-2687vW @ 3.00GHz</td>
</tr>
<tr>
<td>MTBF</td>
<td>60,000 hours</td>
<td>60,000 hours</td>
<td>60,000 hours</td>
<td>60,000 hours</td>
<td>60,000 hours</td>
</tr>
</tbody>
</table>

## NTA

<table>
<thead>
<tr>
<th>Hardware</th>
<th>NTA 2000E</th>
</tr>
</thead>
<tbody>
<tr>
<td>Interfaces</td>
<td>2<em>GE Copper, 1</em>RJ45 Serial, 2*USB</td>
</tr>
<tr>
<td>Operating System</td>
<td>CentOS</td>
</tr>
<tr>
<td>Hard disk</td>
<td>1TB (at least 10GB free space)</td>
</tr>
<tr>
<td>Memory</td>
<td>128G at least 32GB free space</td>
</tr>
<tr>
<td>CPU</td>
<td>Intel(R) Xeon(R) Processor E5-2620 v4 @ 2.10GHz</td>
</tr>
<tr>
<td>MTBF</td>
<td>60,000 hours</td>
</tr>
</tbody>
</table>

## VIRTUAL ADS

<table>
<thead>
<tr>
<th>Host</th>
<th>Item</th>
<th>Recommended Configuration</th>
</tr>
</thead>
<tbody>
<tr>
<td>CPU</td>
<td>Intel(R) Xeon(R) CPU E5-2687vW @ 3.00GHz</td>
<td>vCPU (processor cores)</td>
</tr>
<tr>
<td>Memory</td>
<td>128G at least 32GB free space</td>
<td>Memory</td>
</tr>
<tr>
<td>Hard disk</td>
<td>1TB (at least 10GB free space)</td>
<td>Storage</td>
</tr>
<tr>
<td>Operation system</td>
<td>CentOS</td>
<td>Hypervisor support</td>
</tr>
<tr>
<td>1000M NIC support</td>
<td>1210, 1350, 82571, 82576, 82580 (up to 8)</td>
<td>Mitigation capacity</td>
</tr>
<tr>
<td>10Gb NIC support</td>
<td>82599, X710/XL710 (up to 4)</td>
<td>license options</td>
</tr>
<tr>
<td>Virtual NIC support</td>
<td>NIC other than those above (cannot guarantee the capacity)</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Virtual ADS</th>
<th>Item</th>
<th>Recommended Configuration</th>
</tr>
</thead>
<tbody>
<tr>
<td>CPU</td>
<td>Intel(R) Core(TM) i7-2600 CPU @ 3.40GHz 4 cores and 8 threads</td>
<td>1*2CPU</td>
</tr>
<tr>
<td>Memory</td>
<td>16GB</td>
<td>1*4CPU</td>
</tr>
<tr>
<td>Flows/sec</td>
<td>30,000</td>
<td>120,000</td>
</tr>
</tbody>
</table>

## VIRTUAL NTA

<table>
<thead>
<tr>
<th>Item</th>
<th>Recommended Configuration</th>
</tr>
</thead>
<tbody>
<tr>
<td>CPU</td>
<td>Intel(R) Core(TM) i7-2600 CPU @ 3.40GHz 4 cores and 8 threads</td>
</tr>
<tr>
<td>Memory</td>
<td>16GB</td>
</tr>
<tr>
<td>Flows/sec</td>
<td>30,000</td>
</tr>
<tr>
<td>Item</td>
<td>Recommended Configuration</td>
</tr>
<tr>
<td>--------------</td>
<td>------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Hard disk</td>
<td>1TB + 2GB</td>
</tr>
<tr>
<td>NIC</td>
<td>2</td>
</tr>
<tr>
<td>CPU</td>
<td>Intel® Xeon® CPU E5-2650 v3 @ 2.30GHz 10 cores and 20 threads. Assign 2 cores to virtual machine.</td>
</tr>
<tr>
<td>Memory</td>
<td>32GB Assign 8G to virtual machine.</td>
</tr>
<tr>
<td>Hard disk</td>
<td>1TB + 2GB</td>
</tr>
<tr>
<td>NIC</td>
<td>6</td>
</tr>
</tbody>
</table>