MANAGED DDoS SERVICES

REVENUE MODEL FOR INTERNET SERVICE PROVIDERS

NEED

There is a tremendous need to help solve the risk and threat of outages caused by DDoS attacks, and this is precisely where providers can step in with new Managed DDoS Service offerings that can generate new revenue. Internet Service Providers (providers) understand that a significant percentage of DDoS attacks targeting their commercial customers can be defeated by anti-DDoS technology deployed within the provider's network itself. When deployed, residential networks can be protected as well.

TARGET

Providers must fully understand they are not normally the target of DDoS attacks. In most cases their customers are the target. If providers can defeat all DDoS attacks targeting their customers, they should be able to recognize a return on their investment for doing so. Not only can providers recognize new revenue streams by defeating DDoS attacks, they can also ensure attacks do not impact their own infrastructures and their services as a side benefit.

IMPACT

Nearly every provider has been impacted by DDoS attacks in recent months. Some attacks have targeted the provider's commercial customers, while other attacks have targeted the provider's infrastructure itself. Those who offer residential services have openly shared the fact that they have experienced DDoS attacks against their own residential infrastructures; impacting large numbers of customers in turn. In some cases, using black holes (null routes) was simply not an option; due to many residential customers being NAT'd behind a single IP address under attack.

DEMAND

Studies indicate that significant number of organizations would like to see their provider offer Managed DDoS Services. In addition, those same studies indicate customers would be willing to pay a modest up-charge for Managed DDoS Services delivered by their provider. Not only can providers protect their commercial and residential customers from DDoS attacks, there is also a need to protect the provider's infrastructure as well.

APPROACH

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 defeated by On-Premises DDoS Defenses. In addition to mitigating a large majority of the DDoS attacks experienced by using the on-premises defenses deployed, those same defenses can defend residential networks and the other services currently being delivered by the provider.

GETTING STARTED

Often, providers of all sizes do not know where to begin when attempting to build a revenue model for Managed DDoS Services. The next sections are intended to help a provider build a case for Managed DDoS Service offerings.

NSFOCUS

BENEFITS

Generate new revenue with Managed DDoS Services

Create differentiation from your competitors

Retain current customers and attract new customers

Defeats all DDoS attacks against your customers

Lowest Total Cost of Ownership (TCO)

Complete Service Provider-ready solution

Quick and easy install into your network

Deploy as much mitigation capacity as needed

Automatic hand-off with NSFOCUS Cloud Centers

Shortens time to redirection and cloud mitigation

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

PROJECTIONS REQUIRE ASSUMPTIONS

When building financial projections for Managed DDoS Services, several assumptions must be made based upon data points collected from different research, for example: surveys, questionnaires, analyst reports, industry trade publications, and researchers.

For this example, there are two data points that are *unknown in most cases:*

- **Managed DDoS Service Penetration Rate** - How many subscribers will buy the new service?
- **Average Up-Charge Percentage for Managed DDoS Services** - What will subscribers be willing to pay for the new service?

OBSERVATIONS ON PENETRATION RATES AND UP-CHARGE PERCENTAGES

- Based upon previous research and real-world usage cases, NSFOCUS has observed that a **Managed DDoS Service Penetration Rate** of between 25% and 50% percent is a reality for their commercial customers.

- In addition, NSFOCUS has observed that an **Average Up-Charge Percentage for a Managed DDoS Services** of between 1% and 10% percent is a reality for all customers.

Based upon these two data points, projections can be made and a new revenue model can be calculated.

MANAGED DDoS SERVICES - DATA POINT COLLECTION

When building projections to support the case for Managed DDoS Services , there are several other data points that must be collected and added to the projections as follows:

- **Types of Current Service Packages** - These are the different service packages already being purchased by the various customers
- **Number of Current Subscribers** - These are the number of subscribers that purchase the different service packages
- **Current Monthly Charges** - These are the current charges ($) for the different service packages being purchased by the customers
- **Current Monthly Revenue** - These are the gross revenue figures obtained from the customers purchasing the existing service packages
- **Managed DDoS Service Penetration Rate** - These are the rates of existing customers that would purchase the new Managed DDoS Services
- **Number of Managed DDoS Service Subscribers** - These are the numbers of new subscribers who purchase Managed DDoS Services, based upon the estimated penetration rate
- **Average Up-Charge Percentage for Managed DDoS Services** - These are the average up-charges that customers would be willing to pay for the new Managed DDoS Service offering
- **Additional Monthly Charges** - These are the additional charges customers would pay for Managed DDoS Services
- **New Monthly Price** - These are the new monthly prices that includes the costs for Managed DDoS Services
- **New Monthly/Yearly Revenue** - These are the new revenue figures that would be recognized for Managed DDoS Services

PROJECTIONS FOR MANAGED DDoS SERVICES - CALCULATIONS

The table below show the projections for an example service provider. Since every provider has different values that would be entered into the table, the projections would likely differ from one provider to another.

Managed DDoS Services - ISP Example: New Revenue Projections	1	2	3	4	5	6	7	8	9
Type of Current Service Packages	Number of Current Subscribers	Current Monthly Charges	Current Monthly Revenue	Managed DDoS Service Penetration Rate	Number of New Managed DDoS Service Subscribers	Average Upcharge Percentage for Managed DDoS Services	Additional Monthly Charges for Managed DDoS Services	New Monthly Price	New Monthly Revenue
150 Mbps Commercial Subscribers	2000	$250	$500,000	25%	500	5%	$13	$263	$6,250
1 Gbps Commercial Subscribers	500	$1,000	$500,000	40%	200	5%	$50	$1,050	$10,000
10 Gbps Commercial Subscribers	20	$5,000	$100,000	50%	10	5%	$250	$5,250	$2,500
Residential Subscribers	15000	$50	$750,000	100%	15000	3%	$2	$52	$22,500
New Revenue									
New Monthly Revenue from Managed DDoS Service									**$41,250**
New Annual Revenue from Managed DDoS Service									**$495,000**

DISCUSSION ON CALCULATIONS AND RESULTS

In the projections shown above, we can see that the example provider offers four different service packages, and we can see the number of subscribers they currently have for each service package. These figures would likely be different in almost every case. However, providers could easily enter their own service packages and number of subscribers into a similar table/calculator. Below are the example values.

- 150 Mbps Commercial Subscribers = 2000 subscribers
- 1 Gbps Commercial Subscribers = 500 subscribers
- 10 Gbps Commercial Subscribers = 20 subscribers
- Residential Subscribers = 15000 subscribers

In the above table, notice the text in red under the column named "Managed DDoS Service Penetration Rate". In this case, the penetration rate for **commercial subscribers** is a modest 25%-50%. This rate is based upon the research that nearly 50% of commercial subscribers would purchase Managed DDoS Services. A range between 25% to 50% is a reality.

Also in the above example, notice the text in red under the column named "Average Up-Charge Percentage for Managed DDoS Services". In this case, the average up-charge for commercial subscribers is a modest 5%. This percentage is also based upon the research that buyers would likely purchase Managed DDoS Services for a small up-charge percentage. A range between 1% and 10% is a reality.

The final figures that need to be addressed is the case of "Residential Customers". Since residential customers are unlikely to pay for Managed DDoS Services (even if it was offered), there must be a way of recovering the costs associated with protecting residential networks from the impact of DDoS attacks. In this case it is highly recommended that an increase of 1%-3% be added to *all residential customers,* which would only add $2 to their regular monthly charges in the case above.

NEW REVENUE FROM MANAGED DDoS SERVICES

As we can see in the example above, and based upon assumptions, research, and current data points, a service provider offering Managed DDoS Services using the figures shown in the table, would generate **$495,000/year in new gross revenue** from delivering Managed DDoS Services.

BEST PRACTICES AND RECOMMENDATIONS

Once a Managed DDoS Service has been implemented, the next challenge that providers face is how to market, sell, and deliver the new service. Below is a list of best practices and recommendations that have proven to work in nearly all cases.

SELECT A SERVICE PROVIDER-READY SOLUTION

- Select, purchase, and deploy On-Premises DDoS Defenses that support multi-tenant policy management out-of-the-box. In addition, ensure the solution supports a white-label, web-based customer portal that allows customers to view their own traffic, alerts, attacks, and resolutions with dashboards, reports, and traffic analytics.

MARKET THE MANAGED DDoS SERVICE TO ALL COMMERCIAL CUSTOMERS

- What has been observed as the best marketing model, is to make a blanket offering to all commercial customers to adopt Managed DDoS Service from the provider. Make the offering to all clients (via email or other means of communication) that they can now opt-in and pay an up-charge for Managed DDoS Services. Providers could even reduce their up-charge percentage for those that opt-in early; hoping to gain more penetration of the available customer base.

MAKE IT CLEAR WHAT HAPPENS IF THEY DON'T

- If they opt-out, make it very clear that if the commercial customer comes under attack and they are not signed up, they will be null-routed, and all traffic to their network will be blocked. This will cause an outage on the customer's network. Highlight the fact that DDoS attacks against commercial customers can also impact others in the network. Since this is the case, all DDoS attacks must be blocked either by null-routing, or by DDoS mitigation. The Managed DDoS Service blocks all bad (DDoS) traffic and allows all good traffic. When used, customers under DDoS attack will still be able to operate and will not incur an outage.

HAVE A CUT-OFF POINT IN THE SLA

- When commercial customers sign up for the service, ensure there is a maximum DDoS attack-size that will be mitigated as part of the Managed DDoS Service, defined in the SLA.
- For example, if a commercial customer experiences a DDoS attack under 5 Gbps, the attack will be mitigated as part of the service.
    - If a commercial customers comes under a 6 Gbps attack or greater, they will have the option to pay an additional up-charge, or be null-routed.
    - Consider the number of times the Managed DDoS Service can be utilized for any given period of time, by any single commercial customer. Some providers offer unlimited DDoS mitigation while other have a limit to the number of times the service can be used
    - Do not offer unlimited Managed DDoS Services with unlimited SLAs.

HAVE A BACK-UP PLAN

- Ensure you have an agreement in place with a Cloud DDoS Defense Provider in the case of a massive DDoS attack against a single customer, group of customers, or the provider's infrastructure itself. If the network is impacted by an attack that exceeds the capacity of the On-Premises DDoS Defenses, or the capacity of the provider's Internet Bandwidth, then it will be impossible to meet the Managed DDoS Service SLAs.

ADDRESS ATTACKS AGAINST RESIDENTIAL CUSTOMERS

- The recommendation concerning residential customers is to have a customer-wide price increase for all residential customers that is very small (1% -3%) for a "new service" they will benefit from. Since DDoS attacks can impact anyone connected to the Internet, market the increase by highlighting that the increase will benefit all customers with more reliable services and uptime.