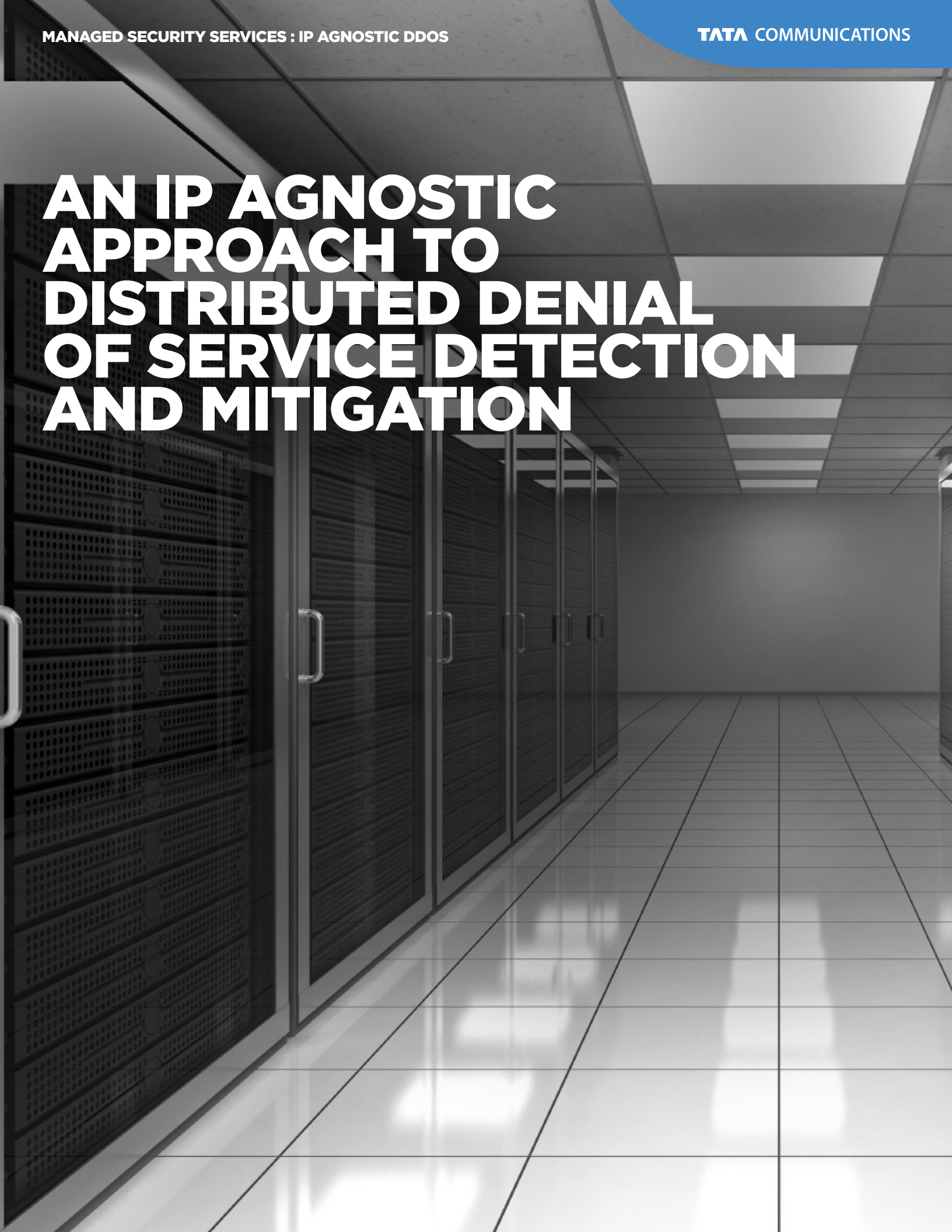


AN IP AGNOSTIC APPROACH TO DISTRIBUTED DENIAL OF SERVICE DETECTION AND MITIGATION

Overview

Distributed Denial of Service (DDoS) attacks saturate target networks with service requests that consume the capacity of the devices fronting the networks. Easily launched by semiskilled hackers, these attacks can be highly targeted at a very specific application or resource, or more broad-based when launched at network routers. But regardless of the specific target, the result of the attack is a denial of access to customers, partners or employees and disruption of normal business processes. In many cases, Internet Control Message Protocol (ICMP) floods last as long as 10 hours, repeated over 10 days. By targeting web sites, hosted applications, and network infrastructures, DDoS attacks bring mission-critical systems and business operations to a halt, losing revenue opportunities, decreasing productivity and damaging business reputations.

Over the past few years, DDoS attacks have evolved from random exploits carried out by rogue hackers to targeted, criminal acts conducted for a specific purpose such as extortion and market manipulation. Attackers wait until an important event (e.g., a major sports event or politically motivated conflict) and threaten a targeted organization with attack if payment is not made. While e-retail businesses were among the earliest DDoS victims, any business that relies on the web to reach customers, partners and employees poses a potential target.

Perpetrators of these attacks are sophisticated criminal organizations and/or political operatives whose intent is to consume the finite availability of an organization's computing and network resources. This is accomplished by exploiting weaknesses in software design, implementation or lack of network infrastructure capacity. In this way, attackers attempt to absorb their target's available bandwidth and server capacity to disrupt legitimate use of web sites, applications, systems and networks. Launching a crippling DDoS attack requires little expertise, and traditional network security mechanisms are not designed to handle DDoS mitigation.

The effectiveness and ease of launching a DDoS attack is in direct contradiction to the high cost and trouble it causes victims. The annual CSI/FBI Computer Crime and Security Survey consistently identifies DDoS as the leading computer-related security threat relative to total financial losses.

Practical Considerations in Mitigating Attacks

Time-consuming, Tedious Work

Traditional information security products are not designed to handle DDoS mitigation. Without the appropriate tools and root-cause analysis, determining whether an attack is actually occurring is complex, time-consuming and tedious work. In a traditional environment, all IP traffic destined for a Dedicated Internet Access (DIA)/Internet Leased Line (ILL) customer flows natively toward that customer. In this scenario, the customer receives both "good" and "bad" traffic and the determination as to whether a customer is under attack is largely a manual process. In this scenario, initial detection of an attack most frequently occurs when users find critical services unavailable.

For the IT team, this kicks off a tedious process of elimination to ascertain the root cause. In terms of remediation, it is common for the collateral damage of an attack to be as bad, if not worse, than the attack itself. Diagnosis involves troubleshooting (what are essentially numerous moving parts) at the customer premise, the service provider to customer edge, and one or more service provider networks.

Multiple Providers, Greater Complexity

Most of Tata Communications' enterprise customers practice a multihomed approach in securing bandwidth. Rather than purchasing bandwidth from a sole provider, which could leave an organization vulnerable in case of an outage or other incident, most organizations rely on multiple carriers to supply capacity for a specific site. In the case of a data center, for example, a company might buy service from two or three different service providers to provide system redundancy. Contracting with multiple carriers reduces the risk of a single point of failure, by leveraging multiple power grids and network paths. In this way, mitigating and detecting a DDoS attack would involve three different providers, adding complexity to an already difficult task. DDoS detection and mitigation, therefore, requires a planned approach to address multiple carriers, ensuring that public routing changes are implemented for the duration of the attack.

Tata Communications' Detection and Mitigation Solution

Business Benefits Summary

- Reduces tedious fault resolution to identify DDoS attacks
- Maintains usability of critical services that would otherwise be lost due to malicious traffic floods
- Improves security visibility with 24x7x365 traffic monitoring and analysis so customers are notified when an actionable event occurs
- Optimizes IT spend by eliminating the need for additional server capacity
- Advanced filtering of malicious and abusive traffic means only legitimate traffic is forwarded
- Leverages Tata Communications' security expertise to customize an effective mitigation response
- Utilizes bandwidth more effectively by filtering malicious traffic in Tata Communications' network before customer's resources can be impacted

In-the-cloud Protection

Enabling an effective DDoS detection and mitigation service within the ISP network, or "in the cloud," enables timely analysis, identification and reporting before attack traffic reaches its destination. Tata Communications' DDoS Detection and Mitigation Service provides cloud-based, anomaly identification, notification and mitigation. The detection service analyzes backbone traffic patterns and continually "baselines" expected traffic patterns and values. The detection service also effectively differentiates anomalous traffic and alerts accordingly, based on customer-defined alerting thresholds. This range of alerting and mitigation options ensures quick notification and provides critical information to IT to choose the most appropriate remediation methods. Cloud-based DDoS Detection and Mitigation spares businesses from extended and costly outages while also alleviating the stress and tedium created by DDoS root-cause analysis and remediation.

DDoS security features were designed and built into Tata Communications' IP backbone, therefore offering a mature solution. By managing DDoS threats on the backbone, instead of at the customer's premise, threats are detected early on, far away from the customer's network.

IP Agnostic Approach

To accommodate enterprise customers' requirement for redundancy, Tata Communications has designed a DDoS Detection and Mitigation solution that accommodates many customers' practice of using multiple bandwidth providers. Through this solution, traffic flow data is monitored remotely by Tata Communications. When a DDoS attack is detected, traffic is rerouted from all carriers to traverse Tata Communications' lines. Affected traffic is then scrubbed and routed back to the customer.

Unique baseline profiles of normalized traffic patterns make it possible to detect attack anomalies when customer traffic falls "out-of-profile." The DDoS detection analysis tools feature built-in profiles of common attacks that are independent of a customer's "normal" traffic patterns.

When an attack is detected, the analysis tools generate corresponding alerts via email and on an included security portal. Anomalies are rated as high, medium or low, depending on customer link speed and configured thresholds. Tata Communications quickly notifies customers of all high-severity alerts by phone. Traffic is then rerouted to Tata Communications' scrubbing centers until the malicious activity has ceased and is then transferred back to its normal state, restoring the original multiprovider infrastructure.

Service Options

Tata Communications offers several service options for DDoS Detection and Mitigation, including both on-net and off-net.

On-net

On-net occurs when the customer has contracted for either of Tata Communications' enterprise Direct Internet Access (DIA) or wholesale IP Transit (IPT) services. Proactive detection and mitigation over these networks prevents malicious traffic from ever reaching the customer's network.

Network detection examines traffic flow data across Tata Communications' network for each customer address to determine anomalous activity. If a DDoS attack is detected and the customer chooses to mitigate the attack, malicious traffic is then rerouted through Tata Communications' regionally distributed mitigation centers. These facilities "scrub" and drop attack packets while forwarding "clean" traffic toward the appropriate destination.

For on-net options, Tata Communications also provides detection and mitigation within a customer's multihomed, multi-SP environment. In order for Tata Communications to provide mitigation for traffic on a third-party SP, the attack traffic needs to be rerouted onto Tata Communications' network.

For example, Tata Communications detects attacks even if traffic is being load-balanced across all providers. When an attack has been detected—either through Tata Communications' cloud detection, or an on-site detection solution (managed IDS-IPS)—the customer turns down the /24 (or identified summarization address block) of the attack address to the other providers. This causes traffic from all providers destined for that IP address (including all traffic within that address range) to only have a path via Tata Communications' network. The appropriate attack traffic is then rerouted to the regional Tata Communications' scrubbing facility and all clean traffic is forwarded to the customer via Tata Communications' DIA port.

Tata Communications' DIA port must be sized to support additional traffic during the attack. In addition, the mitigation protection level is appropriately sized relative to the protection required by the application/system/network. Tata Communications is the only provider advertising the super block but cannot guarantee that all providers accept a /24 advertised across peering points.

Because Tata Communications cannot guarantee the performance of third-party networks, on-net options are strongly recommended.

Off-net

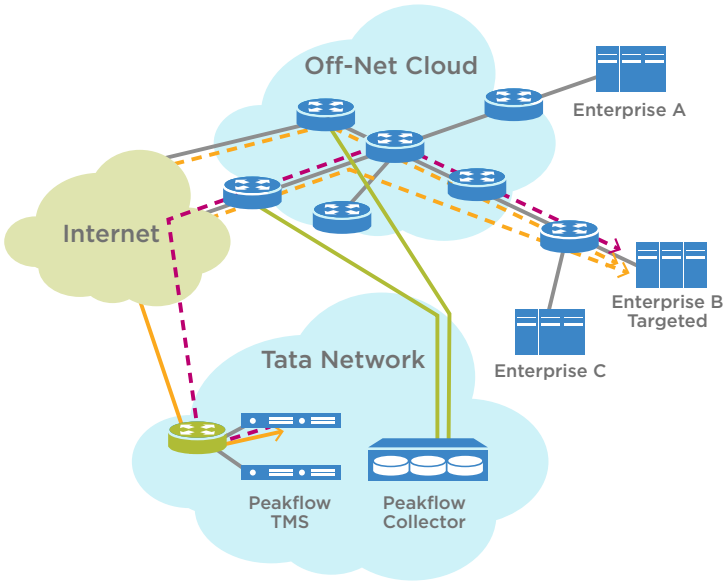
The off-net setup is for customers that currently do not have direct DIA or IPT connection to Tata Communications' backbone. With the off-net option, Tata Communications helps overcome three technical challenges, including attack detection, rerouting attack traffic for mitigation, and returning cleansed traffic to the customer.

To detect traffic, Tata Communications must receive off-net flow data. This is accomplished by "pointing flow" from the customer's upstream routers to Tata Communications' routers. If the routers do not support flow, dedicated flow sensors can be placed inline on each of the customers' transit connections. This CPE provides flow data back to Tata Communications and is used to mitigate attacks.

Off-net mitigation establishes a BGP "multihop" session across the customer's current provider networks to route traffic across Tata Communications' network. The BGP session must allow all routes that could require mitigation. The customer must only announce these routes in times of a DDoS event as the GRE return path is necessary for returning the cleaned traffic.

Ensuring that traffic is routed to Tata Communications requires either that customer netblocks be more specific than those announced to all other providers or that routes be announced without BGP. Cleansed traffic is returned via the public Internet through encrypted GRE tunneling. Tata Communications strongly recommends that all the customer's current providers support larger frames (larger then 1524) to ensure cleansed traffic reaches the desired destination.

The following graphic represents a high-level architectural view of off-net service options. The solid blue lines represent the flow data being sent from network routers to Tata Communications' collection devices. The dotted red lines represent attract traffic (pre-mitigation) crossing the customer's network and third-party transit providers. The solid red lines represent the mitigation function and reflect the new traffic pattern into Tata Communications' mitigation centers once the routing change has been made. The green line shows cleansed traffic leaving the Tata Communications' mitigation centers via GRE tunnel crossing the Internet and reaching the desired customer destination.



Dedicated or Shared Service

Tata Communications also offers the choice of either dedicated or shared service. Dedicated service offers a guaranteed amount of capacity on the backbone to be used for DDoS detection and mitigation. This option is appropriate for applications such as military or air traffic control. In the dedicated mitigation option, traffic is rerouted through customer-dedicated mitigation capacity. The dedicated mitigation option offers customers guaranteed availability.

The shared option offers customers a lower cost alternative and is delivered on a best effort basis. In the shared option the traffic is rerouted to shared mitigation "farms". Tata Communications carefully monitors shared mitigation capacity so that subscribing customers may be confident of mitigation availability in the event of a DDoS attack. Both mitigation options are contracted in Gb increments. Tata Communications currently boasts the world's largest Arbor deployment.

Service Components

All hardware and software elements of the On-net network-based DDoS Detection and Mitigation service are managed and maintained within Tata Communications' network infrastructure. Service requirements are for a Tata Communications' DIA or IPT port (DDoS Detection and Mitigation can also be provided for managed hosting applications, located in Tata Communications' IDC) at specific locations where detection coverage exists.

Internet Circuit

DDoS Detection and Mitigation requires a DIA or IPT port from Tata Communications for on-net options 1 through 3. Internet access speeds ranging from 1G to 10G are supported. Access speed support includes tiered and burstable circuits, in addition to redundant circuits, such as double, diverse, and shadow ports. (Detection for burstable ports are sized to the full port size.) Tata Communications works with customers ahead of time to ensure circuits fall within the service coverage area and that flow sampling is possible on network traffic.

As mentioned previously, Tata Communications' DDoS Detection and Mitigation can also scrub malicious traffic originating from third-party providers and then reroutes the traffic back to the desired destination via preassigned, encrypted GRE tunnel. Due to the fact that the DDoS Detection service is directly linked to the IP access speed on a DIA port, upgrades or downgrades to the port's access speed trigger an equivalent upgrade or downgrade to the detection service.

IP Address Block

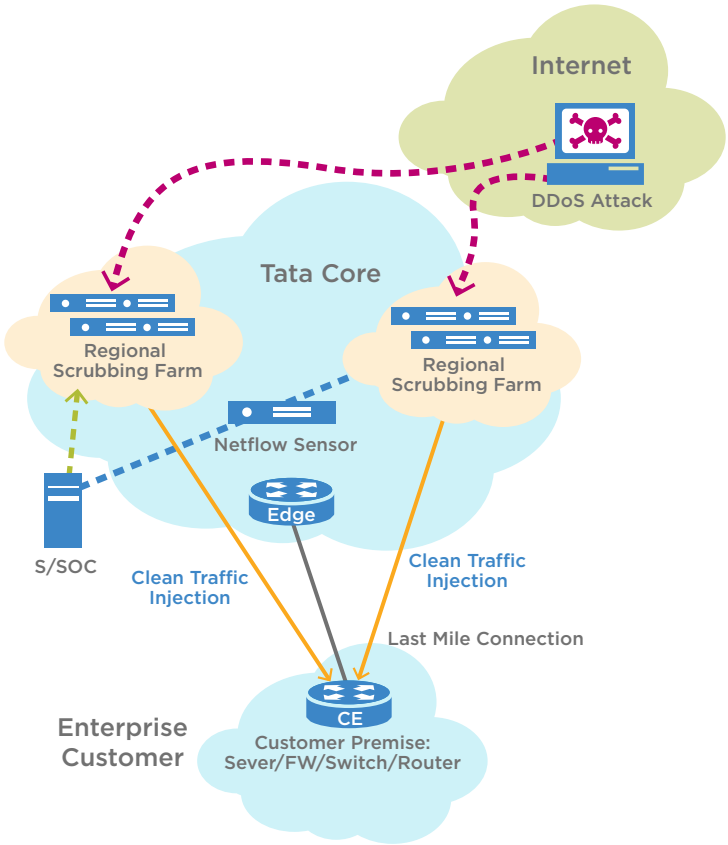
DDoS Detection and Mitigation samples all traffic within the public IP address block that has been defined for a subscribed customer. During implementation, Tata Communications collects all IP address information for the customer's relevant sites that the DDoS Detection and Mitigation service samples. Subsequent changes and updates to a customer's IP address block can be made either electronically through the Security Service Customer portal or by contacting the Security Services Operations Center (SSOC) via email.

Security Service Portal

DDoS Detection and Mitigation customers are provided with secure, web-based access to the Security Service portal, which enables a variety of management and monitoring functions. The portal is designed to provide customers with visibility into network traffic, including high, medium and low severity alerts identified through ongoing sampling of IP traffic for DDoS anomalies.

How It Works

Standards-based traffic analysis occurs at the edge of the network. Flow information is reported and further processed within Tata Communications' SSOC for detailed behavioral analysis. The solution's multi-tiered architecture is shown below:



Tata Communications' DDoS Detection service uses both statistical and behavioral analysis methods, as opposed to most intrusion detection systems that provide signature-only analysis. The service also offers the benefit of detecting attacks for which signatures have not been written (e.g., "zero-day" threats).

Real-time Sampling and Anomaly Detection Function

Various sampling mechanisms at the network edge (aggregation layer) are utilized to build a flow record and are then analyzed for behavioral trending and anomaly detection.

Mitigation

Tata Communications has built a globally distributed network of regional mitigation centers to filter malicious traffic that would otherwise saturate a customer's broadband Internet connectivity. A predefined BGP speaker advertises the specific (e.g., /32, /23 or /24) address that is being attacked to trigger the network to reroute malicious traffic to the scrubbing facility(ies). (This process only reroutes traffic destined for the specific IP address(es).) Post-mitigation, traffic is returned to the customer through an encapsulated GRE tunnel to a predefined access router within the customer's network.

Mitigation Sizing

Mitigation delivers a type of "application availability insurance." As with any insurance policy, mitigation should be sized according to enterprise risk plus the probability of attack size and frequency. A lower mitigation subscription level confronted with a large-scale attack will be easily overwhelmed. Using a traditional risk management framework, Tata Communications' team helps customers weigh the cost of service disruption with the cost of availability insurance. A non-mission- critical application plus a low probability of a high volume attack can subsist at a lower mitigation level. Conversely, a mission-critical application plus a high probability of a high-frequency, high-volume attack requires a mitigation level that is several multiples greater than the port speed.

Trigger Methods

Tata Communications activates mitigation via BGP speaker within the network in several ways, including the following:

1. Via cloud-based detection, Tata Communications' Security Operation Center identifies an attack, consults with the customer for mitigation authorization, and then proceeds with mitigation.
2. Customer identifies the attack and notifies Tata Communications to activate mitigation efforts.
3. Via cloud-based detection, Tata Communications' Security Operation Center identifies an attack, which then triggers preapproved automatic mitigation directives.

Flow Collection

The basic premise behind flow collection and sampling is to ensure a router records certain information about IP packets that traverse through an interface. For purposes of the DDoS Detection and Mitigation service, Tata Communications uses these capabilities to gather information regarding flows toward a subscribed customer. Note that strict confidentiality and privacy policies are actively enforced regarding customer flow data.

Packets with similar characteristics can be grouped together in a flow. A flow is defined as a set of packets with the following in common:

- Source IP address
- Destination IP address
- Source port number
- Destination port number
- Layer protocol type
- ToS byte
- Input logical interface

All packets with these characteristics are combined into one flow record, along with additional information regarding these flows such as the source and destination AS (Autonomous System), etc. Once collected, flow records are kept locally on the router and periodically exported via UDP to network-based collection devices.