ALCATEL-LUCENT INTEGRATED DDOS PROTECTION SOLUTION

STRATEGIC WHITE PAPER

TABLE OF CONTENTS

1. DDOS ATTACKS INCREASING IN SOPHISTICATION AND SCALE

Distributed Denial of Service (DDoS) attacks on enterprise and service provider networks are increasing in both scale and sophistication. In 2011, the largest attacks topped 60Gbps, with increased prominence of attacks over 10Gbps. As a matter of interest 2010 experienced a largest sustained attack of 100Gbps. An increased trends towards applications level attacks and attacks directed towards mobile networks is another highlighted trend today.

The sheer volume of a DDoS attack can quickly overwhelm enterprise defenses. As a result, enterprise Chief Information Officers (CIOs), already reeling from information technology (IT) budget constraints imposed by economic conditions, are increasingly looking to outsource DDoS protection to their service providers. By outsourcing DDOS protection, enterprises expect to mitigate attacks in the carrier cloud before they reach the enterprise network.

But because DDoS attacks travel over a service provider network they also impact a service provider's business. Therefore, to deliver a secure carrier cloud, service providers must protect their own networks and their customers' Internet Data Centers (IDCs). The imminent threat of attack, combined with the business opportunity to offer cloud-based DDoS protection to enterprises, is the reason why service providers implement network-based DDoS protection solutions.

The Alcatel-Lucent Integrated DDoS Protection Solution offers a ground-breaking approach to cloud-based detection and mitigation of DDoS attacks. It integrates the Arbor Networks Threat Management System (TMS) software with the Alcatel-Lucent 7750 Service Router (SR) and works in conjunction with Arbor Networks collector platform which performs DDOS detection and analysis. This integrated DDOS protection solution offers a number of unique benefits:

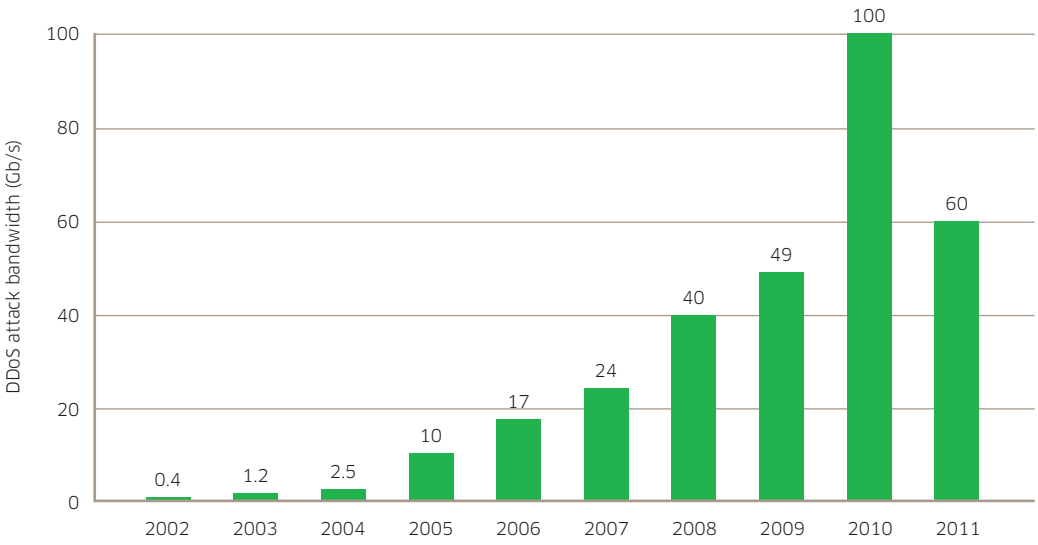
- Mitigates DDoS attacks before they enter the carrier network: The solution enables distributed detection and mitigation of attack traffic .This minimizes the need to backhaul traffic to a central TMS appliance and mitigates the DDoS attack closer to the location of attack.
- Simplifies DDoS network design: The integrated DDOS protection solution simplifies existing scrubbing center designs. The 7750 SR supports traffic grooming and threat mitigation functions, thus eliminating the need for separate grooming routers and TMS appliances.
- Enables new and differentiated DDoS services: Enterprises worldwide want secure, cloud solutions that are sufficiently robust to handle their most mission critical applications. Cloud-based protection enhances a service provider's portfolio of business services. It complements existing Business Internet virtual private network (VPN) services and can underpin an emerging portfolio of trusted, carrier cloud applications for a wider range of verticals, customers, and geographies.

2. DDOS THREAT LANDSCAPE & IMPACTS

A DDoS attack is a targeted attempt to make the network or application unavailable to its intended users. DDoS attacks have a damaging impact on enterprises, consumers and service providers. Attack traffic usually enters a service provider network where it consumes network bandwidth and resources. It then flows through to enterprise/IDC customers, where it saturates network resources and cripples applications and services. All indications are that DDoS attacks will continue to grow in sophistication, and scale (Figure 1):

- **Increasing sophistication:** There is an escalating arms race between attackers — who continuously raise the bar to outwit security vendors — and IT security teams — who implement defensive strategies to thwart them. Attacks have evolved from host-to-host attacks, which try to exhaust a central processing unit (CPU) on targeted services, to volumetric attacks, which leverage botnets to target and knock out network infrastructure, such as routers and firewalls, to highly complex application-level attacks, which exploit specific vulnerabilities in IDC services and enterprise applications.

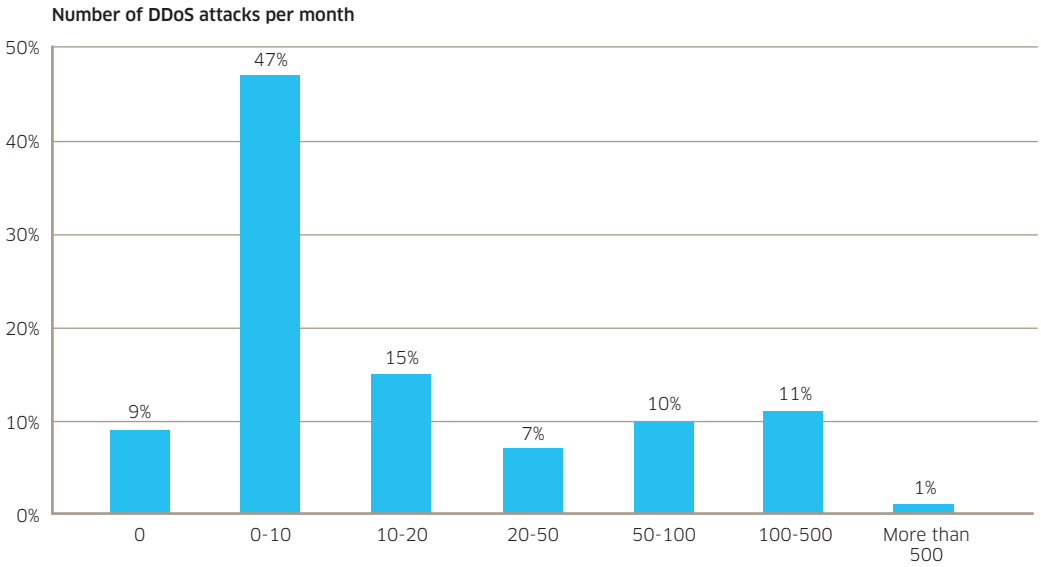
Figure 1. DDoS attacks increasing in sophistication and scale



Source: Arbor Networks-2011 Worldwide Infrastructure Security Report (WISR), January 2012

- **Increasing scale:** Attacks are also increasingly distributed in nature, making it almost impossible to identify and shut down perpetrators with traditional solutions. According to Arbor Networks 2011 Worldwide Infrastructure Security Report (WISR), bandwidth for sustained attack in 2011 reached 60Gbps with 2010 experiencing a sustained attack topping 100Gpbs. The increased prominence of 10G and higher attacks in 2011 continues to highlight the significance of DDoS attacks.
- **Increasing frequency:** DDoS attacks have become daily events. According to Arbor Networks most recent WISR(2011 WISR, January 2012) –, 91% of respondents see at least 1 DDoS attack per month up from 76% in 2010 and 44% of respondents see 10 or more attacks per month up from 35% in 2010 (Figure 2)

Figure 2. DDoS attacks increasing in frequency



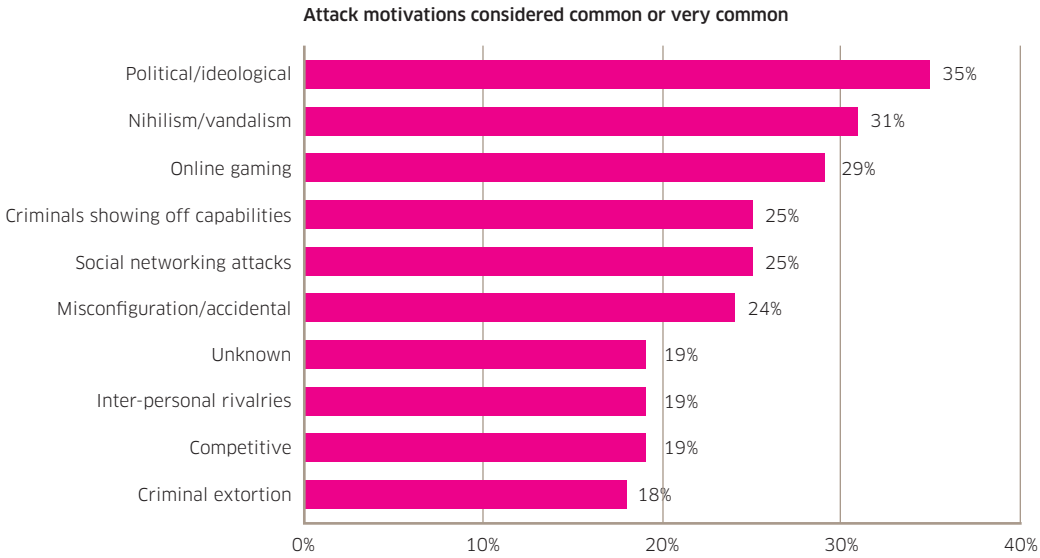
- 91% of respondents see at least 1 DDoS attack per month up from 76% in 2010
- 44% of respondents see 10 or more attacks per month up from 35% in 2010

Source: Arbor Networks 2011 Worldwide Infrastructure Security Report (WISR), January 2012

The Arbor 2011 WISR report indicates a increase in the prevalence of ideologically-motivated 'hacktivist' DDoS attacks (Figure 3). Top two attack motivation categories are fueled by personal beliefs and inclinations of attackers

This is a significant finding, with major implications in terms of threat assessment and continuity of operations for network operators, governmental bodies, law enforcement agencies and end customers alike.

Figure 3. DDoS attack motivations



- Top two attack motivation categories are fueled by personal beliefs and inclinations of attackers
- Exponential increase in risk of being attacked

Source: Arbor Networks 2011 Worldwide Infrastructure Security Report (WISR), January 2012

2.2 Impact on enterprises & small and medium businesses (SMBs)

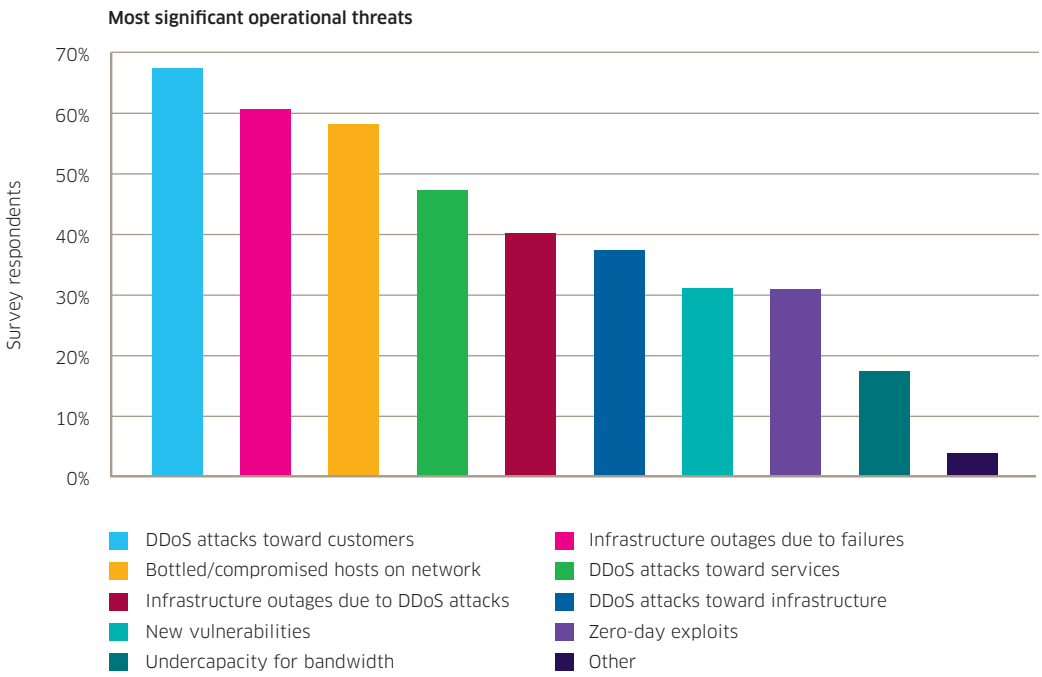
DDoS attacks and security breaches create serious problems for large enterprises & small and medium businesses (SMBs). The problems range from lost revenue and business process disruptions, to loss of market share and reputation if the attacks impact customers and receive media attention. Additionally, enterprise IT evolution is opening up new vulnerabilities for attackers to exploit. Cloud computing services and IPV6 migration are both major discontinuities that could bring as yet undiscovered threats. Enterprises are struggling to allocate increasing amounts of their IT budgets to maintain security awareness, hire and train security personnel, and perpetually upgrade their security systems. Meanwhile, SMBs are struggling with an even greater shortfall in security investments that has left most companies at risk.

Given these business conditions, enterprises and SMBs can no longer maintain the arms race against increasingly savvy DDoS attackers and large-scale attacks. Therefore, it is not surprising that DDoS protection is the number one security service that enterprises and SMBs say could be most effectively offered as a cloud service by service providers.

2.3 Impact on service providers

Service providers manage the carrier cloud network infrastructure and services over which DDoS attacks flow. The Arbor Networks 2010 WISR notes that 61 percent of service provider respondents believe that DDoS attacks towards end customers create a significant operational threat (Figure 4). Botnets and their unwanted effects (including DDoS attacks) are considered to be the biggest threats, as are DDoS attacks targeted at service provider ancillary services, such as Domain Name System (DNS), Web, and e-mail servers.

Figure 4. Most significant operational threat to service providers



Source: Arbor Networks, Inc.

In addition, service providers are forced to deal with the collateral damage from DDoS attacks. This includes reduced network and service availability, which create customer dissatisfaction, as well as potential customer churn. Unfortunately, a reactive approach to DDoS attack prevention results in higher operational costs for service providers and unpredictable timelines for fixing problems.

Fortunately, service providers can leverage the same infrastructure they use to protect themselves to launch highly profitable, cloud-based, DDoS attack mitigation services for enterprises. A managed DDoS attack mitigation service (Clean Pipes) for enterprise customers provides the ideal opportunity for revenue generation.

3. DDOS PROTECTION SOLUTIONS

3.1 Limitations of traditional DDoS mitigation approaches

Traditional approaches to DDoS protection employ stateful firewalls and Intrusion Protection Systems (IPS). These approaches impose several constraints on the detection and mitigation of DDoS attacks.

To identify and mitigate attacks, many SPs and enterprises deploy stateful firewalls and Intrusion Protection Systems (IPS). Tools like Access Control Lists (ACLs) and remotely triggered black holing (RTBH) are still widely used.

ACLs are a form of DDoS mitigation that can block valid attempts to access resources. In many cases, large volumes of ACLs are known to significantly reduce router and network performance.

Another approach referred to as source- or destination-based remotely triggered black holing (RTBH) is also common, despite the fact that RTBH blocks all traffic to the target (both the good and bad).

But these traditional devices and tools complete the DDoS attack by becoming choke points or by blocking access to the very servers or services they are trying to protect. Another drawback is their limited ability to detect distributed attacks. DDoS attack detection and prevention requires network-wide visibility and flow analysis that stand-alone devices are unable to provide.

In addition, bot infestations (a subset of which are used to launch DDoS attacks) can only be uncovered by careful analysis of all content entering a site, desktop or server. This is a CPU-intensive process that requires a constant stream of new filters to match malware executable files as they morph minute by minute.

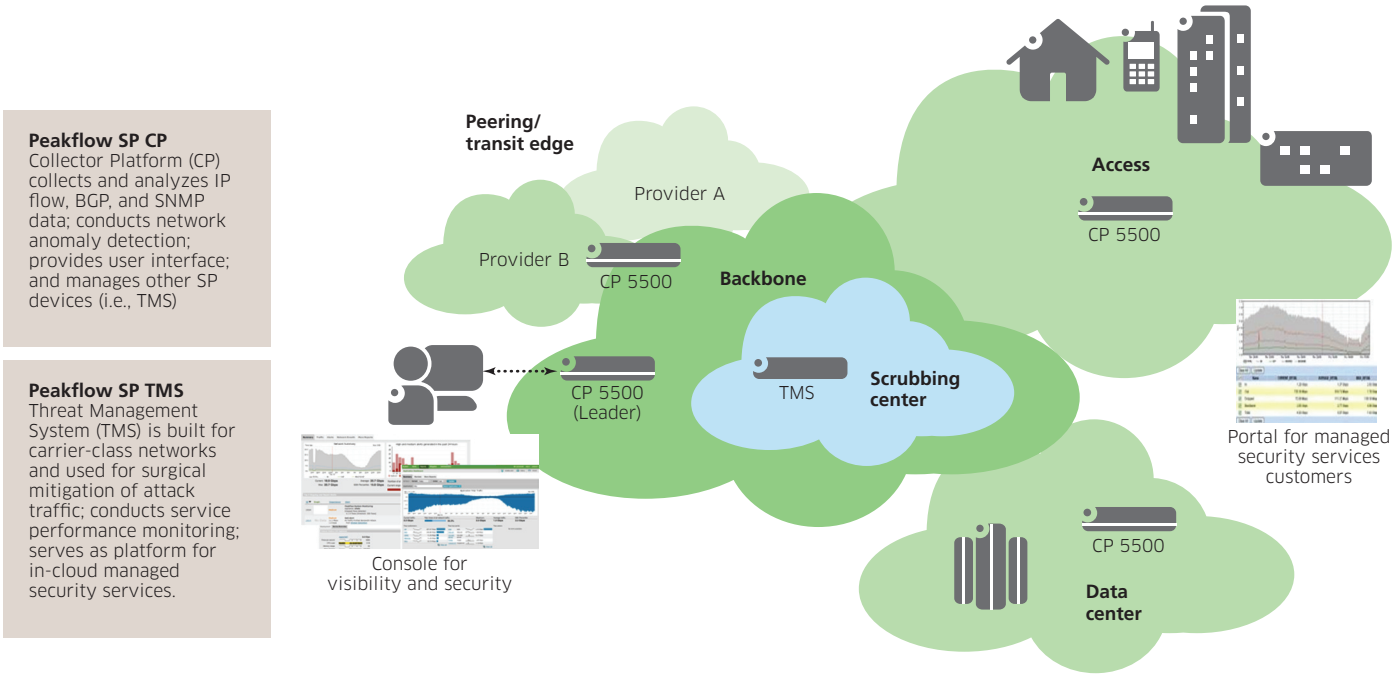
Given the limitations of traditional approaches, it is evident that a more scalable solution is required. The ideal solution must intercept DDoS-related botnet activity in the network and allow content security appliances/software at the branch and data center to optimize limited CPU resources at all times.

3.2 Arbor Networks Peakflow service provider DDoS prevention solution

Arbor Networks is a leading provider of network security solutions for service providers and enterprises. The Arbor Networks Peakflow service provider solution overcomes the limitations of traditional IPS- and firewall-based DDoS mitigation offerings by providing network-wide visibility using network behavior analysis (NBA) and anomaly detection capabilities out of band.

The components of the Arbor Networks Peakflow service provider solution are depicted in Figure 5.

Figure 5. Arbor Networks Peakflow service provider solution with centralized DDoS Scrubbing Center



The Arbor Peakflow service provider Collector Platform (CP) appliances collect and analyze flow information from existing network elements (routers) to provide cost-effective visibility and DDoS attack detection capability

The Arbor Peakflow service provider Threat Management System (TMS) appliance is specifically designed to mitigate a DDoS attack by surgically removing the attack traffic while keeping legitimate traffic. The CP appliance detects the suspicious traffic, which is redirected to the Peakflow service provider TMS appliance where attack mitigation (scrubbing) takes place.

The Arbor Peakflow service provider PI (Portal Interface) appliance serves as the user interface, which may also provide a means to offer a portal for managed security services.

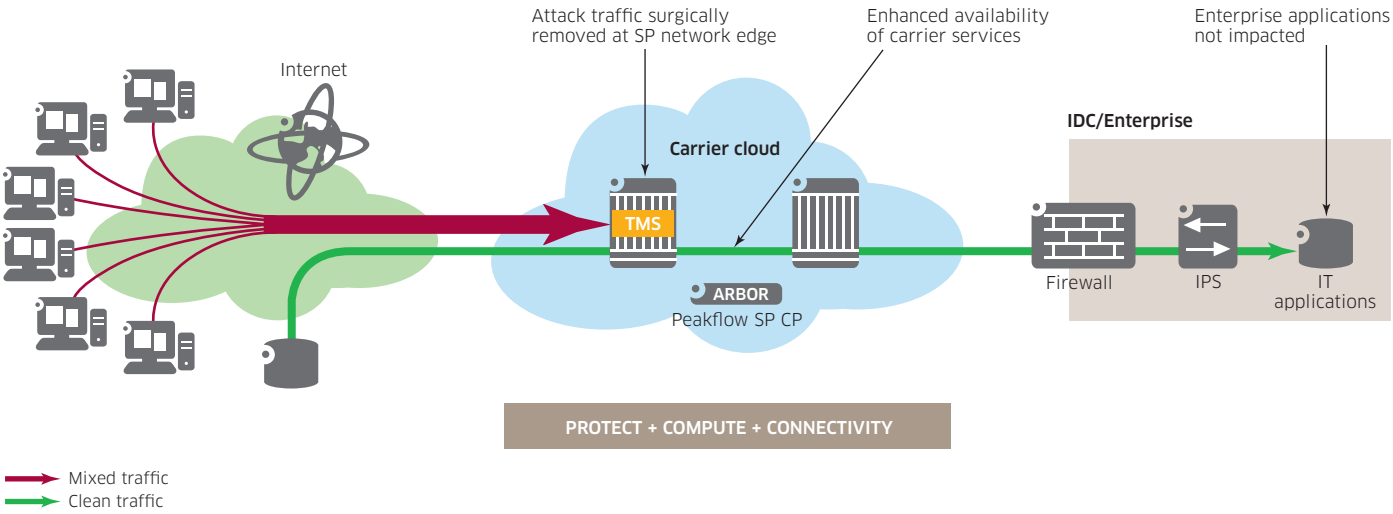
Over 60 percent of the world's service providers use the Peakflow service provider solution to identify threats that target their infrastructure and services today. Dozens of service providers worldwide participate in the Arbor Networks unique Fingerprint Sharing Alliance that feeds all Peakflow products with the network behavior

"fingerprints" required to identify DDoS attacks and botnet activity quickly. And Arbor's Security Engineering and Research Team (ASERT) are recognized security experts in global carrier threat activity and traffic analysis, as well as members of many advisory boards, such as Reseaux IP Europeens(RIPE, French for "European IP Networks").

3.3 Alcatel-Lucent Integrated DDoS Protection Solution

To meet the challenges of increasing DDoS scale, Alcatel-Lucent has partnered with Arbor Networks, to create a carrier cloud security solution that provides carrier-grade DDoS security for service provider networks and enterprises (Figure 6).

Figure 6. Alcatel-Lucent 7750 SR Integrated DDoS Protection Solution



The new solution integrates Arbor's market-leading Peakflow service provider TMS software with the Multiservice Integrated Services Adapter (MS-ISA) card of the award-winning Alcatel-Lucent 7750 SR. This integrated solution detects potential security attacks and removes them before they have a chance to affect a service provider network or an enterprise IDC.

With this solution, the Peakflow service provider CP appliance, detects anomalies via network behavior analysis. It then signals the TMS MS-ISA in the 7750 SR to surgically mitigate attack traffic. To ensure the 7750 SR DDoS mitigation solution does not become a bottleneck, only suspect traffic is forwarded to the MS-ISA TMS for scrubbing, or to a series of MS-ISA TMS blades via round-robin load balancing. Attack packets are dropped by the MS-ISA TMS using a series of attack identification and mitigation techniques, and clean packets are forwarded by the router to their original destination.

The Alcatel-Lucent solution has the capacity to scale to support both DDoS mitigation and network services across a broad customer base. It scales to over 60 Gb/s of DDoS scrubbing per service router, with all other services active.

In addition, it provides benefits traditional DDoS approaches cannot offer:

- The integrated DDOS protection solution simplifies existing scrubbing center designs. The 7750 SR supports traffic grooming and threat mitigation functions, thus eliminating the need for separate grooming routers and TMS appliances.

- The 7750 SR integrated TMS function may be leveraged to deploy DDoS protection in a distributed model. The distributed model eliminates the need to backhaul traffic to a central TMS appliance and mitigates the DDoS attack closer to the location of attack. As a result, network bandwidth is not wasted.
- The integrated solution enables DDoS scrubbing across a wider range of verticals, customers, and geographies, opening up new opportunities for DDoS mitigation services to enterprises and SMBs..
- Service providers can customize their DDoS deployment architectures with a combination of the Alcatel-Lucent Integrated DDoS Protection Solution and the appliance-based solution from Arbor Networks.

This network-based, integrated DDoS protection solution is the ideal choice for scaling service provider managed DDoS security services. In addition, it addresses the needs of service providers who wish to protect their network infrastructures from DDoS attacks, an imperative for carrier cloud services.

4. SERVICE PROVIDER USE CASES AND BENEFITS

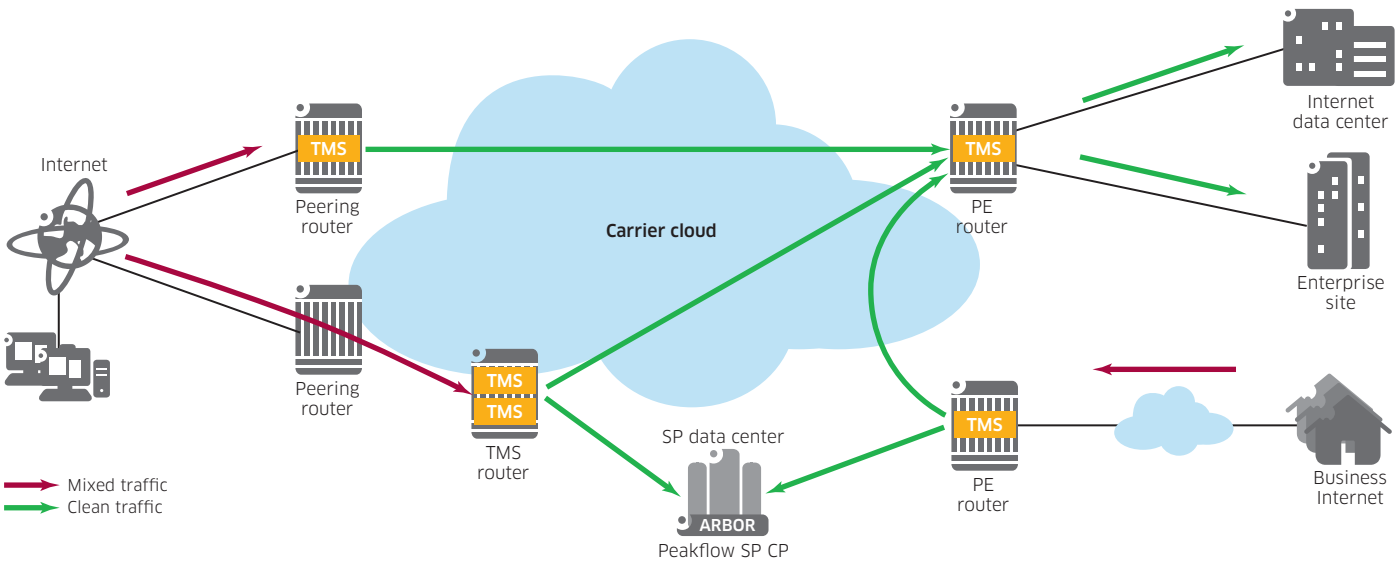
4.1 Deploy new/scale existing managed DDoS protection services

The Alcatel-Lucent Integrated DDoS Protection Solution offers a ground-breaking approach to mitigation of DDoS threats. It is the ideal choice for:

- Service providers considering greenfield deployment of managed DDoS protection services
- Service providers using Arbor Networks for DDoS threat mitigation that want to expand their service footprint and lower their operational costs

The solution enables service providers to differentiate their existing VPN and business Internet offerings by providing value-added protection from a wide range of threats, including DDoS attacks and botnets (Figure 7). It may be installed in a centralized or distributed scrubbing center model.

Figure 7. Integrated DDoS Protection Deployment Architectures



FLEXIBLE ARCHITECTURES FOR DISTRIBUTED AND/OR CENTRALIZED SCRUBBING

The solution enables new threat mitigation services for enterprises struggling to keep up with escalating security costs. Service providers that currently offer threat monitoring services based on Arbor Networks appliances can introduce this solution to scrub traffic for an additional charge. According to Arbor Networks, service providers who are using this system today generate anywhere from $8000/month to well over $100,000/month in new revenue per customer, depending on the bandwidth of the links being protected.

4.2 Protecting service provider infrastructure from DDoS attacks

Most service providers are concerned about attacks and threats from their end users. The architecture described in section 4.1 can also be implemented by service providers to protect their own networks and services (business, residential and mobile) from escalating DDoS threats. The solution can be used to protect services and associated infrastructure from a wide range of threats, including TCP stack/generic flood attacks, fragmentation attacks, application layer attacks, connection attacks, vulnerability exploit attacks and malware pipes (botnets).

A proactive approach to implementing DDoS prevention solutions will protect service provider assets and help retain customer confidence.

5. CONCLUSION

The Alcatel-Lucent Integrated DDoS Protection Solution is unique in the industry. It is ideal for service providers who want to upgrade and scale their current DDoS services, as well as those who want to implement a new solution.

This ground-breaking solution integrates the best-of-breed DDoS threat mitigation solution from Arbor networks in the industry-leading and proven Alcatel-Lucent 7750 Service Router platform. The integration of Arbor's TMS capability into the 7750 SR's MS-ISA cards helps service providers:

- Protect and defend their networks, as well as their enterprise customers' networks
- Differentiate themselves by providing a path forward to a more secure carrier cloud and future carrier cloud services
- Optimize DDoS mitigation efforts with less cost and more efficiency, and enable greater scale, lower operating costs and simplified operations for a more secure carrier cloud

Alcatel·Lucent