RADinsight Threat Intelligence

Telecom Business Security Services

To safeguard their normal business operation, enterprises need to protect their resources from malicious traffic, minimize attack surfaces, and secure access to corporate resources. In many cases, this complex task is too challenging to handle internally. Hence, many organizations prefer to outsource managed solutions from communications service providers (CSPs). According to analyst firm Analysis Mason, 61% of small businesses and 79% of medium businesses prefer to purchase cyber security services along with network and internet services, as opposed to them being standalone or part of an IT service. This is a perfect opportunity for CSPs to expand their offering with managed cyber security services.

RADinsight TI (Threat Intelligence) allows CSPs to augment their security service offering with network-embedded security architecture that is implemented at customer and network edges. This enables CSPs to deliver secure access and malicious traffic prevention to their business customers.

DDoS in Telecom

Distributed Denial-of-Service (DDoS) attacks are one of the key risks that disrupt normal operation. These attacks have increased dramatically recent times. According to RADware's 2024 Threat Report, DDoS attacks per customer grew by 94% in 2023 compared to 2022. The average DDoS attack volume per customer also increased by 48% in the same year. Additionally, the sophistication of these attacks has risen, causing significant disruptions to both CSPs and enterprises.

RAD

Your Network's Edge®

DDoS mitigation services by over-the-top (OTT) providers are currently dominating the market. They are either being sold directly to enterprises or resold by CSPs. However, to remain competitive, CSPs should be able to offer enterprise customers affordable DDoS protection solutions that are based on their own network's intelligence. This would allow them to address different sets of functional and commercial requirements, while monetizing their network and keeping its performance and integrity.

DDoS Defense Strategies

The most popular method to thwart a DDoS attack is by "scrubbing" suspicious traffic, meaning rerouting suspicious traffic to dedicated scrubbing centers where it's analyzed. Legitimate traffic is then routed back to its destination, while confirmed malicious traffic is blocked. Here are various types of scrubbing, and their use depends on the perceived risk and available budget:

Reactive scrubbing is mainly used by customers with a low perceived risk. It is activated on customer request when that customer experiences a DDoS attack. As result, traffic coming from the internet to the customer is rerouted to the scrubbing center using BGP (Border Gateway Protocol), typically within 15 min of alert. The scrubbing center filters out malicious traffic and passes on clean traffic towards the protected destination. This method consumes the least amount of scrubbing resources and is therefore the least expensive one. However, it leaves the enterprise exposed to the attack until the scrubbing process is activated, which takes valuable time during which the enterprise can be compromised.

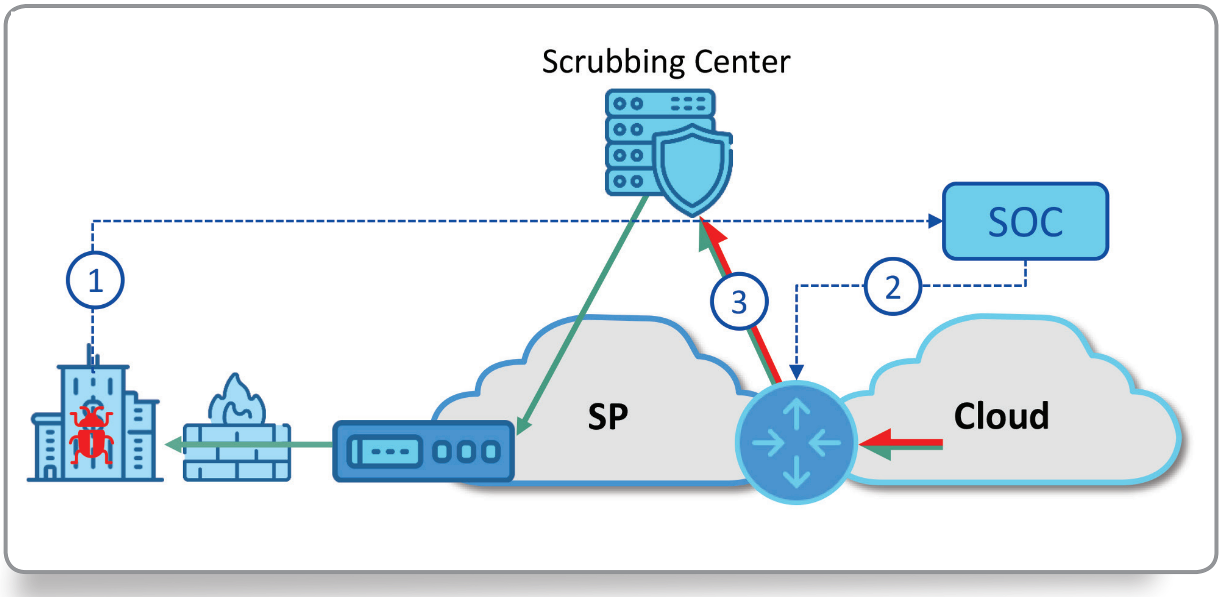

Figure 1. Reactive Scrubbing

Proactive scrubbing is used for businesses with a higher perceived risk, who are experiencing more frequent DDoS attacks. In this method, inbound traffic is constantly monitored by the service provider via an additional detection module. Upon detecting an attack (typically within 2 minutes), the infected traffic is rerouted to the scrubbing center using BGP. The traffic remains active for a period defined by the service provider pricing policy, which could range from four hours to unlimited. The detection is based on NetFlow analysis, and its cost depends on the NetFlow sampling rate. Due to cost considerations and the nature of aggregated traffic, the detection module is normally tuned to a relatively high-resolution threshold, making it suitable for volumetric attacks and large enterprise traffic. However, the majority of DDoS attacks are short and peak below 1Gbps, so they might be detected too late or be completely missed by scrubbing center detection modules. These low volume attacks can take down an SMB (small to medium business) firewall in a second, enabling a cybercriminal to infiltrate and map a company's network, and possibly install malware to cause significant damage.

Low volume DDoS attacks don't require extensive resources to launch – they can be carried out from a single machine so that virtually anyone can launch it. That is also the reason why these attacks are very popular among DDoS-for-hire services targeting SMBs.

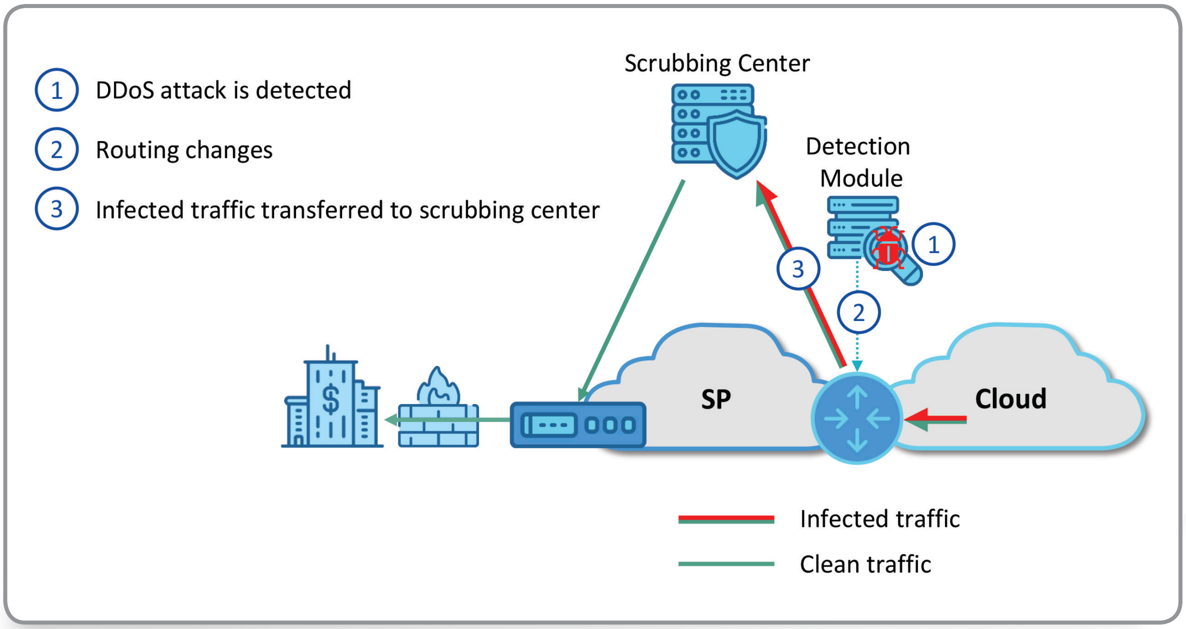

Figure 2. Proactive Scrubbing

Always-on scrubbing is the most effective, but also the most expensive type of scrubbing. It implies permanent rerouting of traffic to the scrubbing center. This method is used for customers with "clean pipe" requirements or when the scrubbing detection sampling rate is too low for a timely attack detection on SMBs with relatively low bandwidth.

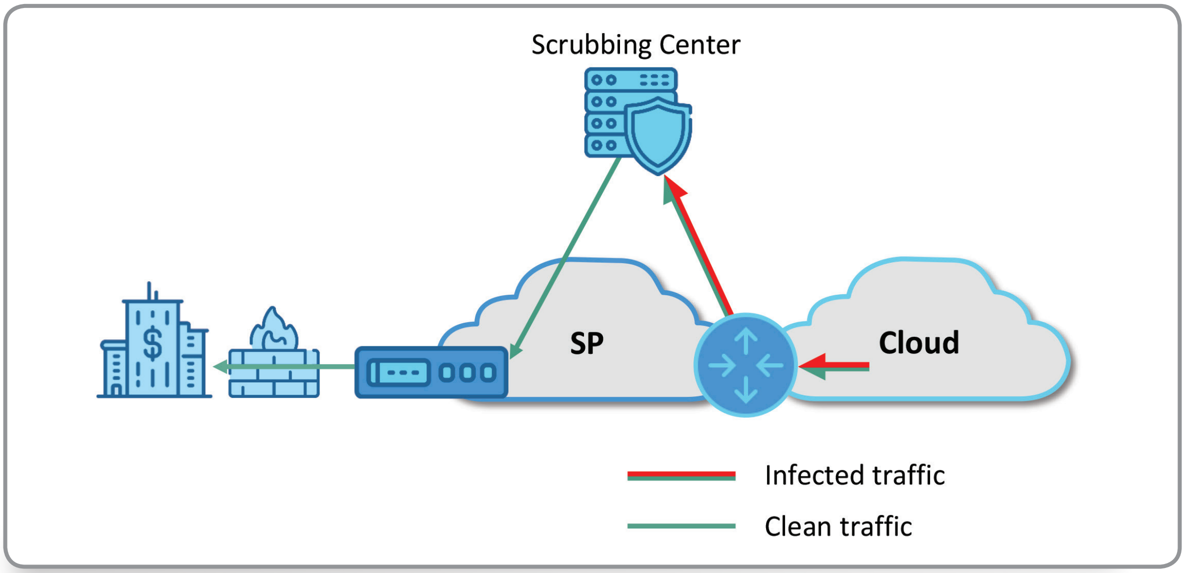

Figure 3. Always-on Scrubbing

In addition to scrubbing techniques, there are also In-line appliances that operate directly in the path of the network traffic to inspect and filter it in real-time. These can be used as an alternative to scrubbing centers. Although they provide fast mitigation of DDoS attacks, they require a substantial hardware footprint to accommodate inspection of the entire traffic. They are also quite expensive, become ineffective when saturated and create additional weak points in the network.

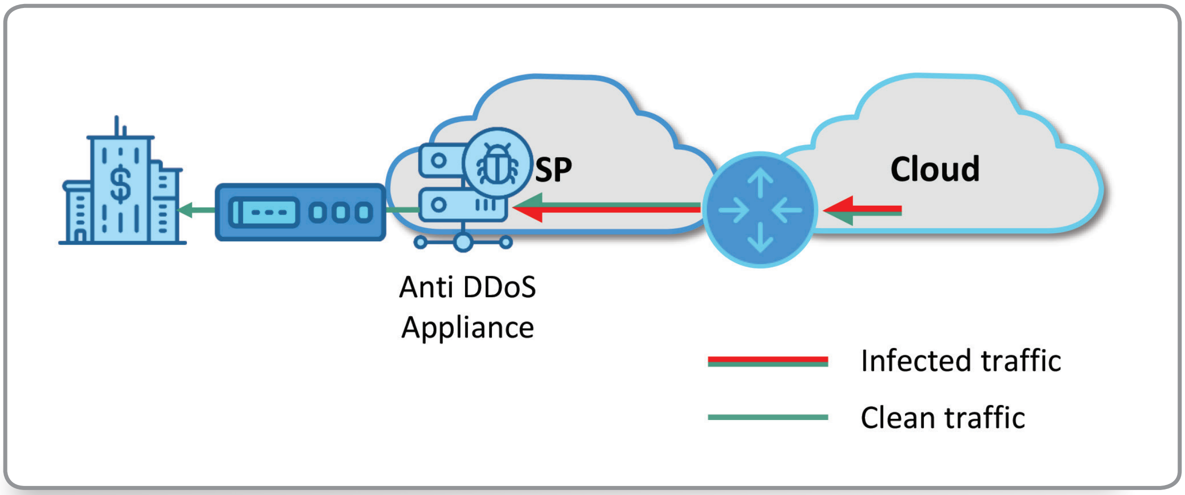

Figure 4. In-line Appliance

RADinsight Threat Intelligence

RADinsight TI (Threat Intelligence) is a disaggregated, software-based DDoS protection solution that is distributed across customer and network edges. It operates on top of existing network hardware to provide proactive DDoS protection over Ethernet access and managed routers. It addresses the needs of enterprises of all sizes, providing CSPs with a competitive solution for their business customers.

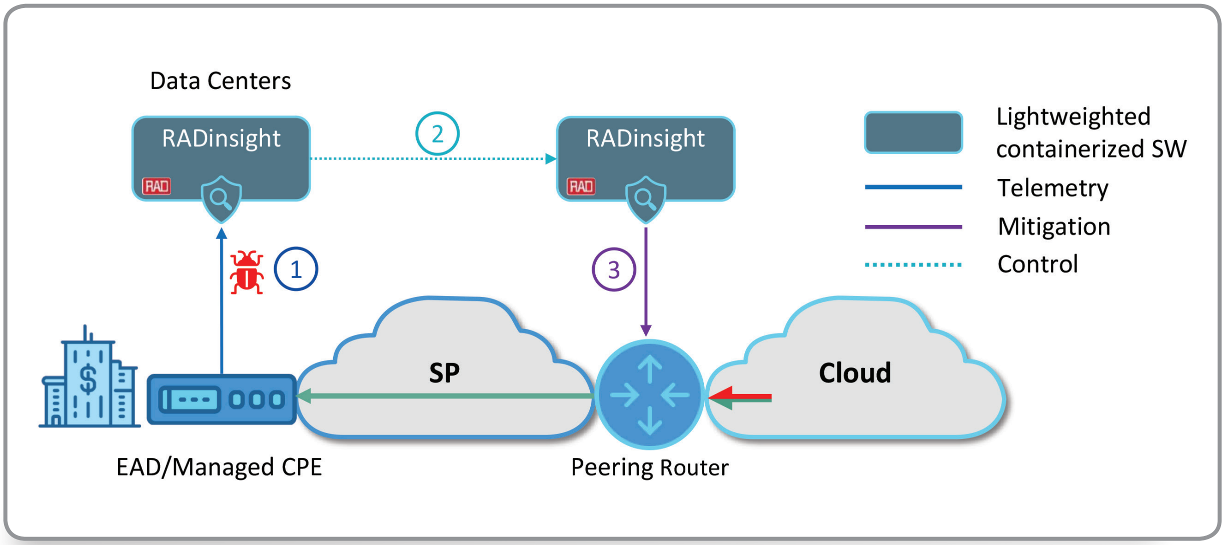

Figure 5. RADinsight TI: Access Embedded Security

RADinsight TI solution:

- Allows bundling with Ethernet Access or managed CPE as an add-on
- Allows CSPs to offer attractive security services to new customers, enabling them to eliminate the cost barrier
- SaaS model helps controlling investments
- Provides a better service with distributed detection for all attack volumes
- Scales with access bandwidth
- Improves network utilization/lowers network cost by eliminating the need to traffic rerouting
- Multi-vendor support

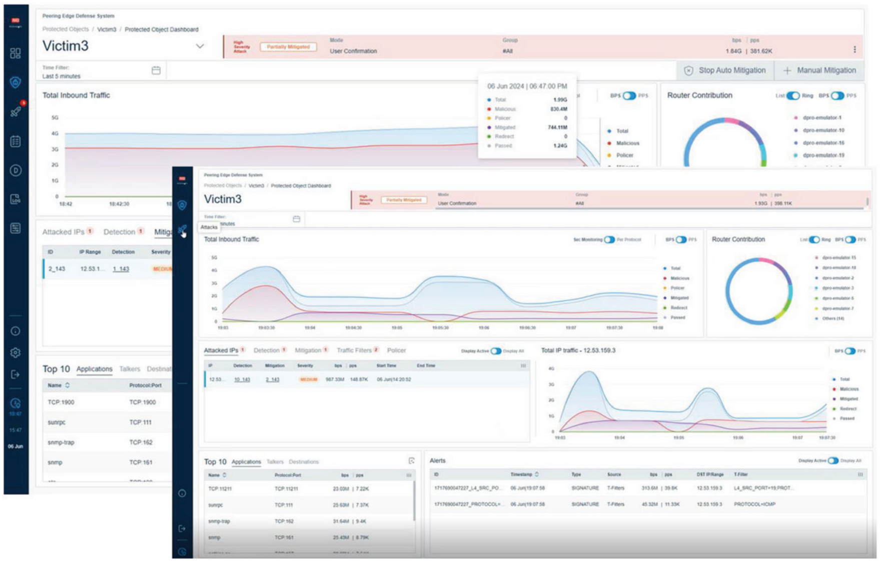

Figure 6. RADinsight TI GUI. SP and customer view

Technology and Architecture

RADinsight TI includes the **RADinsight TI Collectors**, which are located in regional data centers to collect telemetry from Ethernet access devices/managed routers. These collectors employ advanced AI algorithms to detect and classify orchestrated DDoS attacks through the **RADinsight Detectors.**

The RADinsight Detectors utilize the hardware of peering routers to mitigate attacks once detected at the customer edge. The mitigation policies are set by RADinsight TI Controller, which also exposes APIs towards the security management platforms used by the service provider. Fully containerized, the RADinsight TI Controller can be deployed on public clouds or at customer premises.

Significant TCO Reduction

RADinsight provides dramatic reduction of cost for hardware and the associated power, rack space, cooling, and similar requirements.

The growth in volume of both network traffic and DDoS attacks strains scrubbing capacity, especially as networks become more distributed with more peering points, resulting in network starvation as traffic needs to backhaul towards existing scrubbing centers at the expense of available bandwidth. RADinsight TI saves network resources needed for backhauling malicious traffic for scrubbing.

RADinsight TI requires much less ongoing engineering and network adjustments, maintaining CSP network architecture as is.

RADinsight TI applies a SaaS model and disaggregated architecture for gradual and controlled deployment and investments.

To learn more about RADinsight Threat Intelligence, contact us at market@rad.com.

Your Network's Edge®