

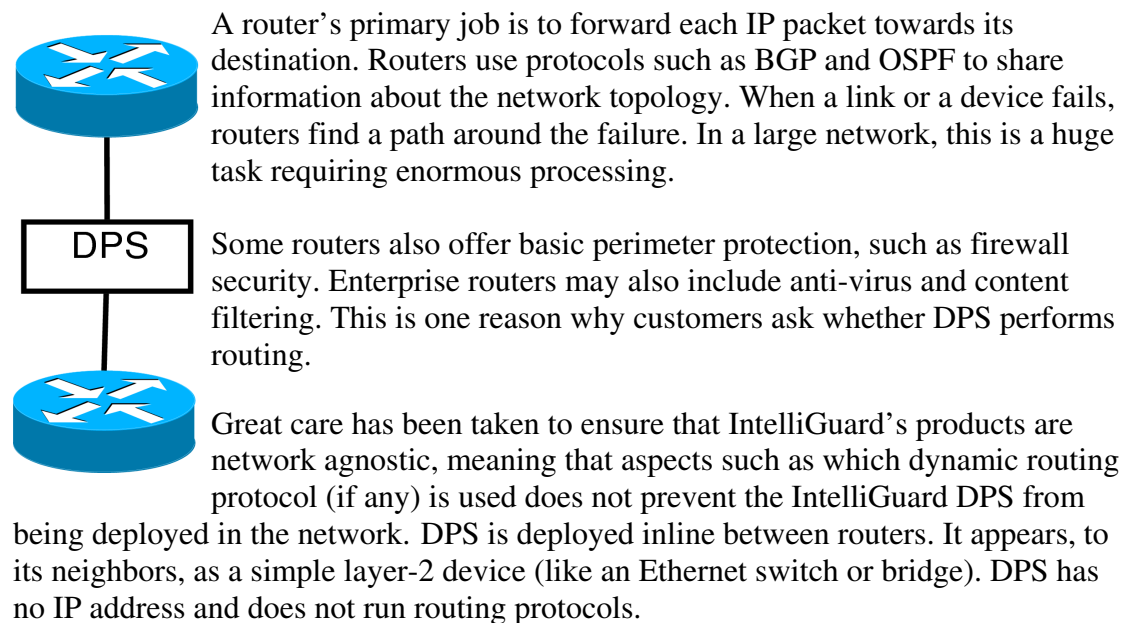
IntelliGuard DPS Inline Deployment

Summary

The IntelliGuard DPS is the only network security system available that maximizes the throughput of legitimate traffic in the face of DDoS attacks.

DPS is deployed **inline**, providing superior protection, carrier-class performance and High Availability.

Inline Deployment Explained



Superior Protection

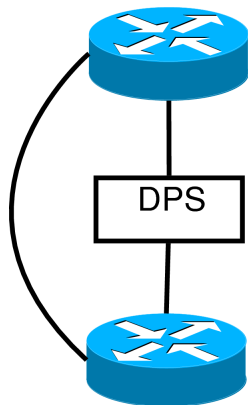
Inline deployment enables DPS to offer superior protection compared to other security products that appear as layer-3 devices:

- DPS has no visible IP addresses that can be targeted by attackers. Other security products can be attacked directly, and valuable processing power must be wasted in preventing those attacks, reducing throughput.
- DPS does not need to run routing processes. This has two benefits:
 - There are no routing processes to attack. Other security devices can be attacked using forged routing messages. Even if these attacks fail, they can consume processing power.
 - DPS offers greater protection during network instability. Large attacks sometimes cause network instability and rerouting. While the network reconverges, routers consume vast amounts of processing power. DPS preserves its power for defeating the attack.

Carrier-Class Performance and High Availability

Routing is used by some network security devices to participate in protection mechanisms. This is not necessary for DPS.

A faulty DPS cannot disrupt the network. In the case of catastrophic hardware, software or power failure, DPS network interfaces enter hardware-bypass mode, transforming DPS into a bridge.



In contrast, layer-3 security products use IP rerouting. A Computer World test¹ showed that even the best devices experienced a 4-second fail-over delay. Route reconvergence can take seconds or even minutes, disrupting IPTV, VoIP, gaming and other real-time applications.

For the most demanding High Availability requirements, a redundant unfiltered link can be added using a secondary route with a higher metric, as shown in the diagram. Alternatively, routers can be configured to provide active-active (shared load) and active-passive (hot standby) configurations for DPS.

Inline-on-demand?

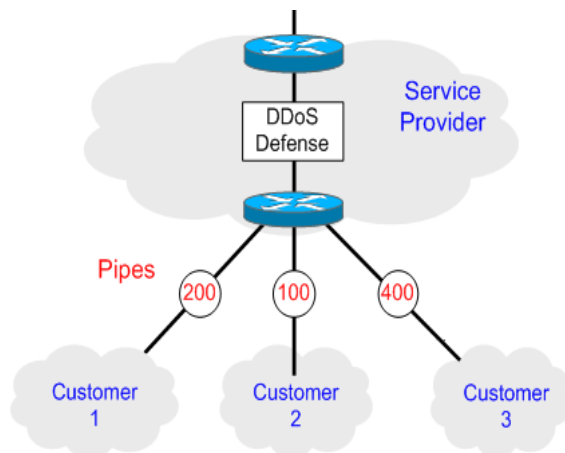
Some security devices monitor traffic, and only switch inline – to filter traffic – when required. This might be perceived to increase reliability and minimize latency (by having one less device inline), or reduce cost by sharing the security device across several zones.

Inline-on-demand has huge disadvantages and is not needed by DPS:

- Attackers can target the switching mechanism. By controlling attack frequency, the device can be forced to continually switch in and out, resulting in dropped traffic and potential network instability.
- Attack response time suffers during switching inline. In contrast, DPS adds less than 50 microseconds' latency and responds to attacks in under a second.
- During a large DDoS attack, **many** links will be flooded and require filtering. Shared devices will fail to protect exactly when they are most needed.

Cost-effective Multi-zone Deployment

Traditional IPS systems try to match packets against huge attack signature libraries. This is CPU-intensive and won't work against today's DDoS attacks, which resemble regular traffic from multiple sources. In contrast, DPS maximizes legitimate traffic using a superior methodology that makes better use of expensive CPU resources.



DPS is best deployed at high-bandwidth aggregation points in the network edge. Zoned protection enables protection of up to 64,000 downstream nodes, links, servers, and services, as if each had its own DPS.

With superior CPU utilization and protection of up to 64,000 zones, DPS reduces deployment costs without the need for compromises such as inline-on-demand.

¹ <http://www.computerworld.com.au/index.php/id:721551919>