SD-WAN

https://campus.barracuda.com/doc/104380812/

SD-WAN provides multi-path VPN tunnels across all providers, thereby offering redundant, reliable, and failsafe network connections. When the VPN tunnel is up, it can transmit traffic as long as at least one ISP link is operational. Admins can retain full control over how each link is used, or they can configure the advanced balancing and bandwidth management features to optimally use the available bandwidth. SD-WAN combines a multi-transport VPN tunnel with the following advanced VPN routing, balancing, and shaping features:

- Dynamic Bandwidth and Round Trip Time (RTT) Detection
- Performance-Based Transport Selection
- Adaptive Bandwidth Protection
- Last Mile Optimization (FEC)
- Adaptive and Static Session Balancing
- Failover Support
- Multi-Provider Load Balancing

SD-WAN policies are applied to all sites simultaneously and define the behavior of the VPN and non-VPN traffic such as routing, failover, load balancing, and application prioritization. Fallback links are used only in case of failovers and only for the traffic that is allowed to use fallback links.

> When enabling Last Mile Optimization on Barracuda SecureEdge, the SD-WAN policies known as Override Categories will have Forward Error Correction (FEC) enabled for all categories.

For more information on SD-WAN policies, see SD-WAN Policies.

Figures

1. app_categories.png