NS1.

How Aldi Süd Can Achieve Higher Network Efficiency with Smart Traffic Steering

No matter the type of organization you work for, the business of operating enterprise networks and applications is almost certainly growing more complex. The number of migration projects moving production applications and workloads across different on-premise and hybrid cloud environments is increasing. And the number of software updates being deployed is also growing as more enterprise development teams adopt Agile, DevOps, or CI/CD practices.

The need to maintain site reliability and user experience in the face of these changes puts enormous pressure on network and operations teams to improve their efficiency and effectiveness. This is particularly evident as recent events have compelled organizations of all sizes and across all industries to adopt new work approaches that keep employees safe at home. But many organizations are grappling with the issue of balancing employee productivity with efficient and secure networks.

The answer lies in smart traffic steering. By applying smart traffic steering tactics, not only will you simplify and optimize your network operations, but you'll ensure that your employees' work-at-home experience with company technology is neither problematic nor complicated.

SECTION 1

Business risks for inefficient network operations

For years, many organizations have leveraged their own networks and virtual private networks (VPNs) to provide seamless connectivity without compromising security for employees who travel or work remotely. These endpoints are typically set up to support 5 to 10 percent of a company's workforce at any given time.

Ongoing network and VPN support for 100 percent of the workforce at companies around the world is unprecedented. This "new normal" is putting unforeseen stress on both corporate and public networks, and there are serious business risks to having inefficient network operations in a challenging time.

Disengagement and lost productivity. Your employees are stressed, so even with the increased demand on networks, your staff needs to be able to use company technology problem-free as they work from home. If they can't connect or they get kicked off their network or VPN because traffic is higher than normal, you'll see higher rates of disengagement and productivity.

Solve It

Add new VPNs or networks and endpoints in multiple regions to support increased demand. Depending on your architecture, this can be done through a cloud provider by increasing seats, by adding licenses to your existing VPN hardware solution, or by purchasing and deploying new VPN servers.

Increased security risks. VPNs are designed to be encrypted tunnels that protect traffic, making them a secure choice for enabling remote work. This remains true even with more people connecting to these networks. However, cybercriminals take advantage of chaotic times to attack corporate infrastructure, like VPNs. They'll typically obtain a person's network credentials to access the VPN and, by extension, the employer's networks and systems. With a huge jump in VPN users, the pool of potential victims of lost credentials is higher than ever.

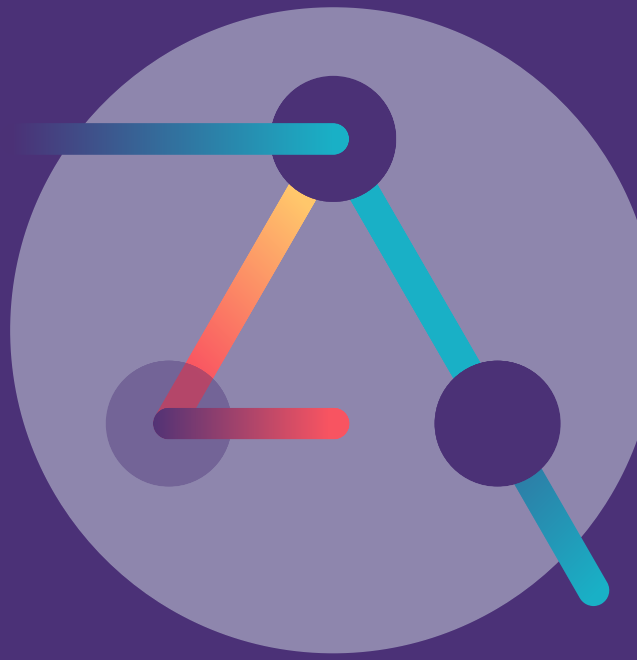
Solve It

Enable and require two-factor authentication as a second layer of protection. With two-factor authentication, even if a cybercriminal obtains credentials, they can't access the network without additional information, such as a one-time-use security code sent to a preselected mobile number or, ideally, to a token application.

Overloaded VPN capacity. Endpoints that choose networks, or having users choose network endpoints based on location, are particularly problematic: They don't account for the latency and congestion created when many users try to access the same network from the same general area. Worse, if users can't connect to their normal endpoint due to high traffic volume, they'll often select a backup without considering its location or load.

Solve It

Apply smart traffic steering at the DNS layer to optimize server use. While increasing the number of VPN servers improves capacity, there may still be issues with performance or availability if users log into the same VPN server. Without traffic steering, when employees log into the network, they select the best endpoint and likely continue connecting to that endpoint for days or weeks regardless of usage or capacity.



SECTION 2

5 ways smart traffic steering helps your network operations

Traffic steering helps you incorporate real-time telemetry to automate routing to the fastest and best performing point of presence for each user, minimizing latency and preventing regional overload that could crash systems.

Most networking teams are familiar with basic traffic steering policies, but smart traffic steering goes further: It adds real-time infrastructure data and configurable logic, new options for improving productivity.

The key to achieving this operational efficiency is being able to embed smart decision-making capabilities within the network infrastructure itself, and this requires data and logic. Combining data and logic enables you to implement custom decision-making logic easily by chaining together simple, single-purpose algorithms. And, having this capability at the DNS layer empowers you with more flexibility in steering enterprise users to application resources than ever before.

Once these capabilities are implemented, you'll see five key improvements in your network operations.

1. You'll be able to **improve site reliability** with live data and logic.

Traditionally, availability problems have been handled through an incident-response process with alerts to the IT service desk, the operations team triaging and escalating events to appropriate teams, and a resolution or fix. But all of this takes time, and this can impact user experience.

With smart traffic steering capabilities, network teams can automatically route users to alternative application resources until the problem is resolved, without having to reconfigure Layer 3-4 routing or physical network devices. Similarly, once a problem is resolved and your monitoring solution recognizes that the resources are back online, metadata is updated, the resource that went down becomes a viable option again, and user traffic returns to original routing patterns.

All the while, users will see the application as available.

2. You can **prevent issues proactively** with global load balancing.

The ability to intelligently balance load across multiple data centers or colocation facilities is particularly important if you've set limits on how much capacity you can handle from a specific location. As you get close to the high watermark you've set, the more traffic you'll want to shed to other locations.

With smart traffic steering, you can bring in live capacity data through APIs and integrations. As the number of connections creeps up toward the limit you set, more traffic will be sent automatically to other locations. Conversely, as the connections slide downward, less traffic will be directed to other locations.

3. You can **mitigate operational risk** with blue/green deployments.

Another way to improve operational efficiency is to remove the risk of migrating traffic between two environments. Instead of having one cutover date where all users are directed to the new environment, you can ramp up the percentage of traffic directed to the new environment in stages. This capability is useful in multiple scenarios, including:

- Rollouts of a new version of software or service
- Migrations of existing applications to a new environment (for example, from on-premise to cloud)
- Canary testing software changes in production environments

With smart traffic steering, you can define which subnets, geographies, or networks are steered to this new environment and what percentage of traffic goes where to ensure a consistent application experience for users during the transition. You mitigate risk because any problems with the new environment will affect a much smaller percentage of the user base. And once you've ensured that everything functions properly, transitioning the remaining traffic in stages is easy because you have an orchestration system in place.

4. You can **avoid application availability issues** with fast DNS propagation.

The more short-lived application and infrastructure resources become, the more important it is to have DNS records accurately reflect the changes that automated deployment and auto-scaling create. If a DNS server half a world away hasn't been updated to show that one service has been deployed with IP addresses released by the removal of another service, all sorts of application problems will occur. Smart traffic steering can help you prevent users from seeing the application as unavailable, as well as help you avoid wasted time and effort spent troubleshooting the differences in records.

5. You can **get up to speed quickly** with a single API.

IT efficiency means being able to leverage existing skills and familiar tools. The right smart traffic steering tool will be able to integrate your “Infrastructure as Code” orchestration tools and provide libraries to ensure your teams are empowered with their choice of languages and tools. This eliminates a steep learning curve before your teams can be productive with APIs to orchestrate provisioning, deployment, and CI/CD pipelines.

The efficiency gains from applying smart traffic steering capabilities can add up to a significant level of success for enterprise network and application teams. Not only will you experience optimized network operations, but you'll ensure your employees can rely on company technology in a stressful time.

NS1 is a market leader in smart traffic steering. Our **Pulsar** traffic steering solution helps you achieve these network improvements by enabling customized routing policies, automated intelligent traffic steering, and guaranteed optimal end-user experiences.

Contact NS1 today to learn how your organization can benefit from smart traffic steering.

NS1.