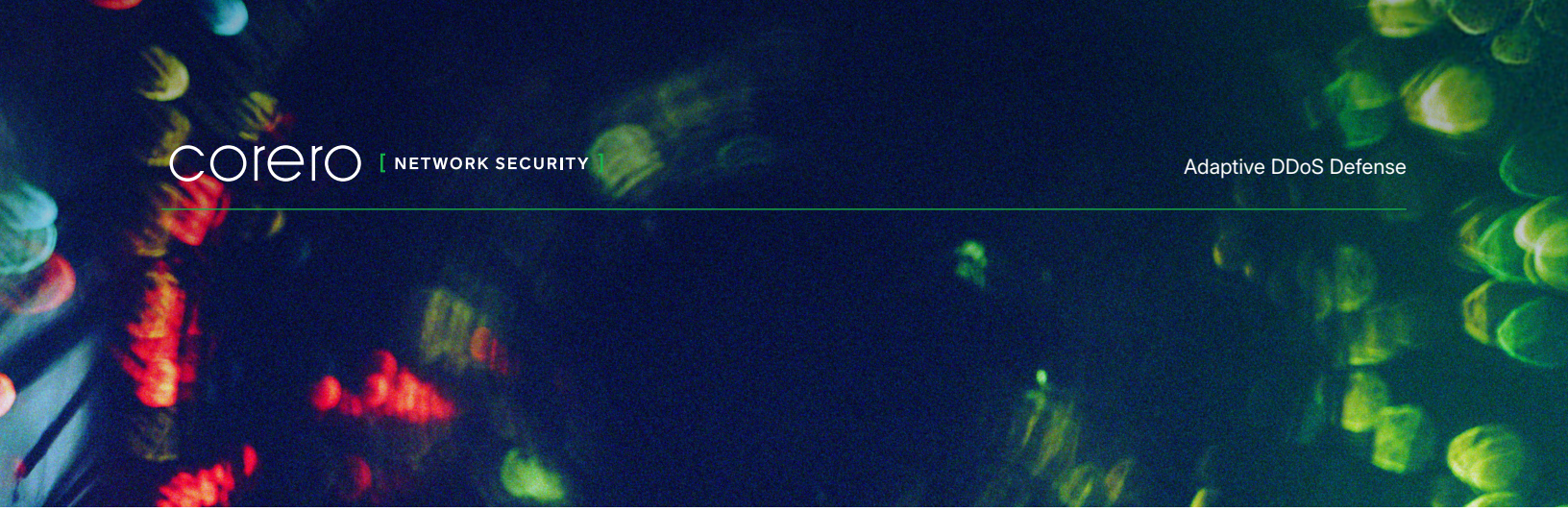

Stop Brute Force Attacks Before They Disrupt Access

Real-time control that blocks threats before they reach your infrastructure

Brute-force attacks don't just target credentials. They overwhelm the infrastructure behind them, including VPNs and authentication systems, often locking out legitimate users. Even when the login attempts fail, the volume alone can knock out access. **That's where Zero Trust Admission Control (ZTAC) in the CORE platform steps in.**

Listen, if your network is the hottest club in town, you need a bouncer who actually checks the list. ZTAC is that bouncer. It doesn't just wave people through—it reviews every access request in real time, checks credentials, and decides who gets in and who doesn't. High-risk traffic is blocked before it ever reaches your VPNs, firewalls, routers, or APIs. That keeps things smooth for everyone who belongs.

The system is stateless and cloud-based, so enforcement is instant. With SmartWall ONE™ as the enforcement point, you can update allow and block lists quickly, without delays or reboots.

No lag. No friction. Just smart, consistent protection that keeps the right users in and the wrong ones out. **We make sure only the right people get in and maintain a real-time profile of who should have access.**

Continuous Validation Without the Delay

With ZTAC, every access request is evaluated before it creates risk.

This isn't reactive detection. It's proactive enforcement. Adaptive policies continuously verify the identity and behavior of users, devices, and applications.

You stay protected without bottlenecks. Your team stays focused without chasing false positives.

- **Suspicious sources are blocked before they reach VPNs or web apps**
- **Repeated login attempts are throttled or denied**
- **Access list updates are reflected immediately**
- **Legitimate users continue without delay**

Protect the Infrastructure That Keeps You Connected

VPNs, firewalls, routers, and web services are frequent targets for credential abuse and vulnerability exploits. Even when attackers fail, brute-force traffic can degrade or block access. Most access control solutions rely on stateful inspection. They build context over time, which adds lag and complexity under load. We take a different approach.

CORE uses a stateless architecture that filters bad traffic before it ever reaches your infrastructure. It evaluates each request in real time using attribute-based metadata—such as user role, device posture, behavior patterns, and location.

The result: no session buildup, no infrastructure strain, and no delay. And when it's time to update access lists, changes apply instantly without reboots or manual effort.

A Better Way to Allow Access

Implementing a full Zero Trust architecture can introduce excessive complexity.

While traditional access controls still have a role, ZTAC simplifies access enforcement by providing real-time, centralized decisions without the overhead of managing multiple systems or policies.

- **Cloud-managed policy with local, in-line enforcement**
- **Instant policy enforcement for rapid updates**
- **Real-time evaluation that blocks threats without slowing users**
- **Proactive threat blocking that stops brute-force attacks before they hit infrastructure**
- **Attribute-based logic for rich, context-aware decisions**
- **Shields remote access infrastructure from exploits and credential abuse**

You don't need to sacrifice performance for protection. With our solution, you get consistent access, fewer disruptions, and lower operational strain, no matter how large or distributed your environment.

Redefine Access Control with ZTAC

Take control of access without the complexity. A new way to stop credential abuse, eliminate login floods, and keep your infrastructure running smoothly without slowing down your team. **Let's talk.**