perimeter 81

5 Steps to Streamline Security for your Hybrid Network

Build unified security across your services and locations with these steps in mind

Organizations using a tall stack of security tools can manage access for different users and groups to their network resources, like AWS, Salesforce, on-prem apps, data centers and more. Complications arise when a growing workforce needs more frequent remote access, and when the level of security offered by a complex array of security tools declines, due to missed configuration gaps, poor network performance and more. At this point, security must be managed from a higher administrative (and technical) level.

Trying to sync multiple security solutions together and keep customer data private in this hybrid environment is like trying to transfer water from one sieve to another without spilling. To reduce the attack surface and hide resources from the web, and to save admins the trouble of manually configuring multiple tools for multiple unpredictable users, the following five steps are a great place for IT teams to start streamlining their networking and security.

1. Consolidate control of networking and security

Admins can maintain security control across environments and users, but for secure global access to both cloud providers and on-prem hardware, this can quickly become burdensome. Firms with hybrid networks and platforms must overcome the hassle and precarious security hygiene involved in configuring the correct settings within each solution, while double-checking across platforms to ensure there aren't configuration gaps.

Software-defined networking solutions can help admins implement the type of user-centric, segmented approach necessary for easily manageable hybrid security. These solutions can connect **all network resources** and draw perimeters around and between them, improving visibility and making it easy to give any user access only to the specific resources they need for their roles.

2. Build a Zero Trust security policy

A least-privilege or Zero Trust model is better for security as it enables limited access based on role, device, and other identifiers – reducing the attack surface. But admins need a way to identify users on the network and determine which segments and services they can connect to. Identity Providers (IdPs) are a way to condition access to the network on a simple Single Sign-On (SSO) process, giving admins the ability to automatically identify the employee behind a connection and enforce access and other security policies for each user and role.

A unified network security solution integrated with a SAML 2.0 IdP makes it easy to obtain visibility, as well as control access and traffic between any object, service, address, or user on the network. This unified model can also more seamlessly adapt to the nuances of a hybrid workforce with various devices, locations, and time zones.

3. Supplement your security tools

Adding extra layers of security including 2-factor authentication and proxying is always a safe bet, and although these tools are simple and easy to deploy, it's crucial to do it the right way. Manipulating settings within a standalone VPN to account for network nuances, regions, policy and more is nearly impossible. It's much more practical to tunnel global connections through a proxy as a prerequisite for access to the entire network, protecting all resources with industry-level encryption.

Holistic security tools make it easy to enforce security configurations on users within the broader network, for example by mandating that contractors accessing a certain application must authenticate multiple times and can only access during their work hours, or by automatically requiring an encrypted connection when a user tries to gain access via an unfamiliar Wi-Fi connection. These tools also make it possible to remove barriers for trusted admins on managed devices and familiar networks.

4. Unify and monitor data streams

Hybrid networks transmit sensitive customer data from multiple resources the world over, and must enjoy a level of monitoring and data capture that is holistic across all data flows.
Logging is more difficult to accomplish when administrators must set up logs for each service separately, and coordinate and consolidate these logs themselves. Even with a SIEM (Security Information and Event Management) service, admins must still chase after errant traffic sources and destinations to prove compliance.

perimeter 81

Better and less expensive compliance management is obtained by monitoring in a comprehensive manner, across every single resource and user connected to the network. Transplanting SIEM integration and applying it to the whole network is easy with log forwarding from your network's software foundation. This makes it easy to corral and orchestrate traffic sources using any SIEM solution you prefer, like Amazon S3, Azure Sentinel, Splunk and others.

5. Build a wider base for infrastructure management

A definitive element of hybrid work is the displacement of employees from their normal office-based work and into "remote" settings, whether a cafe or their home office. Connecting branch offices and remote workforces demands a flexible network infrastructure that balances security and speed. Standalone VPNs from third-party providers, even those labeled as business solutions, are unable to satisfy this demand.

Adding security to the stack and applying it to various regions can be a difficult endeavor that requires manual configuration for user policies and traffic flows, as admins must piece together the connections between their environments and the various ports, addresses, and protocols of services from other providers, as well as on-prem solutions.

Protecting the network and keeping traffic private and speedy is easier when admins can directly deploy encrypted tunnels from within their network security platform, not from outside it.
Cloud-based SaaS tools encapsulate your applications and on-prem solutions as individual parts of many on the network, and make it easy to manage traffic between objects, users, addresses and services.

Complete the checklist with Perimeter 81

Perimeter 81 is a network security platform purpose-built for hybrid workforces. Our platform helps admins connect all the pieces of their network and set up fast, encrypted connections and Zero Trust access policies for users anywhere in the world. Perimeter 81 Zero Trust access uses IdP to provide identity- and context-based access policies for individuals, as well as internal network objects and services. Available via a lightweight cross-platform client application for employee access as well as through secured browser-based application-specific access, Perimeter 81 allows total control of the inside and outside of your network through a single management console.

perimeter 81

Contact Us

Perimeter 81 Ltd.

www.perimeter81.com

+1-929-575-9307

Request a Demo

Follow Us