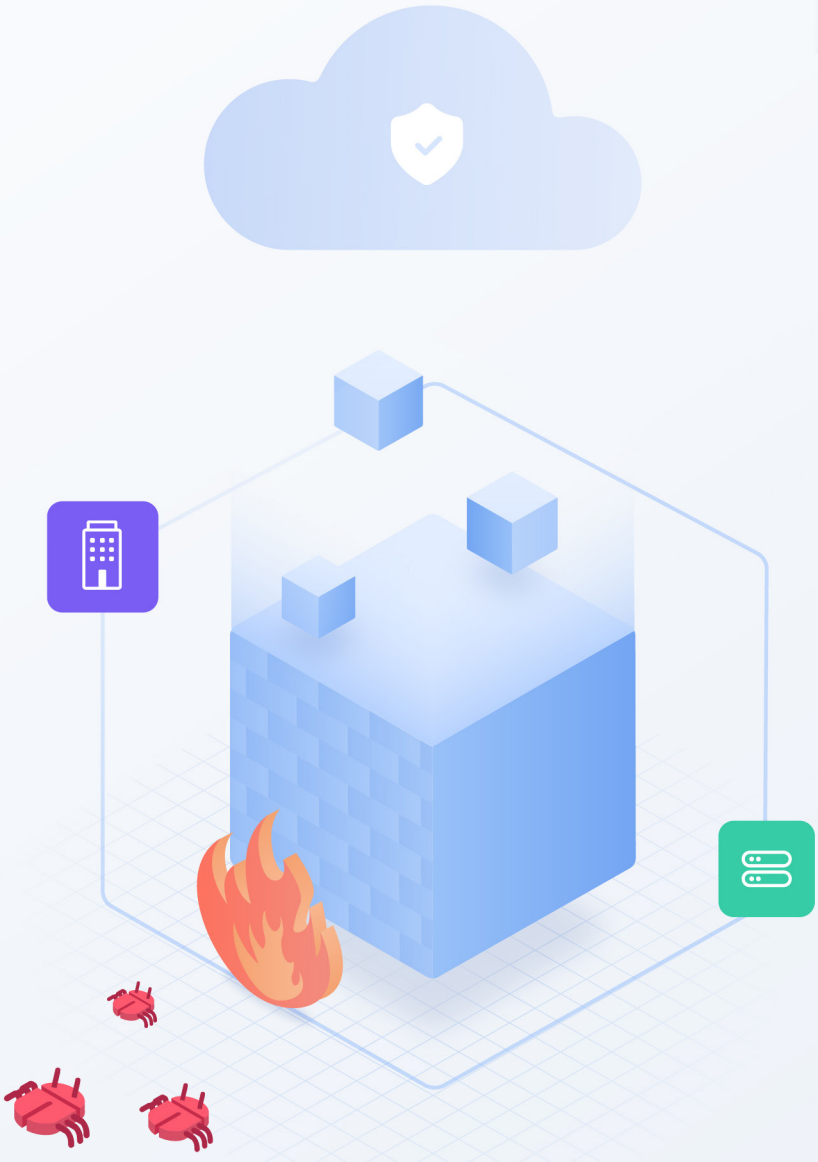
perimeter 81

Firewall as a Service: Bringing the Firewall into the Cloud Era

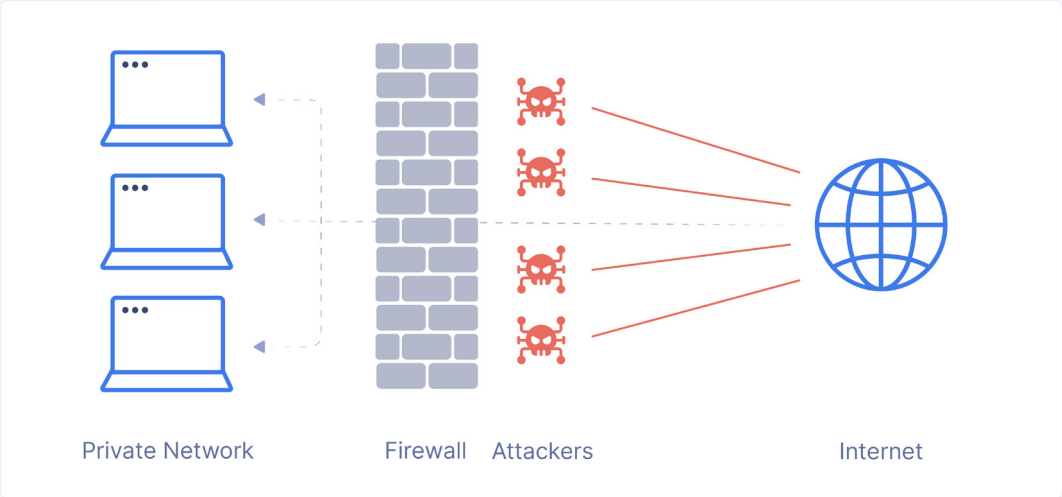


perimeter 81

Introduction

The traditional firewall concept has protected networks and users for almost thirty years against cyberattacks by blocking malicious or unnecessary network traffic from both public and private sources. Initially deployed for on-premises network or device security, firewalls exist either as software applications or computer hardware appliances such as Internet gateway servers that control network access, monitor traffic and filter out malicious or unwanted network traffic. This unauthorized traffic is normally flagged and blocked, while approved traffic and users can access network resources based on organizational security policies.

However, with the growth of both hybrid and multi-cloud environments, these traditional or legacy firewalls have become prone to misconfigurations, less transparent, more difficult to manage and unable to scale across enterprise networks. And although properly configured firewalls may effectively block some attacks, they do not guarantee that a computer or network is completely secure against threats such as sophisticated malware, malicious insiders or third-party threats.



The Need for Firewall as a Service

Today, traditional firewall deployments should be thought of as a legacy cybersecurity solution that presents a challenge for modern security professionals. Alternatively, Firewall as a Service (FWaaS) is a more modern concept that brings the original firewall into the cloud era. With FWaaS, an organization can manage all of its on-premises and cloud resources using a single, managed and cloud-hosted firewall service that enforces global security policies across all users and network resources.

According to Gartner, “FWaaS offers a significantly different architecture for branches or even single-site organizations. It also offers greater visibility through centralized policy, increased flexibility and reduced capital costs by using a fully or partially hosted security workload.”

perimeter 81

All network traffic coming from an organization's headquarters, branch offices, remote workers, or cloud services is controlled and routed through the centrally managed FWaaS platform. Using encryption protocols such as IPSec and SSL, organizations can establish a secure connection between users' devices and network resources, combined with FWaaS to deliver multifaceted protection and a reduced attack surface.

Finally, combined with a Zero Trust Network Access (ZTNA) solution, organizations can define security policies that authenticate users, and filter content and application traffic while protecting network resources down to the device level. ZTNA then further reduces an organization's attack surface by implementing least-privilege access policies in tandem with FWaaS rules.

Firewall-as-a-Service Benefits

Enhanced Network Visibility

FWaaS solutions provide a single platform and centralized hub for monitoring and managing network activity across multiple locations and traffic sources.

Scalability

FWaaS configurations scale with organizational and traffic growth in terms of security protection, users and new potential threat adaptability. With cloud-based firewall services, network administrators can easily add new branch offices and users, add more network capacity, and extend security coverage to additional resources.

Simplified Infrastructure

With network traffic originating from data centers, corporate offices, branch offices and remote workers, FWaaS solutions synchronize endpoints and firewall policies into one streamlined and unified platform.

Easy Configuration

Cloud-based firewalls can be deployed in modular ways to do specific jobs. For instance, a FWaaS can be configured to only direct traffic, but it can also filter URLs from within the network and defend against attacks. IT admins are able to choose which firewall functions to consume and which to ignore.

Remote Worker Protection

In the "work from home" era, FWaaS extends network defenses to remote employees by enabling them to connect to the FWaaS through a Business VPN or Network as a Service (NaaS) with automatic security when using the internet or cloud resources such as Salesforce or AWS.

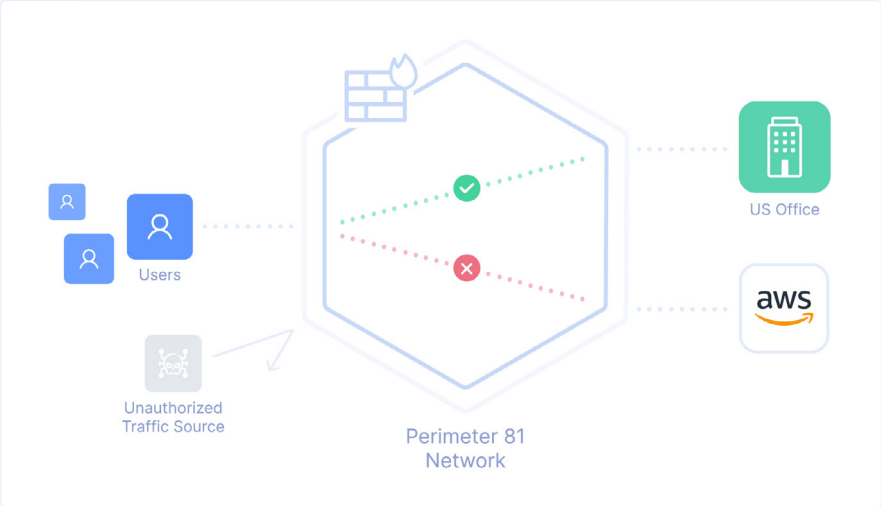
Policy Enforcement Streamlining

Security administrators can define organizational security policies across network locations, on-premises and in the cloud using their FWaaS platform.

perimeter 81

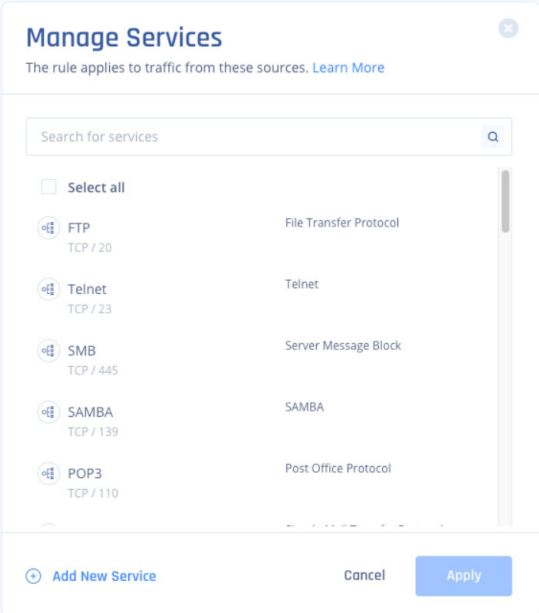
Network Traffic Control (NTC) from Perimeter 81

Perimeter 81's Network Traffic Control (NTC) solution provides a cloud-based Firewall as a Service, enabling easy, centralized control of traffic between sources and destinations on any public or private network. NTC allows IT administrators to segment Layer 3 and Layer 4 access based on user or group identities for granular network access while providing a single platform to manage network resource access and apps.



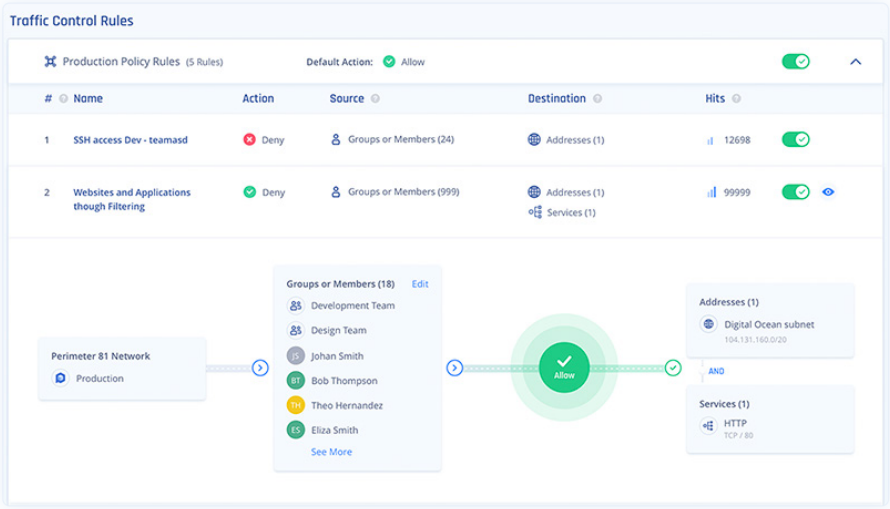
This means that IT administrators can easily control who is accessing which resources, protocols and ports directly from their Perimeter 81 console. Network Traffic Control rules can be applied to servers and services globally, extending a layer of security and protection inside and outside of the organization.

For example, with NTC parallel rules can ensure that a manager on a business trip has secure access to branch resources, that only developers have access to the organization's MongoDB server, and that all employees have unobstructed access to Zoom services.



perimeter 81

NTC works in tandem with two crucial security concepts — encrypted tunneling and custom access rules based on user identity. The users and groups to which NTC rules apply are easily set up for your network, and can be defined based on the qualifiers relevant to your organization's security — OS, device type, role, or location. Network Traffic Control user-based access management combined with Perimeter 81 encrypted tunnels also provides Firewall as a Service utility for more precise and autonomous network control.



Traffic Rules for Tighter Network Control

Add Access Rules to Networks

Create access rules within any network by selecting the relevant network, name the rule you wish to add and then choose the traffic sources (users and groups, addresses, or services), the traffic destinations (including addresses or services) and whether to deny or allow access when the rule is in place. As soon as you apply the changes, the rule will be activated.

Map Traffic Policies

Network Traffic Control provides an easy, comprehensive view into all of your existing network traffic rules. At the click of a button you can expand the rule to get a simple and interactive infographic displaying the details of user and group lists, IP addresses and specific services that are allowed or denied access according to how the rule was set up.

Prioritize and Optimize Rules

Easily select which rules inside a network take precedence over others by dragging and dropping the rules you've created into a specific order, then saving your changes. Rule prioritization helps create orderly traffic policy that leaves nothing to chance, and more effectively reduces the attack surface of the most sensitive network resources.

perimeter 81

NTC and the Perimeter 81 Platform

Network Traffic Control rules further strengthen and define the security posture of organizations that already take advantage of Perimeter 81's platform security features, including:

Security on All Devices

Bring-your-own-device (BYOD) policies multiply the number and variety of devices connecting to your network. Ensure only authorized devices connect to your virtual desktops with NaaS endpoint security.

Cloud Agnostic Integration

The ease with which our solution integrates into your virtual office, whether local or cloud-based, enables organizations to protect all their resources in a unified fashion.

Safe Remote Access

Automatic Wi-Fi security lets remote workers connect to sensitive resources from the public internet without fear of exposure, while encrypted tunnels shield data sharing from prying eyes.

IP Whitelisting

Explicitly define the IP addresses that are allowed to access the network, granting IT teams a stronger grip on security and also the ability to assign static IPs to automatically trusted sources of traffic.

Precise User Segmentation

Beyond the capabilities of traditional security solutions, the addition of granular policy-based permissioning helps organizations exercise greater control over those entering their virtual infrastructure.

About Perimeter 81

Perimeter 81 is a leading Secure Access Service Edge (SASE) provider that has taken the outdated, complex and hardware-based network security technologies, and transformed them into one unified, scalable and easy-to-use software solution—simplifying secure access for the modern and distributed workforce. Founded by two IDF elite intelligence unit alumni and serial entrepreneurs, CEO Amit Bareket and CPO Sagi Gidali, Perimeter 81 is headquartered in Tel Aviv, the heart of the startup nation, and has offices in New York and California. Perimeter 81's clients range from small businesses to Fortune 500 corporations across a variety of sectors, and our partners are among the world's foremost integrators, managed service providers and channel resellers.

perimeter 81

Contact Us

Perimeter 81 Ltd.
www.perimeter81.com
+1-929-575-9307

Book a Demo