Technical Validation

Securing Your Network with Perimeter 81

Comprehensive Security without the Complexity

By Alex Arcilla, Senior Validation Analyst

October 2022

This ESG Technical Validation was commissioned by Perimeter 81 and is distributed under license from TechTarget, Inc.

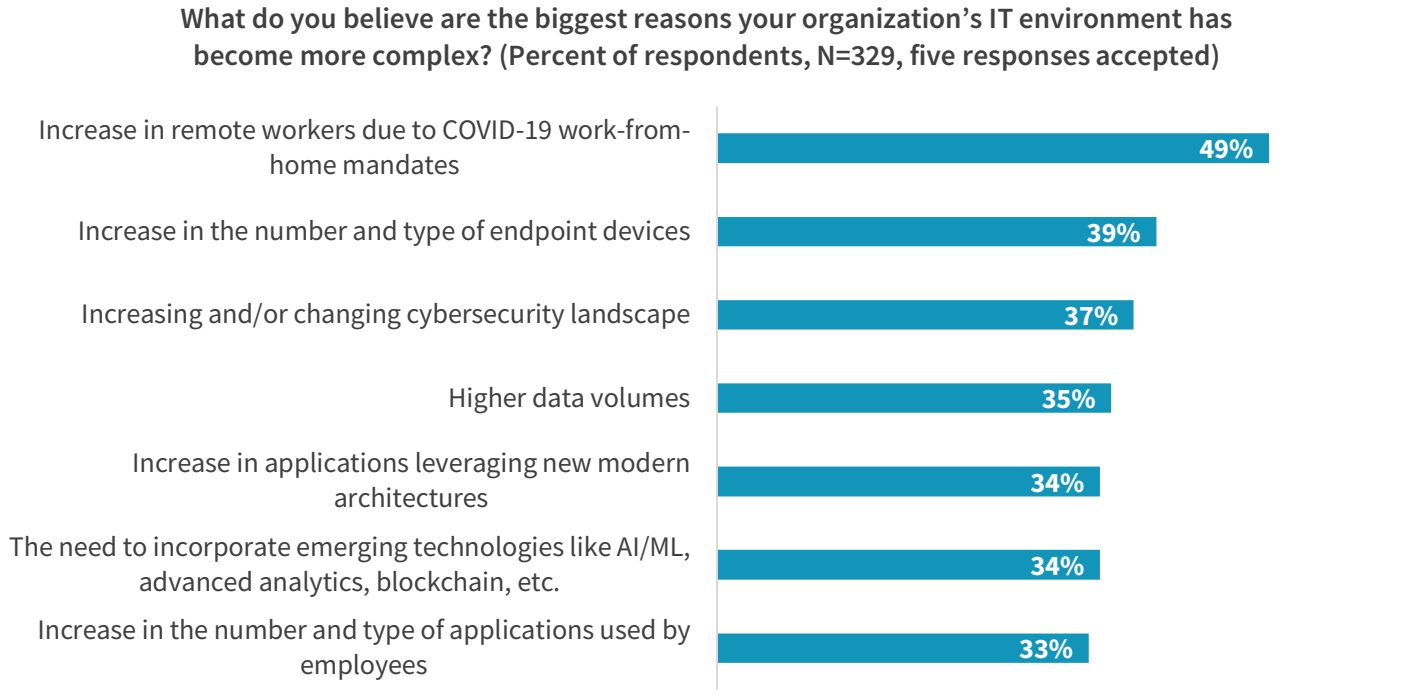
Introduction

This ESG Technical Validation documents our evaluation of Perimeter 81. We examined how this cloud-based service can help organizations to establish a zero trust network security posture without creating unnecessary network complexity or incurring unwanted capital and operational expenses.

Background

According to ESG research, 79% of survey respondents view their IT environments as equally or more complex than they were over two years ago.[1] While respondents cited the increase in remote workers due to COVID-19 work-from-home mandates (49%) as a top reason for this complexity, today's remote and hybrid work arrangements have contributed to other sources of complexity, particularly the increasing and/or changing cybersecurity landscape (37%) and the increase in the number and type of applications used by employees (33%, see Figure 1).

Figure 1. Top 7 Reasons for Complexity in IT Environment



Source: ESG, a division of TechTarget, Inc.

As organizations deal with a highly distributed and hybrid workforce, with applications originating either on-premises or from the public cloud (e.g., SaaS applications), the idea of a fixed network boundary no longer exists. Organizations can no longer rely only on backhauling traffic from every point that traffic enters an organization to a corporate data center via virtual private network (VPN) tunnels in order to screen and filter traffic. This approach to ensuring network security degrades overall performance, increases latency, and incurs unnecessary costs.

The lack of a fixed network perimeter also makes it challenging for organizations to easily secure their environments, as a dynamic attack surface now exists. Bad actors are increasing their attempts to compromise any organization's security, with ransomware becoming more of the norm.

[1] Source: ESG Research Report, *2022 Technology Spending Intentions Survey*, November 2021. All ESG research references and charts in this technical validation are from this research report.

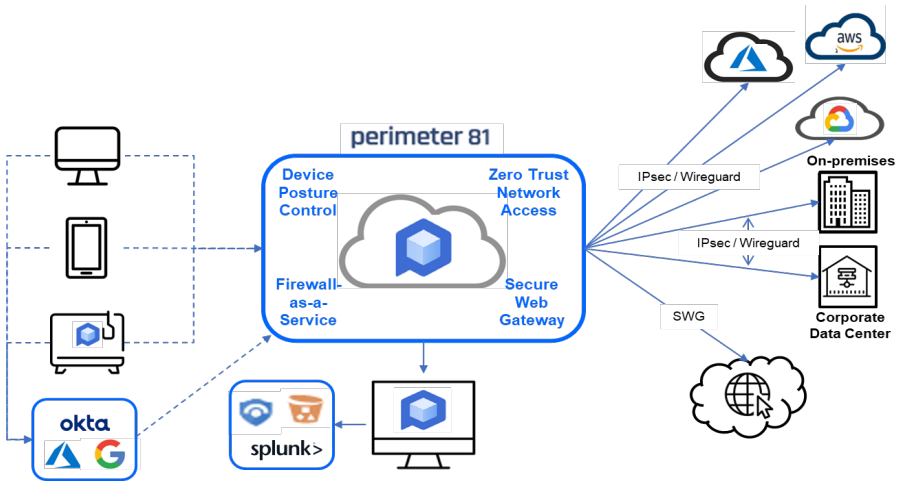
Traditionally, organizations have cobbled together multiple hardware and software-based products, as well as multiple monitoring tools, for maintaining an acceptable level of network security. However, using these disjointed products, with their separate interfaces, adds an additional layer of complexity that does not address all security gaps, leading to inefficient ways for identifying, isolating, and removing both known and unknown threats. Capital and operational expenses accrue unnecessarily, as the use of multiple security point products leads to manual and inefficient workflows.

Perimeter 81

Perimeter 81 is designed to secure any connection between end-users (regardless of their location) and any IT resources within an organization's hybrid cloud—public cloud resources, on-premises data centers, SaaS applications —and the public internet. This cloud-based managed service enables organizations to comprehensively secure their networks against a dynamic attack surface. Perimeter 81 delivers traffic inspection, monitoring, filtering, and prevention capabilities, removing the need for organizations to use multiple and disjointed hardware and software-based products, along with the traditional security monitoring tools.

To address the lack of a fixed network perimeter, organizations can use Perimeter 81 to securely connect users with select hybrid cloud resources via IPsec VPN or Wireguard tunnels. By using a microsegmentation approach, zero trust network access (ZTNA) is established, as end-users are connected only to those resources needed to complete their work. With Perimeter 81, organizations can decrease both the complexity, operational overhead, and risk associated with providing all users with blanket access to all IT resources using multiple point-to-point VPN tunnels (see Figure 2).

Figure 2. The Perimeter 81 Solution



Source: ESG, a division of TechTarget, Inc.

Perimeter 81 further helps an organization to establish a zero trust network security posture for every user session via the following capabilities:

- *Device posture control* - As a first line of defense, Perimeter 81 protects unauthorized devices from accessing the network by inspecting registered devices for items such as the presence of specific software (e.g., antivirus) to verify that the device meets the organization's defined requirements, especially when preventing events such as credential theft.
- *Firewall-as-a-service* - During a user session, network traffic is filtered based on security policy defined according to specific characteristics such as IP addresses, ports, authorized users, groups, locations, device types, and application-aware rules.
- *Secure web gateway* – To screen inbound traffic from the public internet, Perimeter 81 employs a URL filtering engine that categorizes requests into a set of predefined website types (e.g., financial, healthcare, adult content) and either

allows, blocks, or alerts users trying to access them according to company policy. This service also provides malware protection to prevent users from downloading malicious content onto their devices.

To simplify user access management, organizations can leverage third-party identity providers (IdPs), such as Okta. Instead of organizations tracking and updating access credentials to specific IT resources, Perimeter 81 enables users to gain access via existing IdP credentials.

With Perimeter 81, organizations can establish a comprehensive network security posture without spending excessive time and effort on evaluating, purchasing, testing, learning, and implementing multiple point products and monitoring tools. Regardless of size, organizations can experience shorter time to value, decrease overall capital and operation expenses, and lower overall risk to their network security.

ESG Technical Validation

ESG evaluated the Perimeter 81 service via remote demonstrations conducted at Perimeter 81's headquarters in Tel Aviv, Israel. We evaluated how Perimeter 81 can help organizations decrease network and operational complexity; reduce time to deploy, scale, and update their network security architecture; and gain end-to-end network visibility of their security posture. The demonstration utilized a production environment consisting of internal Perimeter 81 users located in the United States and Europe.

Decreasing Network and Operational Complexity

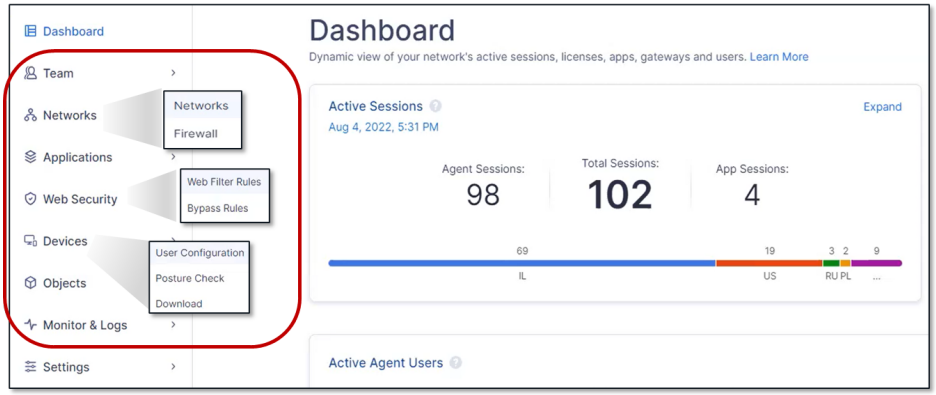
Building out and managing a network security architecture has traditionally been a do-it-yourself (DIY) effort. Organizations would need to evaluate, purchase, and learn how to configure and use multiple components—hardware and software products and their associated management systems and security monitoring tools. Spending time configuring multiple tools, as well as mastering the skills to manage them, ultimately makes it inefficient to bolster an organization's network security.

With the Perimeter 81 platform, organizations can configure, deploy, and manage a network security architecture via a single web-based console. This cloud-based service also enables security event monitoring and log data collection to alert organizations of security issues that require attention. By relying on a single unified platform, IT managers can increase their network security, monitor all user activity, and reduce configuration time and costs.

ESG Testing

We began our evaluation by navigating to the home page of the Perimeter 81 interface associated with the test environment. As noted in Figure 2, the Perimeter 81 service provides the firewall, web gateway, and device posture control capabilities for any virtual connection between the end-user and hybrid cloud resources. This "integration" is reflected in the menu shown in Figure 3. From this single interface, we could access all the necessary tools for organizations to configure a zero trust network security posture.

Figure 3. Securing Networks, Applications, and Devices via a Single Interface



Source: ESG, a division of TechTarget, Inc.

ESG noted that the need to work with multiple and disjointed security point products was eliminated. An administrator could configure, manage, and monitor its network architecture by navigating through these menus, without the need to work with additional third-party tools and interfaces. IT administrators also do not need to learn specific security skill sets associated with vendor-specific network, application, and device security products, thus minimizing any existing skills gap.

We also noted that Perimeter 81 can help to decrease network complexity. Organizations no longer need to deploy multiple products and tools to reinforce network security. The more network-related products that are deployed, the more complex the network is to operate and manage. With Perimeter 81, organizations only use one service to deploy a holistic network security architecture.

Why This Matters

Deploying and maintaining a traditional network security architecture becomes too complex when considering the multiple security products to be configured and deployed, the associated management systems to be learned, and the security monitoring tools to be used for detecting any potential threats and attacks.

ESG validated that Perimeter 81 removes this complexity by enabling organizations to architect, deploy, and monitor a network security infrastructure from a single interface via its menu-driven workflows. The need to work with multiple and disjointed components is eliminated.

Reduce Time to Deployment

The traditional way of building out an organization's network security architecture can easily last weeks or months. While this approach was acceptable when the network perimeter was fixed, it is not acceptable when users can be located anywhere in the world while having access to cloud-based resources over the public internet. The rise of distributed applications has also contributed to the lack of a fixed network security perimeter.

Establishing VPN tunnels for each individual user to any IT resource within an organization's hybrid cloud is impractical, costly, and difficult to achieve without causing unnecessary network complexity and, simultaneously, adding a huge amount of operational overhead. Excessive time spent on deployment decreases the time that an organization's network is secure from potential threats and attacks.

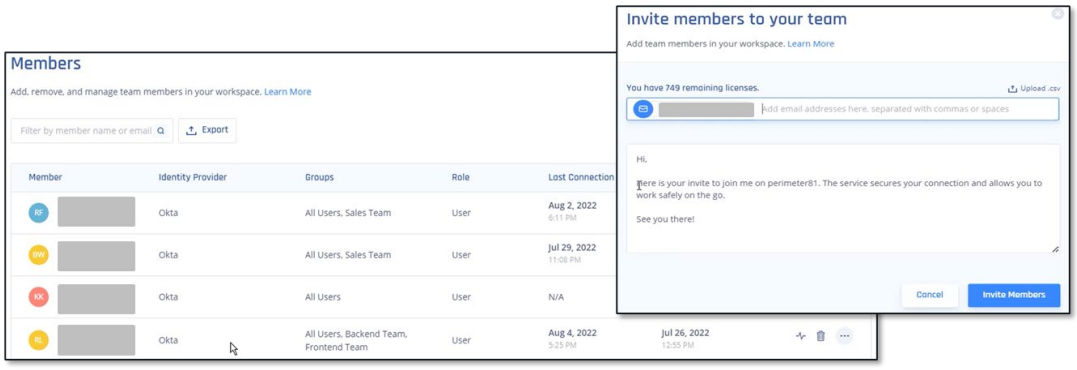
On the other hand, organizations can drastically reduce deployment time of a zero trust network security posture with Perimeter 81. By regulating how specific users access IT resources, while filtering both application and web traffic to remove both known and unknown threats, Perimeter 81 helps organizations to close security gaps with little delay.

ESG Testing

ESG first registered a new user and device with Perimeter 81 so that ZTNA could be established with any of the hybrid cloud resources in the test environment. From the ***Members*** page, we clicked on the "*Invite Members*" button that prompted Perimeter 81 to send an email to the device of a new member. The email contained instructions on how to install an agent onto the device, such as a desktop or mobile phone (Figure 4).

We noted that this approach can eliminate the time spent on configuring and issuing a device with the proper security settings to a new employee, helping to reduce operational overhead and expenses. (We should note that an IT administrator still has the option to install this agent onto multiple devices simultaneously.) ESG also observed how an existing member can be added to a group, simplifying how an organization determines the resources a group member can access and, more importantly, ensuring that security policies are applied consistently.

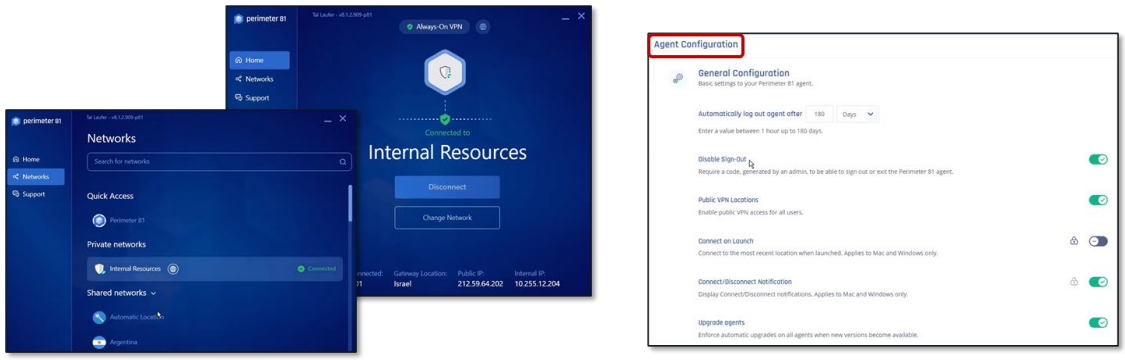
Figure 4. Securing Devices of New Organization Members



Source: ESG, a division of TechTarget, Inc.

Once the agent was installed (as shown on the left-hand side of Figure 5), ESG saw that a user does not need to perform any additional configuration. However, an administrator could choose to remotely configure agents (see right-hand side of Figure 5) to add or modify security measures as required, without the need to physically access the device.

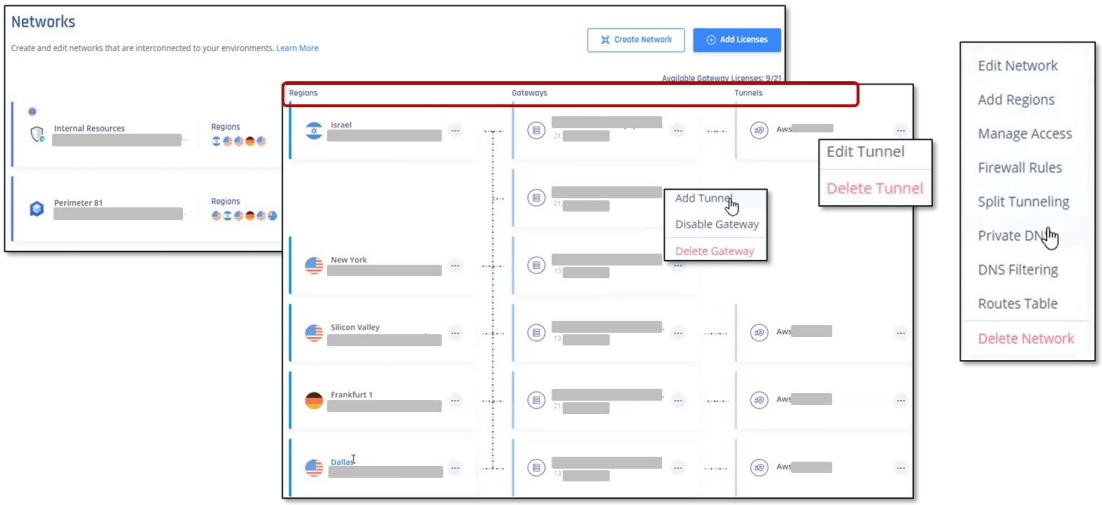
Figure 5. Implementation of Agent on User Device



Source: ESG, a division of TechTarget, Inc.

ESG then examined how Perimeter 81 can help organizations deploy their network security architecture by establishing the user-centric connections to hybrid cloud resources. On the ***Networks*** page (shown in Figure 6), we viewed how Perimeter 81 divided IT resources into "networks," a logical grouping or subset of resources that can be accessed. Networks were laid out from left to right, detailing the regions in which users were located, the Perimeter 81 gateways that were accessed, and the secure tunnels connecting to resources deployed in an AWS European region.

Figure 6. Representation of "Networks" by Perimeter 81



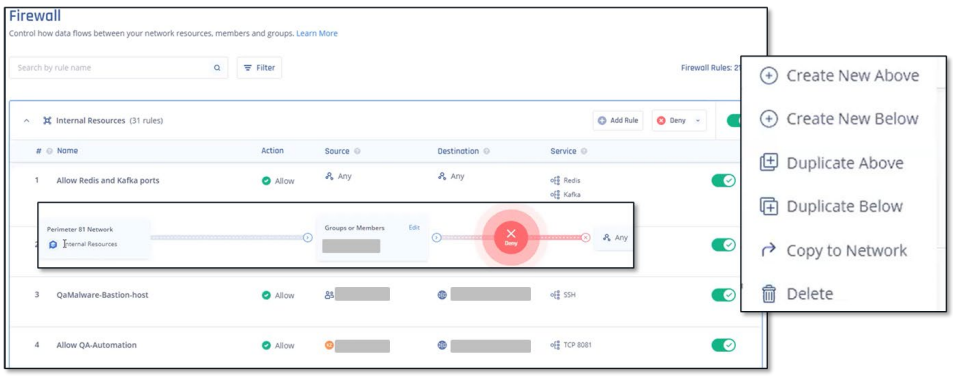
Source: ESG, a division of TechTarget, Inc.

We observed how an administrator could modify the VPN tunnels or gateways that connect specific users or user groups to an organization's IT resources, simply by using pop-up menus associated with specific line items. As shown in Figure 6, both gateways and tunnels could be modified to allow or deny access as security policies changed. We also noted that Perimeter 81 networks could be modified or deleted should organizations want to change how specific resources are grouped and accessed (e.g., adding regions in which new IT resources are operating).

As we examined how user-centric connections to specific IT resources were created, ESG observed that using Perimeter 81 to establish these connections is much simpler than deploying individual VPN tunnels for every user using multiple VPN servers and routers. Imagine the number of these components needing to be deployed throughout a hybrid cloud environment and the amount of time required for creating multiple tunnels. And should access policies for specific IT resources change, existing tunnels may need to be torn down and re-established for any given number of users. Without Perimeter 81, ESG saw how time and operational expenses can be wasted in setting up these tunnels, while leaving IT resources vulnerable to attack.

ESG then reviewed how an administrator can define how traffic is filtered for any user or user groups accessing the "networks" displayed in Figure 6. As shown in Figure 7, we could create new rules, duplicate existing rules to modify for additional use cases, or copy an existing rule to filter traffic in another network. Rules could also be arranged in order of importance as dictated by business requirements.

Figure 7. Managing Firewall Rules for Individual Users and User Groups

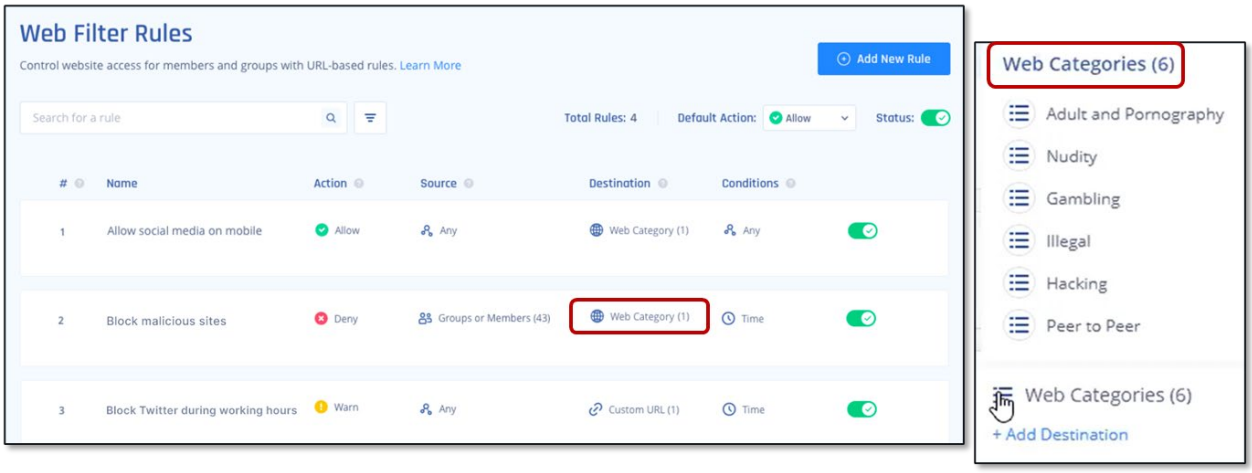


Source: ESG, a division of TechTarget, Inc.

ESG picked up on how Perimeter 81 eliminates the need to deploy, configure, and manage firewalls at multiple locations within the network. Since an administrator can use Perimeter 81 to configure and deploy rules allowing or blocking specific traffic, regardless of where traffic has originated, configuring and updating rules on individually deployed firewalls is unnecessary, saving both time and associated costs. More importantly, ESG noted the consistency maintained in creating and applying these firewall rules, thus minimizing the presence of security gaps.

Finally, ESG examined how Perimeter 81 simplifies the creation, deployment, and management of rules filtering web traffic. As shown in Figure 8, we used the ***Web Filter Rules*** page to input and modify rules governing traffic originating on the public internet, such as social media applications. Rules could be configured to allow or deny access or flash a warning should specific web traffic attempt to enter the network. We also saw how Perimeter 81 simplifies how rules are created, as they can be based on IP addresses, URLs, or web traffic categories (e.g., gaming, hacking).

Figure 8. Managing Web Traffic Filtering Rules



Source: ESG, a division of TechTarget, Inc.

Since these web traffic filtering rules apply regardless of where that traffic enters the network, ESG saw how Perimeter 81 eliminates the need to deploy multiple secure web gateway appliances. As we observed when creating and deploying firewall rules, ESG noted that organizations no longer need to spend the time and resources to install and configure gateway appliances throughout a network, avoiding more overhead and expenses.

Why This Matters

Protecting against network security threats and attacks is a 24/7 job. Any time spent on deploying, updating, and scaling a network security architecture leaves the organization vulnerable. Deployment time must be minimized.

ESG validated that the Perimeter 81 platform can dramatically reduce the time for organizations to deploy their network security resources. All required tasks to secure traffic from the network, application, and web traffic perspectives can be completed with a single interface, without the need to physically install hardware and software-based products or navigate multiple configuration tools. Security risk, as well as the related capital and operational expenses typically associated with deployment and configuration, are greatly minimized.

Establishing End-to-end Network Visibility

Maintaining a zero trust network security posture cannot be accomplished without full visibility into existing network connections between users and hybrid cloud resources. Using multiple tools and disjointed interfaces may provide

visibility, but not in an integrated way, thus potentially leaving room for blind spots and added risks. Also, navigating between these multiple tools wastes time that can be spent on detecting potential security issues as soon as they arise.

Because the Perimeter 81 platform delivers the tools needed to build out and deploy a zero trust network security architecture in one place, traffic data is already collected, aggregated, and processed in one place. Analyzing and presenting that data can be completed in real time for any connection.

ESG Testing

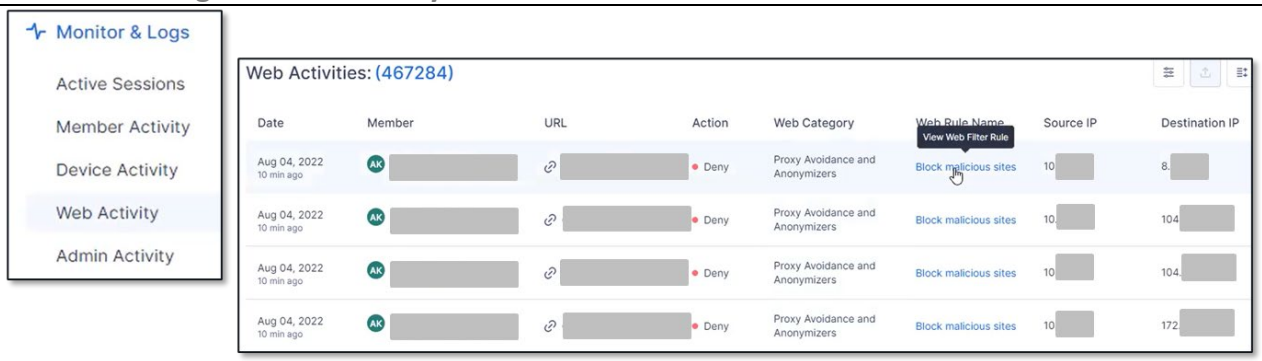
From the ***Dashboard*** view, ESG reviewed the metrics and charts that Perimeter 81 presents to help an administrator monitor network security. Along with metrics that track how an organization consumes the Perimeter 81 service, such as number of active user sessions, member licenses, and active gateways, Perimeter 81 tracks both the number of active sessions and total bandwidth consumed over time (see Figure 9). ESG found that these specific views could flag unusual network activity that may be related to suspicious behavior (e.g., a higher amount of user activity during off-work hours).

Figure 9. Monitoring Network User Activity over Time

Source: ESG, a division of TechTarget, Inc.

With Perimeter 81, ESG also saw how activity detail could be tracked from the user, device, and web traffic perspectives (see Figure 10). By providing an administrator with the ability to examine network activity at a granular level, ESG could see how Perimeter 81 provided comprehensive visibility so that time to detection and resolution decreases, thus minimizing overall exposure and risk.

Figure 10. Monitoring Network Activity over Time



Source: ESG, a division of TechTarget, Inc.

Since network activity could also be tracked by navigating through a single interface, ESG noted how Perimeter 81 can also decrease the time and effort spent on identifying suspicious behavior. The need for using multiple and disjointed monitoring tools can be eliminated, thus minimizing operational overhead and costs.

Why This Matters

Having "full" visibility means that an organization must be able to view, at any given time, how users connect to the organization's network. Ideally, organizations would not need to collect and aggregate traffic data from multiple tools and interfaces, as this can lead to visibility gaps. Navigating between multiple monitoring tools to identify suspicious behavior and the root cause can also prove to be inefficient and costly.

ESG validated that the Perimeter 81 platform provides end-to-end visibility for each active user session and the security network architecture as a whole. Specifically, we saw how organizations can monitor both high-level and granular activity (from the user, device, and web traffic perspectives) by navigating through Perimeter 81's single interface. Not only can time to identify suspicious activity decrease, but operational overhead and related costs can also be minimized, as the need to work with traditional, yet separate, monitoring tools can be eliminated.

The Bigger Truth

As applications become more distributed and transition to public cloud environments for both IaaS and SaaS, organizations face the daunting challenge of securing user access to their IT resources. With the lack of a fixed network perimeter, backhauling traffic to a corporate data center for security purposes is impractical and expensive. Now that the attack surface is fluid and dynamic, building out a zero trust network security posture becomes difficult when relying on the deployment of multiple hardware and software-based security point products throughout the network. Security gaps emerge while overall visibility is incomplete, leading to increased vulnerability.

The Perimeter 81 cloud-based service is designed to help organizations establish a zero trust network security posture in light of a dynamic network perimeter. By securely connecting users with specific IT resources—either located on-premises or in the public cloud—organizations can maintain a zero trust network security posture, regardless of where the users or IT resources are located. With this user-centric approach to security, organizations can apply security policies consistently at the user or user group level with Perimeter 81. Additional policies also secure an organization's network via device posture control and application and web traffic filtering.

Throughout our evaluation, ESG validated that the Perimeter 81 cloud-based service can help organizations to:

- Decrease both network and operational complexity by enabling organizations to architect, deploy, and monitor a network security infrastructure from a single interface. The need to work with multiple and disjointed security point products and monitoring tools is eliminated.
- Reduce time to deployment of a zero trust network security posture to minimize capital and operational expenses and, more importantly, overall security risk.
- Establish end-to-end visibility, as user activity and network traffic can be monitored at granular levels, thus reducing time to identification and isolation of suspicious behavior or threats.

ESG strongly believes that Perimeter 81 can drastically simplify how organizations can secure networks in light of a constantly evolving perimeter, with hybrid work arrangements and the continued use of distributed applications. If your organization is looking to bolster its network security without the typical overhead and costs associated with traditional network security architectures, then ESG suggests placing Perimeter 81 on your short list for evaluating security solutions.