Leveraging Existing Infrastructure to Enforce Zero Trust Security

In the cyber defense domain, traditional perimeter defense strategies use firewall devices to protect the enterprise network from the external internet. But as recent history has proven, resourceful adversaries can successfully break through perimeter defenses using social engineering and novel zero-day attacks.

Defenders have responded with a new approach: zero trust security, which assumes the adversary has already breached the perimeter. Internal devices and users are not to be trusted by default, just because of their location inside the network. The idea is to stop the lateral transmission of malware and ransomware inside the enterprise network after the inevitable perimeter breach.

To stop lateral movement, one could separate the internal environment into many granular network segments, each protected by a firewall device. By doing so, one could enforce policies to stop unauthorized traffic between the segments, while allowing valid business processes to proceed, thus preventing ransomware or malware from spreading unchecked throughout your critical systems.

But it would be prohibitively expensive to acquire and implement so many firewall devices. Likewise, it would be prohibitively complicated to manage the firewall rules configured on them to control the communications between the many new network segments.

The solution to this problem is to leverage the resources you already own. In fact, you already have all the firewalls you need—every windows operating system has either Windows defender or the newer Windows Filtering System. The Linux operating system kernel comes with the Netfilter firewall. These thousands of software firewalls already present in your enterprise environment can be used to define network micro-segments, and be policy enforcement points to prevent the propagation of unauthorized traffic.

The challenge is in management of these distributed software firewalls. Defining the right micro-segment policies and managing the firewall rules for that many operating system-based firewalls in a large enterprise would be daunting. The solution is to add a centralized zero trust policy engine and a unified administrator user interface which would allow you to:

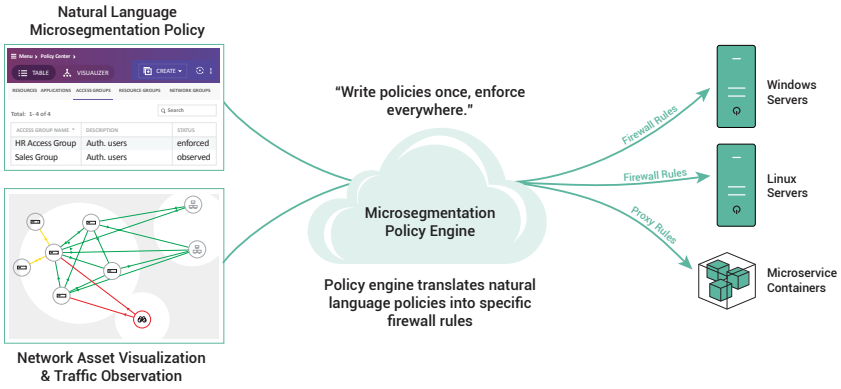
- Identify all the devices on your network and tag them with descriptive data for use in defining the correct microsegments.
- Define traffic policies for communication between microsegments in natural language, and then translate those policies into firewall rules in the required formats for the different operating system-based firewall versions which are present in your environment: also known as “write once, enforce everywhere.”
- Visualize network traffic and do an impact analysis of traffic policies before enforcing them. In this way you would not interfere with valid traffic that enables the important business processes of your organization.
- Control microsegment access policies for endpoints that are both on-campus and used by remote users, in the same administrative environment, so two separate sets of solutions and sets of policies need not be administered. This is becoming increasingly important in the new business paradigm of “work anywhere,”

where the bulk of users are remote or hybrid workers in a shared office environment. It is the confluence of secure encrypted network access (known as zero trust network access or ZTNA) with microsegmentation policy enforcement.

- Protect modern web applications which are architected using containerized microservices. Microservices communicate using application programming interfaces, so traffic policies cannot be enforced using IP addresses and ports as they are in traditional applications. Instead, the zero trust solution can use the orchestration tools and sidecar proxy technologies already in place in most microservice environments as enforcement points.

This incremental addition to your environment would multiply the value of the existing software firewalls already present in your systems. But as a caveat, the solution to centrally manage microsegment traffic policy should not introduce a new proprietary kernel-level software firewall. Any solution that alters the out-of-the-box Windows or Linux operating system introduces on-going complexity and headaches when OS upgrade and patching is performed. Furthermore, it compromises the overall idea of leveraging existing capabilities in your network infrastructure.

Centralized Management of Existing Operating System Firewalls



A solution to manage traffic between well-defined microsegments of the network inside the perimeter can successfully protect your critical systems and data from the specter of laterally spreading malware and ransomware. It can also stop the unauthorized movement of enterprise data. Adding a solution that delivers zero trust security by leveraging the hundreds (or thousands) of Windows and Linux software firewalls already present in your enterprise will give you the added benefit of multiplying the value of your existing infrastructure investments.

Simplifying Your Journey to Zero-Trust Architecture

ColorTokens is a leader in delivering innovative and award-winning zero-trust cyber security technology solutions such as network micro-segmentation, endpoint hardening and whitelisting, cloud and container security, and zero-trust network access. ColorTokens is a US corporation headquartered in Silicon Valley, and has approximately 400 employees world-wide, with offices in the United States, the United Kingdom, the Middle East, and India serving a diverse client base in both the public and private sector. For more information, please visit **colortokens.com.**