Critical Characteristics of Effective Zero Trust Microsegmentation Tagging

Zero trust microsegmentation today represents a crucial security initiative for many organizations, and tagging is a critical piece of understanding and managing the networked infrastructure. "Tags" are descriptive labels that, when applied effectively to IT resources, are mandatory elements of a microsegmentation project, and can be the difference between a network that is secure and one that is vulnerable to cyberattacks.

Tags: the Basis for Achieving Zero Trust

Tagging is a process whereby users add descriptive metadata (tags) to their IT systems, applications, and other critical resources, for understanding the organization and its interconnected ecosystem. A tag consists of two components: a key and a value to identify a resource. The key describes the type of tag: for instance, the key could represent the "application," "role," or "environment," while values could be "CRM," "web," or "acceptance." Tags are uniquely defined by any combination of key + value pair.

Within a micro-segmented infrastructure, tags are vital in identifying and describing assets, containers, users, applications, and relationships. This functionality enables the organization to parse its IT assets and more accurately group them into zones of least privilege access controlling end-users' application access and/or the communications among application resources.

Only when tags are applied correctly can enterprise-wide visibility be improved, security policies be appropriately assigned, and assets managed accordingly.

More Tag Options = Improved Security

In order to adequately align devices to applications to business functions, most enterprises require the ability to tag or label these critical assets at the most granular level. However, not all vendors provide flexible tagging options, a limitation that leaves IT assets without crucial details associated with the roles these systems play, the flow of IP traffic they funnel, and their exposure to the outside world. Limits in tag types cause a lack of visibility in the network and the inability to comprehensively deploy security policies across critical systems and assets, resulting in gaps in the organization's security posture that could allow attackers to exploit them. Critical characteristics and direct benefits of having flexible tagging options include increased visualization (mapping), effective policy deployment (enforcement), and asset management (control).

Increased Network Visualization

Visualization of network and IT device interactions serve multiple purposes: clarifies acceptable and intended patterns that follow the least privileged principle, guides the setting of allowable pattern variances, and creates a baseline from which to detect and track potentially malicious pattern deviations. Tags are vital components for achieving granular network visualization by enabling more detailed information about an asset or system. Examples of this are: what kind of asset is it; what is its function; what systems, applications or other assets does it communicate with; what group is it a part of (or should be); are there dependencies associated with it; is it exposed to the outside world, etc. Utilizing multiple numbers of tag types, a more granular graphic diagram, or map, of the key components becomes increasingly more visible and easily understood and managed.

While not all vendors offer multiple tagging options, custom tags deliver more in-depth layers of identification beyond the standard ones of "application," "roles," and "assets," to include business and organization layers that deliver more granular descriptors, like business unit, department, or location.

Tagging can provide insights into the assets themselves, depending on how they are labeled, to assist in properly segmenting them into different trust zones and assigning appropriate access privileges.

Effective Policy Deployment and Enforcement

Automated guidance in policy creation and point-and-click functionality based on the system or application's business logic serves multiple objectives – it adds meaningful context to application security policies, and it assists in identifying paths of potential lateral movement among applications that share common resources. This is more effective if the traffic flows are graphically displayed in different colors representing the security policy status, i.e., what's allowed/not allowed. This gives the customer quick insights for making adjustments to the policies easily and accurately.

Since tags are the foundation of policy deployment and are necessary for enforcement, having multiple tagging options available offers the organization flexibility and scalability, as there is no limitation on the number of policies per workload. Applying tags to any asset makes policy definition simple to implement and can even be extended to users with remote access.

Conclusion

When it comes to zero trust microsegmentation, leveraging flexible, multi-option tags is a critical component. These tags can be used to identify and group together assets based on a wide range of criteria such as business unit, the functional area, environment type (production/testing), server type (web/ database), or any other metadata that is important for the organization. Once tagged, these groups then become small security zones that can be monitored and secured with granular policies.

When it comes to tagging, organizations should consider the following calls-to-action:

1 Invest in a solution that offers robust and flexible tagging capabilities that enable detailed descriptions of assets, visibility of the network, and granular enforcement policies tailored to specific requirements.

2 Leverage as many tags as needed to then group assets based on relevance to the organization such as business units, functional areas, environments, server types, and other criteria.

3 Decide which teams, business units, environments, and applications will be needed for tagging strategy success. This generates precise, focused tags that have buy-in from the entire team and answer critical questions.