algosec

Secure application connectivity.
Anywhere.

Enhancing Zero Trust network security with AlgoSec's application-centric approach

An AlgoSec whitepaper

In today's interconnected and rapidly evolving business landscape, securing data and systems requires more than traditional security models can offer. As organizations embrace digital transformation, applications become critical for business operations, but they also introduce new complexities and security challenges. The **Zero Trust** model, built on the principle of "never trust, always verify," shifts away from relying solely on perimeter defenses. It assumes threats can emerge from any point, whether inside or outside the network.

As networks grow and hybrid environments span on-premises and cloud infrastructures, attack surfaces expand, making it harder to ensure security. This whitepaper explores how organizations can simplify Zero Trust implementation through **application-based segmentation**, and how AlgoSec's solutions help facilitate this transformation.

Why Zero Trust?

Digital transformation is reshaping industries, with applications at its core. These applications connect businesses to customers and power innovative services. However, as the number of applications grows, so does the complexity of networks, along with an increase in security risks. In hybrid environments, where applications and data flow freely across different infrastructures, traditional security models prove inadequate. The risks posed by security breaches — such as ransomware attacks, data theft, and service disruptions — can damage a company's reputation and bottom line.

Zero Trust offers a more effective approach by securing every layer of the network, limiting access, and continuously verifying trust.

The core principles of Zero Trust

Zero Trust is based on three foundational principles:

1. **Verify explicitly:** Every access request is authenticated and authorized based on all available data, such as user identity, location, device health, and workload context.
2. **Use least privilege access:** Access is granted with the minimum permissions necessary for users or applications to perform their tasks, reducing exposure to attacks.
3. **Assume breach:** The network is treated as compromised by default, and segmentation is used to contain threats, limiting lateral movement within the network.

Network segmentation is a core aspect of implementing Zero Trust, as it helps isolate different parts of the network, limiting the potential spread of attacks. However, despite its importance, segmentation poses significant challenges for many organizations.

Challenges with network segmentation

While segmentation is a fundamental element of Zero Trust, organizations often face difficulties in its implementation. According to a recent survey by AlgoSec, only 5% of companies have fully deployed network segmentation, while 75% struggle with enforcement. The main challenges include:

- **Unclear objectives:** Organizations may lack clarity on how segmentation aligns with broader business goals, leading to misaligned priorities.
- **Limited visibility:** Without comprehensive insight into traffic flows, devices, and applications, identifying the right segmentation boundaries is challenging.
- **Complex infrastructure:** Hybrid networks incorporating firewalls, cloud security, and micro-segmentation solutions complicate segmentation efforts.
- **Lack of automation:** Manually configuring segmentation policies is time-consuming and prone to errors, especially across large, hybrid networks.

Application-based segmentation: a more effective approach

AlgoSec's **application-centric approach** to network segmentation overcomes these challenges by focusing on securing application connectivity rather than just the infrastructure. This shift provides deeper visibility into application traffic patterns and enables more precise, automated security controls.

- **Application discovery and visibility:** AlgoSec provides a comprehensive view of application traffic flows, enabling organizations to map how applications communicate across the network. This visibility is critical for identifying optimal segmentation points.
- **Simplified policy management:** AlgoSec automates the creation and enforcement of security policies based on discovered application flows. This ensures consistent, reliable security controls across hybrid environments.
- **Automated change management:** AlgoSec translates application connectivity into precise firewall security controls, minimizing the risk of misconfigurations and ensuring that segmentation policies are maintained over time.

Building Zero Trust with AlgoSec

AlgoSec's platform offers comprehensive tools that enable organizations to build and maintain effective Zero Trust architectures:

- **Firewall management:** AlgoSec centralizes firewall policy management across on-premises, cloud, and hybrid environments, automating security enforcement and ensuring consistent Zero Trust policies.
- **Micro-segmentation:** AlgoSec helps organizations design micro-segmentation strategies aligned with application connectivity needs. By visualizing network traffic at both the macro and micro levels, AlgoSec ensures that segmentation policies enhance security without disrupting business processes.
- **Secure access service edge (SASE):** AlgoSec's application-centric view complements SASE architecture by protecting application connectivity across any infrastructure. This unified approach ensures consistent policy enforcement and application of Zero Trust principles.
- **Cloud security:** In multi-cloud environments, AlgoSec provides centralized visibility and management of security policies, maintaining consistent Zero Trust controls across cloud platforms.

The benefits of application-centric segmentation

An application-based approach to Zero Trust segmentation offers significant advantages:

- **Limit breach impact:** Segmentation confines breaches to specific areas, reducing the extent of damage.
- **Strengthen security posture:** : Smaller, well-defined segments with specific security controls offer stronger protection for critical assets.
- **Reduce lateral movement:** Segmented networks present attackers with greater barriers to moving laterally, containing potential threats.
- **Simplify compliance:** Isolating sensitive data within specific segments makes it easier to meet regulatory requirements.
- **Enhance operational efficiency:** Proper segmentation reduces network congestion, optimizes resource usage, and simplifies troubleshooting, ensuring continuous protection for business-critical applications.

Macro and micro segmentation: a comprehensive defense

While micro-segmentation offers granular control, macro-segmentation — dividing larger network areas such as internal and external zones — provides additional protection. Combining both strategies enhances security by limiting exposure to broad attacks while ensuring precise control over critical segments of the network.

Macro-segmentation: Separating larger parts of the network limits exposure to attacks, ensuring that different zones, such as sensitive data or regulated systems, are isolated.

Micro-segmentation: This fine-grained approach restricts access at the individual application or workload level, further reducing risk.

By adopting both strategies, organizations build a stronger, more resilient network defense.

How AlgoSec supports Zero Trust network segmentation

AlgoSec's application-centric Zero Trust solution simplifies segmentation and enhances security across hybrid networks by:

- **Visualizing application connectivity:** Providing end-to-end visibility into how applications interact within the network.
- **Automating connectivity changes:** AlgoSec automates security changes based on Zero Trust principles, ensuring that policies adapt to evolving network conditions.
- **Mitigating risk:** Continuously identifying and mitigating risks within segmented network areas, protecting business-critical applications.

Conclusion

As businesses expand and evolve, the need for robust, scalable security solutions becomes paramount. **Zero Trust**, with its focus on continuous verification and network segmentation, offers a proven strategy for reducing risks. AlgoSec's application-centric approach simplifies this process by providing automation, visibility, and the ability to manage both micro and macro-segmentation effectively.

By leveraging AlgoSec's platform, organizations can implement and maintain an efficient, secure, and resilient Zero Trust architecture — ensuring continuous protection for business-critical applications while enhancing overall operational efficiency.

algosec

AlgoSec.com