lokblok

toughnet

Toughnet provides hardened, secure networking connectivity for your users and applications

WHAT IS IT?

Toughnet is an ultra-secure Zero Trust Network Access (ZTNA) integrated within the Toughbrowser application, which utilizes the Toughkey HSM to validate and authenticate endpoints.

WHAT DOES IT DO?

Lokblok Toughnet ensures highly secure connectivity integrated into individual applications (rather than the whole platform) through identity-bound AppWANs (Application Specific Wide Area Network) using logical isolation, least-privileged-access and application micro-segmented connectivity for superior data protection and granular control. Micro-segmented connectivity is a network architecture approach that divides a network into small, isolated segments to increase security and control over network traffic.

Toughnet implements microsegmentation at the app-level. Each app can only access its policy-permitted resources.

What does Toughnet mean for web applications and services? Close all open inbound firewall ports. No exceptions, no whitelisted IPs. Replace 100s of firewall ACLs with one inbound firewall rule: deny-all.

What does it mean for the edge? Application traffic not just secured from end to end but also from application to application.

Under the hood, the edge device generates a unique identity and certificate from the Toughkey hardware security module which in turn serves as a security ignition key to provide authentication before allowing the application specific connections – i.e., Lokblok Toughnet does not permit any data to flow until it has explicitly identified, authenticated and authorized from Toughkey providing maximum protection for the data and metadata.

Nothing gets on Toughnet without an X.509 certificate based identity and authentication. Toughnet supports automated enrollment, PKI and certificate renewals. Toughkey, a Hardware Root of Trust (HRT), stores and protects your X.509 credential, which is much more difficult to steal or hijack than passwords, SMS codes, etc (and the X.509 can be paired with other MFA solutions for additional layers). Lokblok Toughnet does not permit any data to flow until it has explicitly identified, authenticated and authorized from Toughkey moving policy enforcement all the way back to the initiation of the session.

Toughnet supports mutual TLS (mTLS), not just for ZTNA or compliance requirements, but because it is far more secure. mTLS immediately weeds out unwanted traffic by ensuring only authenticated clients can communicate over Toughnet. Toughet provides mTLS in all directions (east-west as well as north-south), controlled from one platform, across all edges and clouds.

All services remain dark, invisible on the internet, until secure authenticated is completed in both directions.

Lokblok Zero Trust Ecosystem

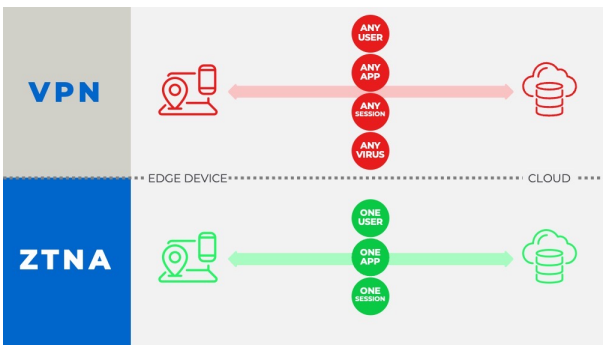
LOKBLOK TOUGHNET HIGHLIGHTS:

- The Lokblok Toughbrowser whitelists the Toughnet application to be the gatekeeper to all approved applications.
- The Lokblok Toughkey device generates immutable identity certificates that are transmitted and exchanged throughout the ZTN components.
- The Lokblok Toughkey and Toughnet platform sets up a highly secure, least privilege access connection from the device back to the application residing in any combination of public and private clouds.
- Lokblok Toughnet is always unknown (dark) to the public Internet (no publicly facing IP address) until an application is ready to transfer data.

WHY USE TOUGHNET?

Everyone knows the importance of securing network traffic; it doesn't need spelling out. So why wouldn't you want to implement the strongest security for your network? It's not just your users, but even your application services that communicate over the web, which even if the traffic is sent via a VPN, is still vulnerable to attack.

VPNs create a secure tunnel between two endpoints, but if one endpoint is compromised, the entire network can be vulnerable to attack. For example, if a user's computer is infected with malware, the VPN could allow the malware to spread to the corporate network. If a VPN is not configured correctly or uses weak encryption, it can also be vulnerable to eavesdropping, man-in-the-middle attacks, and other security breaches.



VPN VS. ZTNA Comparison

VPNs are often marketed as a complete security solution, but they only encrypt traffic between two endpoints. This means that any other traffic on the network, such as application data, email, instant messaging, or file transfers, may still be vulnerable to attack. Additionally, VPNs do not provide granular access controls, which can allow unauthorized users to access sensitive information.

The Toughnet Zero Trust Network is more secure: It assumes that all network traffic is untrusted and enforces strict access controls. Toughnet combines a variety of security measures, including HSM rooted identity and access management, multi-factor authentication, network segmentation, and encryption, to ensure that only authorized users and devices can access sensitive information. This makes it much more difficult for attackers to compromise the network.

TECHNICAL SPECIFICATION

Multi-Factor Authentication
Identify based authorization
Encrypted communications between endpoints
Micro-segmentation of application and resources

SUMMARY

By using Lokblok Toughnet combined with Toughkey, organizations can ensure that their data in motion is protected from potential security breaches and unauthorized access, making it an ideal and effective solution for securely transporting application data between services and servers over the internet.