BLOCK ARMOUR

CASE STUDY

How Block Armour helped a leading telcom provider in Indonesia to enable Zero Trust based Unified Secure Access to IT systems

THE CHALLENGE

Our client is a well-known Indonesian telecommunication services provider. It is an internet service provider and CDMA cellular operator. With around 10,000 employees spread across Indonesia, it has one of the largest IT infrastructures distributed across multiple locations.

Enabling access to the OSS/BSS systems and other critical applications for such a large workforce during the pandemic was difficult, and the organization was unprepared for the sudden transition from an in-office connectivity to a remote working environment. As a result, the organization found itself in an extremely difficult situation, with no precedent for providing secure and compliant access to staff working from home. Moreover, they also wanted to enforce robust access control for internal workforce accessing from LAN environment after appropriate endpoint posture evaluation. Thus the organization wanted a unified secure access solution which permits only compliant and authorized devices to securely access authorized internal applications locally and remotely.

MAJOR CONCERNS

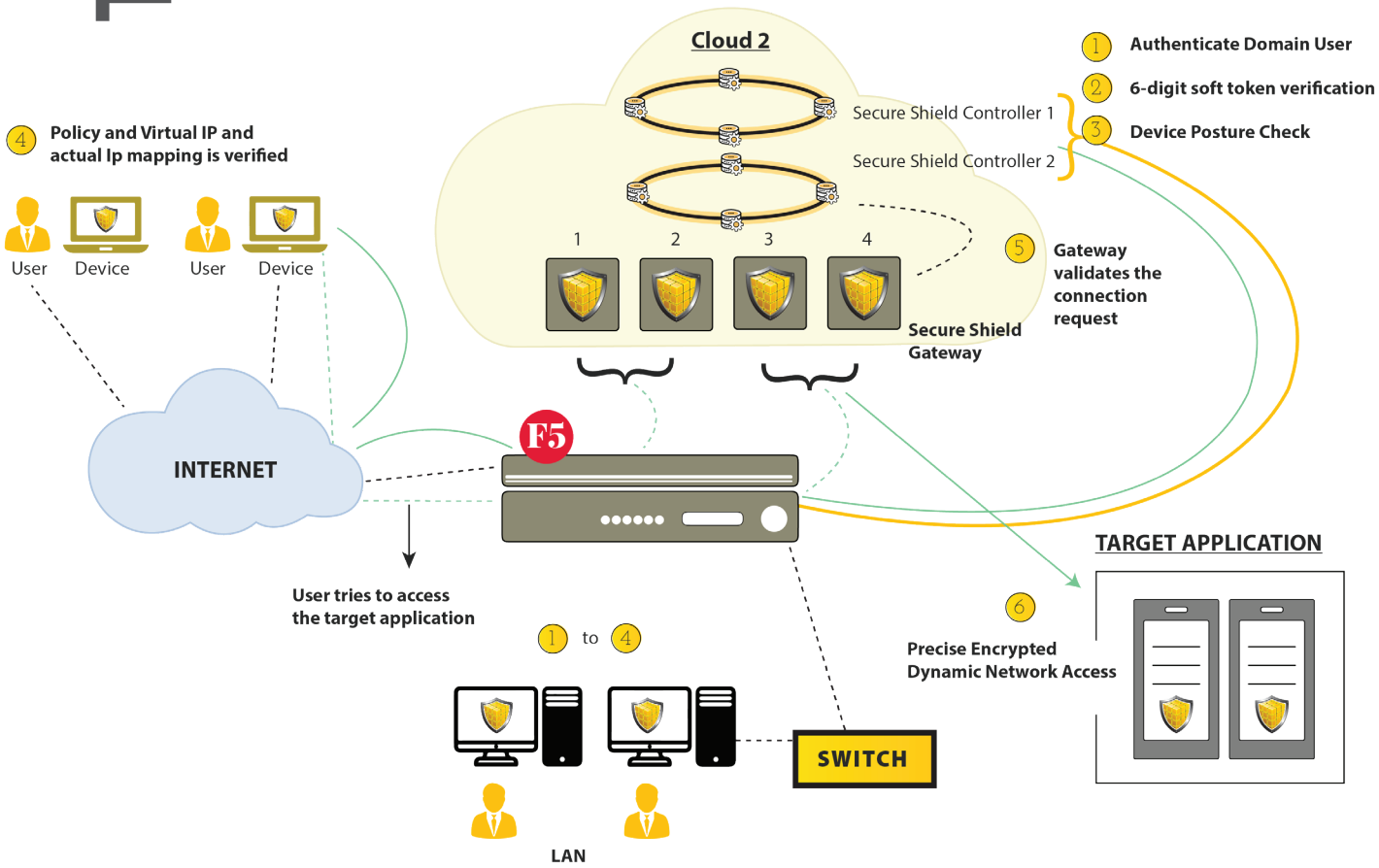
The issues faced by our client were:

- Lack of a unified solution that allows secure access to distributed applications for all employees and contract workers working from home.
- Inability to implement a pre-access device security posture check for the distributed users seeking remote access.
- Lack of proper security measures on personal devices being used to connect to IT systems
- Inability to ensure a micro-segmented access to critical applications based on authorization.
- High risk of malware and ransomware attacks via legacy IPSec VPN tunnel architectures.

THE SOLUTION

Block Armour implemented its Secure Shield solution that provides identity based unified secure access to critical applications from internal and remote networks. The solution is robustly designed using a unique combination of Zero Trust Network Access principles, Software Defined Perimeter (SDP) architecture, and private permissioned Blockchain technology. This organization leveraged the secure remote access capabilities of the solution that provides maximum security during access to critical enterprise systems by ensuring:

- Strong Multi-factor Authentication of users and their endpoint devices,
- Security posture validation of endpoint device prior to access.
- Invisibility of application resources on the network.
- Centralized management of all application access requirements across datacenters.
- Policy based micro-segmented access to critical application resources .
- RSA 4096 bit encryption enabled TLS channel for secure access between internet based endpoint and internal applications.



The Secure Shield Controllers and Secure Shield Gateways are configured in redundancy to accommodate 5000 users to securely access 100 target resources or applications.

The Secure Shield Solution ensured that both the user and the device were validated before giving access to applications. It contains a built-in soft token-based MFA system for added security.

In addition, the solution's Device Posture Check also ensured that only compliant endpoints were authenticated. Furthermore, the micro-segmentation functionality of the system also ensured that only explicitly authorized user and device pairs were permitted access. In this manner, our solution prevents lateral movement by cybercriminals to gain access and exfiltrate sensitive data. Since the Secure Shield solution only provides micro-segmented access to business traffic, all the non-productive traffic originating from personal devices never reaches the corporate network, thus, eliminating corporate network traffic congestion and providing better performance for accessing business applications remotely.

Using Secure Shield, the customer was able to restrict the access to applications only from an authorized user and device pairs reducing the overall attack surface and controlling the access outside of the organization's perimeter. The organization also had visibility into the level of access its employees had and were able to make necessary adjustments as per the requirements.

Secure Shield's pre-access Device Posture Check capability at the end-point ensures that only compliant devices are authorized to access critical applications. This ensures better ROI compared to the traditional NAC solutions that require costly network re-architecture and upgrades. Moreover, the traditional NAC solutions work only in corporate LAN environments and do not support a remote access use case.

With these security measures in place, the Block Armour Secure Shield powered Remote Access solution helped the organization to quickly enable secure access with enhanced security, thereby empowering teams of remote workers without sacrificing security or productivity. The solution also enabled the organization to provide employees with granular, micro-segmented network access to business applications. An added advantage of this solution is that the same security capabilities are offered to the users based on their identity and not their IP. This ensures that in a post pandemic Flexi-working scenario the same security was available to users whether they were in office or working from home.

Block Armour also built certain custom capabilities according to the customer's requirements:

- A command line installation script was provided so that the Secure Shield Agent can be rolled-out via the organization's desktop management solution to the large user base smoothly.
- DNS resolution related features were added to comply and deliver as per the regional government compliance requirements.

BENEFITS OF THE SOLUTION

The customer rapidly deployed the solution for 5000 users to allow the employees to access the company's target applications securely and efficiently from home. Different device posture check policies were created and assigned to devices to ensure compliance. Block Armour has enabled secure access with minimal architectural changes at the customer's location.

With Secure Shield, we were able to address the customer challenges and deliver the following benefits:

1. Providing secure remote access from authorized users and devices and eliminating the risk of rogue individuals and systems connecting to the corporate network.
2. Reducing the attack surface while still enabling access over the Internet to its employees
3. Preventing the risk of malware infections and lateral movement from personal devices as opposed to legacy IPSec VPN based access.
4. Inbuilt Multi-factor Authentication and Device Posture Check capability for users connecting both inside the corporate network and from outside the network perimeter.
5. Ensuring precise and dynamic encrypted channel access to critical business applications of the organization compared to the risky tunnel based approach of legacy IPsec VPN.
6. Ease of deployment and centralized administration of access requirements.
7. Simultaneous access to application resources hosted in multiple data centers.

Email: info@blockarmour.com

Website: www.blockarmour.com

Linkedin: https://www.linkedin.com/company/block-armour/

Twitter: https://twitter.com/BlockArmour