Trout

Overlay Demilitarized LAN - Memo

A new approach to Industrial Networks Security

Overview

The foundational BeyondCorp whitepaper, published in 2014, started with an observation: “Virtually every company today uses firewalls to enforce perimeter security. However, this security model is problematic because, when that perimeter is breached, an attacker has relatively easy access to a company’s privileged intranet.” Over the past decade, zero-trust principles have seen significant adoption in IT and DevOps sectors, but their implementation in industrial networks has been slower and more challenging.

Industrial networks struggle with zero-trust adoption due to limited controls over end assets - often controlled by vendors - and the overall heavy cost to change a costly physical network topology. But as digital transformation demands increased connectivity, both on-premise and remote, industrial networks are put under unprecedented levels of pressure. A pressure that traditional security tools like firewalls and VLANs cannot adequately solve for.

Trout believes a different approach is needed. We propose to start from the assumption that industrial networks should be inherently viewed as insecure (Zero Trust) and advocate for an approach based on the concept of a Demilitarized LAN (DLAN) Overlay.

Introduction

From the early days of IT, security models have distinguished between external (risky) and internal (trusted) environments, using perimeter security to protect internal resources. The castle and moat analogy has been prevalent, with perimeter defense protecting the valuable core.

In industrial settings, digitalization has reached little by little operational assets (also referred as Operational Technology (OT)). Cautious of both the importance of OT assets on the core business operation of the company, and the increased connectivity of their IT footprint, industrial companies have traditionally segmented their network into respective zones. To enforce these zones, network teams have primarily relied on VLAN (Virtual LANs), to categorize generic categories of equipments: Admin, IT, OT, Guest, DMZ, and Untrusted OT (e.g., cameras), and fronted with a perimeter firewall.

VLAN-based segmentation has been accepted as a hard fact to implement security in industrial networks, and should be challenged when used alone. VLAN is a Layer 2 (L2) concept, designed to allow inter-machine communication by abstracting their physical connection. VLANS are not designed to enforce access control policies across a set of devices.

A robust factory network should be designed under the assumption that one asset has been compromised, and build a topology based on this assumption. Defining an OT VLAN fails to achieve this.

Trout

Principles behind Overlay Demilitarized LANs

The Overlay Demilitarized LANs approach is a new model, offering a scalable transition to secure industrial networks. It is underpinned by five principles:

Microsegmentation

Reduce network segment size to the minimal number of assets (ideally only one!) that need to talk to each other without enforcing security controls, defined as a Demilitarized LAN (DLAN)

Encrypted Traffic

Front every DLAN with a proxy and route traffic between DLANs or to the Internet through this proxy, with protocol break capacities to enforce granular controls and get visibility.

Authenticated Communications

On one end, leverage client certificates tied to the machines to authenticate assets and ensure end-to-end encryption. On the other, enforce user authentication via existing authentication mechanisms (OIDC) or new ones (HTTP Knocking).

Network overlay

Deploy a virtual network that very closely resembles the current topology, although within a private DNS space, allowing a seamless transition from current network setups to the more secured, zero-trust and proxied connectivity over time.

Decentralized Firewalls

Configure asset firewalls to only accept proxied-traffic, allowing the network overlay to become the topology of the DLAN, and enforcing the proxy benefits to the asset

These five principles are designed to answer a zero-trust environment. By applying them across multiple cooperating components, industrial network teams are able to deploy best-in-class and agile connectivity.

Components of an Overlay Demilitarized LAN

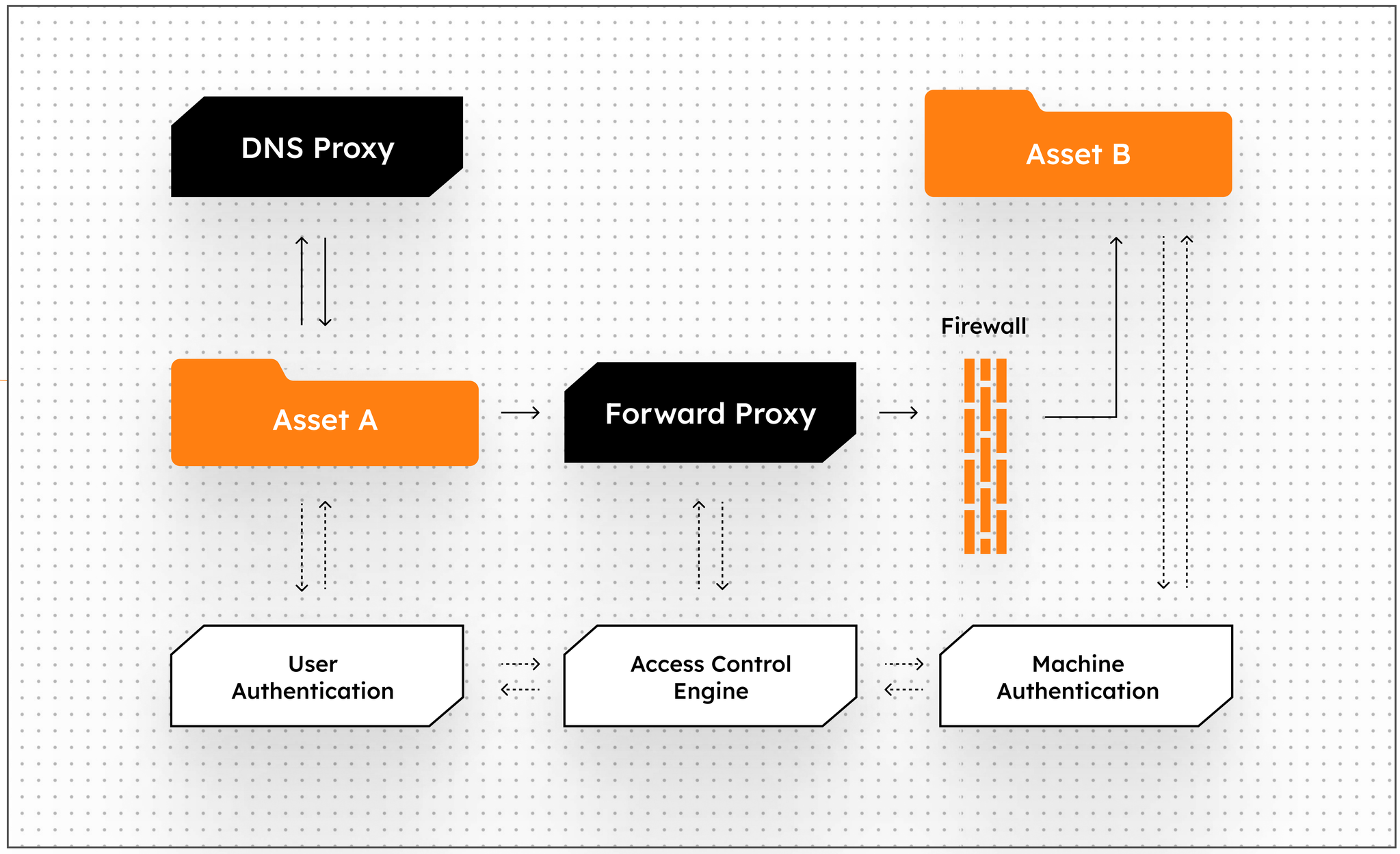


Figure 1 ODLAN components

01 Securely Identifying the Device

Device Identity

To ensure the identity of machines within the network, ODLAN uses client certificates. Each machine is issued a unique certificate by a trusted Certificate Authority (CA). When a machine attempts to communicate with the proxy, it presents its certificate. The proxy then validates this certificate against the CA's records and applies the relevant access logic. This method offers increased protection compared to Layer 2 (MAC address) and Layer 3 (IP address) identification, which are susceptible to spoofing.

Device Certificate Management

A successful ODLAN implementation includes a central system to issue and manage machine certificates over time. Managing certificates securely can be challenging for many industrial organizations, often hindering the adoption of advanced security mechanisms. The Device Certificate Management system must ensure timely refreshes and provide the capability to revoke certificates as needed.

02 Securely Identifying the User

User Certificates

Modern desktop environments (such as Windows Hello for Business) provide a strong, biometric-based authentication mechanism linked with SSL certificates. On those stations, upgrading to a DLAN environment is fully transparent.

OIDC Authentication

Authentication of users is based on OpenID Connect (OIDC) mechanisms. The proxy, running a web server, resolves the identities of users and applies the relevant permissions to the traffic they initiate on the other leg. OIDC is favored over SAML due to its versatility and performance enhancements in comparison to SAML.

HTTP Knocking

For traffic that is not compatible with OIDC, ODLAN provides HTTP knocking authentication. This method allows users to authenticate via a web interface, similar to guest Wi-Fi access in hotels. HTTP knocking serves as a fallback option when a federated authentication system is not available, ensuring secure access control coverage.

Access Control Engine

The ODLAN access control engine integrates with the above authentication mechanisms, enriching them with additional information such as machine state, time and location of access, and communication protocols. This allows IT teams to define use cases matching the reality of the business, using these comprehensive criteria to enforce permissions.

03 Building a Network Overlay

DLAN Namespace

In an Overlay Demilitarized LAN (ODLAN), users can associate a URL with a DLAN, enabling access to assets within the DLAN via a URL prefix. URLs offer a friendly method for users to comprehend and navigate the network topology. For example, users transition from accessing assets via an IP address like 172.55.44.33 to a more descriptive URL like plc7.mainpress.acme.corp. This URL is directly used for the management of asset's certificate (via Fully Qualified Domain Name - FQDN).

DNS Proxy

The initial step in implementing the overlay involves deploying a DNS proxy. By controlling the DNS table - directly or through forward - the ODLAN system can insert new entries and routes, migrating the network from the current structure to the overlay sequentially. When rerouting the traffic, the DNS proxy will specify the route going through the control proxy.

04 Enforce Control

Forward & Reverse Proxy

A DLAN should be fronted by a proxy - with protocol breaking capacities - scaling the implementation of DMZ best practices to the zero-trust reality of the new topology. The proxy offers comprehensive Layer 7 visibility into the communications between users and devices, ensuring detailed monitoring and granular control for each asset. Visibility into the protocols - not simply ip/port - enables stronger understanding of communications and permissions to allocate.

Device firewalls

Industrial environments are characterized by vendor assets, beyond the direct control of the IT team. Attached firewalls are conceived as uncomplicated hardware units that can be directly affixed to the asset, offering minimalistic traffic management, but a close proximity to the actual machine. This methodology remains lightweight at the network edge, ensuring scalability, all the while harnessing the intelligence of the ODLAN.

Encrypted tunnels

The majority of protocols lack native support for proxies. The ODLAN approach to securing these connections involves establishing encrypted tunnels between the edge firewall and the proxy. While this setup may result in a partial loss of visibility and control capabilities for the proxy, it significantly enhances protection against unencrypted traffic. As the system evolves, it can gradually develop or integrate specialized proxies.

Trout

An end-to-end example for Overlay Demilitarized LAN implementation

1 - Define a DLAN

To initiate the process, provide visibility into network traffic with a tap or a pass-through implementation. Protocols like NetFlow are widely adopted for this purpose. By analyzing the existing network traffic, identify the boundaries of the DLAN. These boundaries should align with business use cases, defining a minimal zone - for example, we want to protect our “Machine 12 HMI”.

2 - Define a Namespace

Next, assign a unique name to the DLAN that reflects its operation or the set of assets within it. In our example, “hmimachine12.acme.corp” can be used for. The ODLAN system will dynamically generate a certificate using the Public Key Infrastructure (PKI) and the Certificate Authority (CA) within the environment, and attach it to the device. Additionally, in case several assets have been defined in the DLAN, the ODLAN system should dynamically create prefixes for each asset to facilitate organized and secure network management.

3- Configure Access Control Engine

Establish user and group access to the DLAN based on Role-Based Access Control (RBAC) methods. A best practice should be to enforce least-privilege permissions, which becomes easy to do with ODLAN. In our example, we give our “main floor employees” user group access to “Machine 12 HMI”.

4- Visibility and Monitoring

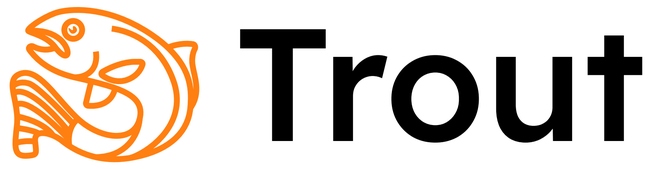
Users can start accessing the DLAN through the defined URL. Traffic to this URL is routed through the proxy, providing comprehensive visibility into communications. Controls can then be implemented to match the exact expected user behavior, ensuring detailed monitoring and granular control over each asset.

5- Agile Access

Too often, robust security designs fall short due to their inability to adapt to real business needs. To address this, ODLAN should incorporate a straightforward notification mechanism that detects new access attempts to a device and offers a simple solution for granting temporary access when necessary. In our example: the remote vendor support team needs to access the HMI system ; the IT admin receives an alert and can grant temporary access by using HTTP knocking security.

6- Lock in New State with Asset Firewall

Finally, at the asset level, configure the firewall to accept traffic only from the proxy. This setup ensures that all communications are monitored and controlled, reinforcing the security and integrity of the DLAN.


Trout