The Modern Secure Access Fabric

An End-to-End Implementation of Zero Trust Onboarding

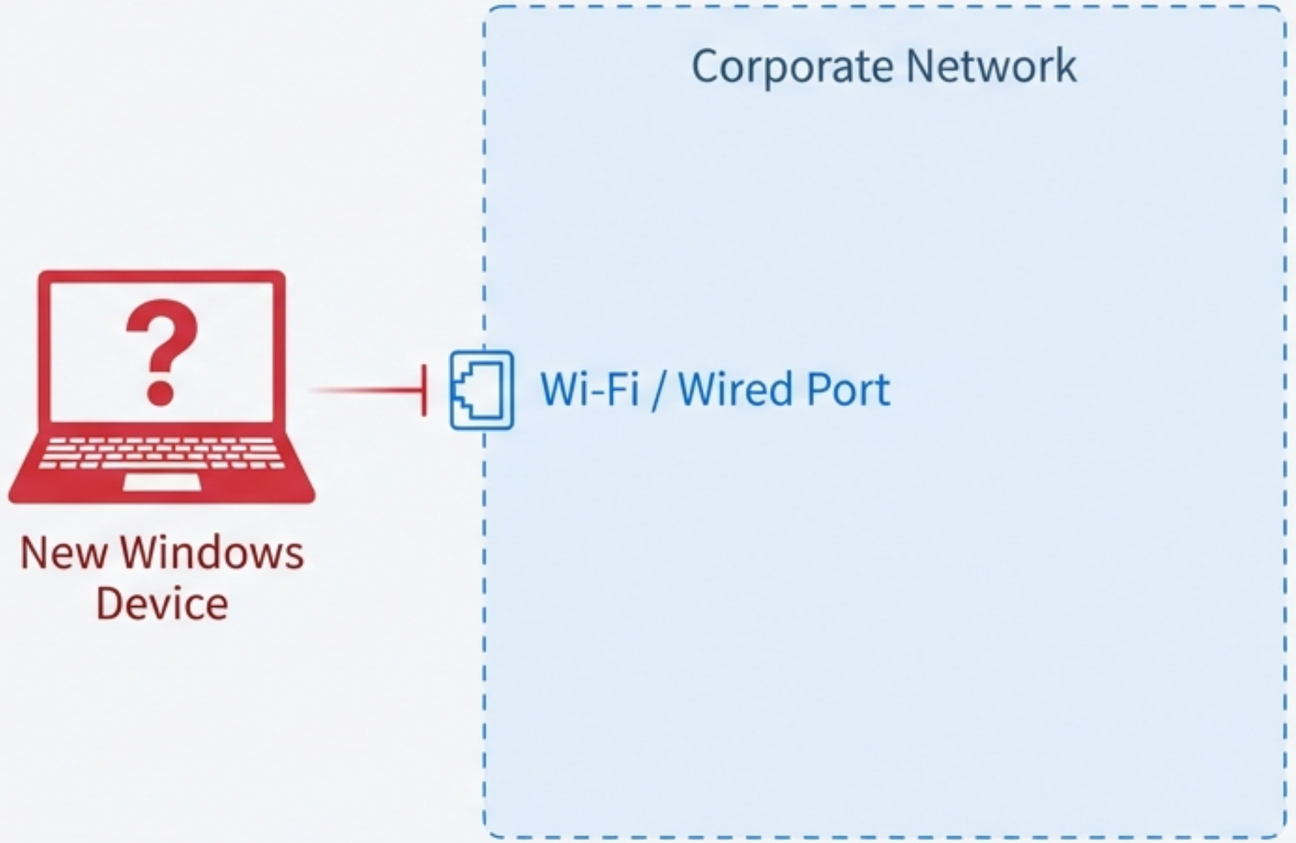
The Journey Begins with an Unknown Device

The Challenge

- A new corporate Windows device is unboxed and powered on.
- It is currently unknown to the network and unmanaged by IT.

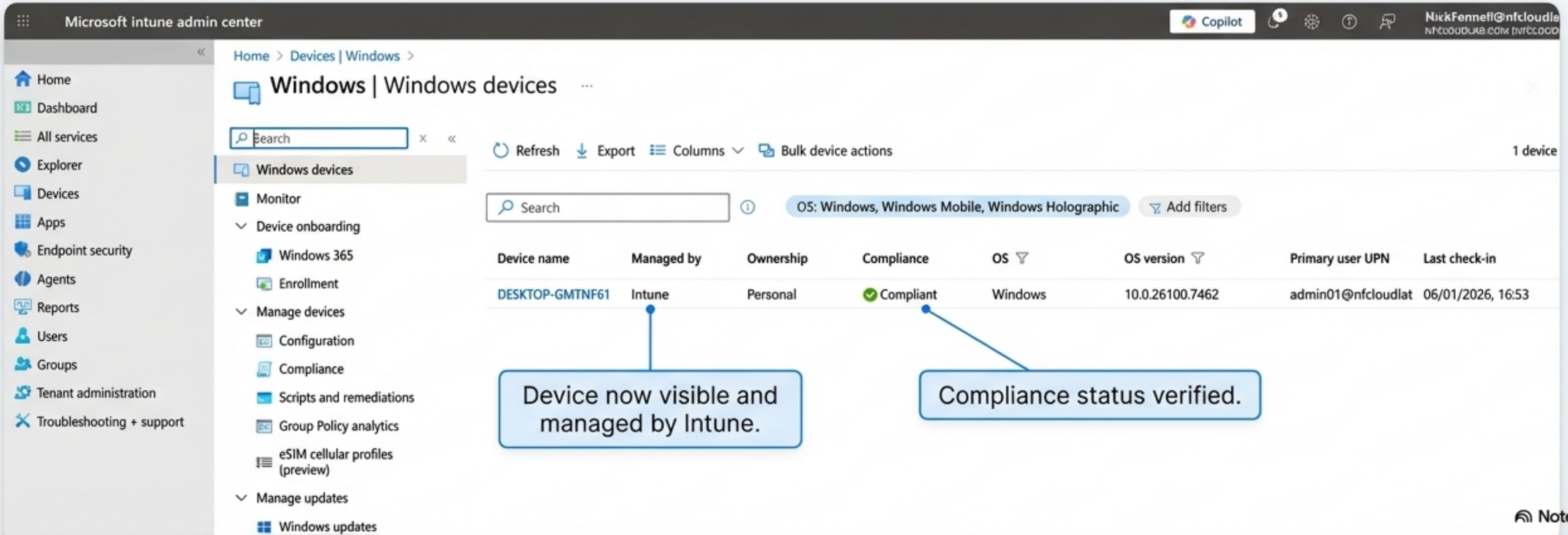
How do we automatically transform this device from an untrusted entity into a compliant, secure, and productive endpoint with appropriate network access?

Initial State Diagram



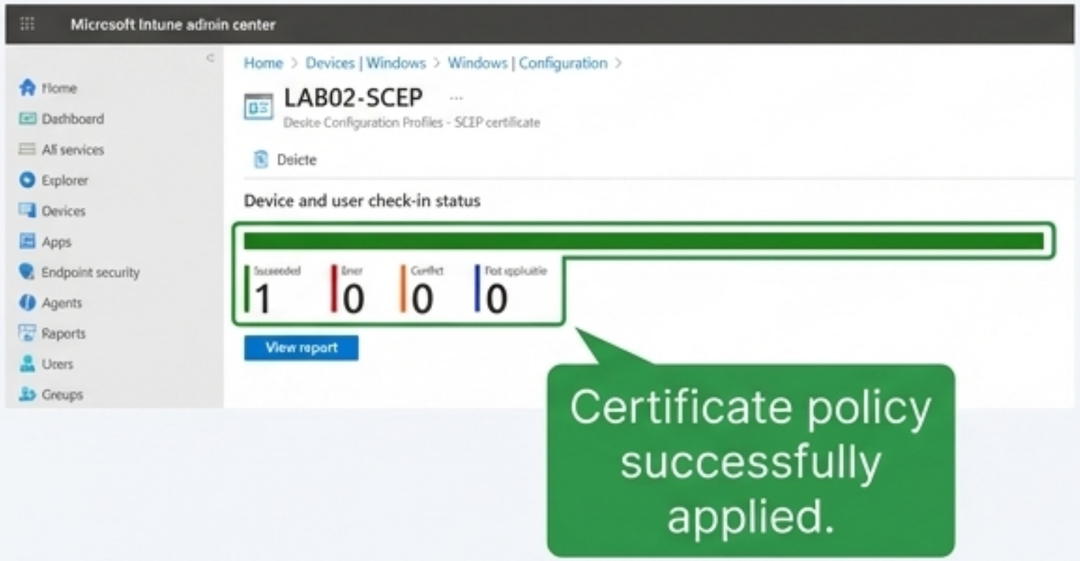
Step 1: Establishing Management with MDM Enrollment

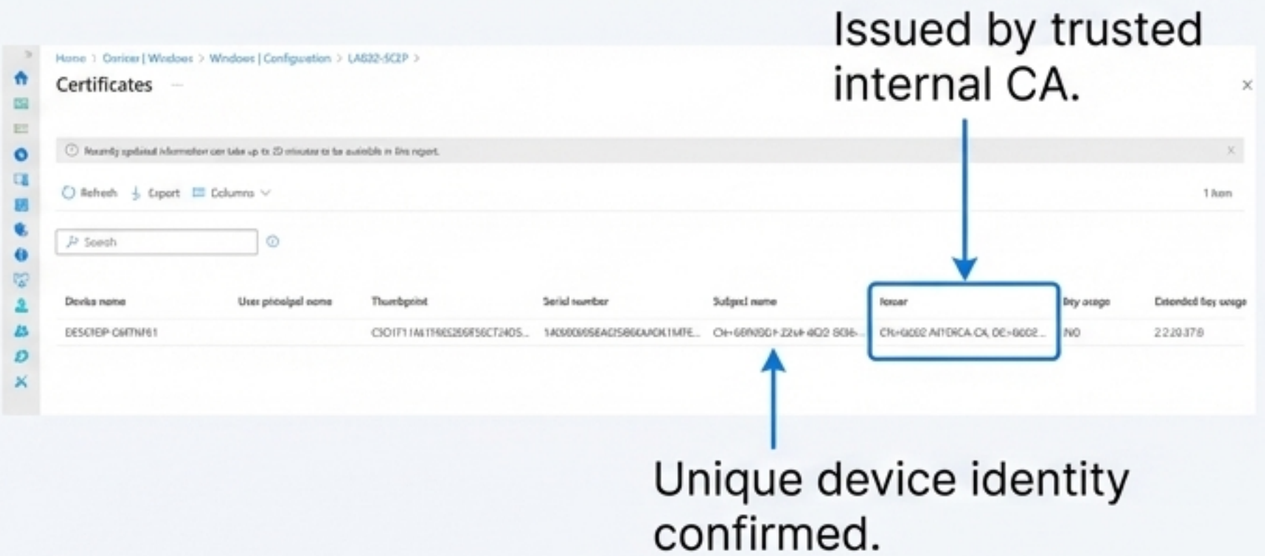
Before granting any network access, the device must be brought under management. Using Windows Autopilot, the device automatically enrolls into the company's Microsoft Intune tenant. Intune now serves as the single source of truth for device compliance and configuration. The user admin01 is associated with the device.



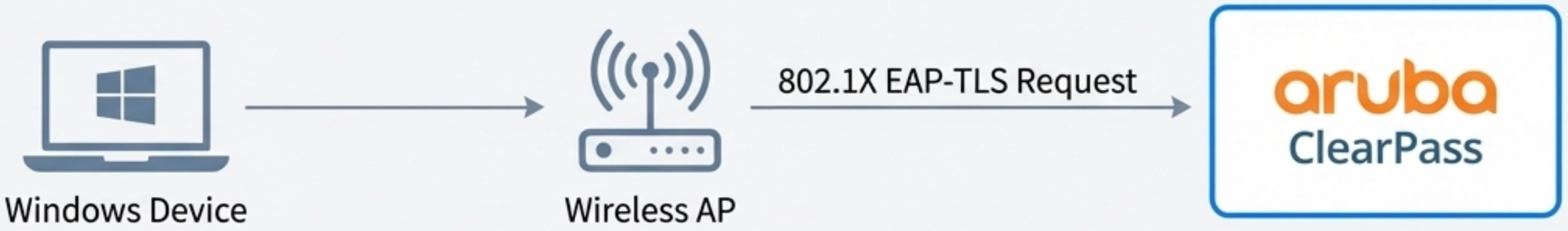
Step 2: Forging a Cryptographic Identity via SCEP

A managed device needs a trusted identity. Passwords are not enough. Intune pushes a `LAB02-SCEP` **configuration profile** to the device. This profile instructs the device to request a client authentication **certificate** from the on-premise Microsoft Certificate Authority (CA) via the NDES/SCEP protocol. The device now possesses a unique, non-exportable identity certificate, issued by the trusted `lab02-INTERCA-CA`.

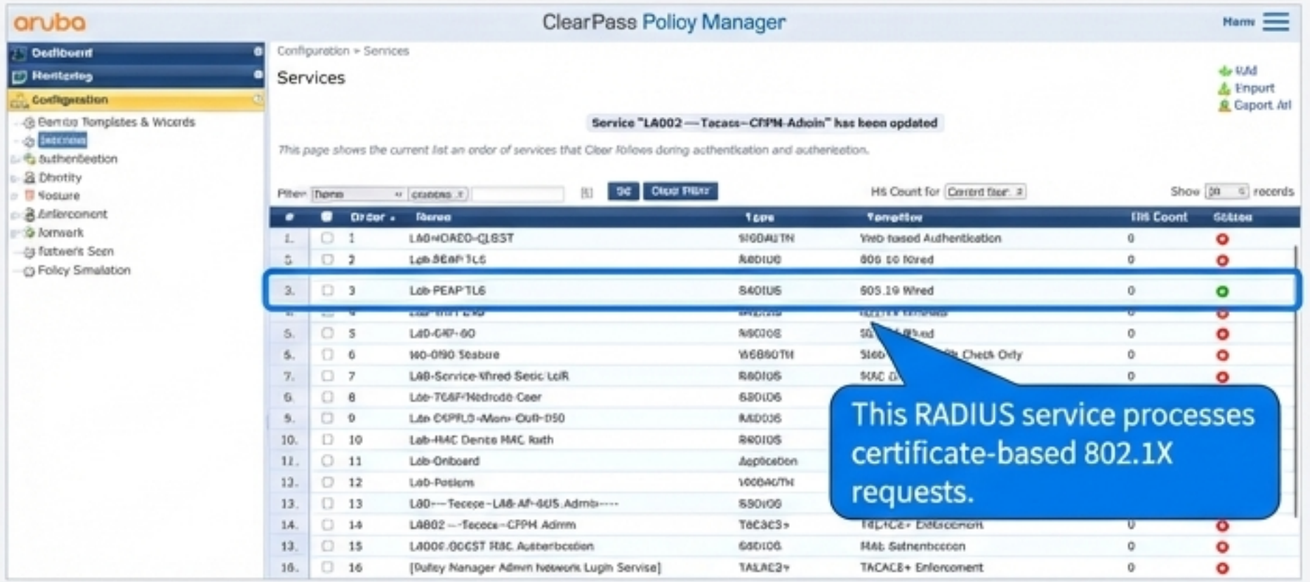




Step 3: The First Connection Attempt with 802.1X



- The device connects to the `LAB` SSID, which is configured for WPA2-Enterprise security.
- The connection triggers an 802.1X authentication request using the EAP-TLS protocol. The device presents its newly issued client certificate as its identity.
- The network infrastructure forwards this RADIUS request to Aruba ClearPass for a policy decision.

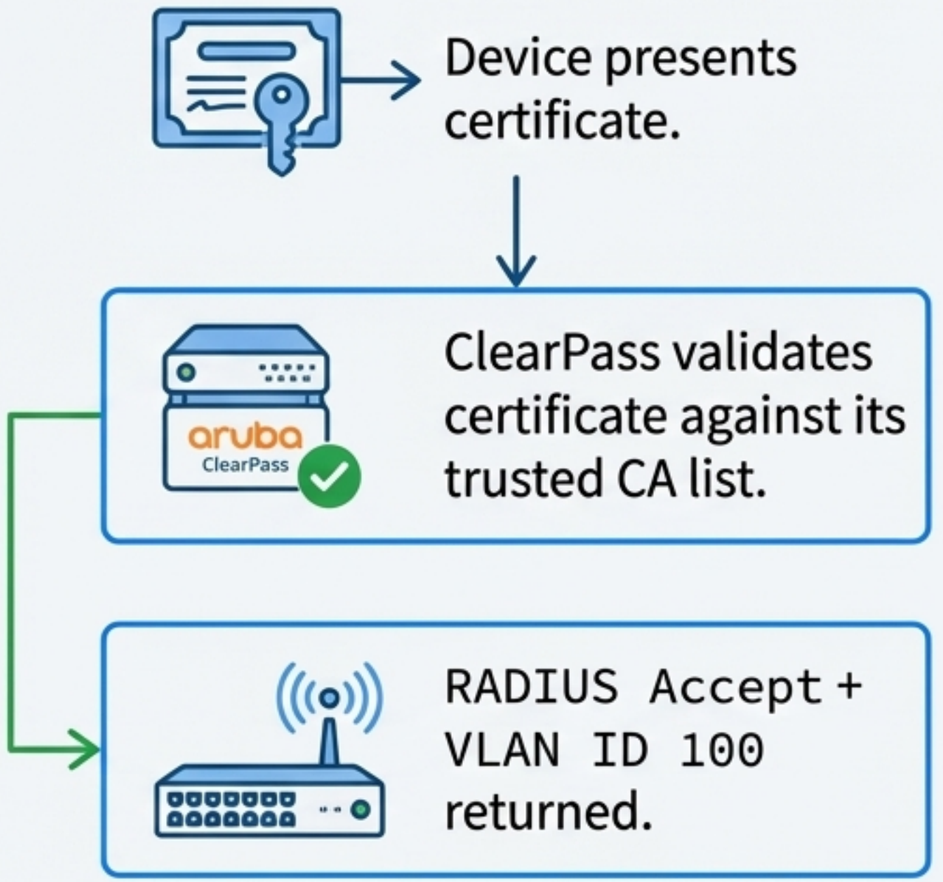


Step 4: ClearPass Validates Identity and Enforces Policy

Authentication: ClearPass receives the EAP-TLS request. It checks the issuer of the client certificate and validates that it was signed by the trusted `lab02-INTERCA-CA`.

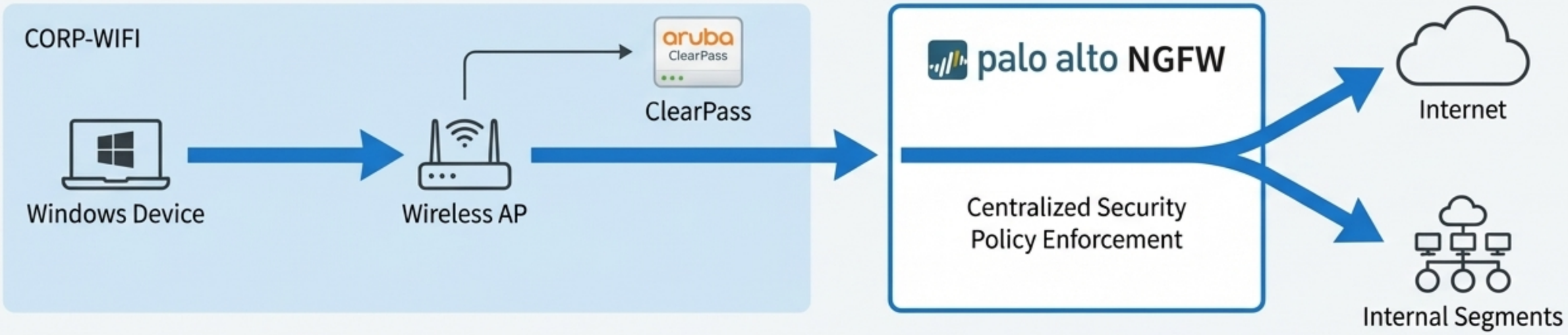
Authorization: After successful authentication, ClearPass checks authorization rules. For example, it can verify the device is still marked as 'Compliant' in Intune via an API call (a key capability).

Enforcement: ClearPass returns a `RADIUS Accept` message to the network device, along with enforcement attributes.

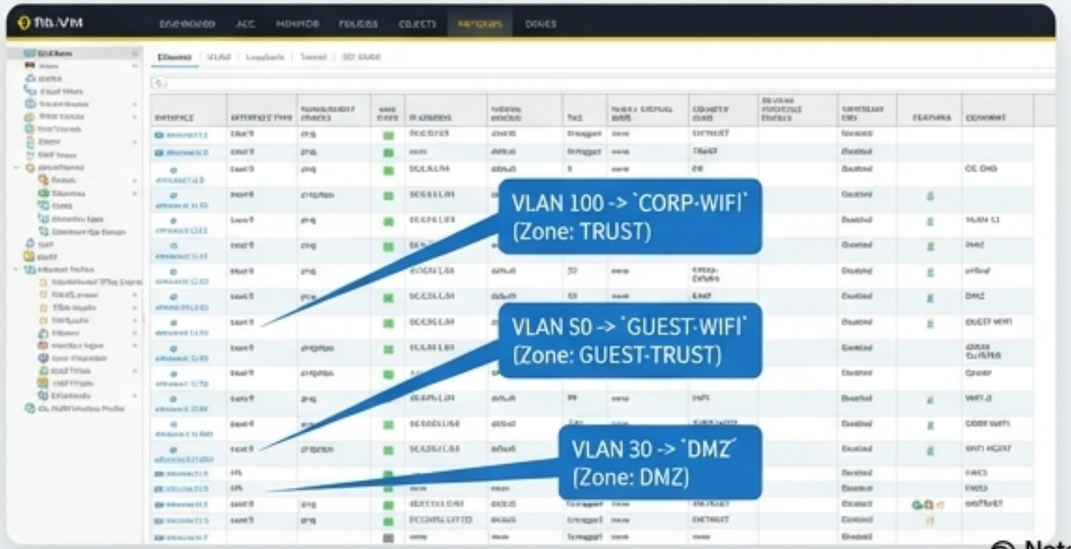


Upon success, ClearPass instructs the switch/AP to place the device in the **CORP-WIFI VLAN (100)**, granting access to trusted corporate resources.

Step 5: The Device is on the Network. Now, Secure the Traffic.



- The device is now on the `CORP-WIFI` network segment (VLAN 100).
- All traffic from this and other segments is routed through the Palo Alto Networks NGFW, which acts as the central point for security policy enforcement.
- The firewall is configured with distinct interfaces and security zones for each VLAN, enforcing a strict segmentation model.

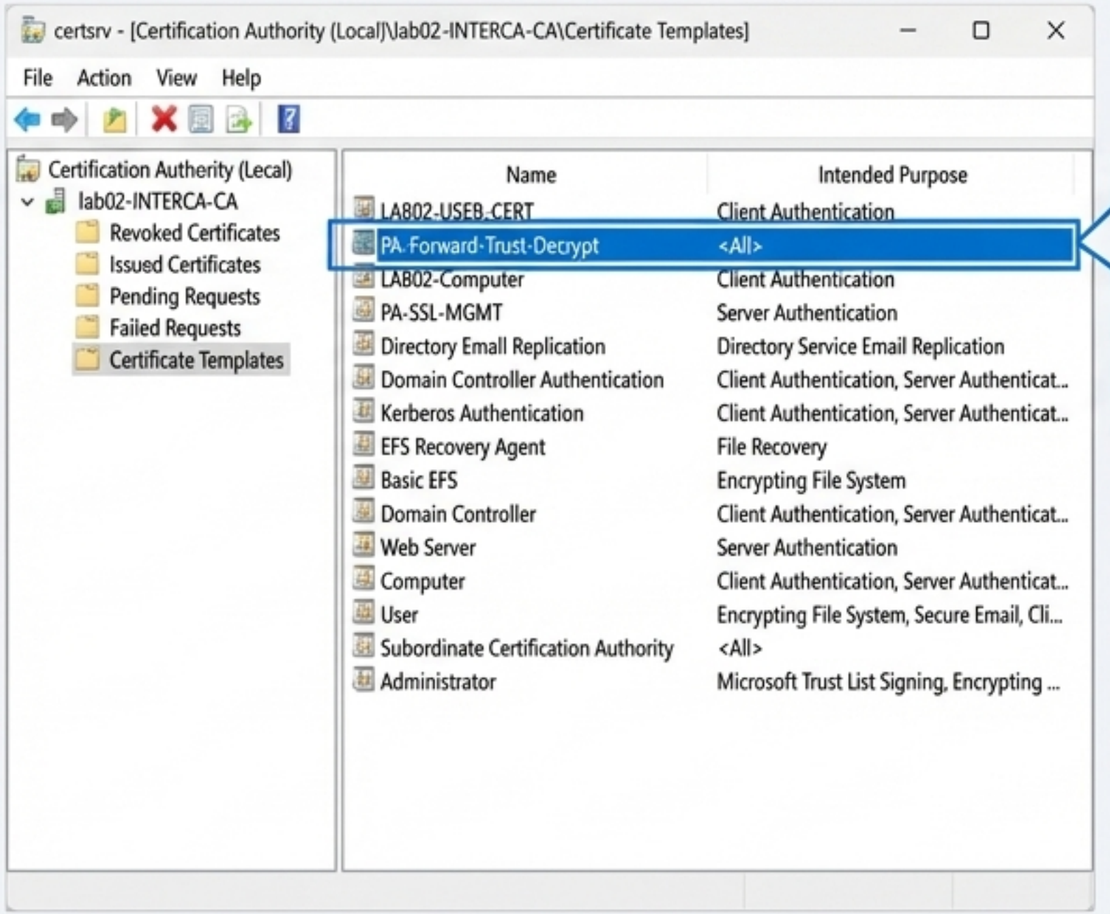


Deeper Inspection: Decrypting Traffic and Identifying Users

To effectively counter modern threats, the firewall must inspect encrypted traffic. The NGFW is configured to decrypt TLS/SSL traffic using a forward trust certificate issued by the corporate CA.

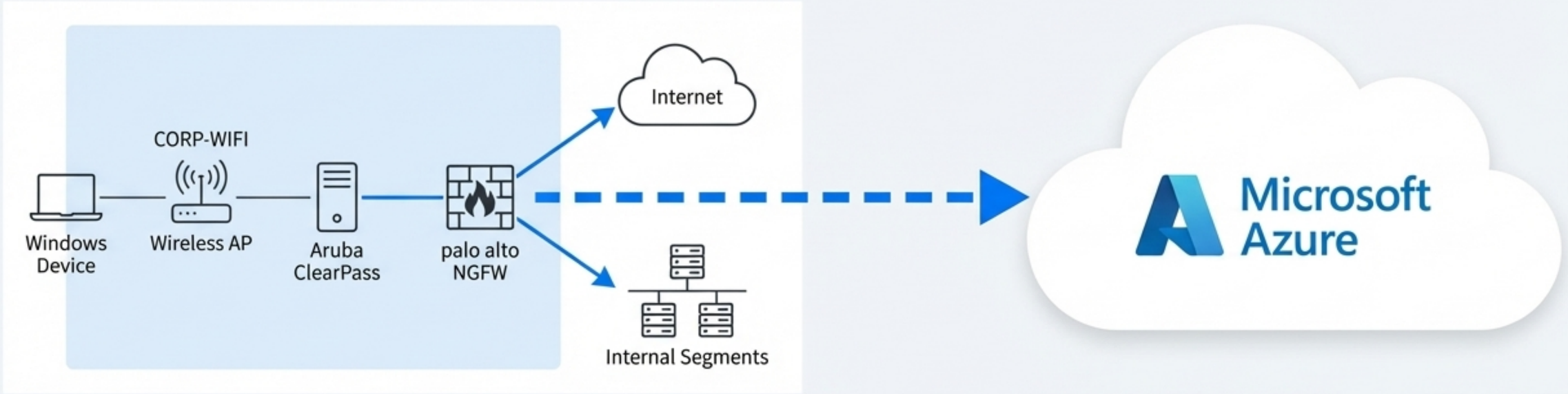
Simultaneously, the firewall's User-ID agent integrates with Active Directory to map the device's IP address (10.0.100.x) to the authenticated user (lab02\admin01).

This allows for security policies based on user identity, not just IP address, enabling application control and threat prevention specific to user roles.



This certificate, issued by the corporate CA, is installed on the NGFW to enable SSL Decryption for outbound traffic.

The Journey Extends: Securing Access to the Hybrid Cloud



The now-trusted user and device need to access applications hosted in a Microsoft Azure Virtual Network (VNet). The security challenge is to extend the same segmentation, policy enforcement, and visibility from the on-premise network to the cloud, creating a seamless and consistent security posture.

Building the Bridge: Site-to-Site IPsec VPN with BGP

- A secure connection is established between the on-premise PA-01 firewall and an Azure VPN Gateway.
- The connection uses an IPsec VPN tunnel with IKEv2.
- Border Gateway Protocol (BGP) is enabled over the tunnel to dynamically exchange routing information. This ensures that on-prem networks (like `10.0.0.0/8`) are automatically advertised to Azure, and Azure VNet prefixes (`172.16.0.0/16`) are learned on-prem.

From Azure ARM Template (`ngfw-s2s-bgp.txt`)

```
{
  "type": "Microsoft.Network/connections",
  "connectionType": "IPsec",
  "connectionProtocol": "IKEv2",
  "enableBgp": true,
  "bgpSettings": {
    "asn": 65001,
    "bgpPeeringAddress": "10.2.2.2"
  }
}
```

From Palo Alto Config (Palo02-LAB02-061225.txt)

```
set network virtual-router default
  protocol bgp
  peer-group BGP-PEER
    peer 10.2.2.2
```

Consistent Policy from the Campus to the Cloud

- With the BGP-enabled tunnel in place, traffic from the user's device (10.0.100.x) to the Azure VM (172.16.0.4) is seamlessly routed and inspected by the Palo Alto NGFW.
- The same User-ID information, application signatures, and threat prevention profiles are applied to this hybrid traffic.
- Azure route tables are configured to force all outbound traffic from the spoke VNet through a Palo Alto Cloud NGFW instance, ensuring that cloud resources are also protected with a consistent policy.

Azure Route Table (`ngfw-s2s-bgp.txt`)

```
{
  "type": "Microsoft.Network/routeTables",
  "addressPrefix": "0.0.0.0/0",
  "nextHopType": "VirtualAppliance",
  "nextHopIpAddress": "172.18.0.4"
}
```

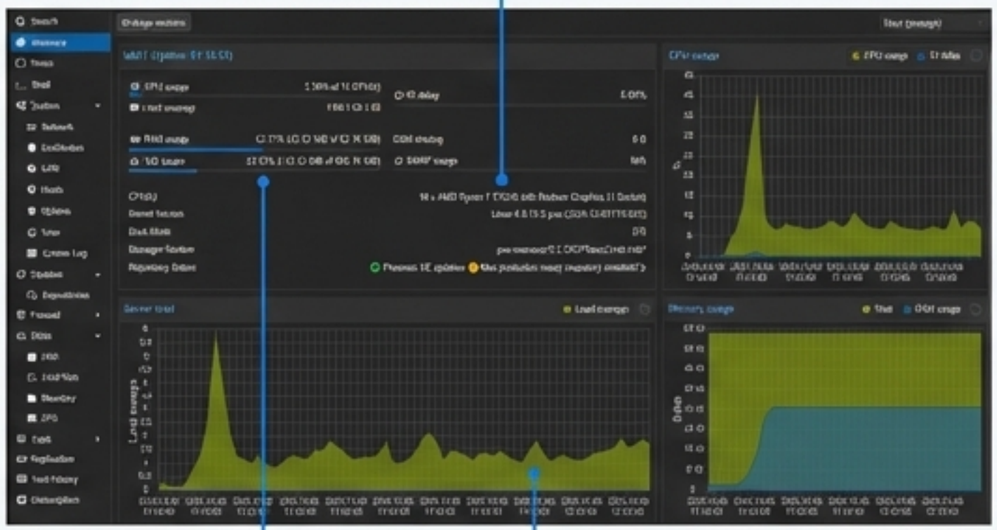
All traffic is forced to the Cloud NGFW for inspection.

Behind the Curtain: The LAB02 Infrastructure Blueprint

Core Virtual Machines

- LAB02-DC02
- LAB02-INTER-CA
- LAB02-CPPM-PUB
- LAB02-PA01-Active
- LAB02-NDES02
- LAB02-Vyos

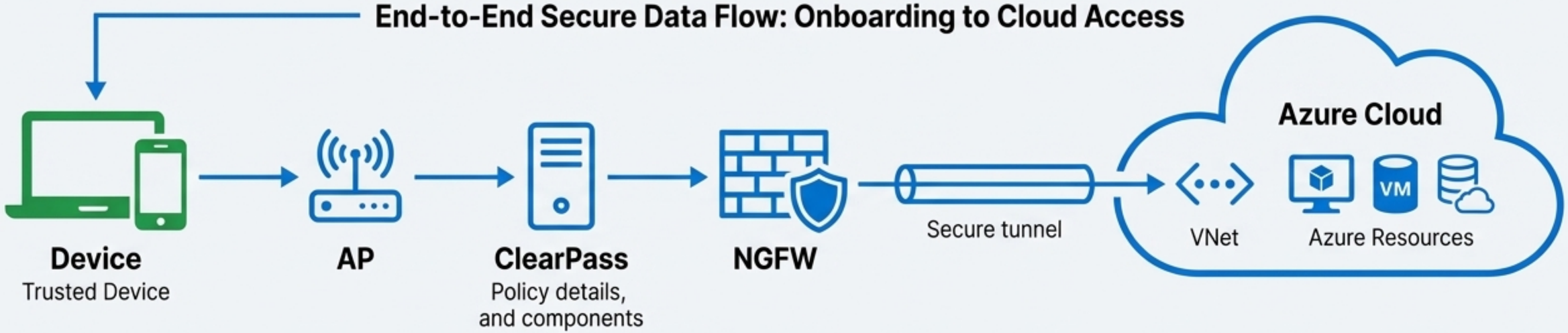
Proxmox Hypervisor



Network Segments

VLAN	Name	Subnet	Purpose
100	CORP-WIFI	10.0.100.0/24	Trusted corporate wireless clients
50	GUEST-WIFI	10.0.50.0/24	Untrusted guest wireless access
20	CPPM	10.0.20.0/24	ClearPass server infrastructure
30	DMZ	10.0.30.0/24	Public-facing services

From Zero to Hero: The Power of an Integrated Security Fabric



Identity is the Perimeter

Device and user identity, verified by cryptography, is the foundation of access control.

Automated, Policy-Driven Onboarding

The process is seamless for the user, requiring zero IT intervention to move from untrusted to secure.

Zero Trust Enforcement

The device is never implicitly trusted. Access is continuously verified and traffic is always inspected.

Consistent Hybrid-Cloud Security

The same granular security policies protect users and data, regardless of where the resources are located.