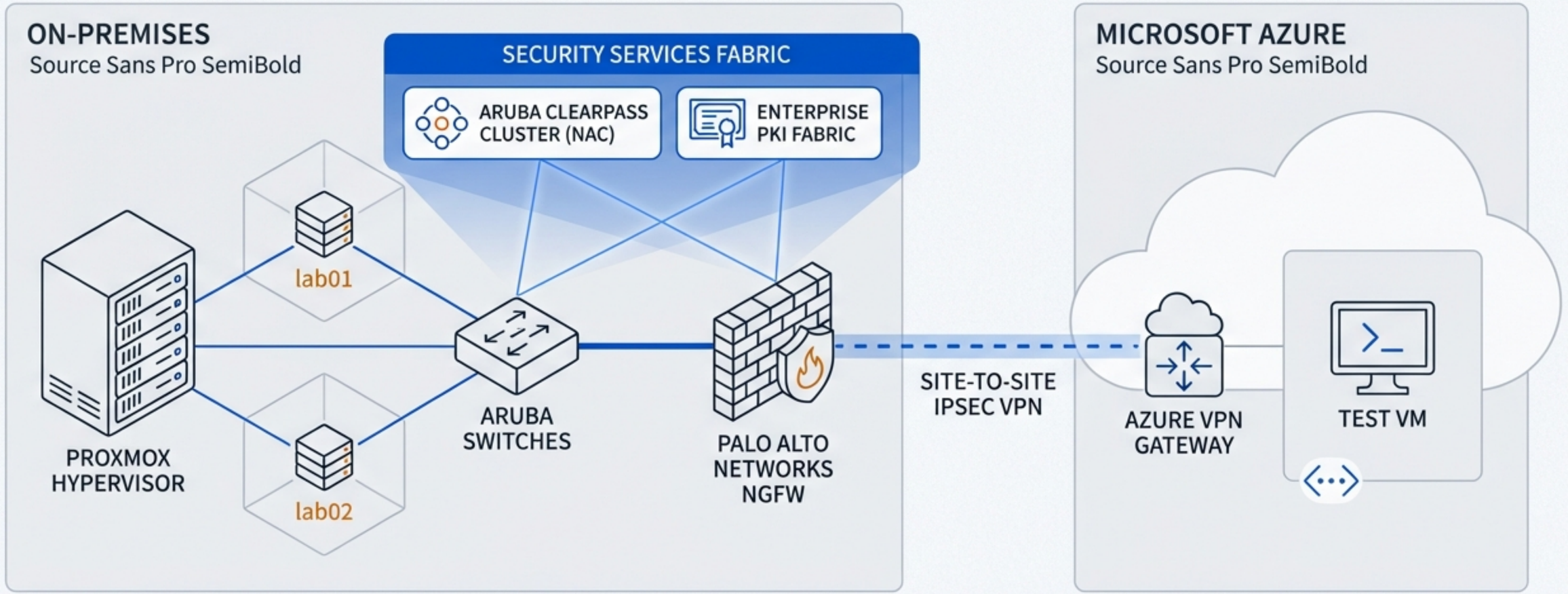
Constructing a Multi-Vendor Hybrid Cloud Security Fabric

A portfolio showcasing the design and implementation of an end-to-end enterprise security lab, from on-premises access control to cloud-native workloads.



The Blueprint: Simulating a Secure, Segmented Enterprise

Multi-Domain Isolation

The lab is architected with two completely separate domains (`lab01`, `lab02`), each with its own Domain Controller and PKI, to simulate distinct business units or security zones.

Centralized Enforcement

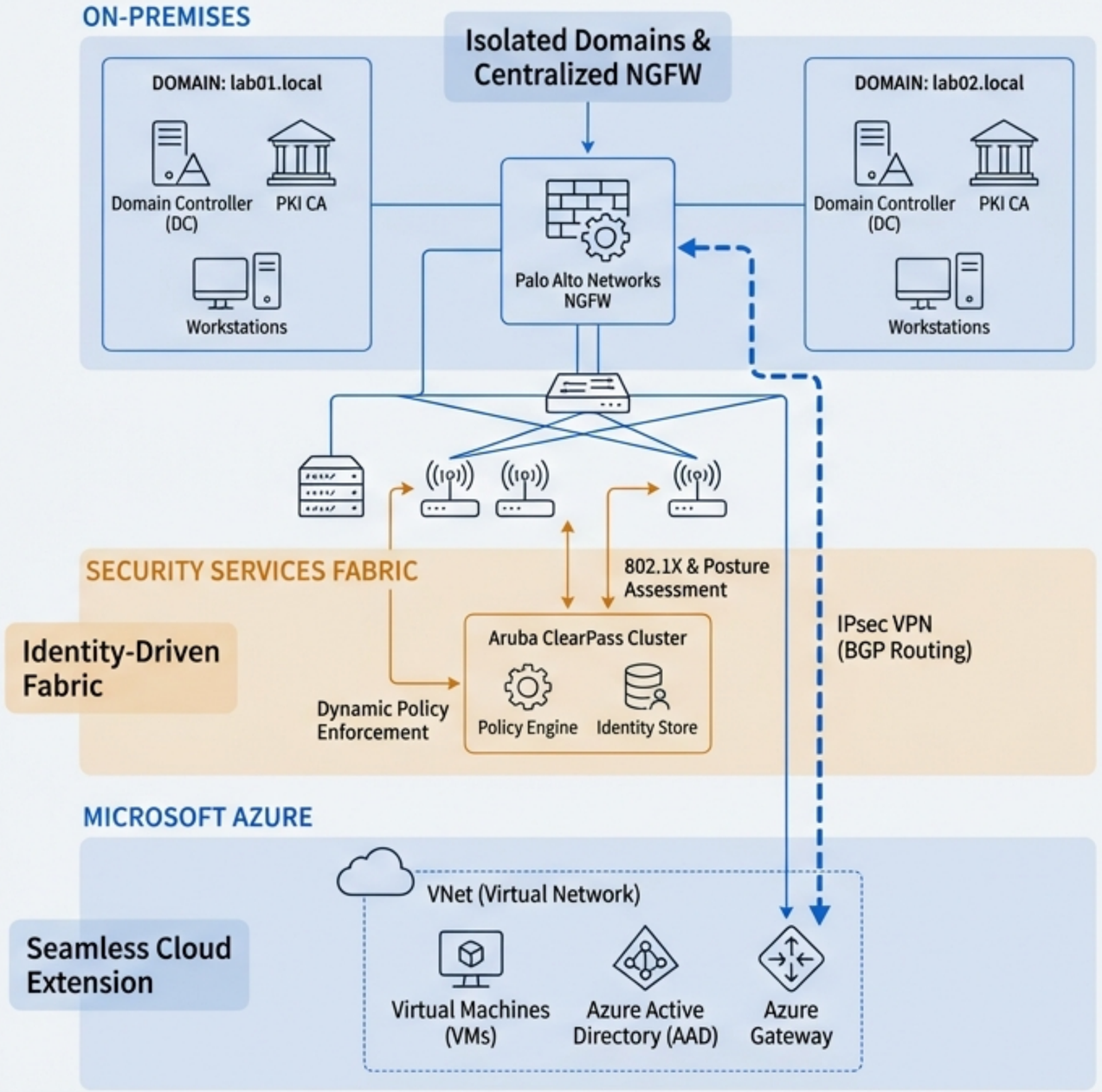
A Palo Alto Networks NGFW acts as the single point of policy enforcement and inter-domain routing, ensuring no traffic can bypass security inspection.

Identity-Driven Access

Network access is controlled by an Aruba ClearPass cluster, moving beyond static IPs to an identity-based model using 802.1X and posture assessment.

Seamless Cloud Integration

The secure on-premises fabric is extended to Microsoft Azure using dynamic BGP routing over an IPsec VPN, treating the cloud as a trusted extension of the data center.



The Foundation Begins with the Virtualization Layer

Hypervisor

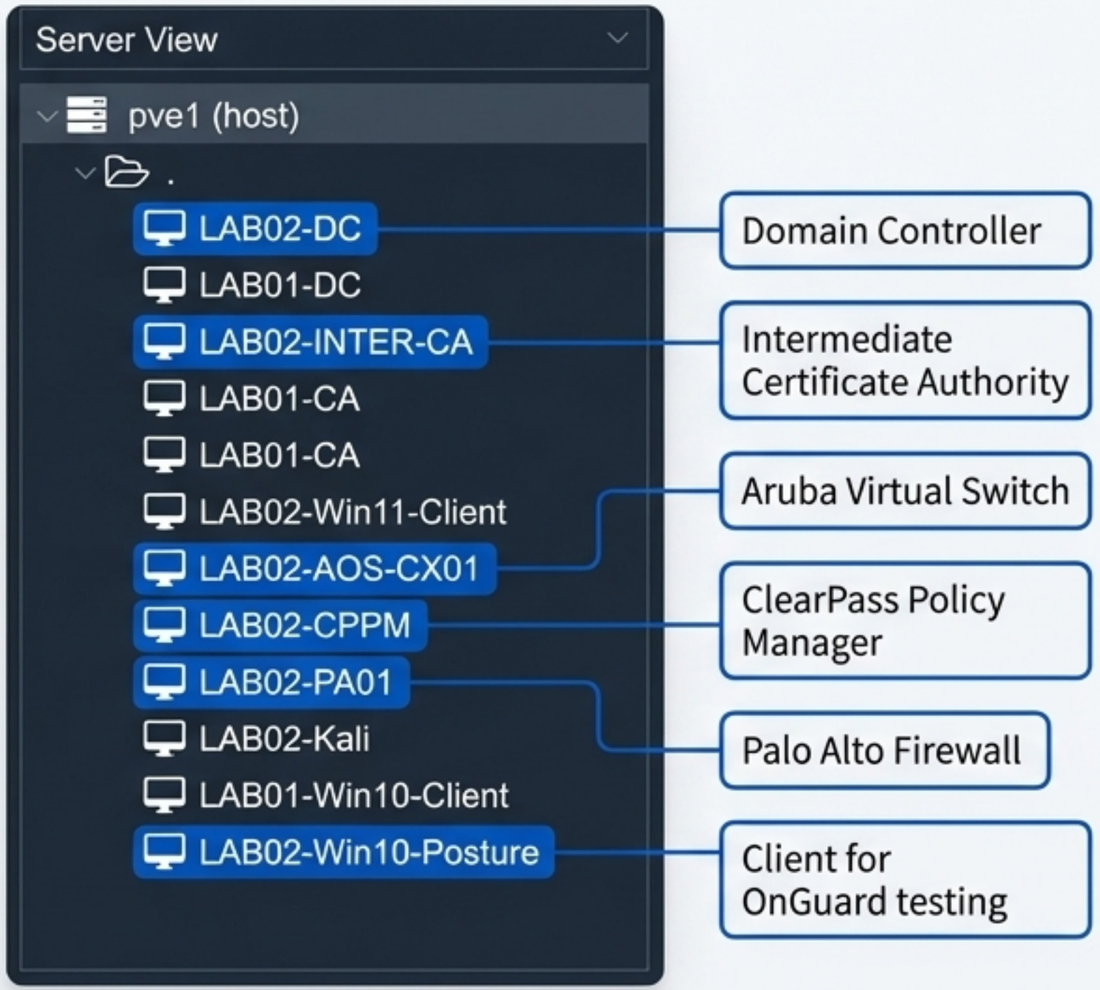
The entire lab is hosted on a single, custom-built Proxmox Virtual Environment (Type 1) host.

Core Network

All internal lab traffic operates within the `10.0.0.0/8` address space.

VM Isolation

Virtual machines are segregated into the `lab01`` and `lab02`` domains for security testing.



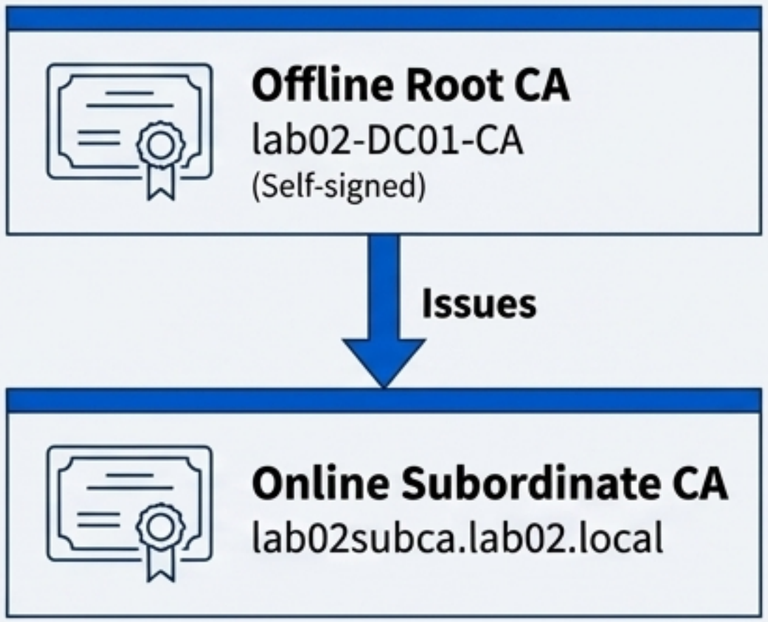
The Palo Alto NGFW is the Core of On-Premises Segmentation

All traffic between security zones is routed through and inspected by the Palo Alto firewall. Virtual interfaces (sub-interfaces) are mapped to specific VLANs, creating distinct zones for different user types and services.

Interface	IP Address	VLAN	Security Zone	Purpose
ethernet1/1	10.0.2.24	Untagged	UNTRUST	External/Internet Connectivity
ethernet1/2	10.0.5.1/24	5	TRUST	Trusted Servers (e.g., Domain Controller)
ethernet1/2.11	10.0.11.1/24	11	Wired-LAN-V11	Corporate Wired Employee Access
ethernet1/2.30	10.0.30.1/24	30	DMZ	Demilitarized Zone for public services
ethernet1/2.60	10.0.60.1/24	60	CPPM	Aruba ClearPass Cluster
ethernet1/2.100	10.0.100.1/24	100	CORP-WIFI	Corporate Wireless Access
ethernet1/2.50	10.0.50.1/24	50	GUEST-WIFI	Guest Wireless Access

A Two-Tier PKI Establishes the Chain of Trust

A secure lab requires a trusted identity source. A two-tier Microsoft Certificate Authority was built for the `lab02.local` domain to issue certificates for all critical infrastructure, including RADIUS servers, web services, and firewall functions.



Key Certificates Issued

RADIUS/EAP Server:
radius.lab02.local

TLS Decryption:
forward-trust.lab02.local

Web Services Wildcard:
*.lab02.local

Device Certificates:
192.168.0.172

Aruba ClearPass Provides Centralized, Granular Access Control

The system uses an Aruba ClearPass Publisher-Subscriber cluster for high availability. Aruba AOS-CX switches query the cluster via RADIUS to make real-time access decisions for every connected device.

Name	Type	Template
LAB-WIRED-GUEST	WEBAUTH	Guest
Lab-Posture	WEBAUTH	Posture
Lab-EAP-TLS	RADIUS	EAP-TLS

```
# Switch points to the ClearPass cluster for
Authentication
radius-server host cppm.duckdns.org

# Enables ClearPass to dynamically change a
client's access (CoA)
radius dyn-authorization enable
radius dyn-authorization client 10.0.60.10
```

Establishes RADIUS server

Enables Change of Authorization (CoA)

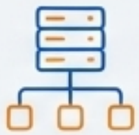
Evidence: Port-Level 802.1X and MAC Authentication

Security policy is enforced at the physical port. The following configuration on an Aruba AOS-CX access switch demonstrates a multi-layered approach, enabling both certificate-based 802.1X for corporate devices and MAC authentication for simpler devices.

```
# Configuration for an employee access port
interface 1/1/3
    # Assigns VLANs dynamically after authentication
    no shutdown
    vlan trunk native 11
    vlan trunk allowed 11,12,13,20

    # Enables 802.1X supplicant support
    dot1x authenticator enable

    # Enables MAC-based authentication as a fallback
    mac-auth enable

    # Forwards DHCP requests to the server
    ip helper-address 10.0.60.10
```

- **Layered Security**: Both `.1X` and `MAC-Auth` are enabled for maximum compatibility.

- **Dynamic Policy**: VLANs are not static; they are assigned based on the role returned by ClearPass.



- **Centralized Services**: `ip helper-address` ensures devices can get an IP and communicate with ClearPass.

Enforcing Zero Trust with Inter-Zone Firewall Policies

With network segmentation and NAC in place, the Palo Alto firewall enforces a Zero Trust security model. Policies are built to explicitly allow required traffic between zones, while an implicit deny rule blocks all other communication.

#	Name	Source Zone	Destination Zone	Application	Service	Action
1	Allow Corp DNS	CORP-WIFI	TRUST	dns, ldap	application-default	Allow
2	Deny Guest to Corp	GUEST-WIFI	TRUST	any	any	Deny
3	Allow DMZ Web Inbound	UNTRUST	DMZ	ssl, web-browsing	service-https	Allow
4	Allow Corp to Internet	CORP-WIFI	UNTRUST	any	any	Allow

Underlying Principle

This structure prevents lateral movement by attackers, as a compromised device in one zone (e.g., GUEST-WIFI) cannot reach critical assets in another (e.g., TRUST).

Gaining Full Visibility with TLS Decryption

To inspect for modern threats, encrypted traffic must be decrypted. The firewall uses a “Forward Trust” certificate, signed by our internal Subordinate CA, to perform a trusted Man-in-the-Middle inspection on traffic from corporate devices.

Step 3

Client trusts the connection because its trust store includes the lab’s **Root CA**.

Step 4

Creates new TLS session to `example.com` and **inspects all cleartext traffic**.

Decryption Profile

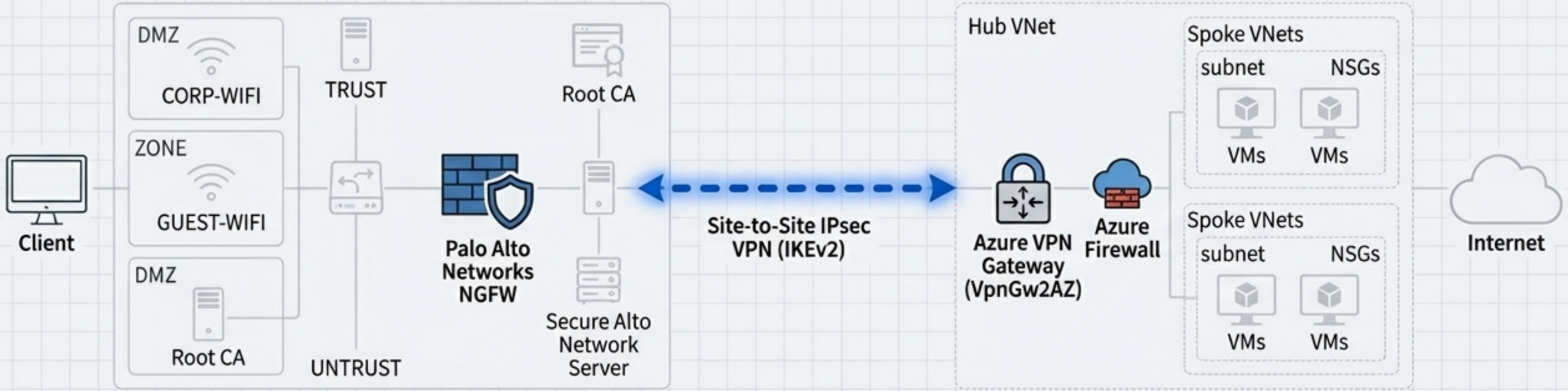
`newcaptive` is configured to use the `forward-trust` certificate for SSL Forward Proxy.

Decryption Policy

The `NDES-SCEP-CERT2025` policy rule is set to action `decrypt` for traffic from UNTRUST to UNTRUST.

Extending the Security Fabric to the Microsoft Azure Cloud

Modern enterprises operate in a hybrid model. This lab extends the secure on-premises network to a hub VNet in Azure using a high-performance, route-based IPSec VPN. BGP is used for dynamic route exchange, eliminating the need for static route maintenance.



Key Connectivity Parameters

Type: Site-to-Site IPsec VPN (IKEv2)
Routing: Border Gateway Protocol (BGP)

On-Prem Gateway: Palo Alto NGFW
Cloud Gateway: Azure VPN Gateway (VpnGw2AZ)

Evidence: Azure Infrastructure Deployed as Code

The entire Azure network environment was defined and deployed using a single ARM template. This ensures consistency, enables version control, and showcases modern cloud deployment practices.

```
{
   // Azure Virtual Network Gateway Configuration
   "type": "Microsoft.Network/virtualNetworkGateways",
   "name": "nfg-vpngw",
   "properties": {
      "gatewayType": "Vpn",
      "vpnType": "RouteBased",
      "enableBgp": true,
      "sku": { "name": "VpnGw2AZ" },
      "bgpSettings": {
         "asn": 65515, // Azure BGP ASN
         "bgpPeeringAddress": "172.16.1.254"
      }
   }

   // On-Premises Gateway Definition in Azure
   "type": "Microsoft.Network/localNetworkGateways",
   "name": "ng-lng",
   "properties": {
      "gatewayIpAddress": "37.228.233.216", // On-prem PA Firewall IP
      "bgpSettings": {
         "asn": 65001, // On-prem BGP ASN
         "bgpPeeringAddress": "10.0.17.5"
      }
   }
```

BGP enabled for dynamic routing

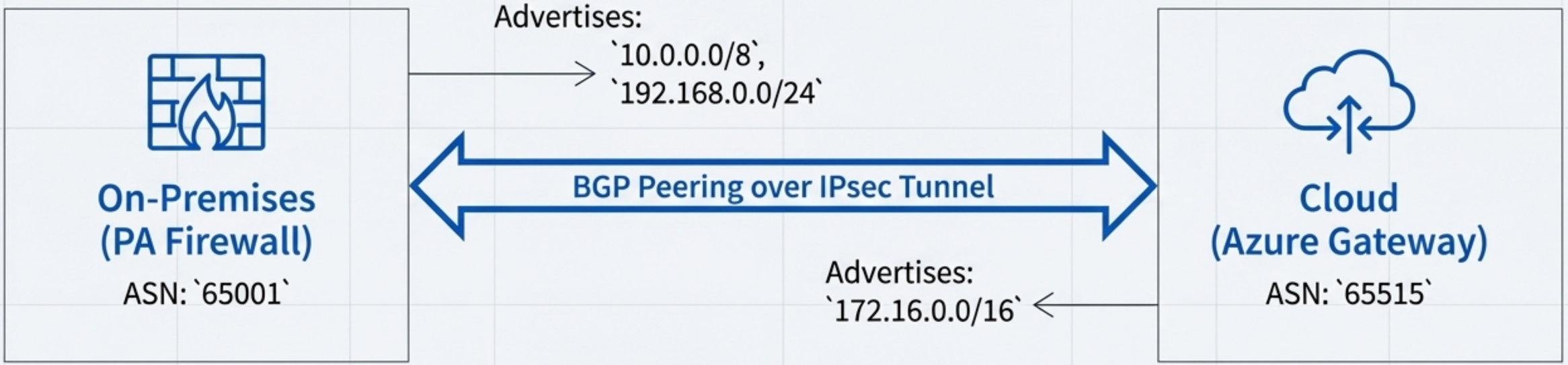
Azure-side ASN

Public IP of On-Prem Firewall

On-Premises ASN

BGP Provides Dynamic and Resilient Hybrid Routing

BGP automates the exchange of network reachability information between the on-premises firewall and the Azure VNet. When a new network is added in Azure, it is automatically advertised to the on-prem network, and vice-versa.

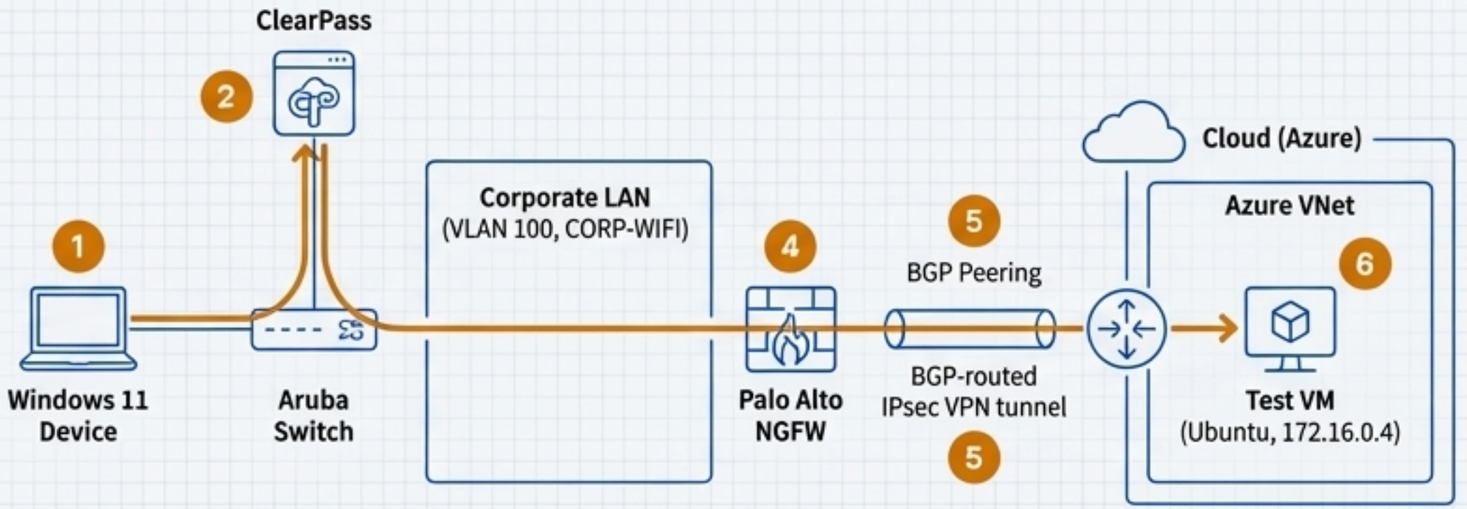


This is vastly superior to static routing, which is brittle and requires manual updates for every network change.

The Result: A Seamless End-to-End Security Fabric

We can now trace a complete user-to-application data flow, demonstrating how each security component contributes to a unified, policy-driven architecture.

1. **CONNECT**: A Windows 11 device connects to an Aruba switch port.
2. **AUTHENTICATE:** ClearPass validates the device's certificate via 802.1X, performs a posture check with OnGuard, and assigns the “Corporate” role.
3. **SEGMENT**: The Aruba switch places the device into VLAN 100 (`CORP-WIFI` zone).
4. **ROUTE & INSPECT**: The user attempts to access a server in Azure. The traffic is routed to the Palo Alto firewall, where it is decrypted and inspected against security policy.
5. **TRANSPORT:** The allowed traffic is sent over the BGP-routed IPsec VPN tunnel to Azure.
6. **ACCESS:** The user successfully connects to the Ubuntu `testvm` (172.16.0.4`) running in the Azure VNet.



Demonstrated Capabilities

On-Premises Foundation

- Type 1 Hypervisor Environment (Proxmox VE)
- Multi-Domain Active Directory & PKI
- NGFW-based L3 Segmentation (Palo Alto)
- Multi-Vendor Switching (Aruba AOS-CX)

Advanced Security Fabric

- 802.1X & MAC Authentication with Dynamic Authorization (CoA)
- Client Posture Assessment (ClearPass OnGuard)
- Centralized Zero Trust Policy Enforcement
- TLS Decryption for Threat Inspection

Hybrid Cloud Integration

- Infrastructure as Code Deployment (Azure ARM)
- Site-to-Site IPsec VPN with BGP Dynamic Routing
- Seamless On-Prem to Cloud Workload Access
- Remote Access VPN (GlobalProtect)