

Beyond the Tunnel: A Lab-Based Comparative Evaluation of Network-Layer VPN and Identity-Aware Reverse Proxy Architectures Against the CISA Zero Trust Maturity Model

Author: Henry Cheung

Advisor: Tanya Baccam

Accepted: July 7th, 2026

Abstract

Network-layer virtual private network (VPN) appliances still anchor enterprise remote access, and repeated mass exploitation of these appliances has made them a recurring initial access vector for ransomware operators. Identity-aware reverse proxies (IAPs), usually marketed under the Zero Trust Network Access (ZTNA) label, are positioned as the replacement. Whether they actually align better with Zero Trust than a modern VPN, or only claim to, has not been tested objectively. To answer that question, a controlled lab was built, six products were deployed across both architectures, and each was put through a 21-test battery mapped to the five pillars of the CISA Zero Trust Maturity Model, with every outcome scored against predictions registered in advance and the raw evidence retained for audit. The architectural advantage is strongest on the Networks pillar, where identity-aware proxy access withholds default network reachability and shrinks blast radius. For the Applications and Data pillars, the results depend primarily on the security features bundled with each product and its platform, and the two architectures converge on Identity because both draw their authentication

strength from the same identity provider. The study contributes a repeatable methodology and a scored matrix that shows where the architectures genuinely diverge. For security architects, it offers evidence-based grounds to make identity-aware proxy access the default for internal web applications, while recognizing that architecture alone does not settle every pillar.

1. Introduction

Remote access infrastructure is one of the most consistently exploited attack surfaces on the corporate internet. Mandiant's M-Trends 2026 report finds that exploits were again the most common initial infection vector for the sixth consecutive year, accounting for 32 percent of the intrusions it investigated, and it documents espionage actors deliberately targeting edge devices such as VPNs and routers, frequently exploiting them before a patch is available (Mandiant, 2026). The Verizon 2026 Data Breach Investigations Report adds that, for the first time in the report's nineteen-year history, exploitation of vulnerabilities overtook stolen credentials as the leading breach entry point, accounting for 31 percent of breaches (Verizon, 2026). The advisories from the Cybersecurity and Infrastructure Security Agency (CISA) keep repeating the same story: a pre-authentication CVE in a VPN appliance, exploited as a zero-day, then used to stage ransomware (CISA, 2024, 2025).

The past three years of VPN appliance compromises bear this out. Ivanti Connect Secure was hit in December 2023 through CVE-2023-46805 chained with CVE-2024-21887 (CISA, 2024). Citrix NetScaler was affected by CVE-2023-4966, better known as Citrix Bleed, in which stolen session tokens bypassed multi-factor authentication across every application behind it. Fortinet FortiOS SSL VPN was exploited at scale in both 2022 and 2024, through CVE-2022-42475 and CVE-2024-21762. Check Point disclosed CVE-2024-24919 in May 2024. The pattern carried into 2025: Ivanti Connect Secure was exploited again through CVE-2025-0282, an unauthenticated remote code execution flaw (CVSS 9.0), exploited as a zero-day from December 2024 and used to deploy custom malware before a patch was available (CISA, 2025). The vendors differ, but the outcome

is the same. Every one of these CVEs is listed in the CISA Known Exploited Vulnerabilities catalog (CISA, n.d.).

That pattern is structural. It is not the fault of any single vendor. Network-layer remote access works by stretching the corporate perimeter out to a remote device. The concentrator that terminates the tunnel is therefore a high-value target, and once it falls, the attacker lands on a routable position inside the network. Identity-aware reverse proxies start from the opposite assumption. The pattern has production roots in Google's BeyondCorp program (Cittadini et al., 2016; Ward & Beyer, 2014), and it drops the perimeter premise entirely. An IAP terminates the user's traffic at the application layer, authenticates against an enterprise identity provider, and authorizes each request individually, so the user never gains a routable network position.

1.1 Research Question

For remote access to internal web applications, does an identity-aware reverse proxy architecture deliver measurably stronger CISA Zero Trust Maturity Model (ZTMM) alignment than a network-layer VPN architecture when evaluated through hands-on lab testing?

1.2 Hypothesis

IAP architectures will outperform VPN architectures in the Networks and Applications and Workloads pillars of the CISA ZTMM. This gap is architectural. It stems from how each model authorizes access, regardless of which product is more mature. A proxy that authorizes each request and never hands out network-layer reachability cannot produce the same default blast radius as a tunnel that places the user on a routable subnet and then depends on bolted-on controls (internal firewalls, segmentation, and access control lists) to contain that reach. That gap is expected to hold regardless of any one vendor's feature set.

2. Research Methodology

2.1 Research Approach

The research adapts the test-driven framework that Carstensen (2025) used for ZTNA evaluation, applying it to compare two architectural categories rather than to rank products within one. A controlled lab is built with two location configurations (untrusted remote and trusted corporate) and a datacenter network containing the protected internal services. Six products are tested: three network-layer VPN products and three identity-aware reverse proxy products. The specific products are named throughout (OpenVPN Access Server, FortiGate, and SoftEther in the VPN category, and Cloudflare Access, Microsoft Entra Private Access, and Pomerium in the IAP category) so that the experiment can be independently reproduced. The battery comprises 21 tests mapped to the ZTMM pillars: 3 Identity, 4 Device, 5 Network, 6 Application, and 3 Data. Each test produces a Pass, Partial, or Fail outcome against explicit Success and Failure criteria. The test-results matrix is the primary deliverable. Lab specifications, per-product deployments, and step-by-step test procedures are in Appendix A.

This research uses a quantitatively dominant approach in the sense described by Johnson and Christensen (2004), in which quantitative, mixed, and qualitative methods are distinguished by their orientation to the scientific method, their objectives, their focus, the nature of the data, and the form of the final report. The method here is deductive. This research tests a specific hypothesis about architectural enforcement capability (Section 1.2) against structured outcomes from a controlled lab setting. The numeric data come from a single instrument: the 21-test battery, with each test scored as Pass, Partial, or Fail against explicit criteria. The analysis then examines how the architectural category aligns with the CISA Zero Trust Maturity Model. The written interpretation of why each result came out the way it did is a qualitative supplement, but the scored matrix is the main analytic tool.

In the SANS Technology Institute's research-strategy taxonomy (SANS, 2021), this fits the “prove or disprove something” pattern. The proposition is that one

architectural category aligns measurably better with Zero Trust than the other, and the lab supplies evidence for or against it.

The independent variable is access architecture, treated as a categorical choice between network-layer VPN and identity-aware reverse proxy. Nested inside it are the specific products within each category, the three VPN products, and the three IAP products. That nested variable was included to see whether the architectural effect dominates the product-implementation effect or is swamped by it. The dependent variables are the 21 per-test outcomes mapped to the five ZTMM pillars (CISA, 2023). Each is scored Pass = 1, Partial = 0.5, or Fail = 0, then rolled up to pillar-level scores, product-level scores, and category means so the architectures can be compared directly.

The two comparison groups are the three VPN products and the three IAP products. To isolate access architecture as the variable under test, the lab environment, identity provider, attack tooling, and test procedures were held constant across all six evaluations. Each product was configured to vendor-documented best practice. The output is a 6×21 outcome matrix that supports comparisons both within a category (product against product) and between the two categories (VPN against IAP).

The research follows the steps of the scientific method as taught in the SANS Research Methods coursework. Section 1 covers the observation and the motivation, namely that mass exploitation of VPN appliances has become a primary ransomware initial access vector. The problem and research question are in Section 1.1, the hypothesis in Section 1.2, and the scope in Section 2.2. Test design is built up in Sections 2.5 and 2.6 and spelled out in Appendix A. Section 3.1 summarizes the procedure for each test in the battery, and Appendix A.9 reproduces them step by step. Section 3.2 presents the data analysis. Section 5 states the conclusions and whether the hypothesis holds.

2.2 Scope

The use case is enterprise remote access to internal web applications. Three things are out of scope as applications that the access product must serve: software-as-a-service access, legacy thick-client applications that need non-HTTP protocols, and attacks that compromise the supply chain or the identity provider from outside the access plane itself.

Out of scope here means not evaluated as a published application; it does not remove non-web services from the threat model. The lab keeps an internal SMB file server (FILE01) on the datacenter subnet as a lateral-movement target because a real intruder probes whatever reachability is granted, regardless of protocol. The Networks-pillar tests use that server only as such a target, to measure post-authentication blast radius, not as an application under test, while the Applications and Data pillars are exercised over the in-scope HTTP path.

2.3 Zero Trust Defined

Zero Trust rejects the idea that anything inside a network perimeter is trusted just because it is inside. Kindervag (2010) introduced the concept at Forrester Research, and NIST Special Publication 800-207 (Rose et al., 2020) later formalized it for federal use. SP 800-207 sets out seven tenets: continuous verification, least privilege access, device and user authentication, dynamic policy enforcement, secure access regardless of network location, visibility and analytics, and the assumption of breach. Its architectural primitives are the Policy Decision Point and the Policy Enforcement Point, and it names three deployment patterns: network microsegmentation, identity-aware proxies, and software-defined perimeter.

The identity-aware proxy pattern predates that federal codification by close to a decade. Google launched its BeyondCorp program in 2011 after Operation Aurora and documented it across a series of practitioner papers in USENIX ;login: between 2014 and 2017 (Cittadini et al., 2016; Escobedo et al., 2017; Osborn et al., 2016; Ward & Beyer, 2014). The Cittadini paper describes Google's production Access Proxy and is the closest direct prior art to the IAP products tested here.

2.4 Measuring Zero Trust

The CISA Zero Trust Maturity Model version 2.0 (CISA, 2023) turns the Zero Trust concept into a five-pillar assessment, with four stages per pillar: Traditional, Initial, Advanced, and Optimal. The five pillars are Identity, Devices, Networks, Applications, Workloads, and Data. Three cross-cutting capabilities run across all of them: Visibility and Analytics, Automation and Orchestration, and Governance. Office of Management

Henry Cheung, henry.cheung@student.sans.edu

and Budget (OMB) Memorandum M-22-09 directs federal civilian agencies to adopt the framework (OMB, 2022). The DoD Zero Trust Reference Architecture offers a second federal view, organized into seven pillars (Department of Defense Chief Information Officer [DoD CIO], 2022).

This research uses the CISA ZTMM as the rubric that anchors the test design. Each test in Section 3 maps to a specific pillar capability. The battery is not meant to cover every ZTMM criterion. It is a focused subset selected to highlight the differences between the VPN and IAP categories, following the targeted sampling approach validated by Carstensen (2025).

2.5 Lab Environment

A controlled lab was built so every product was evaluated under the same conditions. The lab has two location configurations and a single datacenter network holding the protected internal services. Both locations reach the same datacenter via the product under test, which keeps the access architecture as the only thing that changes between evaluations. Appendix A documents the network specifications, virtual machine builds, identity provider setup, internal services, endpoint configurations, and attack tooling in full.

There are three logical networks. The Untrusted Location represents a remote user on an unmanaged network or a hostile public Wi-Fi network. Two Windows 11 endpoints connect from there to the datacenter through the product under test: CLIENT01 is compliant and CLIENT02 is not. The Trusted Location stands in for a corporate office and supports the trusted-network-detection tests. The Datacenter, at 10.0.11.0/24, holds the protected resources. Those are a Windows Server 2016 file server (FILE01) with shares containing a mix of benign and simulated sensitive files, and an Ubuntu 24.04 server (WEB01) running the Damn Vulnerable Web Application. FILE01 is left unpatched for MS17-010 on purpose, to support the EternalBlue test in Section 3.1.4.

2.6 Tested Solutions

Six products are evaluated, three from each architectural category. The products are explicitly named so that the experiment can be reproduced; the analysis remains

Henry Cheung, henry.cheung@student.sans.edu

focused on architectural enforcement behavior, following the test methodology used by Carstensen (2025).

Three network-layer VPN products represent a range of depth of capability. OpenVPN Access Server is an SSL VPN that represents the baseline network-layer remote access pattern, with minimal Zero Trust-adjacent features. FortiGate, deployed as the FortiGate VM evaluation appliance, is a market-leading commercial next-generation firewall and SSL VPN with modern Zero Trust feature additions, including device posture via FortiClient EMS, conditional access, and integrated WAF and IPS. SoftEther is a free, open-source multi-protocol VPN server with broad protocol support and an SSL VPN web portal but limited native Zero Trust integration.

Three identity-aware reverse proxy products represent different deployment models. Cloudflare Access, paired with Cloudflare Tunnel, is a globally distributed cloud-native identity-aware proxy with outbound-only connector tunneling and an integrated edge WAF. Microsoft Entra Private Access is an IdP-native, identity-aware proxy with deep integration with Conditional Access. Pomerium is an open-source, smaller-footprint identity-aware proxy targeting developer and mid-market deployments. Within this category, two implementation styles appear: pure Layer 7 reverse proxies that terminate and forward HTTP only (Pomerium and Cloudflare Access in its HTTP mode), and identity-aware connectors that tunnel arbitrary authorized TCP or UDP to published private resources (Microsoft Entra Private Access). Both withhold default network reachability and authorize per application, which is the property under test; they differ in protocol breadth, and that difference is why Entra Private Access can publish (route) a non-HTTP service such as SMB while a pure reverse proxy cannot, though it does not inspect that non-HTTP traffic at Layer 7.

Products were selected to represent a spectrum of capability within each architecture while remaining obtainable for an independent researcher to reproduce: free or open-source baselines (OpenVPN Access Server, SoftEther, and Pomerium), a commercial evaluation appliance (FortiGate VM, 15-day evaluation license), and trial- or free-tier cloud services (Cloudflare Access on the free tier and Microsoft Entra Private Access via a Microsoft 365 E5 or Entra Suite trial). All six products were deployed in the Henry Cheung, henry.cheung@student.sans.edu

lab and configured according to vendor documentation. Where a product offered multiple configuration paths, the configuration most closely aligned with vendor-documented best practices was used to ensure each product received a fair evaluation. Per-product deployment specifications, including license tiers, are documented in Appendix A.

Two scoping choices follow from testing architectures rather than individual appliances. FortiGate is evaluated in its SSL-VPN mode as the representative of the network-layer VPN architecture; FortiOS also ships a native ZTNA application-gateway module, but that module is itself an identity-aware proxy and is deliberately excluded, because scoring it would place one appliance in both categories and confound the comparison. The same rule holds throughout: each product is exercised in the mode that represents its assigned architecture, and vendor features that cross into the other architecture are out of scope and noted where relevant. The six products also span a deliberate range of capability tiers within each category, from open-source baselines to integrated commercial suites, so results on the feature-dependent pillars (Applications and Data) reflect product tier as well as architecture; the Networks pillar is the cleanest measure of the architectural difference itself.

3. Findings and Discussion

3.1 Testing Procedures

Every product was put through the identical battery, organized by CISA ZTMM pillar. Each test returns Pass, Partial, or Fail based on the stated success and failure criteria. The format is adapted from Carstensen (2025) and reworked here for comparison between the VPN and IAP categories. Appendix A gives the step-by-step procedures, with the exact commands and tools.

3.1.1 Identity Tests

Three tests cover the CISA ZTMM Identity pillar (CISA, 2023) and the NIST SP 800-207 tenets of least privilege and continuous verification (Rose et al., 2020). They

check user-based access differentiation, step-up multi-factor authentication for sensitive resources, and enforcement of phishing-resistant authentication factors.

Test	Success Criteria	Failure Criteria
User-Based Access Differentiation	Policy correctly enforced for both users; ztnauser2 cannot access WEB01.	Policy cannot be configured or both users access WEB01.
Step-Up MFA	MFA prompt triggered only for WEB01 access.	Either always-on MFA, no MFA, or MFA cannot be configured.
Phishing-Resistant MFA	TOTP-only access to WEB01 denied; FIDO2 access succeeds.	Phishing-resistant MFA cannot be enforced as a policy condition.

Table 1: Identity Tests and Success/Fail Criteria

3.1.2 Device Tests

Four tests cover the CISA ZTMM Devices pillar. Each maps to the NIST SP 800-207 tenet of device authentication (Rose et al., 2020) and checks one posture condition: disabled disk encryption, missing endpoint protection, disabled endpoint protection, and outdated malware definitions.

Test	Success Criteria	Failure Criteria
Disk Encryption	Detected disabled BitLocker and blocked access.	Lacked detection capability or allowed access from unencrypted device.
Endpoint Protection Installed	Detected presence of Defender and enforced policy.	Lacked visibility or did not enforce policy.
Endpoint Protection Running	Detected disabled Defender and blocked access.	Failed to detect operational state or enforce policy.
Endpoint Protection Definitions Up-to-Date	Detected outdated definitions and blocked access.	Lacked capability or did not enforce policy.

Table 2: Device Tests and Success/Fail Criteria

3.1.3 Network Tests

Five tests cover the CISA ZTMM Networks pillar. This is where the VPN and IAP architectures were expected to differ the most, so the tests are built to expose that difference. They check external inbound port exposure to internet attackers, network segmentation when an endpoint connects from an untrusted location, service cloaking

against authenticated reconnaissance scans, post-authentication reachability to unauthorized hosts, and whether MITRE ATT&CK lateral-movement reconnaissance techniques work from an authenticated session. Two of these, external inbound port exposure and post-authentication reachability, are by design close to definitional architectural discriminators: an outbound-connector model has no inbound port to expose and grants no routable subnet, so it is expected to pass while a gateway VPN is expected to fail. They are included to quantify the architectural contrast under a common rubric, not as open empirical questions; the service-cloaking and lateral-movement tests carry more empirical weight.

Test	Success Criteria	Failure Criteria
External Inbound Port Exposure	Zero inbound TCP ports exposed to untrusted internet. A Partial is recorded if only an encrypted control-plane port is exposed without application-protocol fingerprinting.	One or more service ports exposed and fingerprintable from external scan.
Network Segmentation (Untrusted)	Blocked LAN access when connected from untrusted location.	Allowed LAN traffic from untrusted location.
Service Cloaking	Nmap could not identify open ports or fingerprint services.	Services fingerprinted without authorization.
Post-Auth Network Reachability	No unauthorized hosts respond to ping or TCP scan.	Unauthorized hosts respond and services are reachable.
Lateral Movement Reconnaissance	T1018, T1046, T1135 all fail to enumerate.	One or more reconnaissance techniques succeed.

Table 3: Network Tests and Success/Fail Criteria

3.1.4 Application Tests

Six tests cover the CISA ZTMM Applications and Workloads pillar. The first two measure the product's Layer 7 visibility and policy capability, including how far that reach extends over the SMB path to FILE01, which Section 2.2 treats as a lateral-movement target rather than a served application. The other four are exploitation tests: the EternalBlue (MS17-010) exploit against the unpatched FILE01 server over SMB, plus Local File Inclusion, command injection, and SQL injection drawn from the OWASP Top Ten (OWASP Foundation, 2021) against DVWA over HTTP.

Test	Success Criteria	Failure Criteria
Application Layer Visibility	Application-protocol identification in logs.	Logs limited to network/transport layer only.
Application-Based Policies	App-layer policy can be expressed and enforced.	App-layer policy not supported.
MS17-010 Exposure Outcome	FILE01 not compromised; no Failed.txt created (by detection, prevention, or no network route).	Exploit succeeds and Failed file created.
LFI Detection	Both payloads blocked and logged.	Either payload exfiltrates file contents.
Command Injection Detection	All three commands blocked and logged.	One or more commands execute on server.
SQL Injection Detection	Both payloads blocked and logged.	Either payload returns database content.

Table 4: Application Tests and Success/Fail Criteria

3.1.5 Data Tests

Three tests cover the CISA ZTMM Data pillar: Personally Identifiable Information data loss prevention, Payment Card Industry data loss prevention, and detection of malicious file transfers. To stay within the web-application use case, all three are exercised over the in-scope HTTP path: the sample files are uploaded through the proxied WEB01 application over HTTPS rather than copied over SMB, so the Data pillar measures whether the access path, together with the platform controls deployed around it, detects and blocks the sensitive upload; Section 3.2.7 attributes the mechanism for each product.

Test	Success Criteria	Failure Criteria
PII Data Loss Prevention	DLP policy detected and blocked PII transfer.	Lacked DLP capability or did not block.
PCI Data Loss Prevention	DLP policy detected and blocked PCI transfer.	Lacked PCI inspection or did not block.
Malicious File Detection	All three malicious files detected and blocked.	One or more malicious files transferred undetected.

Table 5: Data Tests and Success/Fail Criteria

3.2 Test Results

All six products were taken through the complete battery in the lab, following the per-test procedures in Appendix A.9. Each outcome was captured with its supporting evidence (nmap output, proxy and host logs, exploitation console transcripts, and screenshots) and scored against the success and failure criteria in Tables 1 through 5. The aggregated matrix follows, and the results are then discussed pillar by pillar.

		VPN Architecture			IAP Architecture		
Pillar	Test	OpenVPN AS	FortiGate	SoftEther	Cloudflare Access	Entra Private Access	Pomerium
Identity	User-Based Access Differentiation	Pass	Pass	Pass	Pass	Pass	Pass
Identity	Step-Up MFA	Fail	Pass	Partial	Pass	Pass	Pass
Identity	Phishing-Resistant MFA	Fail	Pass	Partial	Pass	Pass	Partial
Device	Disk Encryption	Fail	Pass	Pass	Pass	Pass	Pass
Device	Endpoint Protection Installed	Fail	Pass	Pass	Pass	Pass	Pass
Device	Endpoint Protection Running	Fail	Pass	Partial	Pass	Pass	Pass
Device	Endpoint Protection Definitions Up-to-Date	Fail	Partial	Fail	Pass	Pass	Pass
Network	External Inbound Port Exposure	Fail	Fail	Fail	Pass	Pass	Pass
Network	Network Segmentation (Untrusted)	Fail	Partial	Partial	Pass	Pass	Partial
Network	Service Cloaking	Fail	Fail	Fail	Pass	Pass	Partial
Network	Post-Auth Network Reachability	Fail	Fail	Fail	Pass	Pass	Pass
Network	Lateral Movement Reconnaissance	Fail	Fail	Fail	Pass	Pass	Pass
Application	Application Layer Visibility	Fail	Partial	Fail	Pass	Pass	Partial
Application	Application-Based Policies	Fail	Partial	Partial	Pass	Pass	Pass
Application	MS17-010 Exposure Outcome	Fail	Partial	Fail	Pass	Pass	Pass
Application	LFI Detection	Fail	Partial	Fail	Pass	Pass	Fail
Application	Command Injection Detection	Fail	Partial	Fail	Pass	Partial	Fail

		VPN Architecture			IAP Architecture		
Pillar	Test	OpenVPN AS	FortiGate	SoftEther	Cloudflare Access	Entra Private Access	Pomerium
Application	SQL Injection Detection	Fail	Partial	Fail	Pass	Partial	Fail
Data	PII Data Loss Prevention	Fail	Partial	Fail	Pass	Pass	Fail
Data	PCI Data Loss Prevention	Fail	Partial	Fail	Pass	Pass	Fail
Data	Malicious File Detection	Fail	Partial	Fail	Partial	Pass	Fail

Table 6: Test Results Matrix

One split dominates the matrix. On the five Network tests, the two categories barely overlap: every VPN product fails or partials each one, and every IAP product passes or partials each one. The pillar-by-pillar walk-through below covers where else they diverge and where they unexpectedly converge.

3.2.1 Identity Test Results

All six products handle user-based access differentiation. That is table stakes, and it reveals nothing about the difference between the categories.

Step-up MFA splits the categories, but only partway. OpenVPN Access Server has no policy primitive for it at all. FortiGate can perform step-up MFA once it is configured to connect to an external IdP that provides conditional access. SoftEther only enforces MFA at session establishment, which earns a Partial. All three IAP products do step-up MFA natively through the IdP.

Phishing-resistant MFA enforcement works on FortiGate and on all three IAP products, again through the IdP. OpenVPN Access Server and SoftEther cannot enforce the authentication factor type as a policy condition.

Identity is the one pillar where a modern commercial VPN can close most of the gap. Strong IdP integration brings FortiGate within range of the IAP products, while the lighter VPN deployments fall behind. The architectural difference is muted here because both sides lean on the same external IdP for authentication strength.

3.2.2 Device Test Results

Device posture opens up more daylight between the two. OpenVPN Access Server has no native posture checking and fails all four device tests. FortiGate performs posture checks only when the tunnel comes up, with no re-evaluation during the session. So it earns Partial on the running-state and definition-currency tests, where a posture change mid-session goes unnoticed. SoftEther does basic posture but has no definition-currency check.

Cloudflare Access, Microsoft Entra Private Access, and Pomerium all pass all four. Cloudflare enforces posture through its WARP client; Entra Private Access and Pomerium both gate access through the same Intune device-compliance Conditional Access policy on the shared Entra ID tenant, so a device that fails disk-encryption, endpoint-protection, or definition-currency checks is denied at sign-in. Because the identity provider is the controlled variable held constant across all six products, any product federated to it can enforce the same device-compliance policy; crediting Entra Private Access for that mechanism while withholding it from Pomerium would have been inconsistent, so the same policy is applied to both.

These tests demonstrate admission control. A VPN checks posture when the tunnel comes up and rarely checks again; the proxy and connector models recheck device compliance at sign-in and deny non-compliant devices. Continuous mid-session reevaluation is a documented capability of the per-request reverse-proxy and Intune-gated models, but this battery demonstrates compliant-versus-non-compliant admission rather than proving that mid-session posture changes are caught in real time. The continuous-validation tenet in NIST SP 800-207 (Rose et al., 2020) describes the stronger behavior; the test outcomes show the admission-time gap between the architectures.

3.2.3 Network Test Results

The Networks pillar is where the two architectures diverge most, and it is the most direct test of the hypothesis. All five fall the same way, the VPNs failing and the IAPs passing.

External inbound port exposure is the clearest case. Every VPN product must expose at least one inbound TCP port on a customer-managed gateway, typically 443 for an SSL VPN portal or 4500 for IPsec. The IAP products use outbound-only connectors that the corporate network opens toward the provider's edge, so there is nothing inbound to scan. From an external attacker's host, an nmap scan returns zero open ports against Cloudflare Access, Microsoft Entra Private Access, and Pomerium. The same scan against OpenVPN Access Server, FortiGate, and SoftEther returns the gateway's listening port, and in some cases, banner information detailed enough to identify the specific product.

Network segmentation from an untrusted location separates products that adjust their posture based on the origin of a connection. In the default routed configuration tested, OpenVPN Access Server applied no origin-based logic and blocked no local-LAN traffic from the untrusted location; the product does offer user- and group-level access-control rules, but those gates that internal destinations a user can reach rather than providing the origin-aware segmentation this test measures. FortiGate and SoftEther achieve partial segmentation through always-on tunnel modes that force all client traffic through the tunnel, but in the SSL-VPN mode under test neither varied its posture by trusted versus untrusted origin. FortiOS can make that distinction through FortiClient EMS on-net/off-net tagging, but that capability belongs to its ZTNA module, which is out of scope here (Section 2.6). Cloudflare Access and Microsoft Entra Private Access pass using traffic-steering rules tied to network-origin detection; Pomerium covers it partially.

Service cloaking against an authenticated Nmap scan separates the two categories again. By default, a VPN places the user on a routable subnet, so any service on that subnet that is not specifically firewalled or microsegmented can be fingerprinted; in the representative default deployments tested, those additional controls were not layered on, and the services were fingerprinted. An IAP carries only the authorized application traffic through the proxy, so an nmap scan of other internal addresses returns nothing. There is no network path to them to begin with.

Post-authentication reachability is the most direct measure of blast radius. From an authenticated session, OpenVPN Access Server, FortiGate, and SoftEther all return Henry Cheung, henry.cheung@student.sans.edu

responses for every live host on the datacenter subnet. Cloudflare Access, Microsoft Entra Private Access, and Pomerium respond only for the application the user is authorized to reach. Ping, traceroute, and TCP scans against any other internal address get no reply.

Lateral movement reconnaissance, run with ATT&CK T1018, T1046, and T1135, fails completely against the IAP products and succeeds completely against the VPNs. Those techniques need network-layer reachability, which the proxy model never provides.

The Network results are the core finding of the paper. They support the structural argument that the security difference between the two models comes down to where authorization happens. Authorize at the network layer and the user, by default, inherits a routable subnet; authorize at the application layer and the user inherits a single application. A VPN can be aligned with the IAP's posture by layering in internal firewalls, microsegmentation, and network access control, but that containment is additive, optional, and operationally costly to sustain, whereas the IAP withholds network reachability by default. The gap the matrix captures is therefore one of default posture and operational burden, not of absolute capability, and adding features to the VPN's management plane does not change its default posture.

3.2.4 Application Test Results

Application-layer visibility separates the categories, but not uniformly within the IAP group. VPN products operate at Layer 3 and Layer 4; their logs identify source and destination IP and port, but not the HTTP method, URL, or SMB share name. The reverse-proxy IAPs, Cloudflare Access and Pomerium, terminate the user connection at the application layer and log full Layer 7 details for the HTTP they carry. Entra Private Access is a connector that tunnels the published service rather than serving as a full reverse proxy, so it yields application-aware logging for the HTTP application but does not perform Layer 7 inspection of arbitrary protocols. FortiGate is awarded a Partial: its integrated WAF module produces application-layer logs for HTTP only, while SMB traffic to FILE01 is logged at the network layer.

Application-based policies follow the same shape. The reverse-proxy IAPs (Cloudflare Access and Pomerium) and Entra Private Access can express and enforce HTTP application-layer rules by host, URL, method, and identity, and pass. FortiGate and SoftEther can express only coarse application-aware rules through their WAF or portal, earning Partial. OpenVPN Access Server, operating at the network layer, cannot express an application-layer policy at all and fails.

The web-application exploitation tests (Local File Inclusion, command injection, and SQL injection, all OWASP-aligned) break that clean split, tracking WAF capability rather than architectural category. Cloudflare Access passes them on its integrated edge WAF; FortiGate, also with an integrated WAF, performs partially; Pomerium, an HTTP proxy with no bundled WAF, fails them. MS17-010 (EternalBlue) is grouped separately because it is not a web attack: it targets SMB on port 445, which no WAF inspects, so its outcome is governed by network reachability rather than Layer 7 filtering. OpenVPN Access Server and SoftEther place the client on a routable subnet that reaches FILE01:445, so the exploit completes, and they fail; FortiGate's IPS signature for MS17-010 partially blocks it. The IAP products publish only the authorized HTTP application and provide no Layer 3 path to FILE01:445, so for Cloudflare Access and Pomerium, the exploit cannot reach its target and is recorded as a Pass on the same service-cloaking grounds that drive the Network-pillar results, not on any WAF.

Microsoft Entra Private Access is the exception among the IAPs: it publishes the FILE01 SMB service explicitly, so EternalBlue does reach the host, and its Pass comes from Defender for Endpoint on FILE01 rather than from cloaking. This test is also where observation diverged from prediction. Pomerium had been predicted to fail MS17-010 for lack of a WAF, but a WAF is irrelevant to an SMB exploit, and Pomerium publishes no SMB route, so the attack never reaches FILE01. The corrected observed result is a Pass, which raises Pomerium's Application score to 2.5 and its total to 13.0.

Application-layer threat protection against web attacks, then, is product-driven rather than architectural: a VPN with a strong WAF beats an IAP without one. Layer 7 visibility is the exception. An IAP terminates user traffic at the application layer to do its job, so it produces Layer 7 logs as a byproduct rather than as a feature bought on top.

Henry Cheung, henry.cheung@student.sans.edu

3.2.5 Data Test Results

Data loss prevention was tested over the in-scope HTTP upload path (Section 3.1.5), and on that path, it tracks content-inspection capability rather than architecture. OpenVPN Access Server and SoftEther fail the PII and PCI tests: both are Layer 3/4 tunnels with no content inspection, so the upload passes unread. FortiGate earns Partial because once its SSL-VPN terminates the session, it can apply its DLP and antivirus profiles to the HTTP request bound for the protected web application.

Among the IAPs, Cloudflare Access blocks the PII and PCI uploads at its edge DLP, earning a Pass on both. Microsoft Entra Private Access also blocks all three, but, as Section 3.2.7 details, the enforcement comes from surrounding Microsoft platform controls (Purview DLP and Defender for Endpoint at the managed endpoint and tenant) rather than from the access connector inspecting the upload in line; the score reflects what the deployed Microsoft stack achieved, not an access-plane capability. Pomerium has no DLP or malware inspection of its own and fails all three.

Malicious file detection follows the same capability line. OpenVPN Access Server and SoftEther have no content inspection and fail. FortiGate blocks the upload inline through its antivirus profile, a Partial, alongside its DLP. Cloudflare Access sandboxes and analyzes the upload, but enforcement lags enough that the first transfer still completes, so it earns a Partial; Microsoft Entra Private Access blocks through Defender for Endpoint on the managed device, an endpoint control rather than the access connector; Pomerium fails.

So the Data pillar behaves like the Applications pillar: product features drive the result, and access architecture has little bearing. Terminating traffic at the application layer gives an IAP the opportunity to inspect content, and Microsoft Entra Private Access and Cloudflare Access take it. But a VPN with inline DLP and antivirus, FortiGate, also inspects traffic once it's HTTP, while an IAP that bundles nothing, Pomerium, inspects nothing. The architecture supplies only the opportunity to inspect; whether that inspection happens depends on the product.

3.2.6 Aggregated Pillar Comparison

Table 7 rolls the matrix in Table 6 up into pillar-level scores per product, with each Partial counted as 0.5, then takes the VPN and IAP category means and the gap between them. The gap is shown in two ways: as an absolute score difference and as a percentage of the pillar's maximum possible score. The percentage matters because the pillars carry different numbers of tests, with Identity at 3, Networks at 5, Applications at 6, and so on. In the table, Pass = 1, Partial = 0.5, and Fail = 0; VPN Mean and IAP Mean are the arithmetic means of the three products in each category, Gap (Abs) is IAP Mean minus VPN Mean, and Gap (% of Max) expresses that gap as a percentage of the pillar's maximum possible score.

Pillar	Max	OpenVPN AS	FortiGate	SoftEther	VPN Mean	Cloudflare Access	Entra Private Access	Pomerium	IAP Mean	Gap (Abs)	Gap (% of Max)
Identity	3	1.0	3.0	2.0	2.00	3.0	3.0	2.5	2.83	+0.83	+27.7%
Devices	4	0.0	3.5	2.5	2.00	4.0	4.0	4.0	4.00	+2.00	+50.0%
Networks	5	0.0	0.5	0.5	0.33	5.0	5.0	4.0	4.67	+4.33	+86.7%
Apps & Workloads	6	0.0	3.0	0.5	1.17	6.0	5.0	2.5	4.50	+3.33	+55.6%
Data	3	0.0	1.5	0.0	0.50	2.5	3.0	0.0	1.83	+1.33	+44.4%
Total	21	1.0	11.5	5.5	6.00	20.5	20.0	13.0	17.83	+11.83	+56.3%

Table 7: Aggregated Test Results by Pillar with Architectural Comparison

The aggregate gap is 11.83 points out of 21, or 56.3 percent of the maximum. The IAP architecture comes out ahead on every pillar, but the size of that lead varies widely from one pillar to the next.

Networks show the biggest gap, 86.7 percent of the maximum. Every IAP product scored 4.0 or higher out of 5.0, and every VPN product scored 0.5 or lower. That is the sharpest split in the matrix, and it is exactly what the hypothesis predicted. Separating user identity from network reachability produces a measurable enforcement gap, and even the most modern VPN here does not bridge it.

Applications and Workloads shows a 55.6 percent gap and Data a 44.4 percent gap. These are the two pillars where product capability drives the result more than

Henry Cheung, henry.cheung@student.sans.edu

architecture does: Cloudflare Access and Microsoft Entra Private Access pull the IAP mean up with their integrated WAF and DLP, Pomerium pulls it down with neither, and on the HTTP path FortiGate's inline DLP and antivirus lift the VPN mean as well. The advantage of these pillars is real but product-dependent, so they reflect product tier as much as architecture.

Identity shows the smallest gap, 27.7 percent, because both architectures draw their authentication strength from the same external IdP, Microsoft Entra ID; the real difference there is enforcement cadence. Devices are wider, 50.0 percent: all three IAPs gate device compliance through the shared Entra and Intune stack, while among the VPNs, only FortiGate does posture at all (through FortiClient EMS), with OpenVPN Access Server doing none, and SoftEther only partial. That makes Devices as much a platform-integration result as an architectural one. Every Entra-federated product can use the same Intune Conditional Access, and the gap reflects which products were wired to do so.

The IAP scores now run from 13.0 to 20.5, and the VPNs from 1.0 to 11.5, so every IAP outscores every VPN overall, not only on Networks. The spread that remains within the IAP category is on the feature-dependent pillars: Pomerium, the lowest IAP at 13.0, trails Cloudflare Access and Entra Private Access because it bundles no WAF or DLP, even though it matches them on Identity, Devices, and Networks through the shared identity platform and the proxy architecture. The Architectural category cleanly predicts the network-exposure result; the Application and Data differences track product features.

Two caveats apply when reading these aggregates. First, the headline total gap blends the effects of different kinds. The Network-pillar difference is largely structural (a Layer-3 VPN is expected to fail Layer-3 reachability tests), whereas the Application and Data differences depend heavily on whether a given product ships a WAF or DLP, which is a product-tier question rather than an architectural one. The Network pillar is therefore the cleanest architectural signal in the matrix, and the total should be read as a summary rather than a single architectural measure. Second, the results worth foregrounding are the ones that architecture does not dictate. Identity converges: FortiGate, wired to the same identity provider, nearly matches the IAPs, so the category advantage there is small.

Henry Cheung, henry.cheung@student.sans.edu

Devices widen once every Entra-federated product, Pomerium included gates compliance through the shared Intune stack, which makes that pillar a platform-integration result more than an architectural one. The remaining within-IAP spread is on the feature-dependent pillars, where Pomerium, lacking a bundled WAF or DLP, trails Cloudflare Access and Entra Private Access. The contribution of the Network-pillar result is not that an IAP wins, which the architecture all but guarantees, but that the win is quantified against an external, reproducible rubric and shown to be unmoved by adding modern features to the VPN.

Predicted versus observed. The per-test predictions recorded in advance in Appendix A.10 served as the benchmark against which each observed outcome was scored. Across the 126 test-product cells, observation matched prediction in every case but one: Pomerium on MS17-010, predicted Fail but observed Pass for the reason given in Section 3.2.4. That level of agreement is expected for this instrument and is not a sign of a thin run. Each test measures a deterministic enforcement property (whether an inbound port answers, whether a posture primitive exists and fires, whether traffic content is inspected), so an architecturally correct prediction converges on the observed result rather than scattering around it. The single divergence is the kind of method it is built to surface: it fell on the one cell where the capability reasoning was subtle, since a WAF cannot touch an SMB exploit, and an HTTP-only proxy never routes one, and executing the test is what corrected it. The raw evidence for each cell (nmap output, proxy and host logs, exploitation console transcripts, and screenshots) was retained for audit.

3.2.7 Controls Attributed to the Access Product versus the Surrounding Platform

Because several pillars draw on controls that sit outside the access product, it is worth stating plainly which results belong to the access architecture and which are inherited from the surrounding platform. The Networks pillar is the only one attributable to the access architecture itself: the outbound-connector and reverse-proxy models withhold default network reachability and cloak internal services, and no surrounding product is required to produce that result. The Identity pillar is supplied by the shared identity provider, Microsoft Entra ID, held constant across all six products, so it

Henry Cheung, henry.cheung@student.sans.edu

differentiates products by configuration rather than by access architecture. The Devices pillar is supplied by posture sources that sit beside the access product, namely Cloudflare's WARP client, FortiClient EMS for FortiGate, and Intune device-compliance Conditional Access for Entra Private Access and Pomerium, again a platform-integration result rather than an architectural one.

The Applications and Data pillars are the most platform-dependent. Layer 7 visibility is architectural for the reverse proxies, but the threat-blocking results on the OWASP tests come from WAF features (Cloudflare's edge WAF, FortiGate's WAF and IPS), and the Data results come from content-inspection controls in the surrounding stack: Cloudflare's edge DLP, and for Entra Private Access, Microsoft Purview DLP and Defender for Endpoint operating at the endpoint and tenant rather than the access connector inspecting traffic in line. Microsoft's in-line equivalent, Global Secure Access network content filtering with Purview, is in preview, supports files over HTTP/1.1 only, and is documented for Internet Access egress to unmanaged cloud applications rather than for Private Access to internal applications, so the Entra Data result should be read as a property of the deployed Microsoft platform, not of the access plane. The practical consequence is that the paper's defensible architectural claim is confined to the Networks pillar; the Application and Data advantages are real in the tested deployments but reflect bundled product and platform features and would move with a different product or license tier.

4. Recommendations and Implications for Future Research

4.1 Recommendations for Practitioners

1. Security architects should make identity-aware reverse proxy access the default for new internal web applications. A new web application placed behind a VPN should require a written architectural justification, not just the absence of objections. The Network-pillar results in Section 3.2.3 show that adding features to a VPN does not close the gap.

2. Security teams should treat the existing VPN footprint as an inventory to be drawn down. They should keep one authoritative list of the internal services reachable over VPN, review it on a set schedule, and migrate the web applications onto identity-aware proxy access. Anything that must stay on the VPN needs compensating controls: segmentation away from crown-jewel systems, faster patching, application-layer logging, and detection engineering against the ATT&CK paths in Section 3.1.3.
3. Security teams should require phishing-resistant MFA for all IAP access and for VPN access wherever the product supports it. The proxy model's benefits still rest on the authentication primitive at the identity provider, and weak MFA undercuts the whole thing.
4. Practitioners should not treat the architecture label as the whole answer. Inside the IAP category, application-layer protection and DLP vary widely. Sections 3.2.4 and 3.2.5 show that the gap between Cloudflare Access or Microsoft Entra Private Access and Pomerium is as wide on the Application and Data pillars as the gap between IAPs and VPNs. Each IAP should be evaluated against the actual use case instead of assuming the category name guarantees the capability.
5. Organizations should plan for a hybrid setup as the realistic steady state for the next three to five years. VPNs are still needed for non-web protocols and for legacy applications that cannot tolerate HTTP termination. The two access planes should be kept architecturally separate; a compromised VPN must not be able to reach the IAP's policy decision plane.

Build detection around the ATT&CK paths in Section 3.1.3. In VPN-protected environments, focus on T1190 against the appliance, T1078 for anomalous valid-account use, and T1018 and T1046 for lateral reconnaissance from the appliance subnet. In IAP-defended environments, focus on T1539 session token theft, T1078 anomalous authentication, and odd patterns of authorized application access, such as a user who authenticates cleanly but reaches an application they have never touched before.

4.2 Implications for Future Research

This paper distilled the CISA ZTMM into a focused 21-test battery. Future work should widen it to cover more of the model, including continuous diagnostics, dynamic risk scoring, automated policy enforcement, and real-time threat intelligence. A larger battery would also do a better job of distinguishing between the Advanced and Optimal stages, which is where these results tend to bunch up.

The lab was kept simple on purpose so the build would be easy to reproduce. Future work should extend it to additional endpoint operating systems, such as macOS, Linux, and mobile; more user roles and device types; more application architectures, from cloud-native to hybrid to legacy; and more realistic network topologies that include branch offices and roaming endpoints.

Enterprise-scale scenarios would push the architectures under production-like conditions: a full VPN-to-IAP migration, BYOD access, third-party contractor integration, and identity federation across multiple IdPs. Those would also surface scalability, interoperability, and policy-consistency problems that a single-product lab never sees.

A related line of work is detection coverage rather than prevention. The per-request logging an IAP produces is high-resolution data for behavioral detection. The open question is whether enterprises actually use that data to the level it allows. Comparative studies of detection on real or simulated incidents across the two architectures would show whether the architectural advantage translates into operational detection.

A limitation of the instrument follows from the design. Because several tests, especially on the Networks pillar, measure properties the architectures hold by definition, the close agreement between predicted and observed outcomes partly reflects how the battery was built rather than an independent empirical discovery: the predictions encode the same architectural reasoning the tests probe. The genuinely empirical results are the ones the architecture did not preordain: the convergence of the categories on Identity, the dependence of the Application and Data outcomes on bundled platform features, and the

single case (Pomerium on MS17-010) in which observation corrected a prediction. Future work should separate definitional architectural discriminators from feature-dependent tests at the design stage and weight them accordingly.

5. Conclusion

VPN exploitation now ranks among the most common ransomware initial access vectors. The question this paper set out to answer was whether identity-aware reverse proxies, used for remote access to internal web applications, actually align better with the CISA Zero Trust Maturity Model than network-layer VPNs when tested in a lab.

They do, but only in a specific sense. The strongest architectural result is on the Networks pillar: every IAP scored 4.0 or higher out of 5.0, every VPN scored 0.5 or lower, and the gap was 86.7 percent of the maximum. That gap reflects the default posture. A VPN can be constrained with internal firewalls, segmentation, and network access control, but the reachability it grants by default is structural, and feature additions to the appliance do not change it. The IAP products also outscored the VPNs on the other four pillars, but those margins rest substantially on the shared identity provider, posture sources, and bundled WAF and DLP features rather than on access architecture (Section 3.2.7), so they are better read as advantages of the deployed products and platform than of the architecture itself.

Architecture is not decisive on its own. Inside the IAP category, application-layer protection and DLP vary widely: the strongest IAP beats every VPN tested, while the weakest falls below the strongest VPN on the application-layer tests. How much of the architecture's advantage is realized still depends on the product.

For security architects, the practical move is to make IAP the default for new internal web application access and to draw the existing VPN footprint down on a schedule you can schedule. For researchers, the methodology here is reproducible and extends cleanly to broader ZTMM coverage, larger product samples, and more complex enterprise scenarios.

The defensible conclusion is specific: for remote access to internal web applications, identity-aware proxy access reduces default network reachability and blast radius more effectively than a network-layer VPN, and that advantage is architectural. Broader superiority across all Zero Trust pillars is not established by these results, as the Application and Data outcomes are entangled with platform and product features rather than with access architecture. The network-exposure finding follows from the matrix in Section 3.2 and the reasoning in Section 3.2.3; the narrower scope of the architectural claim follows from Section 3.2.7.

References

- Carstensen, D. (2025). *Evaluating zero trust network access: A framework for comparative security testing* [Master's white paper]. SANS Technology Institute. <https://www.sans.org/white-papers/evaluating-zero-trust-network-access-framework-comparative-security-testing>
- Cittadini, L., Spear, B., Beyer, B., & Saltonstall, M. (2016). BeyondCorp Part III: The access proxy. *login.*, 41(4), 28–33. USENIX Association.
- Cybersecurity and Infrastructure Security Agency. (n.d.). *Known exploited vulnerabilities catalog*. <https://www.cisa.gov/known-exploited-vulnerabilities-catalog>
- Cybersecurity and Infrastructure Security Agency. (2023). *Zero Trust Maturity Model, version 2.0*. <https://www.cisa.gov/zero-trust-maturity-model>
- Cybersecurity and Infrastructure Security Agency. (2024). *Cybersecurity advisory AA24-060B: Threat actors exploit multiple vulnerabilities in Ivanti Connect Secure and Policy Secure gateways*. <https://www.cisa.gov/news-events/cybersecurity-advisories/aa24-060b>
- Cybersecurity and Infrastructure Security Agency. (2025). *Ivanti releases security updates for Connect Secure, Policy Secure, and ZTA gateways (CVE-2025-0282)*. <https://www.cisa.gov/news-events/alerts/2025/01/08/ivanti-releases-security-updates-connect-secure-policy-secure-and-zta-gateways>
- Department of Defense Chief Information Officer. (2022). *Department of Defense zero trust reference architecture*. U.S. Department of Defense. [https://dodcio.defense.gov/Portals/0/Documents/Library/\(U\)ZT_RA_v2.0\(U\)_Sep22.pdf](https://dodcio.defense.gov/Portals/0/Documents/Library/(U)ZT_RA_v2.0(U)_Sep22.pdf)
- Dewhurst, R. (n.d.). Damn vulnerable web application (DVWA). <https://github.com/digininja/DVWA>
- DLPT. (n.d.). *DLP test data*. <https://dlptest.com>

- Escobedo, V., Beyer, B., Saltonstall, M., & Zyzniewski, F. (2017). BeyondCorp 5: The user experience. *;login.*, 42(3), 38–43. USENIX Association.
- European Institute for Computer Antivirus Research. (n.d.). *EICAR test file*.
<https://www.eicar.org>
- Johnson, R. B., & Christensen, L. B. (2004). *Educational research: Quantitative, qualitative, and mixed approaches* (2nd ed.). Allyn & Bacon.
- Kindervag, J. (2010). *No more chewy centers: Introducing the Zero Trust model of information security*. Forrester Research.
- Lyon, G. F. (2009). *Nmap network scanning: The official Nmap project guide to network discovery and security scanning*. Insecure.Com LLC.
- Mandiant. (2026). *M-Trends 2026 special report*. Mandiant.
<https://cloud.google.com/security/resources/m-trends>
- MITRE Corporation. (2025). *MITRE ATT&CK Enterprise matrix (Version 17)*.
<https://attack.mitre.org/versions/v17/matrices/enterprise/>
- Office of Management and Budget. (2022). *Memorandum M-22-09: Moving the U.S. government toward zero trust cybersecurity principles*. Executive Office of the President. <https://www.whitehouse.gov/wp-content/uploads/2022/01/M-22-09.pdf>
- Osborn, B., McWilliams, J., Beyer, B., & Saltonstall, M. (2016). BeyondCorp: Design to deployment at Google. *;login.*, 41(1), 28–35. USENIX Association.
- OWASP Foundation. (2021). *OWASP Top Ten 2021*. <https://owasp.org/Top10/>
- Rose, S., Borchert, O., Mitchell, S., & Connelly, S. (2020). *NIST special publication 800-207: Zero trust architecture*. National Institute of Standards and Technology.
<https://doi.org/10.6028/NIST.SP.800-207>
- SANS Technology Institute. (2021). *SANS research proposal idea strategies*. SANS Technology Institute.
- Verizon. (2026). *2026 data breach investigations report*. Verizon Business.
<https://www.verizon.com/business/resources/reports/dbir/>
- Henry Cheung, henry.cheung@student.sans.edu

Ward, R., & Beyer, B. (2014). BeyondCorp: A new approach to enterprise security. *;login:*, 39(6), 6–11. USENIX Association.

Appendix A: Lab Configurations

This appendix is the build specification for the study. It documents the lab environment, the virtual machine configurations, the identity provider setup, the internal services, the endpoint configurations, the attack tooling, the per-product deployments, the detailed test procedures, and the predicted outcomes with the reasoning behind them. Anyone who wants to reproduce the work can build from it directly.

A.1 Lab Infrastructure

The lab ran on a single Hyper-V host: 32 GB of RAM, an 8-core CPU with virtualization extensions enabled, and 500 GB of SSD. VMware Workstation 17 would work as an alternative. Hyper-V was chosen because it integrates natively with Windows 11 Pro and supports nested virtualization, which made the FortiGate VM appliance easier to stand up.

A.2 Lab Network Architecture

The lab consists of three logical networks corresponding to the two location configurations described in Section 2.5 and the datacenter network containing protected internal services. The networks were implemented as Hyper-V Internal virtual switches with NAT to provide internet egress where needed.

Network	Subnet	Purpose	Internet Egress
Lab-Untrusted	192.168.10.0/24	Simulated remote/hostile network for client endpoints	Yes (NAT)
Lab-Trusted	192.168.20.0/24	Simulated corporate office network	Yes (NAT)
Lab-Datacenter	10.0.11.0/24	Internal services and access-product proxies/connectors	No direct egress (services connect outbound through access-product connector for IAPs; through gateway public IP for VPNs)

Table 8: Lab Network Architecture

A.3 Virtual Machine Inventory

Six virtual machines support the test battery. The product gateway or proxy component for each tested product is deployed as an additional VM on the appropriate network and is rotated as the test battery progresses through the six products.

VM	OS	RAM	Disk	Network	Purpose
CLIENT01	Windows 11 Pro	4 GB	80 GB	Lab-Untrusted	Compliant remote endpoint
CLIENT02	Windows 11 Pro	4 GB	80 GB	Lab-Untrusted	Non-compliant remote endpoint
FILE01	Windows Server 2016	4 GB	80 GB	Lab-Datacenter	SMB file server (intentionally unpatched for MS17-010)
WEB01	Ubuntu 24.04 LTS	2 GB	40 GB	Lab-Datacenter	DVWA web application
WEB02	Ubuntu 24.04 LTS	1 GB	20 GB	Lab-Trusted	Apache web server (trusted-network detection tests)
ATTACKER	Kali Linux 2025	4 GB	60 GB	Lab-Untrusted	Attack-tooling staging and adjacent-network attacker host (Section A.7)

Table 9: Virtual Machine Inventory

An external attacker host was also stood up, a small DigitalOcean droplet with 1 vCPU, 1 GB of RAM, and Ubuntu 24.04 LTS, with nmap installed. It sits outside the lab networks on purpose, to play the part of an attacker on the public internet for the external inbound port exposure test.

A.4 Identity Provider Configuration

The enterprise identity provider was Microsoft Entra ID, running on a Microsoft 365 E5 trial tenant. Two test users were created with different group memberships so identity-based access policy could be tested. WEB01 hosts two internal web applications, a general intranet application and the sensitive DVWA application, published as distinct routes. ZTNA Group 1 held ztnauser1 and had access to both web applications; ZTNA Group 2 held ztnauser2 and had access to the general application only. FILE01 is not a published application in these tests; it serves only as the lateral-movement target on the

datacenter subnet (Section 2.2). Both users had Microsoft Authenticator (TOTP and number-matching) and FIDO2 security key support configured.

Conditional Access policies were set up for the per-product tests and adjusted between evaluations as needed. There were three: a baseline policy requiring MFA, a step-up policy requiring an extra authentication step for WEB01, and a phishing-resistant policy requiring FIDO2 for WEB01.

A.5 Internal Service Configurations

A.5.1 FILE01 (Windows Server 2016)

FILE01 is a Windows Server 2016 VM on the Lab-Datacenter network at the static IP 10.0.11.211. The File Server role was installed and an SMB share called ZTNATest was created with full access for the Everyone group. Windows Server 2016 was a deliberate choice: it is left unpatched against MS17-010 (KB4012212) so the EternalBlue test has something to hit. It also reflects the reality that unpatched, outdated systems keep running in production long after they should.

The ZTNATest share holds three test files. pii_sample.txt is plaintext Personally Identifiable Information, with names, addresses, and Social Security numbers pulled from the dlptest.com sample data repository (DLPT, n.d.). pci_sample.txt holds mock credit card numbers from the same source. An EICAR test file in plaintext is staged for the malware detection test (European Institute for Computer Antivirus Research, n.d.).

A.5.2 WEB01 (Ubuntu DVWA)

WEB01 is an Ubuntu 24.04 LTS VM on the Lab-Datacenter network at 10.0.11.212. A LAMP stack of Apache, MariaDB, and PHP was installed, then the Damn Vulnerable Web Application (Dewhurst, n.d.) was cloned from its public Git repository and set up the standard way. The DVWA security level was set to “low” so the underlying vulnerabilities stay exploitable when no access protection is in place. A file was also created at /var/www/html/DVWA/vulnerabilities/ztna_test.txt with identifiable content for the Local File Inclusion test. WEB01 also serves a second, minimal general intranet web application alongside DVWA, published on a separate route, so the Identity

tests differentiate access between two web applications rather than between a web app and the SMB file service; the access products gate the two by their own layer (per-route policy for the proxies, listener/port access rules for the VPNs).

DVWA was chosen for three reasons. It is actively maintained and runs on the current Apache, so it works on a current OS. It maps to the OWASP Top Ten (OWASP Foundation, 2021), which provides standardized test cases. And Carstensen (2025) used it in the prior SANS-approved ZTNA evaluation, so the results line up with that framework.

A.5.3 WEB02 (Trusted Location Web Server)

WEB02 is a smaller Ubuntu 24.04 LTS instance on the Lab-Trusted network, running a minimal Apache that serves a static page. It supports the trusted-location segmentation check: a product that recognizes trusted networks should allow local LAN reachability to WEB02 without routing it through the access product.

A.6 Endpoint Configurations

A.6.1 CLIENT01 (Compliant Endpoint)

CLIENT01 is a Windows 11 Pro VM on the Lab-Untrusted network, fully patched as of the test date. BitLocker Full Disk Encryption is on for the system drive, and Windows Defender runs with current definitions. A Defender exclusion was added for the test directory (C:) so local antivirus would not interfere with the controlled exploitation runs.

CLIENT01 is the compliant baseline endpoint and handled most of the tests where access was supposed to succeed. As the battery moved from product to product, the corresponding client agent was installed and configured: OpenVPN Connect, FortiClient, SoftEther VPN Client, Cloudflare WARP, Microsoft Global Secure Access client, or Pomerium Desktop client.

A.6.2 CLIENT02 (Non-Compliant Endpoint)

CLIENT02 is a second Windows 11 Pro VM on the Lab-Untrusted network, degraded in three deliberate ways from CLIENT01. BitLocker is off on the system drive.

Henry Cheung, henry.cheung@student.sans.edu

Windows Defender real-time protection is off, set through PowerShell (Set-MpPreference -DisableRealtimeMonitoring \$true and the related cmdlets). And the Defender definitions are stripped with MpCmdRun.exe using the /RemoveDefinitions /All flag. Together these make a non-compliant or compromised device, the kind of weakened endpoint that follows when an attacker disables endpoint protection after gaining a foothold (MITRE Corporation, 2025). For the Endpoint Protection Installed test (Test 5), a separate CLIENT02 snapshot is used in which Windows Defender is uninstalled and unavailable rather than merely disabled, so the protection-absent and protection-disabled conditions are exercised distinctly.

A.7 Attack Simulation Tooling

Three classes of tooling were configured on the local attacker host, a Kali Linux ATTACKER VM, and on the compliant endpoint CLIENT01, to simulate post-compromise behavior, lateral movement, and application-layer attacks.

For network reconnaissance and service fingerprinting, Nmap (Lyon, 2009) was used, with the -sCV combination of TCP SYN scanning, default scripts, and version detection. That mirrors what an attacker actually runs during early enumeration.

For exploitation, the Metasploit Framework was used, specifically the ms17_010_psexec module against the unpatched FILE01 in the EternalBlue test. For the malicious file detection test, a Meterpreter reverse-shell payload was generated with MSFVenom, which ships with Metasploit (msfvenom -p windows/x64/meterpreter/reverse_tcp -f exe -o reverse.exe).

Threat detection was tested with the EICAR test file in both plaintext and COM executable form (European Institute for Computer Antivirus Research, n.d.). The plaintext EICAR exercises basic signature detection, the COM executable stands in for executable malware, and the Meterpreter reverse shell is a realistic post-exploitation payload.

For the SMB enumeration in the lateral movement test, smbmap and smbclient were used to list file shares from the authenticated session.

A.8 Per-Product Deployment Configurations

Each of the six tested products was deployed in the lab according to vendor documentation. Deployment configurations are summarized below. Each product is identified by name so that the deployment can be independently reproduced.

A.8.1 OpenVPN Access Server

OpenVPN Access Server runs as a single VM on the Lab-Untrusted network, with the host forwarding inbound TCP/443 (web admin and SSL VPN) and UDP/1194 (OpenVPN UDP) to it. Routing was configured on the gateway VM so that the VPN client subnet (172.27.224.0/20) could reach the Datacenter network (10.0.11.0/24). ztnauser1 and ztnauser2 both have accounts: ztnauser1 reaches all routed networks, ztnauser2 is limited to FILE01 (10.0.11.211). Two-factor authentication uses the default RADIUS-style setup with a TOTP authenticator.

A.8.2 FortiGate

FortiGate runs as a virtual appliance on a 15-day evaluation license. The SSL VPN service was configured with a public-facing listener on TCP/443 bound to the test domain. FortiClient EMS handles endpoint compliance checks, including disk encryption, antivirus presence, and antivirus running state. SAML single sign-on points at the Microsoft Entra ID tenant for SSO, conditional access, and step-up MFA. The IPS profile was enabled with current signatures, including the MS17-010 signature; the WAF profile was applied to the web-accessible internal applications; and DLP profiles were set for PII and PCI patterns.

A.8.3 SoftEther

SoftEther runs as a Linux service on its own VM. The SSL VPN web portal was bound to TCP/443 and published with a public-facing certificate, and SecureNAT was used to route between the VPN client subnet and the Datacenter network. ztnauser1 and ztnauser2 are local accounts here, because SoftEther does not integrate with Microsoft Entra ID at the SAML level. For the Step-Up MFA test, SoftEther was integrated with a third-party MFA provider over RADIUS. The integration authenticated reliably at session establishment but could not enforce a step-up challenge scoped to a single resource such as Henry Cheung, henry.cheung@student.sans.edu

as WEB01. The reason is architectural: a network-layer VPN authenticates once, when the tunnel is established, and has no per-request policy decision point at which to require an additional factor for a single destination. The RADIUS path reflected exactly that: SoftEther evaluates RADIUS only at connection time, so the provider's Access-Challenge had no consistent hook once the tunnel was up, and the WEB01 step-up prompt fired only intermittently. That behavior (MFA at the door but no reliable per-resource step-up) is what the Partial on Step-Up MFA records: an architectural limit of single-stage tunnel authentication, not a one-off configuration error, and one that applies to per-resource step-up on any network-layer VPN regardless of the RADIUS provider chosen.

A.8.4 Cloudflare Access

Cloudflare Access runs from the cloud-managed dashboard, with a Tunnel connector on a small Linux jumpbox in the Datacenter network. The connector authenticates outbound traffic to Cloudflare's edge, so no inbound port is exposed on the customer network. The public hostname `iap-a.lab` was bound to the WEB01 DVWA instance over HTTP routing, the Microsoft Entra ID tenant was set as the identity provider, and the Access application policies were tied to the ZTNA Group memberships. The WARP client went on CLIENT01 and CLIENT02 for device posture, covering disk encryption, antivirus presence and running state, and definition currency. The WAF Managed Rules were enabled for the WEB01 application.

A.8.5 Microsoft Entra Private Access

Microsoft Entra Private Access uses the IdP's native private access service. A Private Network Connector was installed on a Datacenter VM with outbound-only authentication to the Entra edge, and two Enterprise applications were published: the FILE01 SMB service (10.0.11.211, port 445) and the WEB01 HTTP service (10.0.11.212, port 80). Conditional Access policies on those applications required device compliance, meaning Intune-enrolled and BitLocker-encrypted, plus step-up MFA for WEB01. The Global Secure Access client went on CLIENT01 and CLIENT02. Microsoft Purview DLP policies handled PII and PCI inspection, and Defender for Endpoint was active for malicious file detection.

A.8.6 Pomerium

Pomerium runs as a containerized service on a publicly addressable VM. OIDC was configured against the Microsoft Entra ID tenant for authentication and group-claim policy, and per-route policies were written to bind `iap-c.lab/web01` to `WEB01` and require membership in ZTNA Group 1. Pomerium has no native device-posture capability of its own; for device control, it relies on the identity provider. Because Entra ID is the controlled variable held constant across all six products, the same Intune device-compliance Conditional Access policy used for Entra Private Access was also applied to Pomerium's OIDC application, so a non-compliant device (one failing BitLocker, endpoint protection, or definition currency) is denied at sign-in. Pomerium bundles no WAF, DLP, or malware inspection.

A.9 Detailed Test Procedures

This subsection outlines the execution steps for each of the 21 tests, organized by ZTMM pillar to align with Section 3.1.

A.9.1 Identity Test Procedures

Test 1 (User-Based Access Differentiation): Policies were configured per Sections A.4 and A.8, so `ztnauser1` reached both web applications on `WEB01` (the general intranet app and the sensitive DVWA app) while `ztnauser2` reached the general app only. Authenticating as `ztnauser1` from `CLIENT01` confirmed access to both applications; re-authenticating as `ztnauser2` confirmed that access to the general application succeeded while access to the DVWA application was correctly blocked.

Test 2 (Step-Up MFA): A Conditional Access policy was configured to require an additional MFA challenge when `ztnauser1` accessed the sensitive DVWA application, but not the general application. During testing, `ztnauser1` first reached the general application without an additional prompt; navigating to the DVWA application in the same session triggered the expected step-up MFA challenge.

Test 3 (Phishing-Resistant MFA): Conditional Access was configured to mandate FIDO2 or certificate-based authentication for `ztnauser1` to reach the sensitive DVWA application. Enforcement was verified by first attempting access with only a TOTP code, Henry Cheung, henry.cheung@student.sans.edu

which was correctly denied, then re-authenticating with a FIDO2 security key to gain access.

A.9.2 Device Test Procedures

Test 4 (Disk Encryption): Each product was configured to require a BitLocker-enabled drive on the connecting endpoint. The policy was verified by attempting a connection from the non-compliant CLIENT02 (BitLocker disabled), which was successfully blocked, followed by a successful connection from the compliant CLIENT01.

Test 5 (Endpoint Protection Installed): Policies were configured to require the presence of Windows Defender. Access was then attempted from the separate CLIENT02 snapshot in which Defender is uninstalled and unavailable (Section A.6.2). A pass required the product to detect this absence and block access.

Test 6 (Endpoint Protection Running): The products were configured to verify that Windows Defender was actively running. Using CLIENT02 with Defender's real-time protection manually disabled (as detailed in Section A.6.2), a connection was attempted. The product passed if it detected the disabled state and denied the connection.

Test 7 (Definitions Up-to-Date): A posture check was established requiring Defender definitions to be less than 14 days old. A connection was then attempted using CLIENT02, whose definitions had been intentionally stripped (Section A.6.2), confirming that the outdated posture was detected and access was blocked.

A.9.3 Network Test Procedures

Test 8 (External Inbound Port Exposure): From the external attacker cloud host, an Nmap scan was run against the product's public-facing hostname (`nmap -sCV -p- -T4 <product-public-hostname>`). The number of open TCP ports was logged alongside any service fingerprinting details. A pass required zero exposed ports. Exposing only an encrypted control-plane port without application fingerprinting earned a partial, while exposing identifiable service ports resulted in a fail.

Test 9 (Network Segmentation, Untrusted Location): While connected through the product from CLIENT01, a ping and an Nmap scan were attempted against another host on the local Lab-Untrusted subnet. To pass, the product needed to successfully block local LAN traffic originating from the untrusted location. This test reflects client routing and traffic-steering configuration as well as the access architecture itself.

Test 10 (Service Cloaking): Authenticated as ztnauser1 on CLIENT01, an internal Nmap scan was run against the datacenter subnet (`nmap -sCV -p 1-65535 10.0.11.0/24 -T4`). A passing result meant the scan discovered only the resources the product was configured to publish, and no other host or service on the datacenter subnet: WEB01 alone for the HTTP-only proxies, or WEB01 plus the FILE01 SMB service for products that publish it. A VPN that exposed the rest of the subnet failed.

Test 11 (Post-Auth Network Reachability): An ICMP host discovery sweep (`nmap -sn 10.0.11.0/24`) was combined with a TCP reachability test against port 445 for every address on the subnet. A pass required that responses come back only from authorized hosts.

Test 12 (Lateral Movement Reconnaissance): Three MITRE ATT&CK techniques were chained from the authenticated session, starting with T1018 (`nmap -sn 10.0.11.0/24`), moving to T1046 (`nmap -sCV -p 22,80,135,139,389,443,445,3389 10.0.11.0/24`), and finishing with T1135 (`smbmap -H 10.0.11.211 -u ztnauser1 -p '<password>' followed by smbclient -L //10.0.11.211 -U ztnauser1`). A pass required all three lateral movement reconnaissance attempts to fail to enumerate unauthorized resources.

A.9.4 Application Test Procedures

Test 13 (Application Layer Visibility): Standard HTTP traffic was generated from CLIENT01 to WEB01 alongside SMB traffic to the FILE01 lateral-movement target, and the product logs were then reviewed. The product passed if its logs captured application-layer details, specifically the HTTP method, URL, and SMB share name; a product that carried no SMB path exposed none to surface. HTTP-only proxies are therefore scored on

HTTP visibility alone and are not penalized for lacking SMB visibility, because they do not route SMB at all.

Test 14 (Application-Based Policies): An access policy was created that allowed ztnauser1 to reach one route of the WEB01 application over HTTPS while denying another route, expressed with application-layer attributes (host and URL) rather than IP and port. A pass required that the product could express and enforce the rule at the application layer; a product that merely had no route to a resource was not credited, because absence of a route is not an application-layer policy.

Test 15 (MS17-010 Exposure Outcome): Using CLIENT01, the Metasploit ms17_010_psexec module was launched against FILE01 (10.0.11.211) over SMB. The payload was configured to drop a file named Failed.txt into C:\Users\Administrator\ on success. The test records the security outcome rather than a single mechanism: a Pass means FILE01 was not compromised and no file was created, whether because the product provided no network route to FILE01:445 (service cloaking) or detected and blocked the exploit (IPS or AV); a Fail means the exploit completed. Section 3.2.4 reports which mechanism applied to each product.

Test 16 (LFI Detection): Two Local File Inclusion payloads were submitted to the DVWA application: `?page=../../../../etc/passwd` and `?page=../../../../var/www/html/DVWA/vulnerabilities/ztna_test.txt`. A pass meant the product successfully blocked both requests.

Test 17 (Command Injection Detection): The DVWA Command Injection vulnerability was tested with three standard payloads: `127.0.0.1; id`, `127.0.0.1; ls`, and `127.0.0.1; pwd`. Blocking all three attempts resulted in a pass.

Test 18 (SQL Injection Detection): Two SQL Injection payloads were submitted to DVWA: the classic `1' OR '1'='1` and a variant, `1' OR '8'<'9`. The product passed if both payloads were blocked.

A.9.5 Data Test Procedures

Test 19 (PII Data Loss Prevention): Using the DVWA file-upload page, the pii_sample.txt file was uploaded from CLIENT01 to the proxied WEB01 web application over HTTPS. A pass required the access path, together with the surrounding platform controls, to inspect the payload, detect the PII, block the upload, and log the event.

Test 20 (PCI Data Loss Prevention): The same HTTPS upload process was repeated using the pci_sample.txt file. A pass confirmed the access path and surrounding platform detected and blocked the PCI data transfer.

Test 21 (Malicious File Detection): Three distinct malicious files were uploaded from CLIENT01 to WEB01 over HTTPS: the standard EICAR plaintext file, an EICAR COM executable, and a Meterpreter reverse-shell executable created with MSFVenom. Detecting and blocking all three transfers earned a pass.

A.10 Predicted Outcomes and Architectural Reasoning

This subsection gives the predicted outcome for each test and product, along with the architectural or security reasoning behind each prediction. The predictions were registered in advance and were the baseline each observed outcome was scored against during testing. The single case where observation diverged from prediction, Pomerium on the MS17-010 test, is recorded in Section 3.2.4 and in the predicted-versus-observed summary at the end of Section 3.2.6.

A.10.1 OpenVPN Access Server Predicted Outcomes

OpenVPN Access Server was predicted to score 1.0 of 21, passing only User-Based Access Differentiation. It should fail Step-Up MFA and Phishing-Resistant MFA because it has no per-resource conditional access primitives. It should fail all four Device tests because it has no native posture checking. It should fail all five Network tests because its architectural premise places the client on a routable subnet, which by default exposes inbound ports, allows LAN reachability from untrusted locations, and leaves post-authentication reconnaissance open unless additional internal controls are layered on. It should fail all six Application tests because it operates at the network layer with no

Layer 7 inspection, policy, or threat detection. And it should fail all three Data tests because it performs no content inspection.

A.10.2 FortiGate Predicted Outcomes

FortiGate was predicted to score 11.5 of 21. Identity should reach 3.0 of 3.0 on the strength of its SAML integration with Microsoft Entra ID, which gives it both step-up MFA through Conditional Access and phishing-resistant enforcement at the IdP. Devices should land at 3.5 of 4.0: Pass on Disk Encryption, Endpoint Protection Installed, and Endpoint Protection Running, and a Partial on Definitions Up-to-Date, because posture re-evaluation lags. Networks should come in at 0.5 of 5.0, with a Partial on Network Segmentation from the always-on tunnel modes and a Fail on the other four, because of the network-layer reachability premise. Applications should reach 3.0 of 6.0, with Partial across the application-aware tests reflecting the IPS and WAF. Data should be 1.5 of 3.0: over the in-scope HTTP path (Section 3.1.5), FortiGate's DLP and antivirus profiles inspect the upload to the protected web application and earn Partial on the PII, PCI, and malware tests.

A.10.3 SoftEther Predicted Outcomes

SoftEther was predicted to score 5.5 of 21. Identity should reach 2.0/3.0, with Partial on Step-Up MFA and Phishing-Resistant MFA, since a network-layer VPN authenticates once at tunnel establishment and cannot scope a step-up or factor-type challenge to a single resource the way a per-request proxy can. Devices should be 2.5 of 4.0, given its limited posture support. Networks should be 0.5 of 5.0, hitting the same architectural wall as OpenVPN Access Server and FortiGate. Applications should be 0.5 of 6.0 with no integrated WAF, and Data should be 0.0 of 3.0 with no integrated DLP.

A.10.4 Cloudflare Access Predicted Outcomes

Cloudflare Access was predicted to score 20.5 of 21. Identity should reach 3.0 of 3.0 on native conditional access through the Microsoft Entra ID identity provider. Devices should reach 4.0 of 4.0 because the WARP client does continuous posture evaluation. Networks should reach 5.0 of 5.0: the outbound-only Tunnel removes inbound exposure, the WARP client detects trusted versus untrusted location, the per-

application model cloaks everything else, and authenticated reconnaissance fails because there is no Layer 3 path. Applications should reach 6.0 of 6.0 because the edge WAF blocks the OWASP-aligned attacks. Data should be 2.5 of 3.0 over the HTTP path: Cloudflare's edge DLP blocks the PII and PCI uploads (Pass), and its malware sandbox earns a Partial because enforcement lags the first transfer.

A.10.5 Microsoft Entra Private Access Predicted Outcomes

Microsoft Entra Private Access was predicted to score 20.0 of 21. Identity should reach 3.0 of 3.0 on native Microsoft Entra ID integration. Devices should reach 4.0 of 4.0 on native Microsoft Intune compliance. Networks should reach 5.0 of 5.0 on the outbound-only Private Network Connector and Global Secure Access traffic steering. Applications should reach 5.0 of 6.0: application-aware logging and policy for the published HTTP application are strong, though as a connector it does not inspect arbitrary protocols at Layer 7, but without an upstream Azure Front Door or Application Gateway the native WAF coverage of the OWASP patterns is limited. Data should reach 3.0 of 3.0, enforced by the surrounding Microsoft platform (Purview DLP and Defender for Endpoint at the endpoint and tenant) rather than by the access connector inspecting traffic in line (Section 3.2.7).

A.10.6 Pomerium Predicted Outcomes

Pomerium was predicted to score 12.0 of 21. Identity should reach 2.5 of 3.0, with a Partial on Phishing-Resistant MFA because it relies on the IdP to enforce rather than enforcing natively. Devices should reach 4.0 of 4.0: the same Intune device-compliance Conditional Access policy applied to Entra Private Access is applied to Pomerium's OIDC application, so it gates device state at sign-in through the shared identity provider. Networks should reach 4.0 of 5.0, with Partial on Network Segmentation from untrusted locations and on Service Cloaking. With no bundled WAF or DLP it fails the Application threat tests and all three Data tests. Observed outcome: Pomerium scored 13.0, one point above this prediction. MS17-010 was observed as a Pass rather than the predicted Fail, because EternalBlue targets SMB and Pomerium publishes no SMB route, so the exploit never reached FILE01 (see Section 3.2.4).

A.10.7 Aggregated Predicted Outcomes

The aggregated predicted outcomes were summarized as follows. These are a priori predictions and can be compared with the observed results in Table 7.

Pillar	OpenVPN AS	FortiGate	SoftEther	Cloudflare Access	Entra Private Access	Pomerium
Identity (3)	1.0	3.0	2.0	3.0	3.0	2.5
Devices (4)	0.0	3.5	2.5	4.0	4.0	4.0
Networks (5)	0.0	0.5	0.5	5.0	5.0	4.0
Apps & Workloads (6)	0.0	3.0	0.5	6.0	5.0	1.5
Data (3)	0.0	1.5	0.0	2.5	3.0	0.0
Total (21)	1.0	11.5	5.5	20.5	20.0	12.0

Table 10: Aggregated Predicted Outcomes by Pillar

The predicted category means were 6.00 of 21 for the VPNs and 17.50 of 21 for the IAPs, a difference of 11.50 points, or 54.8 percent of the maximum. The observed category means were 6.00 for the VPNs and 17.83 for the IAPs (the IAP figure one third of a point above prediction, from the single Pomerium MS17-010 divergence) for an observed difference of 11.83 points, or 56.3 percent of the maximum. Networks again gave the sharpest split, with every IAP at 4.0 or higher and every VPN at 0.5 or lower. That result is a direct test of the hypothesis: separating user identity from network reachability creates a measurable Zero Trust enforcement gap that does not depend on any one vendor's maturity.