TAG CYBER

SECURE ACCESS AS A SERVICE: AN INTRODUCTION TO THE AXIS SECURITY PLATFORM

EDWARD AMOROSO, TAG CYBER

axis security

SECURE ACCESS AS A SERVICE: AN INTRODUCTION TO THE AXIS SECURITY PLATFORM

EDWARD AMOROSO

Traditional remote access based on virtual private networks (VPNs) is being replaced with new methods that are influenced by zero trust and related network security models. The Axis security solution[1] exemplifies this new generation of establishing zero-trust based connectivity to critical business resources.

INTRODUCTION

On occasion, the security community will collectively identify the need for a significant shift from some well-known control to an approach that is more effective. The transition from the use of single-factor passwords to multi-factor (or passwordless) authentication is one such example. The transition from signature-based antivirus to advanced endpoint detection and response (EDR) tools is another prominent example.

In this report, we review a third transition — one that has seen recent acceleration due to increased cyber threats, as well as the shift to work-from-home models, spurred along by the COVID-19 pandemic[2]. Specifically, we focus here on the transition from conventional virtual private networks (VPNs) to more advanced secure access solutions that are consistent with cloud-hosted applications and which are typically offered to customers as a service.

The establishment of secure connectivity to apps and data is one of the more prominent initiatives in modern IT and cyber security. This approach helps companies achieve zero trust objectives and is a major component of the shift from existing secure business networks to cloud-based network control. The commercial Axis security platform is used to exemplify this modern approach in practice.

TRADITIONAL ACCESS

The traditional means for providing access to resources has involved three primary use cases. First, end users working from home or otherwise outside the office have used VPNs to remotely connect to corporate networks. The objective has usually been to access applications such as email, human resources tools, and business systems. These VPNs were often supported by large technology companies who would market both the clients and the server to the organization.

Second, business suppliers, partners, and other third parties have used a variety of means for accessing the networks, systems, and applications of their customer organization. In the early days, this might have been a private line access, but it eventually evolved into IPSec or SSL tunnels and other means for establishing secure connectivity to an internet-facing gateway. Such schemes have resulted in many well-known third-party breaches.

Third, businesses have engaged with service providers to create hub-and-spoke networks using multi-protocol label switching (MPLS) technology[3]. The resulting networks were designed to connect remote users to networks, and branch offices to the corporate data center. This arrangement worked well when applications were monolithic and premise-hosted behind a firewall, but the more recent shift to cloud has made these architectures awkward.

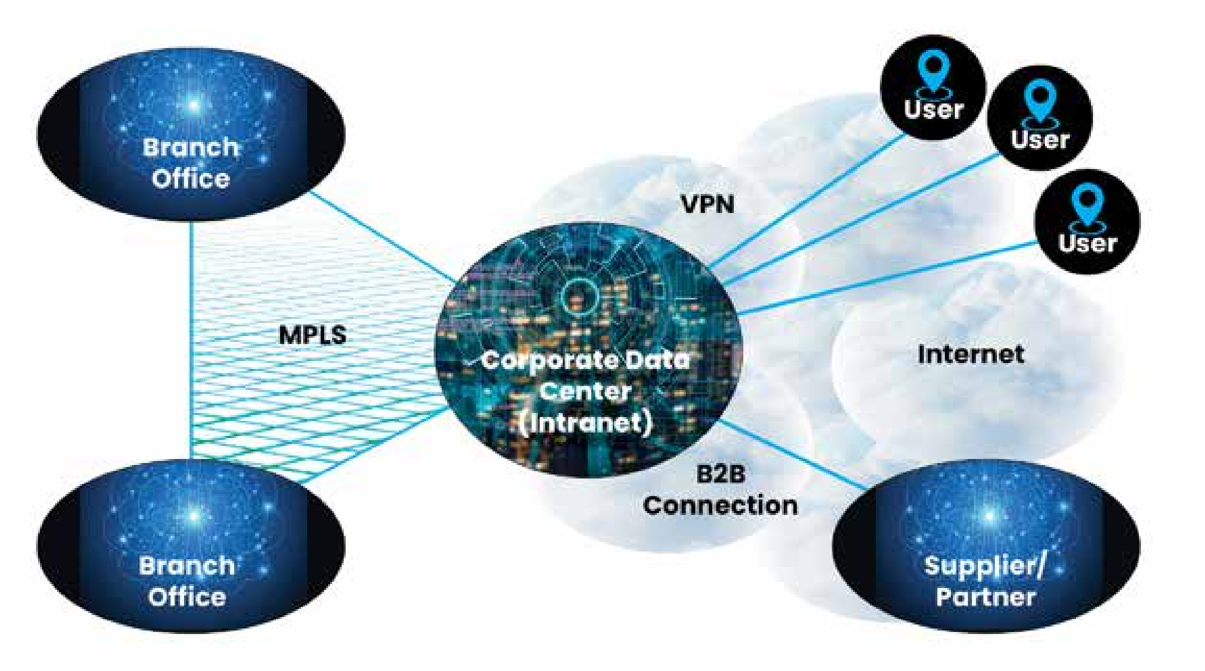


Figure 1. Traditional Use-Cases for Secure Access

While none of these traditional means for remote access have been perfect in terms of user experience and threat avoidance, all have served their purpose acceptably for decades. As such, it is correct to view all three technologies as successful engagements for which the security community should be grateful to the designers. Without these three secure access methods, cyber security might have been even more unruly these past decades than it was.

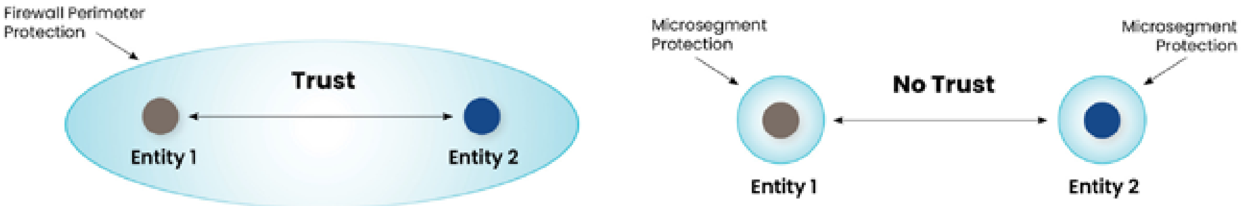
SECURE ACCESS DISRUPTIONS

With the advent of modern accelerated use of cloud-based services, including software as a service (SaaS) applications, all three traditional secure access use cases mentioned above are being severely disrupted. Driving such disruption are two conceptual models that are being adopted across the security community to drive new designs — ones for which the session matters more than the perimeter, and for which control has been pushed to the cloud.

Zero Trust

The zero trust model[4] provides an accurate depiction of the condition that results when a perimeter can no longer protect an enterprise. This often involves the dissolution of the corporate firewall as a primary control for data security. When this occurs, any organization's clients, endpoints, servers, and the like can no longer trust the local network for privacy and security — hence, the zero trust moniker.

A good way to explain zero trust is to start with the firewall-protected perimeter case, where two entities can share freely with no need for mutual authentication. Security depends on the boundary protection of the firewall, but this model is porous, and malware can traverse this arrangement freely. In zero trust, all entities must share using mutual authentication and other security controls, because the boundary protection is removed.



1. Entity 1 and 2 can share freely (bidirectional)
2. No mutual authentication (no 1FA, 2FA, etc.)
3. Shared boundary protection (perimeter)
4. Malware can traverse from 1. to 2. freely

1. Entity 1 and 2 will only share if necessary
2. Mutual authentication (1FA, 2FA, etc.)
3. Local boundary protections (no perimeter)
4. Malware cannot traverse from 1. to 2. freely

Figure 2. Zero Trust Model

The primary influence of zero trust on modern replacements for VPNs is that it reinforces the need to avoid dependence on any perimeter. This is a key difference between VPN usage and modern secure access methods. Where traditional approaches included the goal of establishing remote connectivity to the perimeter-protected enterprise, more modern methods are focused on supporting secure sessions from user devices to cloud- or premise-hosted applications.

SSE

The security services edge (SSE) model[5] references the evolution of modern business networking toward more cloud-oriented management. Such control is a natural progression from early separation of the data and control planes on a network. This innovation, found on modern multi-protocol label switching (MPLS) networks, allowed for all control activity to be implemented in a centralized manner using cloud.

From the perspective of the service provider, the SSE model shifts control into the cloud in a manner consistent with the design of new point of presence (POP) components. This allows for a distributed architecture where enterprise users can access cloud workloads across a network of control gateways that will include the desired security function — with secure access being one of the most important such capabilities.

While the SSE model generalizes network support beyond the user-access case covered by VPNs, it does reinforce the need in modern SAaaS for control to be centrally offered via cloud systems, and for cyber security requirements such as data leakage protection (DLP) and multi-factor authentication to be supported if VPNs are being replaced and upgraded.

OVERVIEW OF AXIS SECURITY PLATFORM

Launched in 2019 and headquartered in San Mateo and Tel Aviv, Axis Security provides a commercially available secure access as a service offering for enterprise customers. While the timing of the launch coincided with pandemic-initiated work-from-home practices, the evolution toward working-from-anywhere had long since started. Zero trust and SSE both exemplify the shift away from VPN access to perimeter-protected networks.

Goals of the Axis Security Platform

The Axis Security Platform is designed with the following major objective: To secure the modern workplace environment based on a foundation of zero trust. This is done through attention to security for work-from-anywhere, securing the business enterprise including all access by third parties, and modernizing the infrastructure with emphasis on transition from hub-and-spoke MPLS to multi-cloud usage by enterprise.

At a more detailed level, the platform uses 350 points of presence to deliver zero trust-based secure access for three primary purposes: (1) To support secure access to private apps in a typical hybrid work arrangement, (2) to ensure security of data as it moves between third-party apps and other services, and (3) to secure SaaS apps as they are accessed by end-users, including from branch offices and data centers.

Application Access Cloud

The commercial implementation from Axis Security delivers secure access and related capabilities through what it refers to as its Application Access Cloud. The infrastructure supporting this Application Access Cloud is designed to allow users to connect directly to applications via a central hub. This has the strong security feature of allowing such access without having to grant full access to an enterprise network.

The approach replaces VPN tunnels and agents in a manner consistent with both zero trust and SSE and supports security analysis and management of every access instance. Such cloud-based control also simplifies deployment and reduces the complexity of the configuration work to support secure access. It supports access for employees, contractors, administrators, and other remote workers to both cloud and premise-based applications.

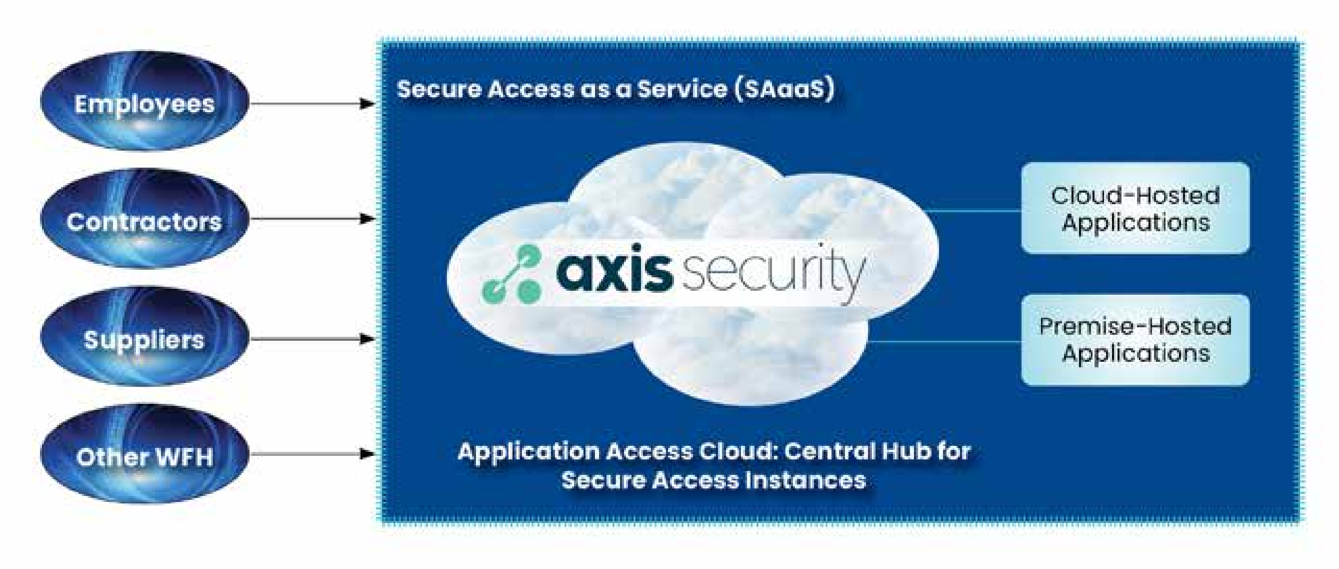

Employees
Contractors
Suppliers
Other WFH
Secure Access as a Service (SAaaS)
axis security
Cloud-Hosted Applications
Premise-Hosted Applications
Application Access Cloud: Central Hub for Secure Access Instances

Figure 3. Application Access Cloud From Axis Security

Secure Access as a Service

From an enterprise customer perspective, the Application Access Cloud enables provision of a secure access as a service (SAaaS) capability. This is encouraging, because traditional VPNs involved a product orientation that required considerable administration and complex configuration work by the customer. By offering secure access in this cloud service model, Axis greatly simplifies one of the major aspects of both zero trust and SSE.

Key Security Features

The centralized hub model also enables the provision of security features and analysis tasks for each access instance, as well as across aggregated access for a company or other group. Desirable security features that are enabled by the Application Access Cloud model include the following:

1. **Application access without network access** – Axis brokers secure 1:1 connections between authorized users without placing users on the corporate network, and places all apps behind the cloud where they are made invisible to Internet-based threats

2. **Inline inspection of traffic** – This capability allows IT to gain visibility into the specific activity that employees and third-parties, brush stroke by brush stroke, for the first time

3. **Continuous adaptiveness** – Customizable policies and Integrations with IDP and endpoint security ensures that access is always adaptive. As context changes, Axis will automatically adapt access rights, and sever any existing connections if the sessions fails to pass the policy check.

4. **Behavioral analysis** - By running secure access through a cloud-based hub, Axis can integrate behavioral analysis to help identify security anomalies, attack campaigns, and other patterns consistent with unauthorized access to resources.

5. **Agent or agentless deployment models** – The Axis agent supports all ports and protocols, and even access to apps like VOIP, P2P and server to client workflows. Agentless allows secure access to web apps, and can even record browser-based RDP sessions, without the need for client

Enterprise customers interested in more information on Axis Security should contact the team directly.[3] The TAG Cyber analysts have spent considerable time reviewing the platform and have concluded that its feature-rich access cloud represents just the type of zero trust and SSE design that is required to advance secure access for enterprise. Their SAaaS is worth taking the time to review.

[1] https://www.axissecurity.com/

[2] https://www.brookings.edu/blog/order-from-chaos/2020/12/28/experts-discuss-the-growth-of-cyber-threats-amid-the-pandemic/

[3] https://en.wikipedia.org/wiki/Multiprotocol_Label_Switching

[4] The original model was introduced by Forrester (see https://www.forrester.com/blogs/tag/zero-trust/) and much of the research requires paywall entry.

[5] The original model was introduced by Gartner (see https://www.gartner.com/en/documents/3957375/invest-implications-the-future-of-network-security-is-in) but the research requires paywall entry.

ABOUT TAG CYBER

TAG Cyber is a trusted cyber security research analyst firm, providing unbiased industry insights and recommendations to security solution providers and Fortune 100 enterprises. Founded in 2016 by Dr. Edward Amoroso, former SVP/CSO of AT&T, the company bucks the trend of pay-for-play research by offering in-depth research, market analysis, consulting, and personalized content based on hundreds of engagements with clients and non-clients alike — all from a former practitioner perspective.

The material in this report is composed of the opinions of the TAG Cyber analysts and is not to be interpreted as consisting of factual assertions. All warranties regarding the correctness, usefulness, accuracy, or completeness of this report are disclaimed herein.