# **Truy cập từ xa vào AWS: Hướng dẫn cho lực lượng lao động kết hợp**

**📖 Bài viết gốc**: [Remote access to AWS: A guide for hybrid workforces](https://aws.amazon.com/blogs/security/remote-access-to-aws-a-guide-for-hybrid-workforces/)

**👤 Tác giả**: Itay Meller và Maxim Raya

**📅 Ngày xuất bản**: 01 tháng 7, 2025

**🌐 Nguồn**: AWS Security Blog

**👨‍💻 Người dịch**: Lý Trung Hậu

**📅 Ngày dịch**: 9 tháng 7, 2025

**⏱️ Thời gian đọc**: 10 phút

## **📋 Tóm tắt**

Bài viết này cung cấp một hướng dẫn toàn diện về các phương pháp và giải pháp của AWS để cho phép truy cập từ xa an toàn vào tài nguyên đám mây, hỗ trợ các môi trường làm việc kết hợp (hybrid workforces). Bài viết phân tích bốn phương pháp tiếp cận chính: dựa trên mạng, dựa trên máy chủ (host), dựa trên ứng dụng và điện toán người dùng cuối (end-user computing), đồng thời giới thiệu các dịch vụ AWS tương ứng như **AWS Client VPN**, **AWS Systems Manager Session Manager**, **AWS IAM Identity Center**, và **Amazon WorkSpaces**. Ngoài ra, bài viết còn đề cập đến mô hình **Zero Trust** với **AWS Verified Access** như một cách tiếp cận nâng cao. Mục tiêu là giúp người đọc hiểu rõ các ưu và nhược điểm (tradeoffs) về chi phí, bảo mật, trải nghiệm người dùng và khả năng giám sát để có thể lựa chọn giải pháp truy cập từ xa phù hợp nhất với nhu cầu của tổ chức.

**🎯 Đối tượng đọc**: Kiến trúc sư bảo mật (Security Architects), Kỹ sư đám mây (Cloud Engineers), Quản trị viên hệ thống (System Administrators), và các chuyên gia IT chịu trách nhiệm về bảo mật và truy cập trong môi trường AWS.

**📊 Độ khó**: Trung bình (Intermediate)

**🏷️ Tags**: [Security Blog](https://aws.amazon.com/blogs/security/tag/security-blog/)

## **📚 Mục lục**

[**Truy cập từ xa vào AWS: Hướng dẫn cho lực lượng lao động kết hợp**](#) **1**

[📋 Tóm tắt](#) 1

[📚 Mục lục](#) 1

[Các trường hợp sử dụng](#) 3

[Những thách thức liên quan đến truy cập từ xa](#) 3

[Các phương pháp tiếp cận khác nhau](#) 3

[Tiếp cận dựa trên mạng (Network-based approach)](#) 4

[Tiếp cận dựa trên máy chủ (Host-based approach)](#) 5

[Tiếp cận điện toán người dùng cuối (End-user computing approach)](#) 5

[Tiếp cận dựa trên ứng dụng (Application-based approach)](#) 5

[Kết hợp nhiều phương pháp trong mô hình Zero Trust](#) 5

[Hiểu rõ các đánh đổi](#) 6

[Kết luận](#) 8

[Về tác giả](#) 8

[📖 Glossary - Thuật ngữ](#) 8

[🔗 Tài liệu tham khảo](#) 9

[Tools và Services](#) 9

[Tài liệu liên quan](#) 10

# Nội dung:

Khách hàng của Amazon Web Services (AWS) có thể kích hoạt truy cập từ xa an toàn đến các tài nguyên đám mây của họ, hỗ trợ hoạt động kinh doanh với tốc độ và sự linh hoạt. Khi các tổ chức áp dụng môi trường làm việc linh hoạt, nhân viên có thể kết nối an toàn với tài nguyên AWS từ nhiều địa điểm khác nhau bằng các thiết bị khác nhau. AWS cung cấp các giải pháp bảo mật toàn diện giúp các tổ chức duy trì sự bảo vệ mạnh mẽ cho tài nguyên của công ty, quản lý các kiểm soát truy cập phù hợp và đáp ứng các yêu cầu tuân thủ trong khi vẫn cho phép môi trường làm việc từ xa hiệu quả.

Bởi vì có nhiều loại workload khác nhau—từ các instance Amazon Elastic Compute Cloud (Amazon EC2) đến các ứng dụng web—đang chạy trên AWS Cloud, do đó cũng có nhiều trường hợp sử dụng truy cập từ xa để sử dụng hoặc vận hành các workload này. Ví dụ, truy cập vào một instance EC2 và hệ điều hành của nó để thực hiện các hoạt động như khắc phục sự cố, phân tích log và truy xuất dữ liệu. Các trường hợp sử dụng khác yêu cầu quyền truy cập vào các ứng dụng web như Jenkins, Salesforce hoặc giao diện người dùng Kubernetes được triển khai trên AWS.

Để hỗ trợ các trường hợp sử dụng này, AWS cung cấp nhiều dịch vụ và tính năng giúp bạn giải quyết các mô hình truy cập bằng các phương pháp khác nhau. Một trong những thách thức chính mà bạn có thể gặp phải khi triển khai các giải pháp truy cập từ xa là hiểu rõ những ưu và nhược điểm của các phương pháp và giải pháp khác nhau. Bài đăng này được thiết kế để giúp bạn quyết định phương pháp truy cập từ xa nào là tốt nhất cho trường hợp sử dụng của mình.

### **Các trường hợp sử dụng**

Trong bài viết này, chúng tôi đề cập đến các trường hợp sử dụng sau:

* Người dùng truy cập vào các ứng dụng web nội bộ được triển khai trong một đám mây riêng ảo (VPC).
* Nhân viên vận hành nội bộ truy cập vào các instance EC2 và Amazon Relational Database Service (Amazon RDS) được triển khai trong một VPC.
* Nhà phân tích truy cập vào dữ liệu nhạy cảm nằm trên Amazon Simple Storage Service (Amazon S3).
* Người dùng truy cập vào các ứng dụng SAML 2.0 và OAuth 2.0.

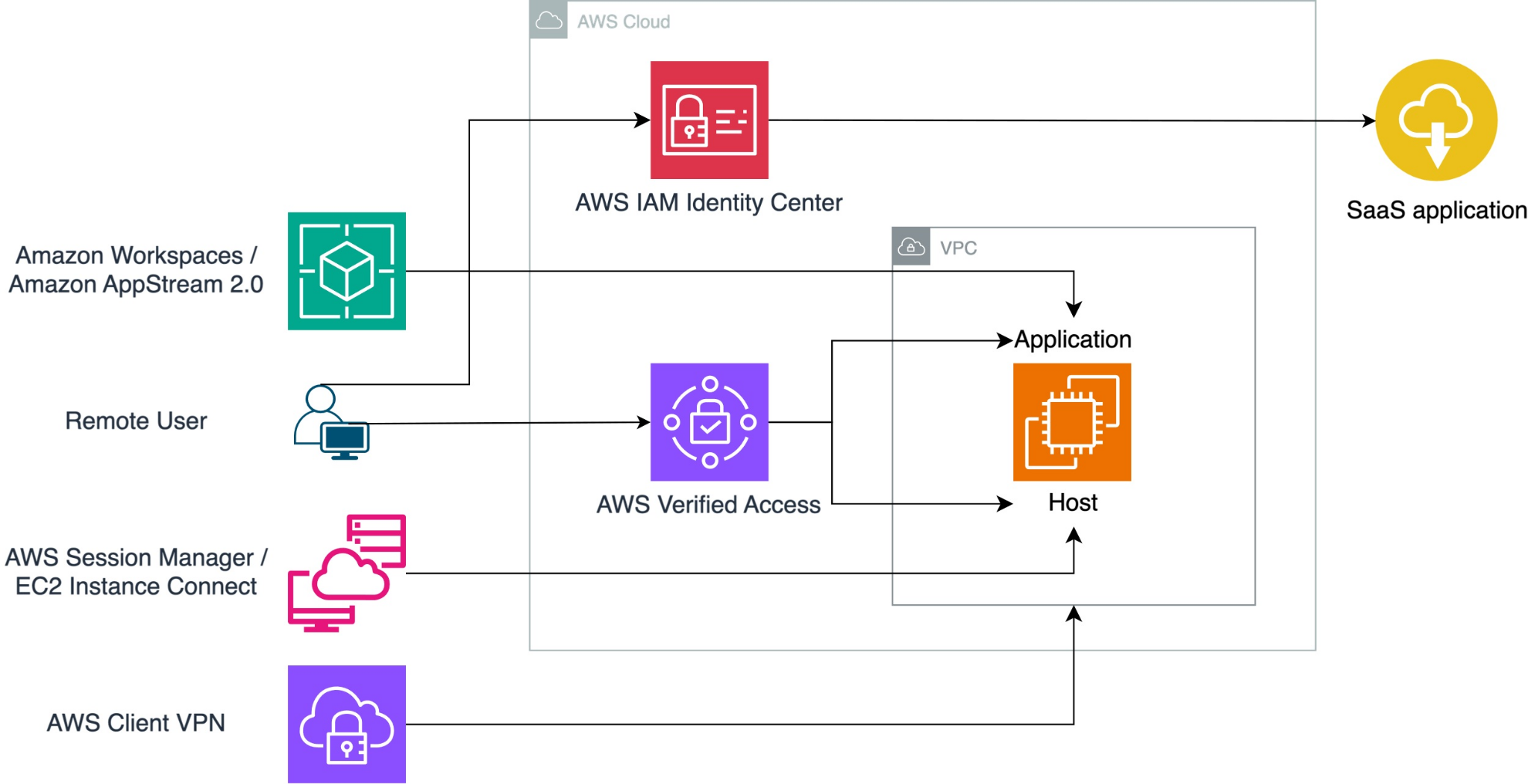
### **Những thách thức liên quan đến truy cập từ xa**

* **Chi phí:** Chi phí của một giải pháp truy cập từ xa là một yếu tố quan trọng đối với các doanh nghiệp.
* **Bề mặt tấn công gia tăng:** Bảo vệ một VPC với nhiều instance EC2, bucket S3 và một cơ sở dữ liệu là một nhiệm vụ khác so với việc bảo vệ danh tính, thiết bị và các kênh liên lạc được sử dụng để truy cập từ xa vào hạ tầng.
* **Rủi ro gia tăng:** Dễ bị tấn công bởi các mối đe dọa kỹ thuật xã hội (social engineering). Con người truy cập vào các workload là mắt xích yếu nhất trong bất kỳ chương trình bảo mật nào, gây ra rủi ro cho dữ liệu và hạ tầng mà nếu không sẽ không tồn tại.
* **Trải nghiệm người dùng (UX):** UX là một yếu tố quan trọng trong truy cập từ xa. Thiếu một UX được thiết kế tốt có thể gây ra rủi ro bằng cách làm cho việc thực hiện các hoạt động hàng ngày trở nên khó khăn hoặc phản ứng nhanh với các sự cố ảnh hưởng đến người dùng ở quy mô lớn.

Một giải pháp để giảm thiểu rủi ro liên quan đến truy cập từ xa là không cung cấp nó ở một số cấp độ nhất định, và đôi khi bạn có thể chọn phương pháp này. Trong những trường hợp này, việc truy cập vào các workload cần được bảo mật chỉ có thể thực hiện được từ các địa điểm đáng tin cậy (như văn phòng công ty) và các thiết bị được quản lý (như máy tính xách tay do công ty cấp). Trong phần còn lại của bài viết này, chúng tôi sẽ nói về các phương pháp và giải pháp có sẵn cho bạn khi bạn cần cung cấp quyền truy cập từ xa từ nhiều địa điểm và thiết bị khác nhau.

### **Các phương pháp tiếp cận khác nhau**

Trước khi đi sâu vào các dịch vụ và tính năng, hãy cùng khám phá các phương pháp khác nhau để cung cấp quyền truy cập từ xa cho người dùng của bạn (thể hiện trong Hình 1). Sự khác biệt chính giữa chúng là ranh giới tin cậy (trust boundary) nằm ở đâu.



*Hình 1: Các phương pháp tiếp cận khác nhau cùng với các giải pháp tương ứng*

* **Tiếp cận dựa trên mạng (Network-based approach):** Người dùng được cấp quyền truy cập vào mạng của bạn thông qua các VPC và được cấp quyền truy cập rộng rãi vào tài nguyên đích thực tế, ứng dụng web hoặc các Instance EC2. Ranh giới tin cậy trong trường hợp này là VPC.
* **Tiếp cận dựa trên máy chủ (Host-based approach):** Người dùng có quyền truy cập vào máy chủ đang chạy ứng dụng. Điều này thường được sử dụng cho quyền truy cập của người vận hành. Ranh giới tin cậy là máy chủ.
* **Tiếp cận dựa trên ứng dụng (Application-based approach):** Người dùng truy cập ứng dụng bằng thông tin đăng nhập của công ty. Đây thường là trường hợp của các ứng dụng phần mềm dưới dạng dịch vụ (SaaS). Ranh giới tin cậy là ứng dụng.
* **Tiếp cận điện toán người dùng cuối (End-user computing approach):** Điện toán người dùng cuối (EUC) là sự kết hợp của các công nghệ, chính sách và quy trình cung cấp cho người dùng quyền truy cập từ xa, an toàn vào các ứng dụng, máy tính để bàn và dữ liệu mà họ cần để hoàn thành công việc. Máy tính để bàn được vận hành tập trung trên đám mây và tương tác bằng cách truyền các pixel đến thiết bị của người dùng. Cách tiếp cận này chuyển ranh giới tin cậy từ thiết bị của người dùng sang máy tính để bàn và dữ liệu nằm trên đám mây.

### **Tiếp cận dựa trên mạng (Network-based approach)**

Phương pháp dựa trên mạng phổ biến khi người dùng cần truy cập vào nhiều tài nguyên nằm trong các mạng cụ thể một cách đơn giản, trong khi vẫn giữ cho các mạng này không kết nối với internet công cộng. Khi cung cấp quyền truy cập ở cấp độ mạng, việc quản lý các cấu hình bảo mật như ủy quyền, xác thực và kiểm toán diễn ra tại tài nguyên (ứng dụng hoặc máy) và thiết bị khách, gây ra những thách thức ở quy mô lớn.

**AWS Client VPN** là một dịch vụ được quản lý hoàn toàn mà bạn có thể sử dụng để kết nối người dùng một cách an toàn với các VPC từ hầu hết mọi địa điểm bằng cách sử dụng các client dựa trên OpenVPN. Người dùng có thể xác thực bằng nhà cung cấp danh tính (IdP) của tổ chức bạn kết hợp với xác thực dựa trên chứng chỉ. Dịch vụ này hỗ trợ các quy tắc ủy quyền hoạt động như các quy tắc tường lửa để cấp cho người dùng quyền truy cập vào các khối CIDR cụ thể dựa trên tư cách thành viên trong một nhóm Active Directory hoặc một nhóm được xác định trong một IdP dựa trên SAML. Ngoài ra, bạn có thể sử dụng các trình xử lý kết nối client để chạy logic ủy quyền tùy chỉnh dựa trên các thuộc tính của thiết bị, người dùng và kết nối.

### **Tiếp cận dựa trên máy chủ (Host-based approach)**

Việc cung cấp quyền truy cập vào máy chủ không phải lúc nào cũng cần thiết. Một cách để giảm thiểu rủi ro liên quan đến truy cập máy chủ trái phép là không cho phép nó và thay vào đó dựa vào các hoạt động hoàn toàn tự động. Trong thực tế, các nhà khai thác và nhà phát triển vẫn yêu cầu quyền truy cập vào máy chủ để có khả năng hiển thị, điều chỉnh cài đặt hệ điều hành, áp dụng các bản vá hoặc khởi động lại dịch vụ theo cách thủ công.

Để truy cập vào các instance EC2, bạn có thể sử dụng các tính năng như **AWS Systems Manager Session Manager** hoặc **EC2 Instance Connect Endpoint**. Cả hai tính năng này đều cung cấp quyền truy cập vào một máy chủ mà không cần phơi bày nó ra internet, và vì chúng sử dụng AWS Identity and Access Management (IAM), chúng xác thực, ủy quyền và ghi lại mọi yêu cầu phiên được thực hiện vào AWS CloudTrail, và cung cấp các khả năng như Điều kiện IAM (ví dụ: aws:SourceIp) để áp dụng quyền truy cập có điều kiện, thường giảm thiểu nhu cầu về một phương pháp tiếp cận dựa trên mạng.

### **Tiếp cận điện toán người dùng cuối (End-user computing approach)**

Các dịch vụ điện toán người dùng cuối như **Amazon WorkSpaces Family** hoặc **Amazon AppStream 2.0** truyền phát máy tính để bàn và ứng dụng dưới dạng các pixel được mã hóa đến người dùng từ xa trong khi vẫn giữ dữ liệu an toàn trong Amazon Virtual Private Cloud (Amazon VPC) của bạn và các mạng riêng được kết nối. Việc truy cập trái phép vào thiết bị khách chỉ tiếp xúc với các pixel được mã hóa, về cơ bản di chuyển ranh giới tin cậy từ thiết bị truy cập tài nguyên sang máy tính để bàn ảo đang chạy trên đám mây.

Khi áp dụng điện toán người dùng cuối để truy cập từ xa, bạn có thể chọn UX và cấu trúc chi phí phù hợp nhất với trường hợp sử dụng của mình (ví dụ: truy cập liên tục vào máy tính để bàn hoặc truy cập theo yêu cầu vào các ứng dụng cụ thể).

### **Tiếp cận dựa trên ứng dụng (Application-based approach)**

**IAM Identity Center** chủ yếu được biết đến với việc đơn giản hóa quyền truy cập của người dùng vào các tài khoản AWS trong một tổ chức ở quy mô lớn. Nó cũng cung cấp quyền truy cập đăng nhập một lần (SSO) vào các ứng dụng web được hỗ trợ, cho phép người dùng truy cập liền mạch vào các ứng dụng này sau khi họ đăng nhập bằng thông tin đăng nhập thư mục của mình.

### **Kết hợp nhiều phương pháp trong mô hình Zero Trust**

Mô hình **Zero Trust** kết hợp nhiều yếu tố bao gồm danh tính người dùng, thiết bị, vị trí và các yếu tố khác để đánh giá và cấp quyền truy cập. Một cách mà bạn có thể triển khai mô hình này để cung cấp quyền truy cập từ xa vào các workload được triển khai trong VPC là sử dụng **AWS Verified Access**. Với Verified Access, bạn có thể cung cấp quyền truy cập an toàn vào các ứng dụng của công ty mà không cần VPN client và hỗ trợ các kết nối dựa trên TCP đến một VPC, cho dù đó là các ứng dụng web hay các instance EC2 hoặc RDS.

### **Hiểu rõ các đánh đổi**

Để chọn giải pháp phù hợp cho lực lượng lao động của mình, hãy làm việc ngược từ trường hợp sử dụng. Bắt đầu bằng cách xác định và phân loại kho tài sản và lập bản đồ những người dùng truy cập nó và các mẫu truy cập của họ.

Bảng sau đây cung cấp một cái nhìn tổng quan về các giải pháp khác nhau và các yếu tố có thể giúp bạn đưa ra quyết định sáng suốt.

| **Giải pháp** | **Trường hợp sử dụng** | **Ranh giới tin cậy** | **Cung cấp quyền truy cập tới** | **Giao thức** | **Trải nghiệm người dùng** | **Xác thực** | **Ủy quyền** | **Khả năng giám sát** |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| **Client VPN** | Truy cập ứng dụng nội bộ; Truy cập của người vận hành vào tài nguyên IP trong VPC | Mạng | VPCs, subnets, security groups | IP | Dựa trên client, native | SSO (SAML), Active Directory, Mutual (certificate) | Theo CIDR, Lambda Authorizer | Ghi log kết nối (CloudWatch) |
| **Session Manager** | Truy cập của người vận hành vào EC2 hoặc on-premises | Máy chủ | Instances: Linux, Windows, MacOS (chỉ EC2) | SSH hoặc RDP | Native | IAM | IAM | CloudTrail, ghi log trong phiên (CloudWatch, S3) |
| **EC2 Instance Connect** | Truy cập của người vận hành vào EC2 | Máy chủ | Instances: Linux hoặc Windows | SSH hoặc RDP | Native | IAM | IAM | CloudTrail |
| **IAM Identity Center** | Truy cập vào ứng dụng SAML 2.0 và OAuth 2.0 | Ứng dụng | Ứng dụng web | HTTP(S) | Native | IAM Identity Center | IAM Identity Center | CloudTrail |
| **Verified Access** | Truy cập ứng dụng web hoặc TCP trong VPC | Amazon Verified Access | Ứng dụng web, tài nguyên TCP | HTTP(S) hoặc TCP | Native | IAM Identity Center hoặc OIDC | Tùy chỉnh bằng chính sách Cedar; Tín hiệu thiết bị | Ghi log mỗi yêu cầu |
| **Amazon WorkSpaces** | Truy cập máy tính để bàn ảo liên tục trong VPC | Máy tính để bàn đám mây | Máy tính để bàn ảo liên tục | WSP hoặc PCoIP | Dựa trên client, hoặc non-native | Nhà cung cấp danh tính | Thành viên nhóm | CloudTrail |
| **AppStream 2.0** | Truy cập máy tính để bàn ảo trong VPC | Máy tính để bàn đám mây | Máy tính để bàn và ứng dụng ảo không liên tục | NICE DCV | Dựa trên client, hoặc non-native | Nhà cung cấp danh tính | Thành viên nhóm | CloudTrail |

### **Kết luận**

Trong bài viết này, bạn đã tìm hiểu về các phương pháp và giải pháp khác nhau để cung cấp quyền truy cập từ xa cho lực lượng lao động của tổ chức bạn. Điều này bao gồm các khuyến nghị chiến thuật về cách tìm giải pháp truy cập từ xa phù hợp nhất với nhu cầu của bạn dựa trên các yếu tố như chi phí, trải nghiệm người dùng và rủi ro. Bằng cách hiểu những đánh đổi đó, giờ đây bạn có thể vạch ra các trường hợp sử dụng khác nhau dựa trên cơ sở hạ tầng và mô hình mối đe dọa của mình và xây dựng một chiến lược truy cập từ xa để đáp ứng nhu cầu của bạn.

### **Về tác giả**

**Itay Meller**

Itay là một Kiến trúc sư giải pháp chuyên gia về bảo mật tại AWS, với nền tảng vững chắc về R&D an ninh mạng và các vai trò lãnh đạo tại nhiều công ty tập trung vào bảo mật. Với chuyên môn sâu về bảo mật đám mây, Itay giúp các tổ chức áp dụng và mở rộng quy mô môi trường AWS của họ một cách an toàn bằng cách giải quyết các thách thức phức tạp về bảo mật và tuân thủ.



**Maxim Raya**

Maxim là một Kiến trúc sư giải pháp chuyên gia về bảo mật tại AWS. Trong vai trò này, anh giúp khách hàng đẩy nhanh quá trình chuyển đổi lên đám mây bằng cách tăng cường sự tự tin của họ vào tính bảo mật và tuân thủ của môi trường AWS.

## **📖 Glossary - Thuật ngữ**

| **English** | **Tiếng Việt** | **Định nghĩa / Ghi chú** |
| --- | --- | --- |
| Remote Access | Truy cập từ xa | Khả năng truy cập vào một mạng hoặc máy tính từ một vị trí ở xa. |
| Hybrid Workforce | Lực lượng lao động kết hợp | Mô hình làm việc kết hợp giữa làm việc tại văn phòng và làm việc từ xa. |
| Trust Boundary | Ranh giới tin cậy | Một ranh giới logic nơi mức độ tin cậy thay đổi. |
| Zero Trust | Zero Trust / Không tin cậy | Một mô hình bảo mật yêu cầu xác minh nghiêm ngặt cho mọi người và thiết bị cố gắng truy cập tài nguyên trên một mạng riêng, bất kể họ đang ở bên trong hay bên ngoài vành đai mạng. |
| End-user computing (EUC) | Điện toán người dùng cuối | Công nghệ cho phép người dùng truy cập từ xa vào máy tính để bàn, ứng dụng và dữ liệu. |
| AWS Client VPN | AWS Client VPN | Dịch vụ VPN được quản lý để kết nối an toàn người dùng với mạng AWS hoặc tại chỗ. |
| Session Manager | Session Manager | Một tính năng của AWS Systems Manager cho phép quản lý các instance EC2 thông qua một trình duyệt hoặc AWS CLI. |
| IAM Identity Center | IAM Identity Center | Dịch vụ giúp quản lý tập trung quyền truy cập SSO vào nhiều tài khoản AWS và ứng dụng kinh doanh. |
| AWS Verified Access | AWS Verified Access | Dịch vụ cung cấp quyền truy cập an toàn vào các ứng dụng của bạn mà không cần VPN, dựa trên nguyên tắc Zero Trust. |

## **🔗 Tài liệu tham khảo**

### **Tools và Services**

* [Get started with AWS Client VPN](https://docs.aws.amazon.com/vpn/latest/clientvpn-admin/cvpn-getting-started.html)
* [Getting Started with Amazon Workspaces](https://docs.aws.amazon.com/workspaces/latest/adminguide/getting-started.html)
* [Getting Started with AppStream 2.0](https://docs.aws.amazon.com/appstream2/latest/developerguide/getting-started.html)
* [Get Started with Amazon Verified Access](https://www.google.com/search?q=https://docs.aws.amazon.com/verified-access/latest/userguide/getting-started.html)

### **Tài liệu liên quan**

* [AWS Security Reference Architecture (AWS SRA)](https://docs.aws.amazon.com/prescriptive-guidance/latest/security-reference-architecture/welcome.html)
* [Unified access to AWS End User Computing services](https://aws.amazon.com/blogs/desktop-and-application-streaming/unified-access-to-aws-end-user-computing-services/)