
APPCONNECT
Your Safety Is Our Priority
Công Viên Phần Mềm Mekong - TP. Mỹ Tho, Tiền Giang
www.appconnect.vn

APPCONNECT CO., LTD

NỘI DUNG:

I. GIỚI THIỆU APPCONNECT
- SẢN PHẨM
- GIẢI PHÁP
- DỊCH VỤ

II. XU HƯỚNG BẢO MẬT ZERO TRUST

III. GIẢI PHÁP BẢO MẬT APPGATESDP
- THÔNG TIN GIẢI PHÁP
- SO SÁNH SDP VS VPN
- ÁP DỤNG VÀO DOANH NGHIỆP
- TÓM TẮT LỢI ÍCH

APPCONNECT CO., LTD

I. GIỚI THIỆU APPCONNECT

APPCONNECT CO., LTD

VỀ CÔNG TY

CUNG CẤP GIẢI PHÁP AN NINH MẠNG APPGATESDP - ZERO TRUST NETWORK ACCESS

APPCONNECT là một công ty chuyên cung cấp giải pháp BẢO MẬT và KIỂM SOÁT kết nối **APPGATESDP**, theo xu hướng bảo mật **ZERO TRUST**, phục vụ cho nhiều doanh nghiệp trong các lĩnh vực khác nhau.

APPCONNECT CO., LTD

ĐỘI NGŨ QUẢN LÝ

Đội ngũ quản lý của **APPCONNECT** là những chuyên gia An Ninh Mạng dày dạn kinh nghiệm, cam kết bảo vệ dữ liệu và hệ thống của doanh nghiệp khỏi các mối đe dọa mạng ngày càng gia tăng.

Quản lý

CEO/Founder
Trần Hoàng Vũ
20 năm kinh nghiệm trong lĩnh vực CNTT và 9 năm kinh nghiệm quản lý dự án CNTT tại VTC Mobile trực thuộc Tổng Công Ty Truyền Thông Đa Phương Tiện VTC

Co-Founder
Nguyễn Anh Khôi
Thạc Sĩ An Toàn Thông Tin
Giảng viên Phân Hiệu Học Viện Kỹ Thuật Mật Mã TP.Hồ Chí Minh

Trưởng Phòng Giải Pháp Bảo Mật
Nguyễn Thông Đạt
Thạc Sĩ Viễn Thông
15 năm kinh nghiệm trong vận hành, triển khai và quản lý CNTT - Viễn Thông

appgate

GIẢI PHÁP APPGATE SDP

AppgateSDP là giải pháp bảo mật truy cập mạng **Zero Trust** được thiết kế để bảo vệ các ứng dụng và dữ liệu của doanh nghiệp khỏi các mối đe dọa mạng, giảm thiểu lây lan **Ransomware** trong môi trường mạng nội bộ.

Tính năng nổi bật:

- Kiểm soát truy cập theo nguyên tắc "ít đặc quyền nhất" (đặc quyền tối thiểu)
- Xác thực mạnh mẽ, đa yếu tố, đa môi trường
- Tích hợp sẵn sàng MFA (Google Authenticator/Microsoft Authenticator)/FIDO2
- Theo dõi và giám sát liên tục
- Ngăn chặn lây lan mã độc trong mạng ngang hàng
- Thay thế VPN truyền thống và NAC, kiểm soát toàn diện kết nối mạng
- Quản lý chính sách truy cập tập trung theo tài khoản người dùng
- Hỗ trợ môi trường Cloud, Hybrid và On-premise
- Tính năng bảo mật nâng cao: Single Packet Authorization (SPA), Micro-Segmentation, Dynamic Access Control, Software-Defined Perimeter

APPCONNECT CO., LTD

www.appconnect.vn

appgate

DỊCH VỤ

APPCONNECT CO., LTD

Công ty cung cấp đa dạng dịch vụ để đáp ứng mọi nhu cầu của doanh nghiệp:

- **Tư vấn giải pháp**: cung cấp dịch vụ tư vấn chuyên sâu về giải pháp bảo mật **AppgateSDP**, giúp doanh nghiệp hiểu rõ về khả năng và lợi ích của giải pháp trong việc bảo vệ mạng và quản lý truy cập an toàn.
- **Triển khai giải pháp**: đội ngũ chuyên gia của công ty sẽ triển khai giải pháp **AppgateSDP** trong môi trường của doanh nghiệp, đảm bảo tính an toàn và hoạt động hiệu quả.
- **Đào tạo sử dụng**: cung cấp các khóa đào tạo chuyên sâu về sử dụng **AppgateSDP**, giúp nhân viên của doanh nghiệp nắm vững các chức năng và quy trình để tận dụng tối đa khả năng bảo mật và quản lý truy cập của giải pháp.
- **Hỗ trợ kỹ thuật:** đội ngũ hỗ trợ kỹ thuật sẵn sàng hỗ trợ trong việc giải quyết các vấn đề kỹ thuật liên quan đến **AppgateSDP**, đảm bảo hệ thống luôn hoạt động ổn định và an toàn.
- **Nâng cấp phiên bản:** cung cấp dịch vụ nâng cấp phiên bản **AppgateSDP**, giúp tiếp cận các tính năng mới nhất và cải thiện hiệu suất của giải pháp để đáp ứng nhu cầu ngày càng tăng của doanh nghiệp.
- **Đào tạo an toàn thông tin cho doanh nghiệp:** Chúng tôi cung cấp các khóa đào tạo về an toàn thông tin cho doanh nghiệp, tập trung vào việc sử dụng **AppgateSDP** như một công cụ quan trọng để bảo vệ dữ liệu và hệ thống của bạn khỏi các mối đe dọa và tấn công mạng.

APPCONNECT CO., LTD

SẢN PHẨM TÍCH HỢP

Cung cấp gói giải pháp bao gồm phần cứng tích hợp tường lửa **pfSense** và giải pháp bảo mật kiểm soát kết nối **AppgateSDP** dành cho doanh nghiệp chưa có hệ thống bảo mật an toàn thông tin.

pfsense là một giải pháp tường lửa lý tưởng cho các doanh nghiệp nhỏ nhờ vào khả năng bảo mật mạnh mẽ và tính linh hoạt. Với các tính năng đa dạng và dễ quản lý, **pfsense** giúp doanh nghiệp nhỏ có thể bảo vệ hệ thống mạng của mình một cách hiệu quả mà không cần đầu tư quá nhiều chi phí.

AppgateSDP Zero Trust Network Access (ZTNA) là một giải pháp lý tưởng cho các doanh nghiệp nhỏ, giúp tăng cường bảo mật, kiểm soát truy cập chặt chẽ, ngăn ngừa lây lan **Ransomware** và hỗ trợ làm việc từ xa an toàn. Với khả năng linh hoạt, dễ triển khai và chi phí hợp lý, ZTNA không chỉ bảo vệ doanh nghiệp khỏi các mối đe dọa mạng mà còn giúp tuân thủ các quy định bảo mật và nâng cao hiệu quả hoạt động.

APPCONNECT CO., LTD

GÓI SẢN PHẨM

GÓI MIỄN PHÍ
(Dành cho Doanh Nghiệp Siêu Nhỏ)

- ✔ **1 tài khoản quản trị**
- ✔ 1 tài khoản không giới hạn máy tính
- ✔ Đầy đủ tính năng bảo mật
- ✘ Thiết bị cài đặt kèm theo
- ✘ Hỗ trợ kỹ thuật 24/7
- ✘ Nâng cấp phiên bản AppgateSDP

MIỄN PHÍ VĨNH VIỄN

GÓI CƠ BẢN
(Dành cho Doanh Nghiệp Siêu Nhỏ)

- ✔ **1 tài khoản quản trị**
- ✔ 1 tài khoản không giới hạn máy tính
- ✔ 4 tài khoản truy cập từ xa (VPN)
- ✔ Đầy đủ tính năng bảo mật
- ✔ Thiết bị cài đặt kèm theo
- ✔ Hỗ trợ kỹ thuật 24/7
- ✔ Nâng cấp phiên bản Appgate SDP

TƯ VẤN

GÓI NÂNG CAO
(Dành cho Doanh Nghiệp Nhỏ)

- ✔ **>= 25 tài khoản theo năm**
- ✔ Không giới hạn máy tính
- ✔ Đầy đủ tính năng bảo mật
- ✔ Thiết bị cài đặt kèm theo
- ✔ Hỗ trợ kỹ thuật 24/7
- ✔ Nâng cấp phiên bản Appgate SDP

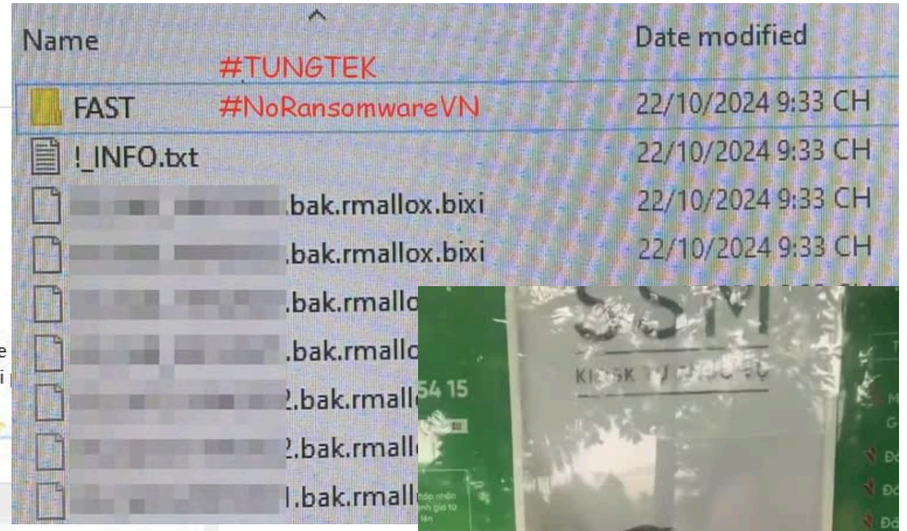
TƯ VẤN

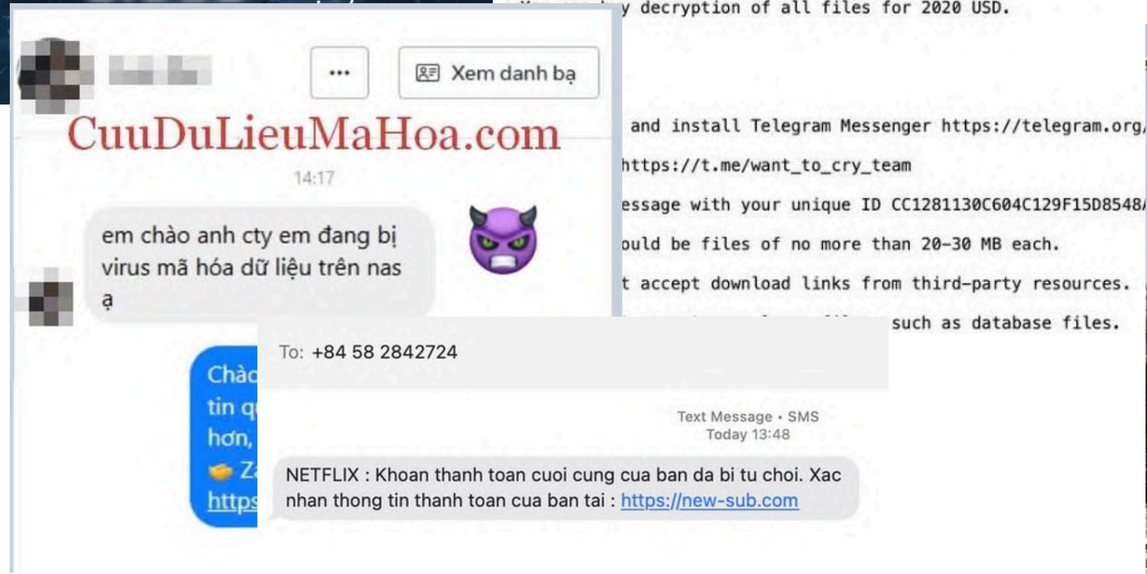
APPCONNECT CO., LTD

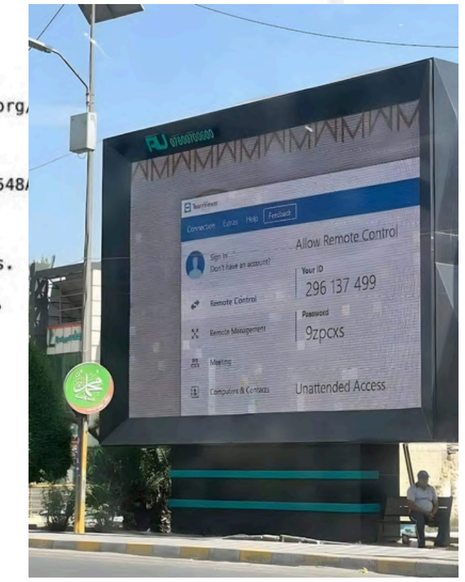
II. XU HƯỚNG BẢO MẬT ZERO TRUST

CÁC SỰ CỐ BẢO MẬT

Bài viết của Ý







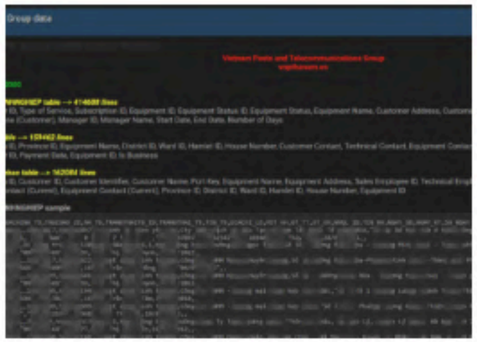
RÒ RỈ DỮ LIỆU

Home › DarkWeb News & Services

Alleged Data Leak of 100 Million Zalo.vn User Records

November 7, 2024 Reading Time: 1 min read

A hacker claims to have obtained a massive database o



Alleged Vietnam Posts and Telecommunications Group Data is For Sale

JULY 11, 2024

A threat actor allegedly compromised the Vietnam Posts and Telecommunications Group database and is selling it on a dark web ...

257,000 Medical Records from the Department of Medical Examination and Treatment Management under Vietnam's Ministry of Health for Sale

MARCH 20, 2024

A threat actor has reportedly put up for sale a database allegedly obtained from the Department of Medical Examination and ...

Xu hướng chuyển dịch kết nối VPN sang Zero Trust

Theo báo cáo rủi ro VPN của hãng bảo mật Zscaler (California) công bố năm 2024:

- ***Các cuộc tấn công VPN đang có xu hướng gia tăng:*** *56% tổ chức cho biết họ đã từng là nạn nhân của nhiều cuộc tấn công mạng liên quan đến VPN trong năm 2023, tăng 45% so với năm 2022.*

- ***Rủi ro bảo mật VPN:*** *91% chuyên gia bày tỏ lo ngại về việc VPN ảnh hưởng đến tính bảo mật trong hệ thống mạng của họ. Nhấn mạnh mức độ rủi ro mà các tổ chức phải đối mặt do điểm yếu cố hữu trong kiến trúc VPN truyền thống.*

- ***Nguy cơ lây lan mạng ngang hàng:*** *53% doanh nghiệp bị xâm phạm thông qua các lỗ hổng VPN cho biết các tác nhân đe dọa đã lây lan mạng ngang hàng trong hệ thống, điều này cho thấy lớp phòng thủ bảo mật đầu tiên để ngăn chặn xâm phạm trong hệ thống mạng đã bị phá vỡ.*

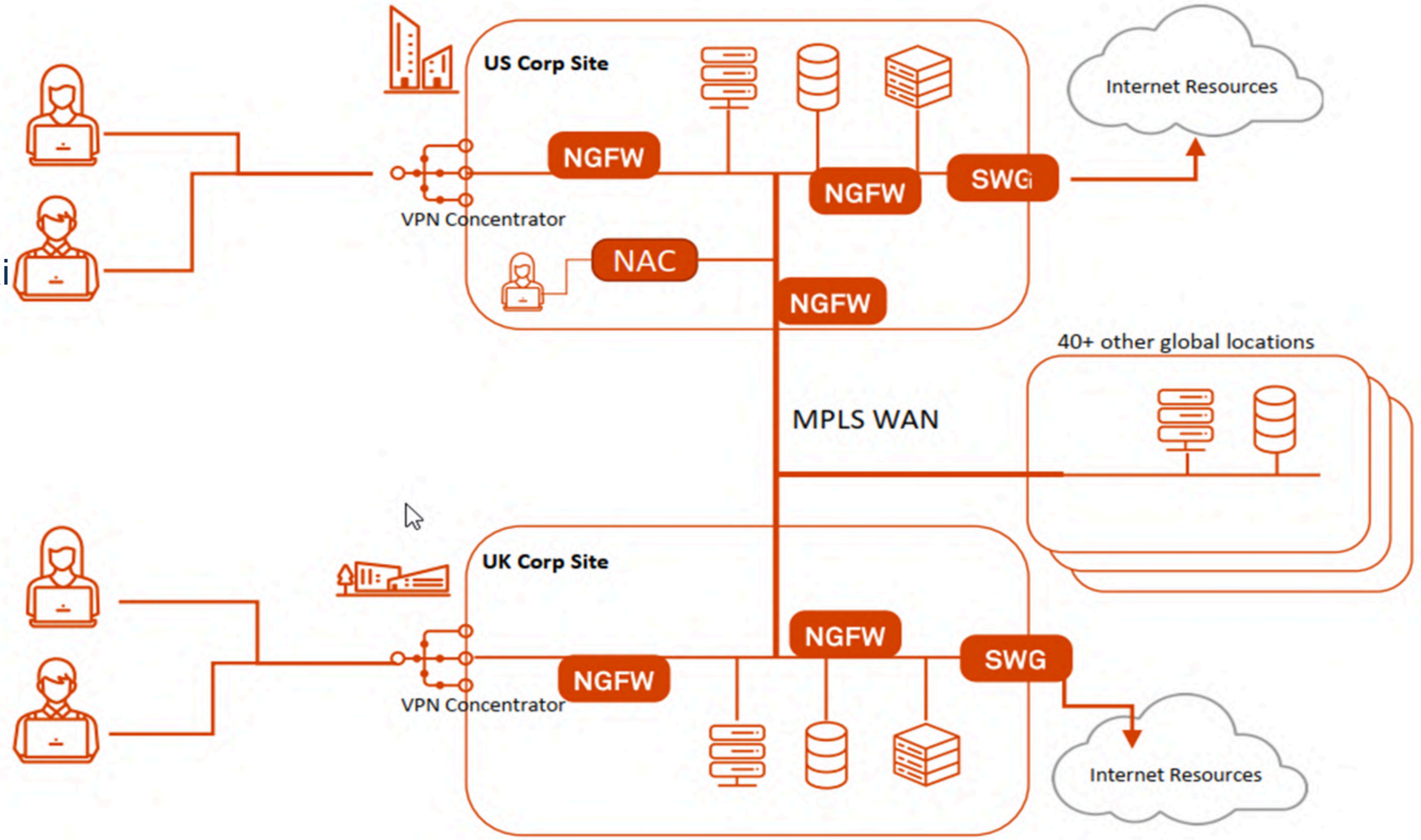
- ***Lo ngại về rủi ro của bên thứ ba:*** *Vì VPN cung cấp quyền truy cập mạng đầy đủ, nên 92% số người được khảo sát bày tỏ lo ngại về các bên thứ ba có quyền truy cập VPN, dẫn đến những rủi ro xâm nhập vào hệ thống mạng của họ.*

- ***Nhiều tổ chức chuyển sang kiến trúc Zero Trust:*** *Theo khảo sát, 78% tổ chức cho biết họ đang có kế hoạch triển khai Zero Trust trong vòng 12 tháng tới*

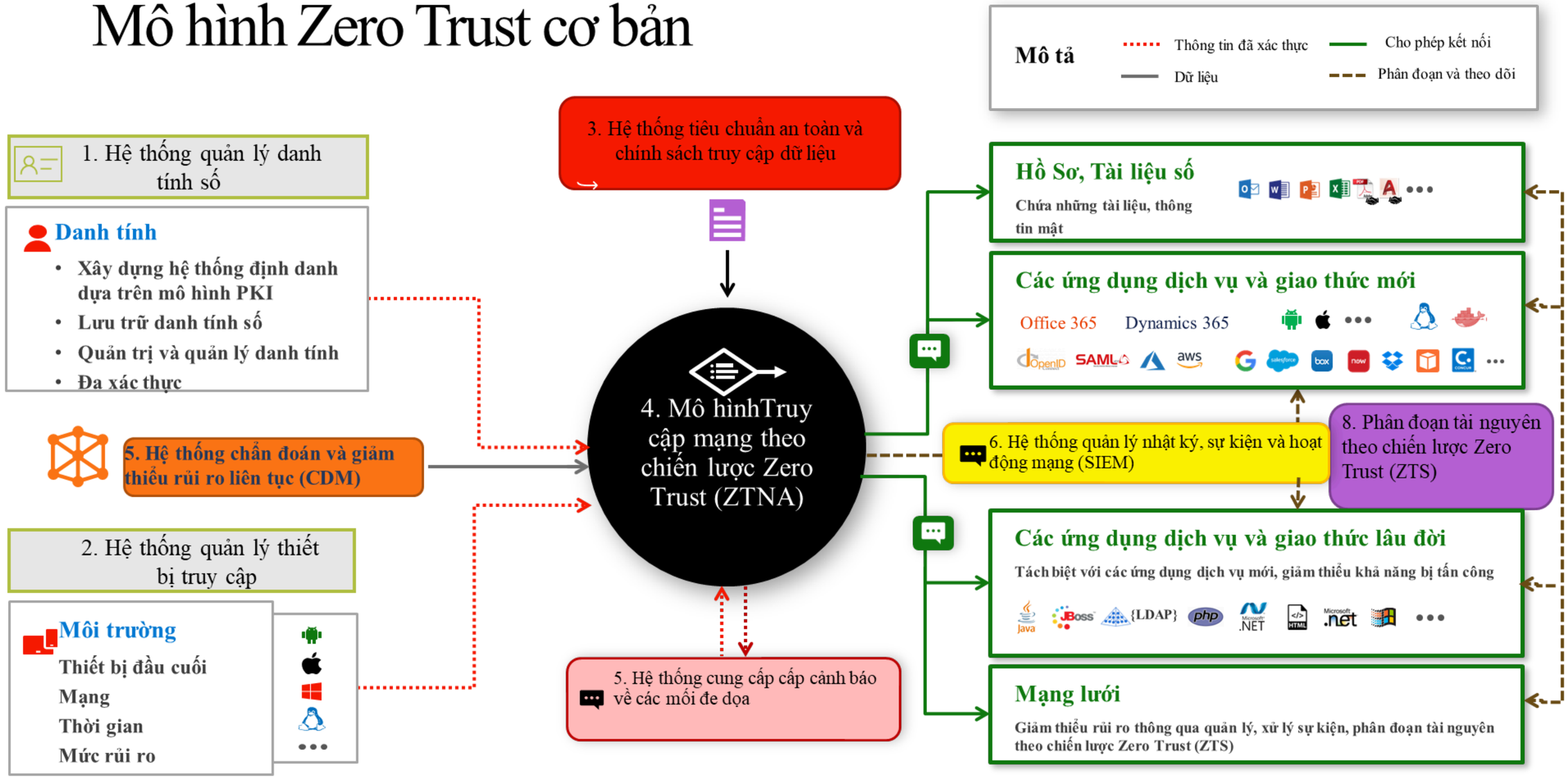
KIẾN TRÚC MẠNG TRUYỀN THỐNG

Nhược điểm:

- Chính sách truy cập bị phân tán, quy trình áp dụng, cập nhật chính sách phức tạp.
- Các cổng dịch vụ có thể bị thăm dò và khai thác
- Đầu tư nhiều tường lửa, kết nối, công cụ kiểm soát làm tăng chi phí và độ trễ cao, giảm hiệu suất
- Quản lý thiết bị cá nhân chưa triệt để.
- Cần tự xây dựng và kết nối với một giải pháp đa xác thực.
- Tồn tại rủi ro tấn công ngang hàng và lây lan mã độc, Ransomware



Mô hình Zero Trust cơ bản



Thông tin đã xác thực
Danh tính số, Môi trường, và kết quả từ CDM

Phân phối và cung cấp tác vụ dựa vào
Hệ thống tiêu chuẩn an toàn và chính sách truy cập dữ liệu

Thực thi chính sách
Tự động áp dụng chính sách lên tất cả tài nguyên có trong mạng lưới

APPCONNECT CO., LTD

III. GIẢI PHÁP BẢO MẬT
APPGATESDP ZTNA

appgate

Giới thiệu Appgate SDP

COMMON CRITERIA

Giải pháp SDP theo chiến lược ZTNA đầu tiên đạt chứng nhận CC.

DEPARTMENT OF DEFENSE (DOD)

Được bộ quốc phòng Hoa Kỳ cho phép hoạt động trong hệ thống.

FEDERAL INFORMATION PROCESSING STANDARDS (FIPS)

Được kiểm thử và đánh giá về chỉ số đảm bảo an toàn (EAL-2).

NATIONAL CYBERSECURITY CENTER OF EXCELLENCE

Được tham gia vào chương trình định hướng an ninh mạng thuộc quản lý của cơ quan NIST, Hoa Kỳ.

DOD CLOUD NATIVE ACCESS POINT (CNAP)

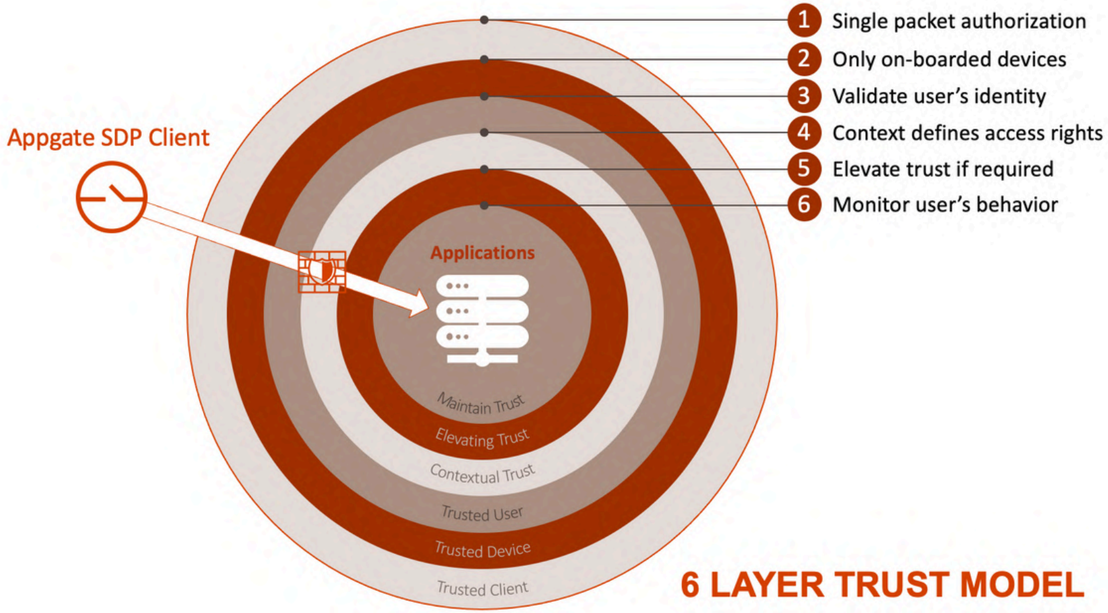
Hoàn toàn phù hợp để nâng cao bảo mật cho đám mây, kể cả đám mây cá nhân.

LÀ GIẢI PHÁP BẢO MẬT ĐÁP ỨNG CÁC TIÊU CHUẨN BẢO MẬT CỦA CHÍNH PHỦ HOA KỲ

Appgate SDP là giải pháp bảo mật và quản lý truy cập được phát triển dựa trên kiến trúc bảo mật Zero-Trust. *Mục tiêu của Appgate SDP là đảm bảo hệ thống triển khai tiếp cận được mô hình kiến trúc Zero-Trust cũng như khả năng tích hợp và thay thế một số phần mềm, giải pháp bảo mật lâu đời.*

Appgate là công ty đa quốc gia*, với văn phòng có mặt ở trên 40 quốc gia và có hơn 3960 khách hàng trên thế giới. Appgate là giải pháp bảo mật truy cập duy nhất theo kiến trúc Zero Trust mà không phụ thuộc vào bất cứ Firewall nào.*

Appgate là công ty bảo mật *được tách ra từ Cyxteria, một trong những nhà doanh nghiệp toàn cầu cung cấp dịch vụ bảo mật, dịch vụ Cloud, và dịch vụ phân tích dữ liệu hàng đầu thế giới. Ngoài ra Appgate SDP được Forrester đánh giá "dẫn đầu" về mô hình bảo mật truy cập theo kiến trúc Zero Trust 2 năm liền.*



6 LAYER TRUST MODEL

CHỨNG NHẬN BỞI CÁC TỔ CHỨC UY TÍN

Australian Government
Australian Signals Directorate

Certificate Number: 2021/133

CERTIFICATE

AUSTRALASIAN INFORMATION SECURITY EVALUATION PROGRAM

This is to certify that

AppGate SDP v5.2.0

produced by
AppGate

has been evaluated under the terms of the
Australasian Information Security Evaluation Program

in the category of
Network and Network-Related Devices and Systems

and complies with the requirements of
Common Criteria EAL 2 augmented with ALC_FLR.1

(original signed)
Karl Hanmore
A/g Head Australian Cyber Security Centre
11 January 2021

The IT product identified in this certificate has been [illegible] accredited and licensed evaluation facility of Australia using the Common Methodology for IT Security Evaluation, (Version 3.1 Revision 5), for conformance to the Common Criteria for IT Security Evaluation, (Version 3.1 Revision 5). This certificate applies only to the specific version and release of the product in its evaluated configuration and in conjunction with the complete Certification Report. The evaluation has been conducted in accordance with the provisions of the Australasian Information Security Evaluation Program (AISEP) and the conclusions of the evaluation facility in the evaluation technical report are consistent with the evidence adduced. This certificate is not an endorsement of the IT product by the AISEP or by any other organisation that recognises or gives effect to this certificate, and no warranty of the IT product by the AISEP or by any other organisation that recognises or gives effect to this certificate, is either expressed or implied.

ACSC Australian Cyber Security Centre

Common Criteria

NIST

ZERO TRUST ARCHITECTURE

SP800-207

SELECTED TO COLLABORATE WITH NCCoE

Gartner

REPRESENTATIVE VENDOR - ZTNA MARKET GUIDE

GARTNER PEER INSIGHTS: 4.8 OF 5 STARS*

FORRESTER®

FORRESTER® WAVE LEADER 2020
Zero Trust eXtended Ecosystem Platform Providers

FORRESTER® NEW WAVE LEADER 2021
Zero Trust Network Access

appgate

Appgate SDP: Industry validated. Government approved. Enterprise trusted.

Nemertes
How ZTNA Drives Network Transformation and Cost Savings
Get Report >

COMMON CRITERIA
First and only Common Criteria-certified ZTNA solution
Learn More >

aws
AWS approved and certified security competency partner
Learn More >

Trusted by the DoD In production environments
Explore Federal >

NIST
NCCoE Collaborator: NIST's "Implementing a Zero Trust Architecture" project
Read Report >

Nemertes
How ZTNA Drives Network Transformation and Cost Savings
Get Report >

COMMON CRITERIA
First and only Common Criteria-certified ZTNA solution
Learn More >

KHÁCH HÀNG TRÊN THẾ GIỚI

THE THIRD FLOOR · NCL NORWEGIAN CRUISE LINE · NEQUI · Secureworks · chewy · WW · GSA · rackspace technology · Bancolombia · VoiceBase

Bancolombia · VoiceBase · RELTIO · DATADOG · U.S. AIR FORCE · ManTech Securing the Future · FINRA · THE THIRD FLOOR · NCL NORWEGIAN CRUISE LINE

APPCONNECT CO., LTD

GIẢI PHÁP BẢO MẬT APPGATE SDP

appgate

CHE DẤU HẠ TẦNG MẠNG

Giảm thiểu nguy cơ bị tấn công và bảo vệ các thành phần của hạ tầng mạng khỏi sự phát hiện và khai thác từ các mối đe dọa

QUẢN LÝ HÀNH VI CON NGƯỜI

Thu thập tất cả thông tin thiết bị người dùng và môi trường sử dụng để đưa vào chính sách truy cập

CHỦ ĐỘNG VÀ LIÊN TỤC

Liên tục theo dõi, giám sát liên tục kết nối đến hệ thống bao gồm trạng thái thiết bị, môi trường kết nối, hành vi kết nối

CHI TIẾT CHUYÊN SÂU

Phân quyền chi tiết đến từng dịch vụ trong hệ thống. Phân đoạn kết nối riêng biệt

LÀ PHẦN MỀM CHO PHÉP NGƯỜI DÙNG LẬP TRÌNH VÀ THÍCH ỨNG LINH HOẠT

Dễ dàng tích hợp với các công cụ bên thứ 3 thông qua API

APPCONNECT CO., LTD

appgate

CÁCH THỨC HOẠT ĐỘNG

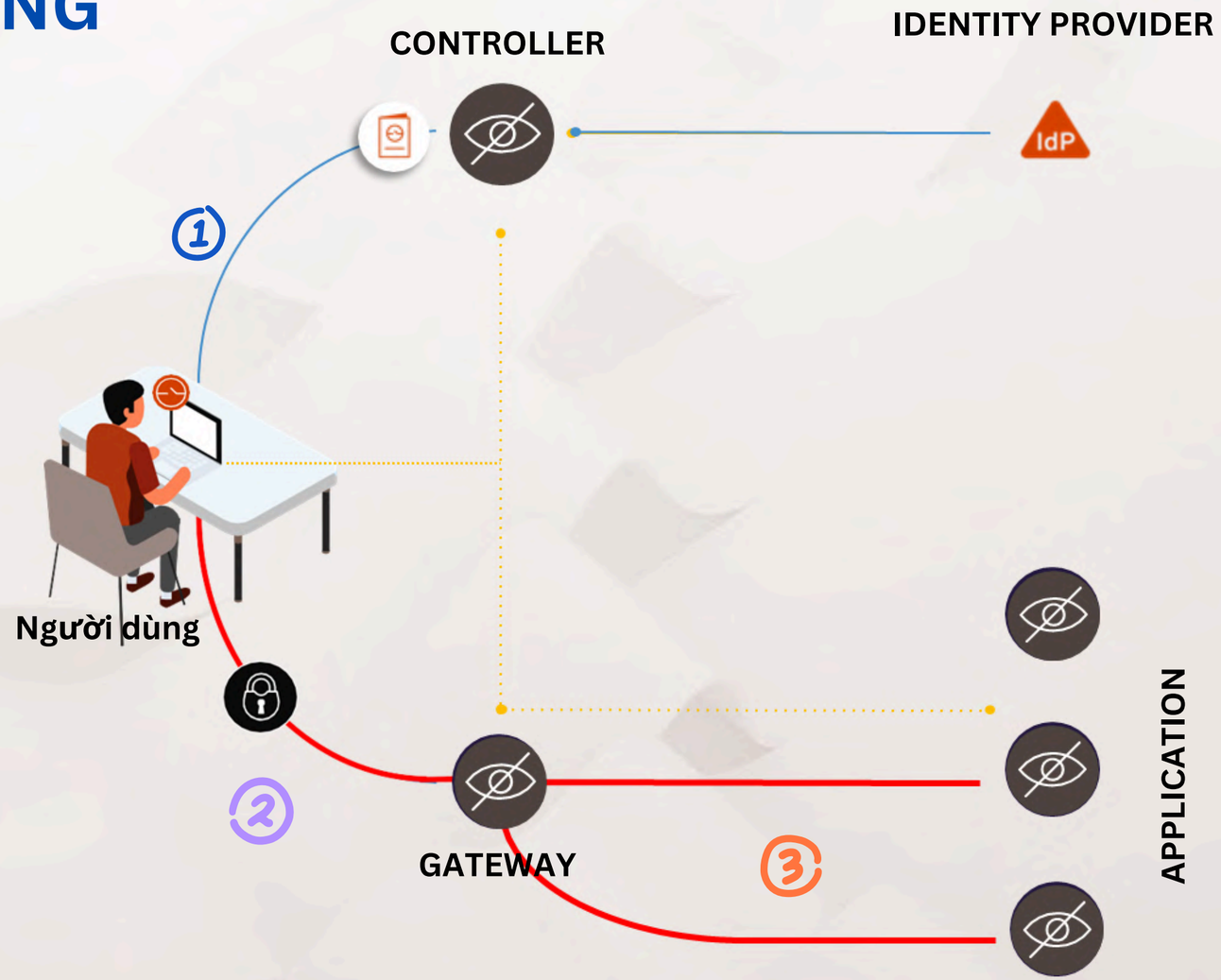
1.Client gửi thông tin người dùng đến Controller bằng giao thức “Single-Packet Authorization (SPA)”.

2.Controller kiểm tra xác thực, phân quyền và phản hồi cho Client.

3.Thông qua SPA, Client gửi phân quyền của mình đến Gateway để Gateway kiểm tra và lọc các ứng dụng theo đúng phân quyền được cấp.

4.Một phân đoạn trong mạng lưới hệ thống chủ động sẽ được tạo ra cho phiên làm việc này.

5.Liên tục theo dõi các biến đổi của phân quyền và chủ động điều chỉnh phân đoạn trong mạng lưới hệ thống để phù hợp với yêu cầu.



KIẾN TRÚC TỔNG THỂ GIẢI PHÁP APPGATESDP

Các thành phần trong AppgateSDP:

1. SDP Client: client cài đặt trên thiết bị người dùng. Có tính năng kiểm soát, giám sát toàn bộ trạng thái của thiết bị kể cả kết nối IN/OUT trong mạng ngang hàng

2. SDP Controller: vai trò trung tâm quản lý xác thực/chính sách/thiết bị/thành phần khác của AppgateSDP

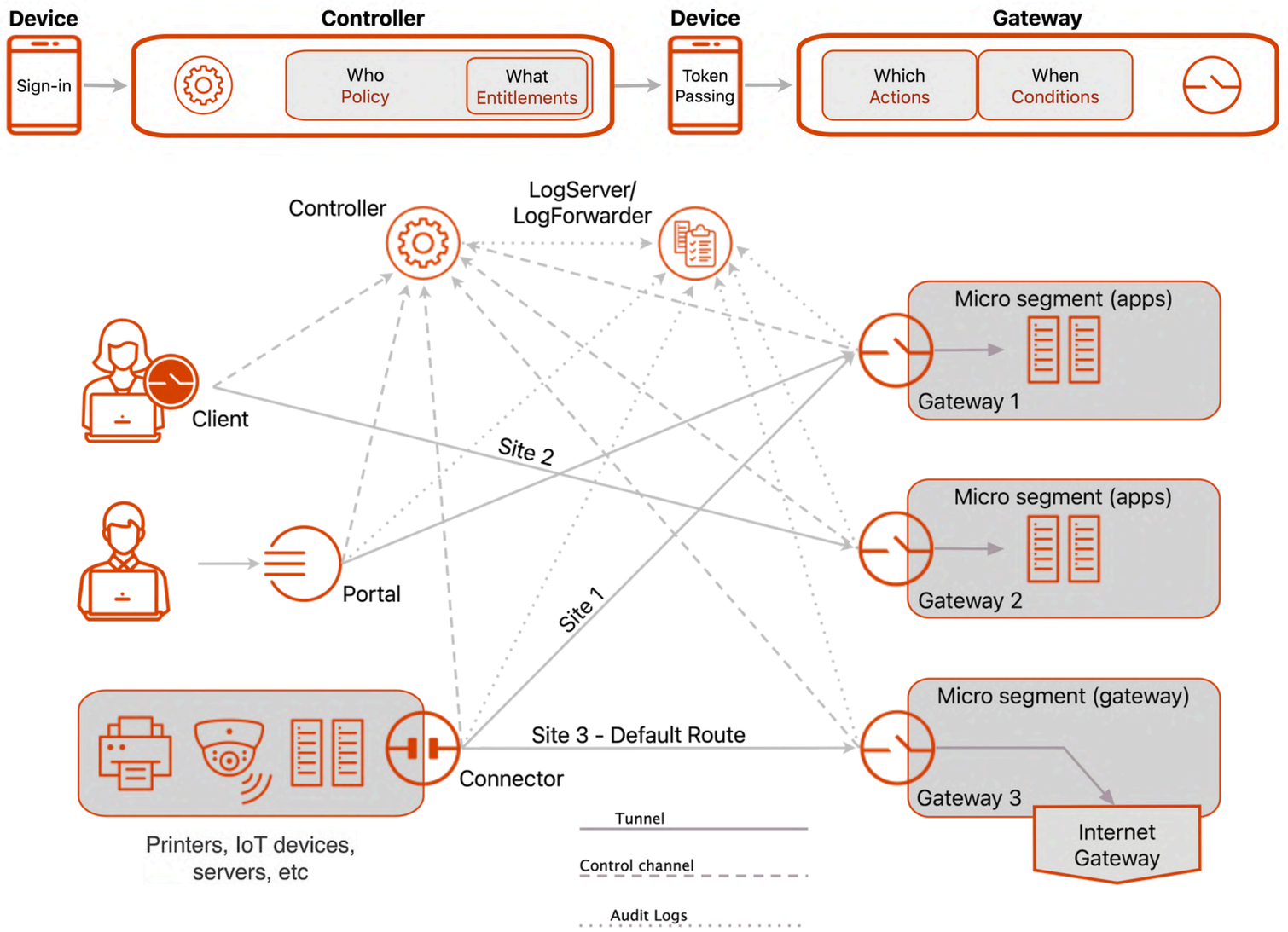
3. SDP Gateway: cổng kết nối đến tài nguyên phía sau. Kiểm tra và thực thi chính sách truy cập.

4. SDP Portal: truy cập tài nguyên thông qua giao diện Website, không cần cài đặt SDP Client lên thiết bị

5. SDP Connector: trung gian kiểm soát và tạo kết nối giữa các tài nguyên mà không cần cài đặt SDP Client. Dành cho các thiết OT, IoT, server-to-server

6. SDP Log Server/Log Forwarder: lưu trữ Logs hệ thống/truy cập hoặc gửi đến hệ thống Logs tập trung hiện có.

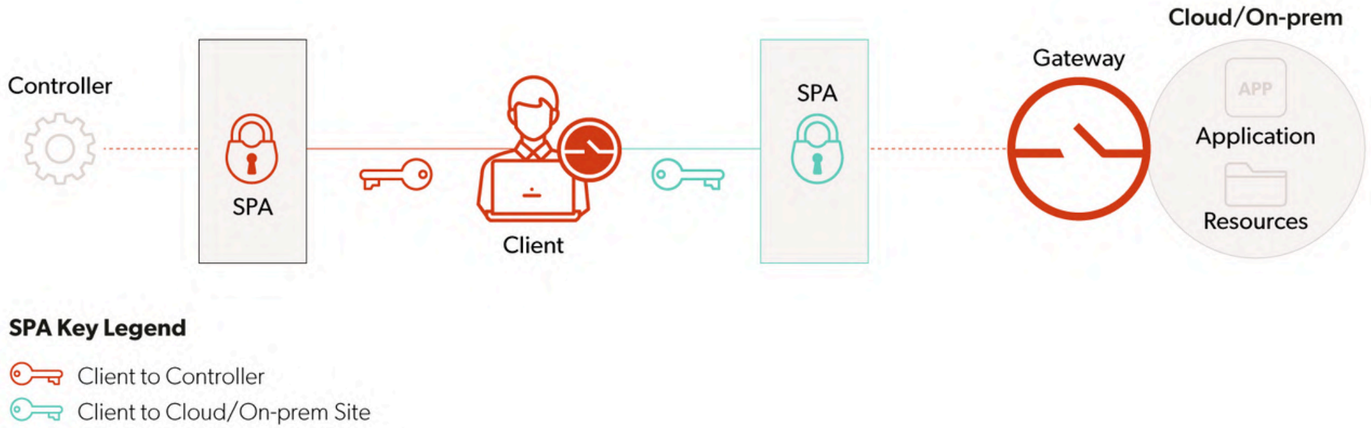
Các thành phần trong AppgateSDP giao tiếp nhau thông qua SPA, điều này giúp thông tin kết nối được bảo mật hoàn toàn, không thể giả mạo và chống tấn công DDoS

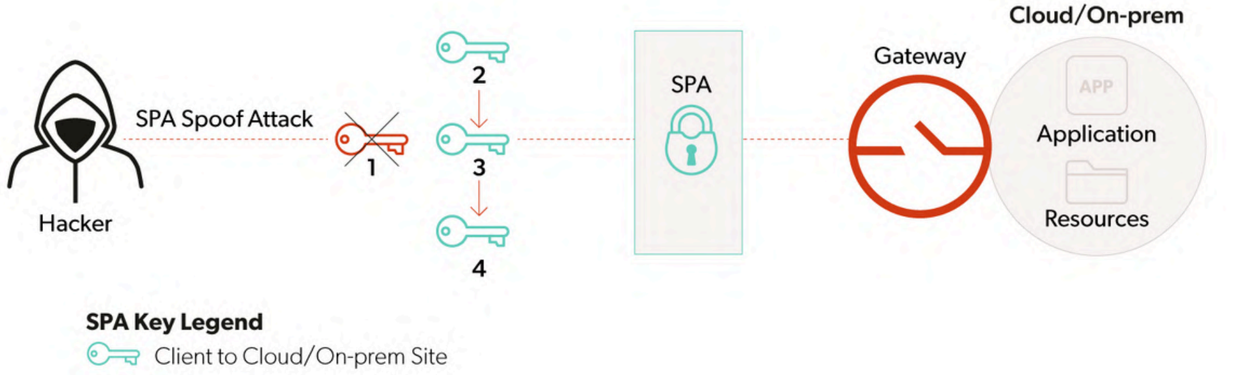


BẢO MẬT NÂNG CAO TRONG APPGATESDP
SPA (SINGLE PACKAGE AUTHORIZATION)

- **Phân phối khóa an toàn:** AppgateSDP sử dụng các khóa bảo mật riêng biệt cho từng giao tiếp. Điều này có nghĩa là mỗi lần bạn kết nối, sẽ có một khóa khác nhau được sử dụng để bảo vệ thông tin.

- **Bảo vệ chống giả mạo:** Appgate không sử dụng các khóa tĩnh cố định cho các yêu cầu ủy quyền. Nếu một kẻ xấu cố gắng giả mạo một gói thông tin, họ sẽ không thể làm điều đó vì khóa sẽ thay đổi liên tục, khiến cho gói giả mạo trở nên vô hiệu.

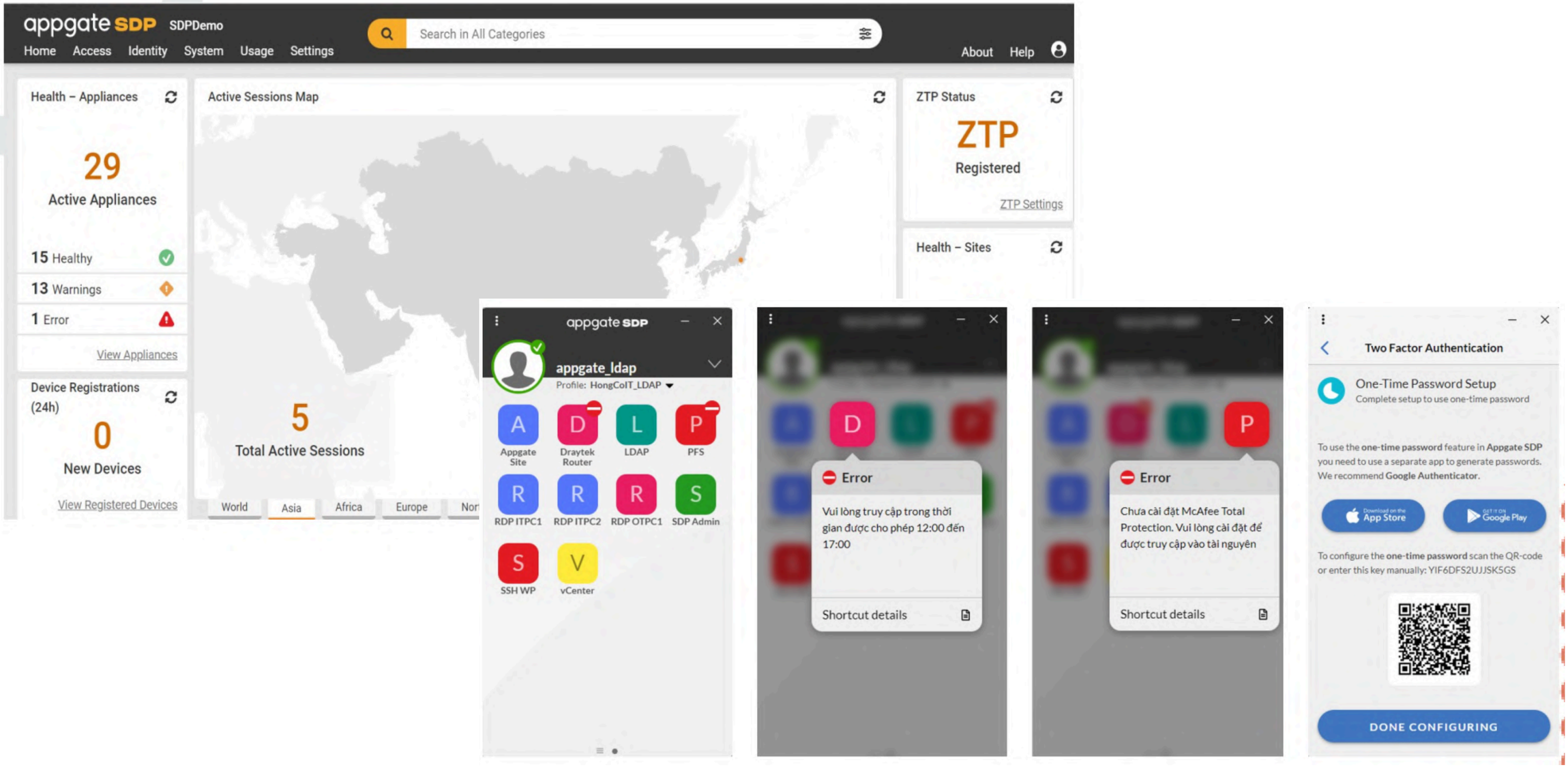




- **Bảo vệ khỏi sao chép:** Mỗi thông điệp SPA được tạo ra theo cách đặc biệt, giúp ngăn chặn kẻ xấu tái tạo hoặc phát lại gói thông tin để truy cập trái phép.

AppgateSDP sẽ tăng cường lớp xác minh quyền truy cập, bảo vệ người dùng, và giúp bảo vệ chống lại các cuộc tấn công DDoS.

GIAO DIỆN QUẢN TRỊ VÀ NGƯỜI DÙNG



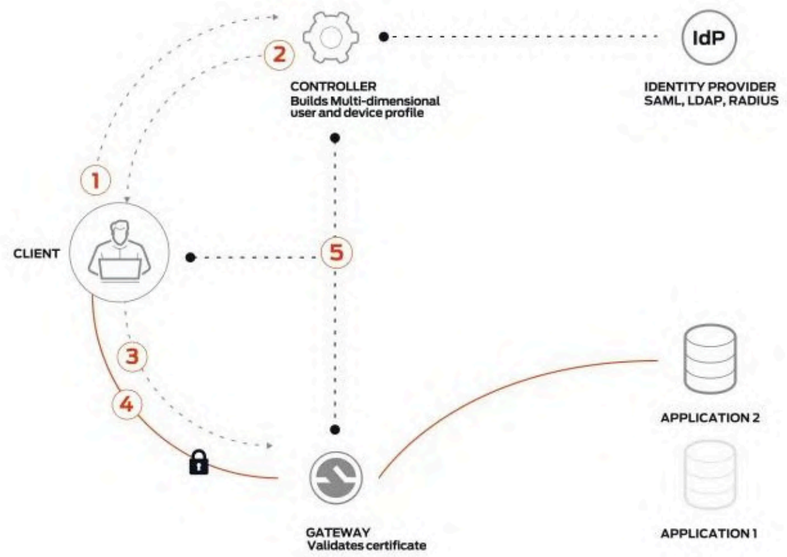
APPCONNECT CO., LTD

SO SÁNH
SDP ZTNA VỚI VPN

KIẾN TRÚC VÀ CÁCH THỨC HOẠT ĐỘNG

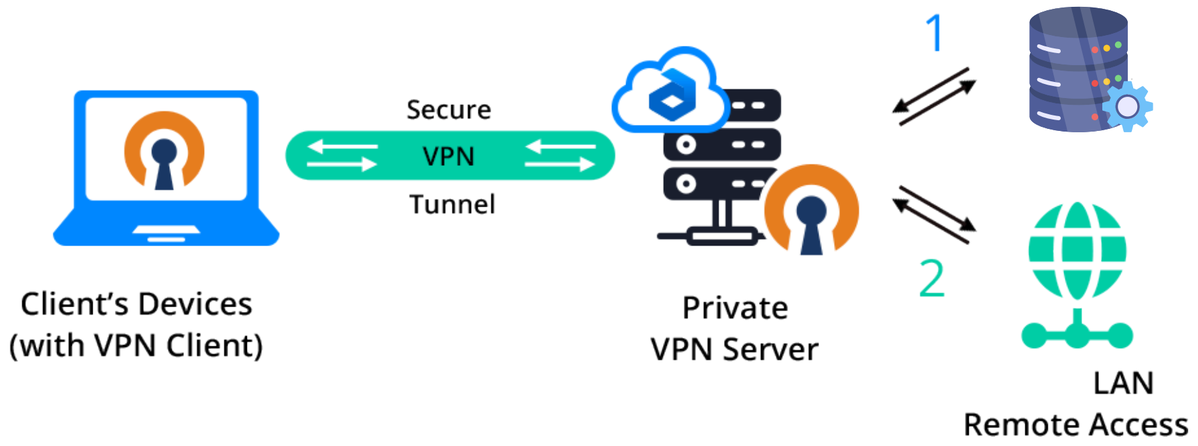
AppgateSDP:

- Dựa trên mô hình Zero Trust, không tin tưởng bất kỳ người dùng hay thiết bị nào mặc định.
- Chỉ những người dùng được xác thực và ủy quyền mới có thể truy cập vào tài nguyên.
- Tạo ra một viền bảo mật xung quanh các tài nguyên, chỉ mở ra cho các kết nối hợp lệ.
- Hiệu quả kiểm soát cả khi sử dụng bên trong hệ thống



OpenVPN:

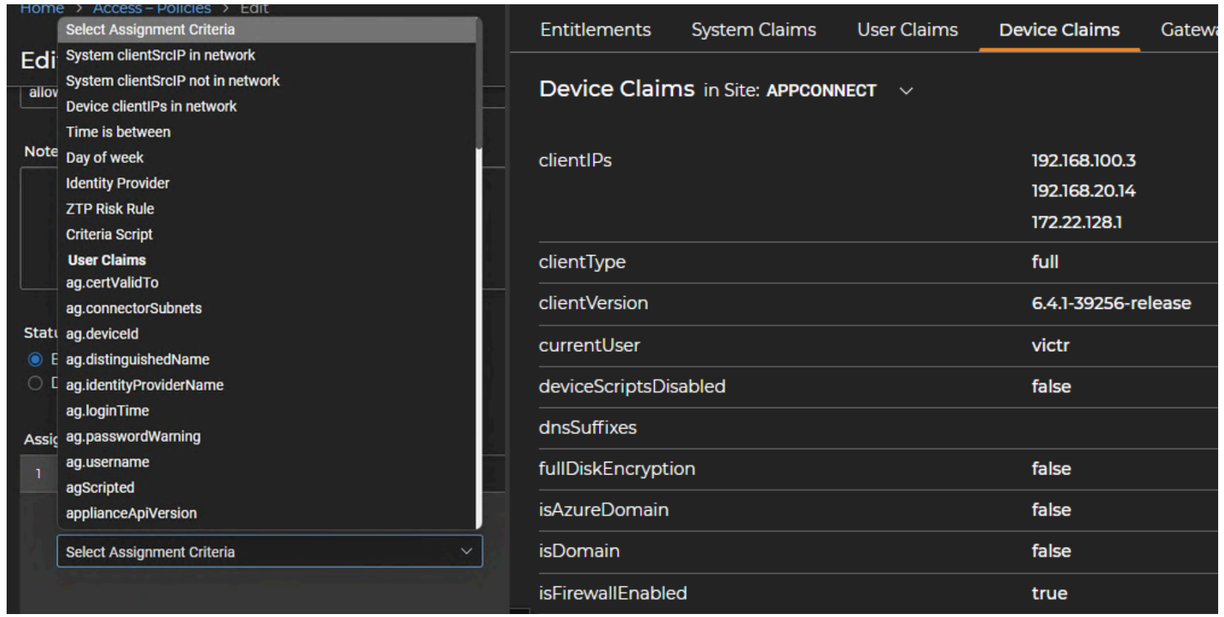
- Là một giải pháp VPN truyền thống, tạo ra một mạng riêng ảo (VPN) để kết nối người dùng từ xa với mạng nội bộ.
- Tin tưởng vào mạng và cung cấp quyền truy cập rộng hơn cho người dùng đã kết nối.
- Tất cả người dùng sau khi kết nối đều có thể có quyền truy cập vào toàn bộ mạng, điều này có thể tạo ra rủi ro nếu tài khoản bị xâm nhập.
- Chỉ để sử dụng tạo kết nối từ mạng bên ngoài vào hệ thống



QUẢN LÝ QUYỀN TRUY CẬP

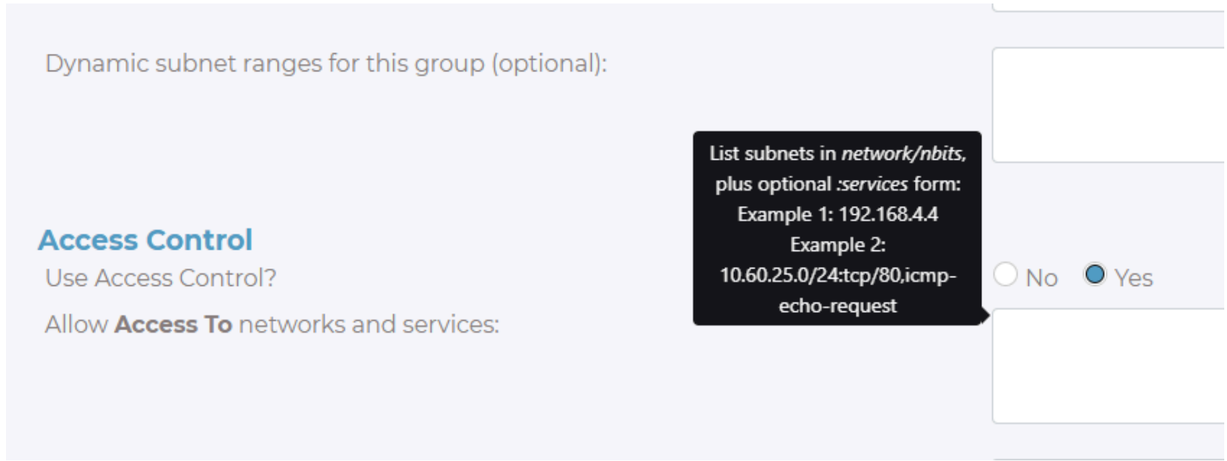
AppgateSDP:

- Quản lý quyền truy cập dựa trên ngữ cảnh (như vị trí, thiết bị, và trạng thái người dùng).
- Áp dụng nguyên tắc quyền truy cập tối thiểu, chỉ cho phép quyền truy cập cần thiết cho từng người dùng.
- Quyền truy cập được quản lý linh hoạt theo ngữ cảnh, dựa trên các yếu tố như thiết bị, vị trí, và trạng thái người dùng.
- Bảo mật đến lớp Ứng dụng, yêu cầu MFA/Mật khẩu khi kết nối



OpenVPN:

- Quyền truy cập thường dựa trên thông tin đăng nhập, không kiểm soát chi tiết theo ngữ cảnh.
- Một khi người dùng kết nối, họ có thể truy cập vào tất cả các tài nguyên trong mạng.
- Quyền truy cập thường cố định và không linh hoạt, có thể dẫn đến việc truy cập không cần thiết.
- Chỉ 1 lớp xác thực người dùng vào hệ thống, không có lớp bảo vệ truy cập ứng dụng



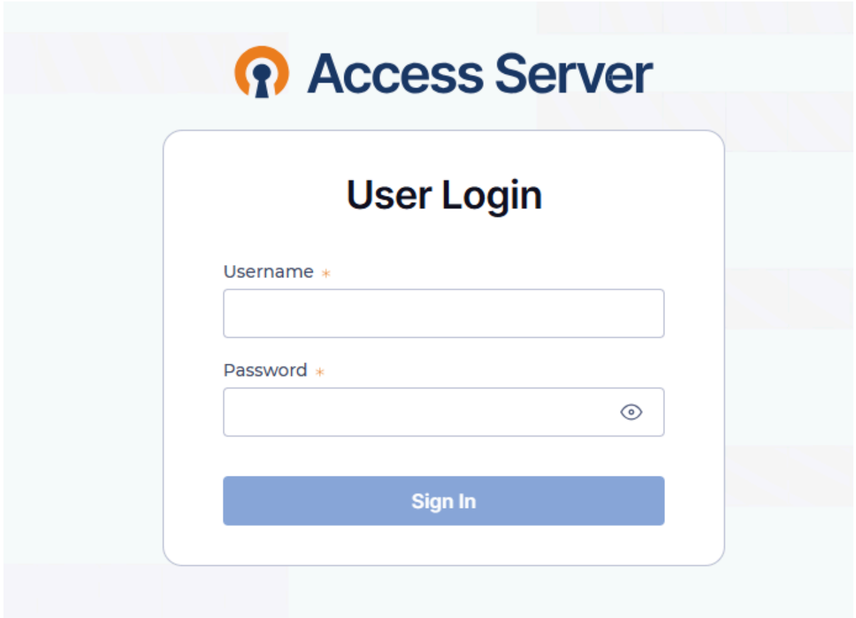
BẢO MẬT

AppgateSDP:

- Tích hợp nhiều lớp bảo mật, bao gồm xác thực đa yếu tố (MFA) và mã hóa mạnh mẽ.
- Giám sát và phân tích hành vi kết nối để phát hiện các mối đe dọa tiềm ẩn. Chấm dứt kết nối khi không thỏa chính sách truy cập được đặt ra
- Không có Web Client, Client được cung cấp Profile Link để tạo kết nối đến hệ thống
- Không lộ PORT kết nối ra ngoài, AppgateSDP sử dụng cơ chế xác thực UDP trước khi mở kết nối TCP
- Sử dụng SPA (Single Package Authorization) khóa bảo mật riêng biệt cho từng giao tiếp. Điều này có nghĩa là mỗi lần kết nối, sẽ có một khóa khác nhau được sử dụng để bảo vệ thông tin. Chống giả mạo thông tin từ Hacker và DDoS

OpenVPN:

- Cung cấp bảo mật thông qua mã hóa, nhưng phụ thuộc vào cấu hình và chính sách của người dùng.
- Thiếu khả năng giám sát và phân tích hành vi mạnh mẽ.
- Bắt buộc phải có Web Client để người dùng đang nhập vào và tải Profile Link, dễ bị tấn công Brute Force
- Lộ PORT kết nối ra bên ngoài, khả năng chống tấn công DDoS yếu



KIỂM SOÁT MÁY TÍNH BẰNG CLIENT

AppgateSDP:

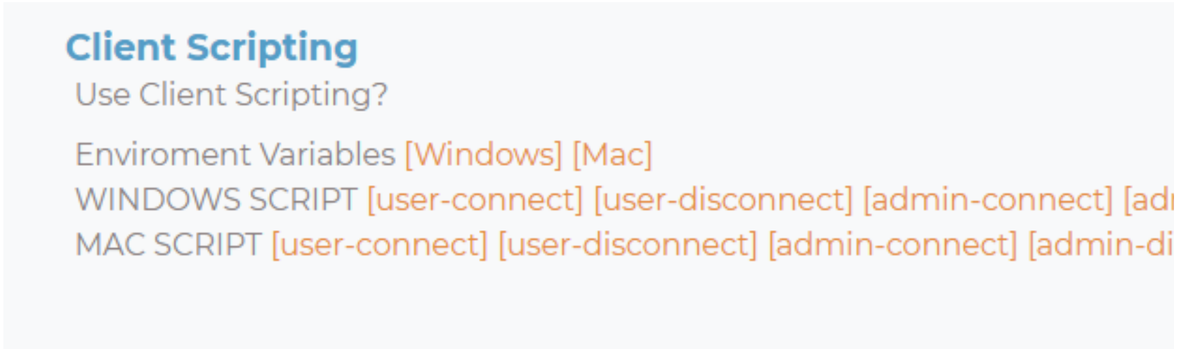
- Client AppgateSDP được cài đặt trên máy tính người dùng có tính năng kiểm soát toàn bộ kết nối IN/OUT của máy tính. Giảm thiểu nguy cơ tấn công mạng ngang hàng
- AppgateSDP có khả năng tích hợp script PS, BAT, EXE thực thi các chính sách thu thập, kiểm soát thông tin máy tính theo chính sách truy cập.
- Client có 3 chế độ cài đặt: FULL, ALWAY ON, HEADLESS đảm bảo service luôn được khởi chạy cùng hệ thống

OpenVPN:

- Client chỉ tạo kết nối đến hệ thống, không có khả năng kiểm soát máy tính.
- Không cách ly và kiểm soát máy tính khi máy tính có nguy cơ không an toàn
- Tích hợp script cơ bản nhưng phức tạp trong cấu hình từ server

Device Claim Scripts

Name ▲	Filename	Checksum (SHA256)
checkAntivirus	checkAntivirus.ps1	f6897b25250081cebf368fddd19d9124a6819f2615f2bb9fce8e603aa3db306a
checkAntivirusName	checkAntivirusName.ps1	dce2039ccla9093d9b06c9baa1e16623e72b783f7547f47d401cd2dcd257f3c4
checkLastScanWD	checkLastScanWD.ps1	ae5467e2c02166a22182d8def9138cd4180db5bfcc2cde8fe6f1b7d19592cc47
checkPhysicalLinuxDevice	checkPhysicalLinuxDevice.sh	45707a68e5cf1dc359ffa25a4903812a70087c2fbe1f3182adf731c215e14651
checkPhysicalWinDevice	checkPhysicalWinDevice.ps1	d3b15d5ee342b71cc6538dec25efc3e83ca507c7bf4c2e0aff40289cb874751f
checkPutty	checkPuTTY.ps1	a92fb139b636e55307ecfba32299248d9202e67809db53b8a40853746163ddbf
checkTeamviewer	checkTeamviewer.ps1	f667ca6869cc5421ec277016bf9d9a9986c938c76604d163daa0faf197999744
checkUSB	checkUSB.ps1	3875a9113259bc41fdca0b2ab4412d1135807f4a2c647b2e7b71577324a2e951
checkWin10-11	checkWinOS.ps1	f5985d531e560b0d51cb402cf296d7a10956513639eb133ed67719ec023f8039
checkWindowsUpdate	checkWinUpdate.ps1	4f83d4072d896c203c69acd4f764f83cd9005adffa8dc221ac1e42935ca2ae81
Crowdstrike - get risk data from macOS	crowdstrike_data_macos.sh	92f730250ab85d2e6adb486620657a3b64c9d481ce99e0cc7f4e11a321c52f27
Crowdstrike - get risk data from Windows	crowdstrike_data_win.bat	f78b500cf66992c6e6a863f5f4ac1a3546d2a7a900780101843b9f20bc6d031b
testEXE	check_client.exe	5f3fe69abe5ab2d45f83621f97be6544e726882ace427a28ccc43c35667d7464



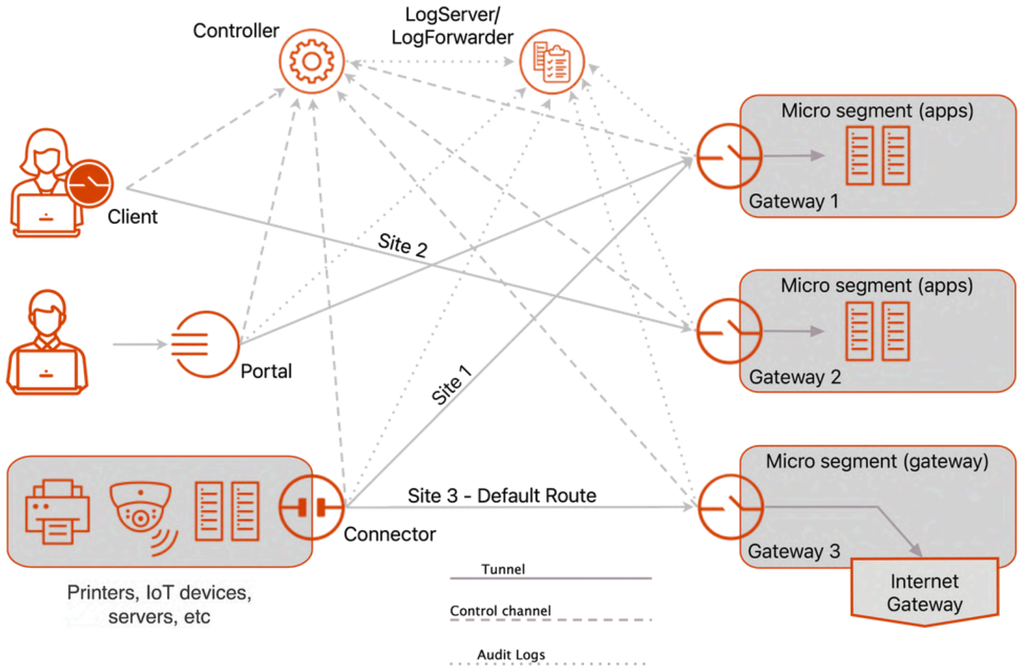
KHẢ NĂNG MỞ RỘNG

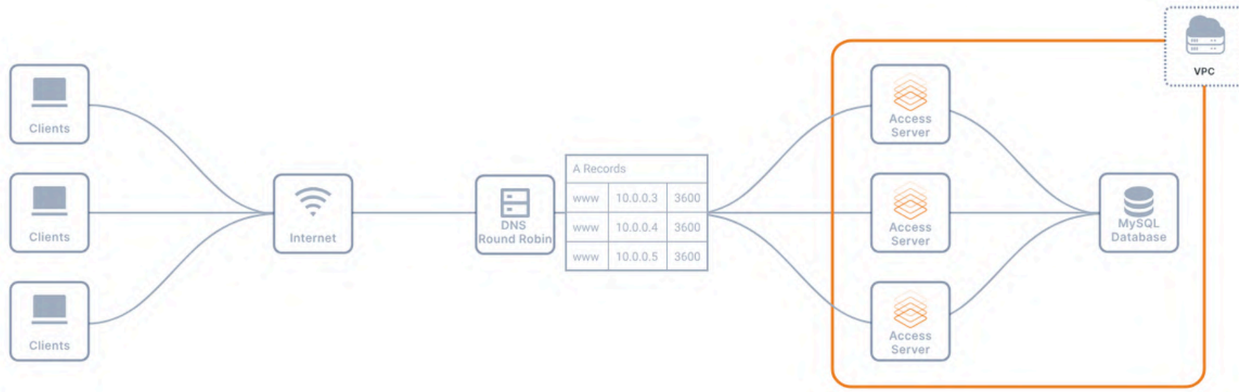
AppgateSDP:

- Dễ dàng mở rộng và tích hợp với các hệ thống bảo mật khác.
- Phù hợp cho các môi trường đa đám mây và các kiến trúc phức tạp.
- Khả năng xây dựng hê thống Dự phòng và Cân bằng tải tốt, chịu tải kết nối số lượng lớn

OpenVPN:

- Khó tích hợp với các hệ thống bảo mật khác trong hệ thống hiện có
- Cấu hình có thể phức tạp hơn khi mở rộng, đặc biệt trong môi trường lớn.
- Cần nhiều công sức để quản lý và duy trì khi số lượng người dùng tăng lên.





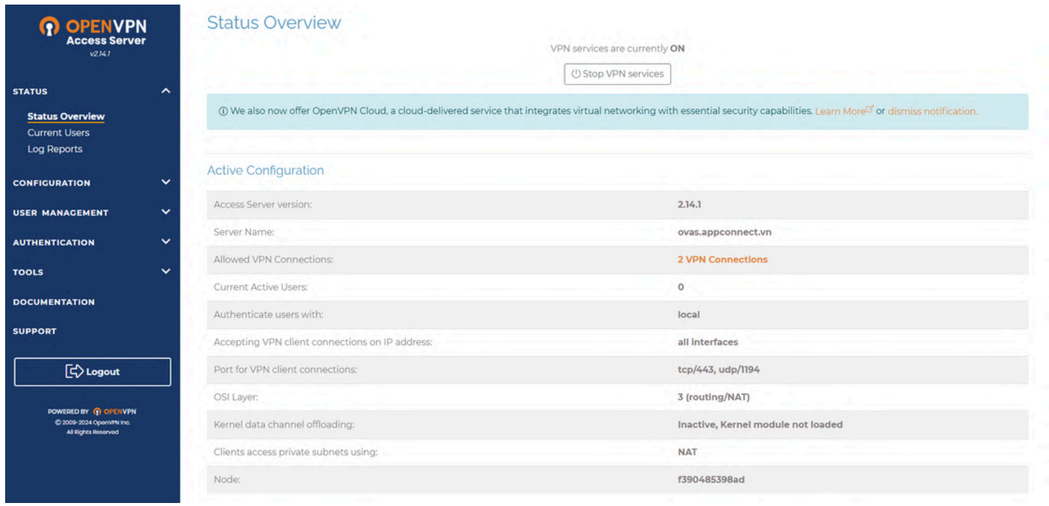
QUẢN LÝ TẬP TRUNG

AppgateSDP:

- Appgate SDP cung cấp giao diện quản lý tập trung cho phép người quản trị dễ dàng theo dõi và kiểm soát tất cả các kết nối và quyền truy cập từ một vị trí duy nhất.
- Hệ thống cho phép cấu hình và quản lý chính sách bảo mật trên toàn bộ hạ tầng mạng mà không cần phải quản lý từng thiết bị riêng lẻ.
- Appgate SDP có giao diện người dùng trực quan, dễ sử dụng, giúp người quản trị dễ dàng theo dõi và quản lý các kết nối và chính sách.
- Cung cấp Dashboard trực quan với các báo cáo và phân tích thời gian thực về hoạt động người dùng và tình trạng bảo mật.

OpenVPN:

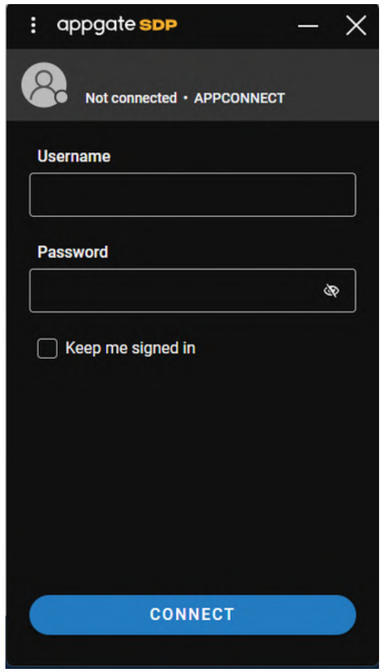
- OpenVPN thường yêu cầu quản lý từng máy chủ và người dùng/nhóm tài nguyên riêng lẻ, điều này có thể làm cho việc quản lý trở nên khó khăn và tốn thời gian, đặc biệt trong môi trường lớn.
- Việc cấu hình và cập nhật chính sách bảo mật không đồng bộ bên trong và bên ngoài hệ thống, làm giảm tính hiệu quả và nguy cơ mất ATTT.
- Giao diện quản trị của OpenVPN thường không trực quan bằng Appgate.
- Không cung cấp tính năng đầy đủ như Appgate.

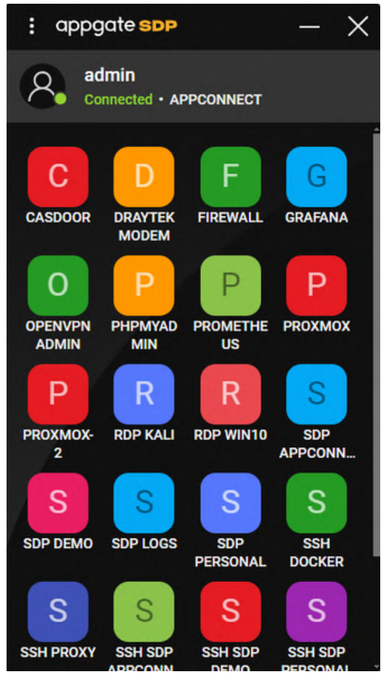


TRẢI NGHIỆM NGƯỜI DÙNG

AppgateSDP:

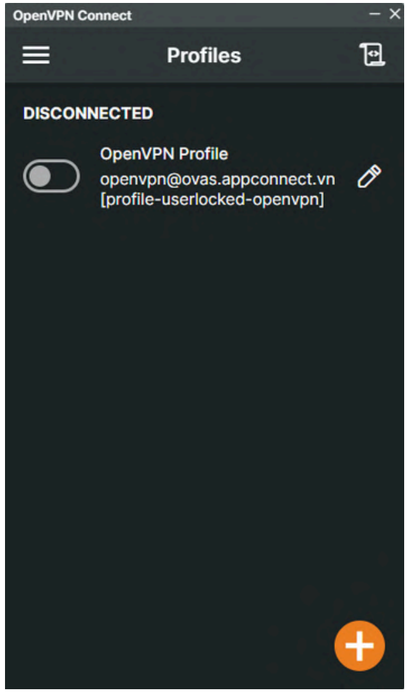
- Cung cấp trải nghiệm mượt mà hơn cho người dùng, với quy trình xác thực linh hoạt.
- Kết nối đến tất cả hê thống không phụ thuộc vào vị trí địa lý của tài nguyên
- Người dùng không cần phải kết nối với VPN truyền thống, mà chỉ cần xác thực một lần để truy cập vào ứng dụng.

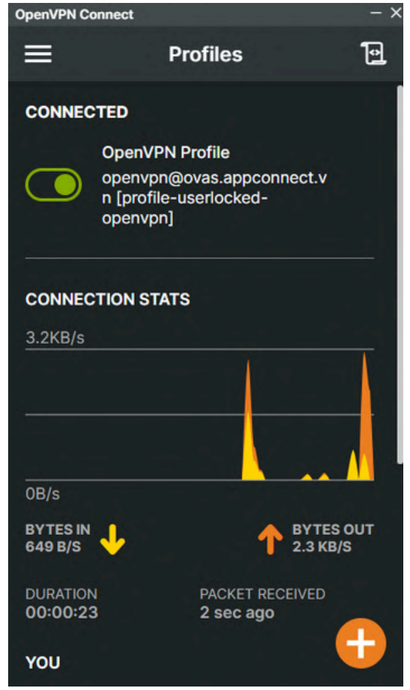




OpenVPN:

- Người dùng phải kết nối đến VPN trước khi truy cập vào tài nguyên nội bộ, có thể cần nhiều bước trong quá trình kết nối.
- Người dùng không thể kết nối đến nhiều hệ thống cùng lúc.
- Có thể gặp khó khăn trong việc cấu hình và sử dụng cho người dùng không quen thuộc.



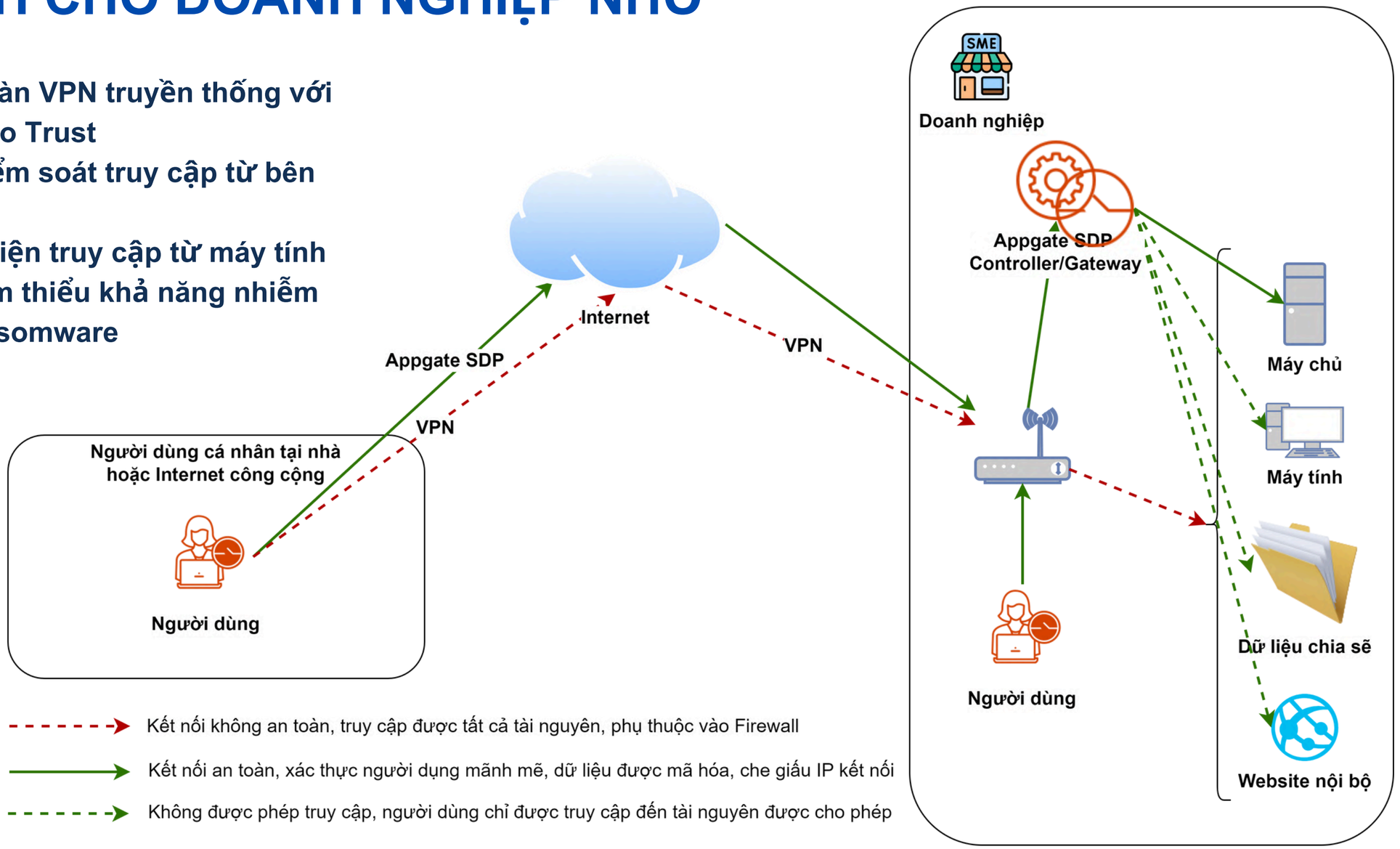


APPCONNECT CO., LTD

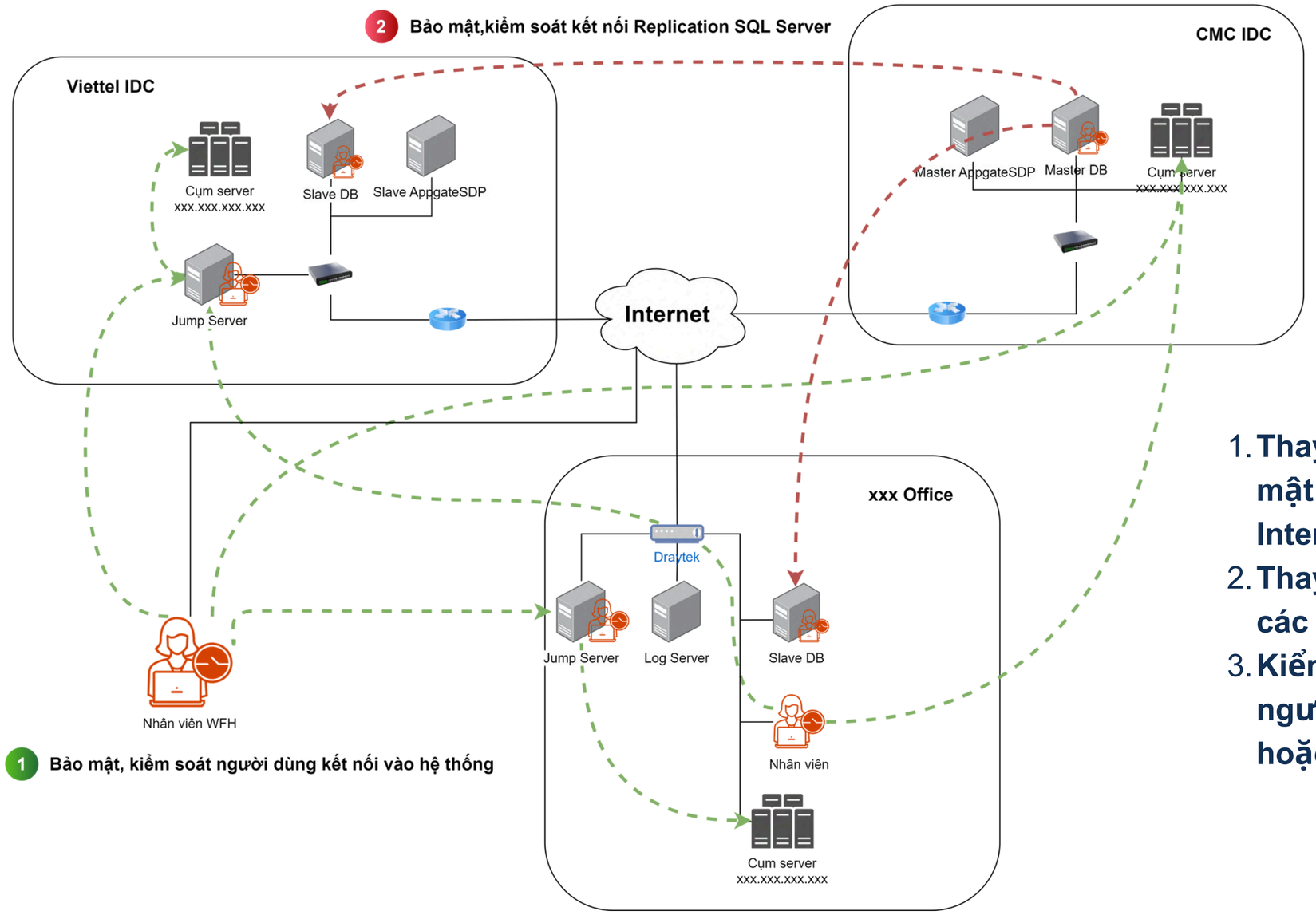
ÁP DỤNG VÀO DOANH NGHIỆP

DÀNH CHO DOANH NGHIỆP NHỎ

1. **Thay thế hoàn toàn VPN truyền thống với bảo mật SDP Zero Trust**
2. **Thay thế NAC kiểm soát truy cập từ bên trong hệ thống**
3. **Kiểm soát toàn diện truy cập từ máy tính người dùng, giảm thiểu khả năng nhiễm hoặc lây lan Ransomware**

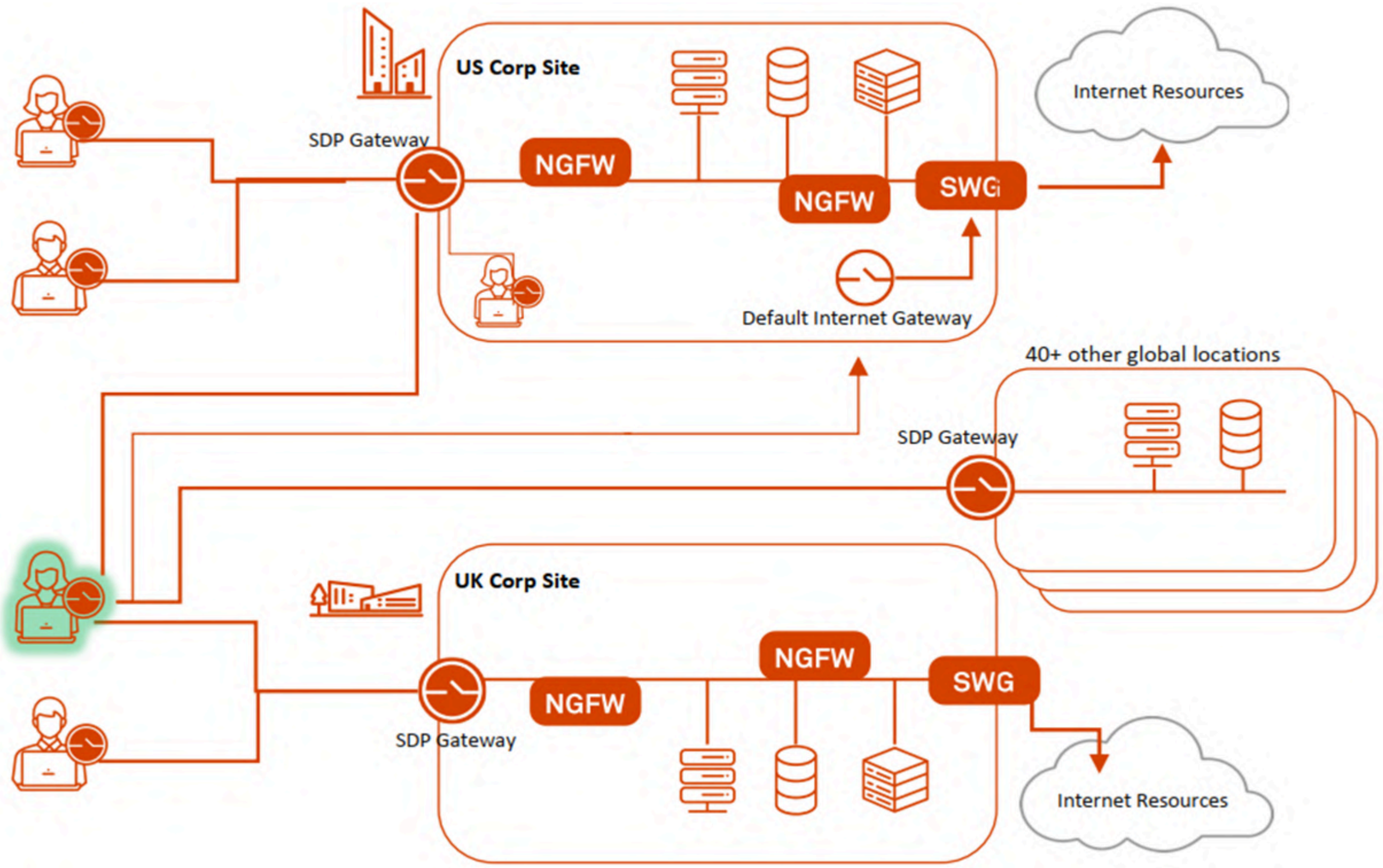


DÀNH CHO DOANH NGHIỆP DỊCH VỤ



1. **Thay thế hoàn toàn VPN truyền thống bảo mật SDP Zero Trust truy cập đến IDC từ Internet và từ Office**
2. **Thay thế VPN kết nối Replicate DB giữa các IDC và Office**
3. **Kiểm soát toàn diện truy cập từ máy tính người dùng, giảm thiểu khả năng nhiễm hoặc lây lan Ransomware**

DÀNH CHO DOANH NGHIỆP/TỔ CHỨC LỚN



- Kiểm soát và xác thực đa yếu tố mọi truy cập
- Chính sách truy cập được quản lý tập trung và thực thi theo ngữ cảnh
- Chặn các hành vi thăm dò và khai thác cổng dịch vụ
- Giảm thiểu chi phí đầu tư và vận hành tường lửa.
- Chính sách truy cập động và linh hoạt,
- Tối ưu quản lý, giám sát thiết bị cá nhân.
- Tích hợp sẵn với MFA.
- Giảm thiểu rủi ro tấn công ngang hàng và lây lan mã độc.

APPCONNECT CO., LTD

TÓM TẮT ƯU ĐIỂM
GIẢI PHÁP APPGATESDP

Tóm tắt ưu điểm vượt trội của AppgateSDP:

- **Bảo mật Zero Trust:** AppgateSDP áp dụng nguyên tắc Zero Trust, chỉ cho phép truy cập vào các ứng dụng và dữ liệu được ủy quyền, bất kể người dùng ở đâu hoặc đang sử dụng thiết bị nào.
- **Kiểm soát truy cập:** AppgateSDP cho phép kiểm soát truy cập chi tiết đến từng ứng dụng, chức năng và dữ liệu, đảm bảo chỉ những người dùng và thiết bị được ủy quyền mới có thể truy cập vào các tài nguyên.
- **Khả năng mở rộng cao:** AppgateSDP có khả năng mở rộng cao, dễ dàng triển khai và quản lý cho nhiều người dùng và ứng dụng.
- **Dễ dàng sử dụng:** AppgateSDP cung cấp giao diện người dùng trực quan và dễ sử dụng, giúp người dùng nhanh chóng truy cập vào các ứng dụng mà họ cần.
- **Quản lý tập trung:** Appgate SDP quản lý chính sách truy cập tập trung tại giao diện quản lý, giúp người dùng có thể đồng bộ 1 chính sách trên tất cả hệ thống mà không phụ thuộc vào Firewall.
- **Đảm bảo hiệu suất:** Appgate SDP có thể giúp tăng hiệu suất truy cập ứng dụng bằng cách giảm tải cho các hệ thống mạng và ứng dụng.
- **Tách biệt với hệ thống hiện có:** không phụ thuộc vào các thiết bị Firewall hiện có trong hệ thống, không ảnh hưởng đến kiến trúc của hệ thống mạng khi triển khai tích hợp Appgate SDP
- **Triển khai bảo mật, kiểm soát toàn diện:** Appgate SDP có thể kiểm soát truy cập bên ngoài (thay thế VPN), truy cập bên trong (NAC), K8s (Kubeneter) và Cloud trên cùng 1 hệ thống quản trị Appgate SDP. Triển khai cho mạng OT, IT, IoT
- **Xác thực đa yếu tố:** cung cấp xác thực MFA (Google/Microsoft Authenticator)/FIDO2 miễn phí khi truy cập vào tài nguyên
- **Giảm thiểu sự lây lan Ransomware, Virus trong mạng ngang hàng**

APPCONNECT CO., LTD

THÔNG TIN LIÊN HỆ

Chúng tôi sẵn sàng hợp tác với bạn. Hãy liên hệ với APPCONNECT qua thông tin liên lạc bên dưới để biết thêm thông tin về sản phẩm, dịch vụ hoặc cơ hội hợp tác với chúng tôi.

APPCONNECT CO., LTD

- Mr. Vũ - 0903 650 110
- Lầu 2, Dãy C, Công Viên Phần Mềm Mekong - TP. Mỹ Tho, Tiền Giang
- sale@appconnect.vn
- www.appconnect.vn - www.appgatesdp.vn

APPCONNECT CO., LTD

Thank you

Cảm ơn bạn đã tham dự buổi thuyết trình về công ty **APPCONNECT**. **APPCONECT** là một công ty tập trung vào việc cung cấp giải pháp kiểm soát, bảo mật kết nối mạng theo xu hướng bảo mật **ZERO TRUST** cho nhiều công ty thuộc các ngành khác nhau. Hi vọng trong bài thuyết trình này, bạn sẽ tìm hiểu thêm về **APPCONNECT** và giải pháp bảo mật **APPGATESDP**. Xin chân thành cảm ơn!