G/On

Soliton G/On là một giải pháp truy cập từ xa, thiết lập kết nối giữa thiết bị từ xa và hệ thống ứng dụng trong hệ thống mạng của một tổ chức. G/On sử dụng cổng bảo mật an toàn để tách thiết bị từ xa khỏi hệ thống mạng, qua đó bảo vệ đường truyền, song vẫn cung cấp đầy đủ các kết nối cần thiết. Máy chủ chứa ứng dụng nội bộ không cần phải kết nối tới mạng Internet mà vẫn **có thể cung cấp đầy đủ tất cả chức năng.**

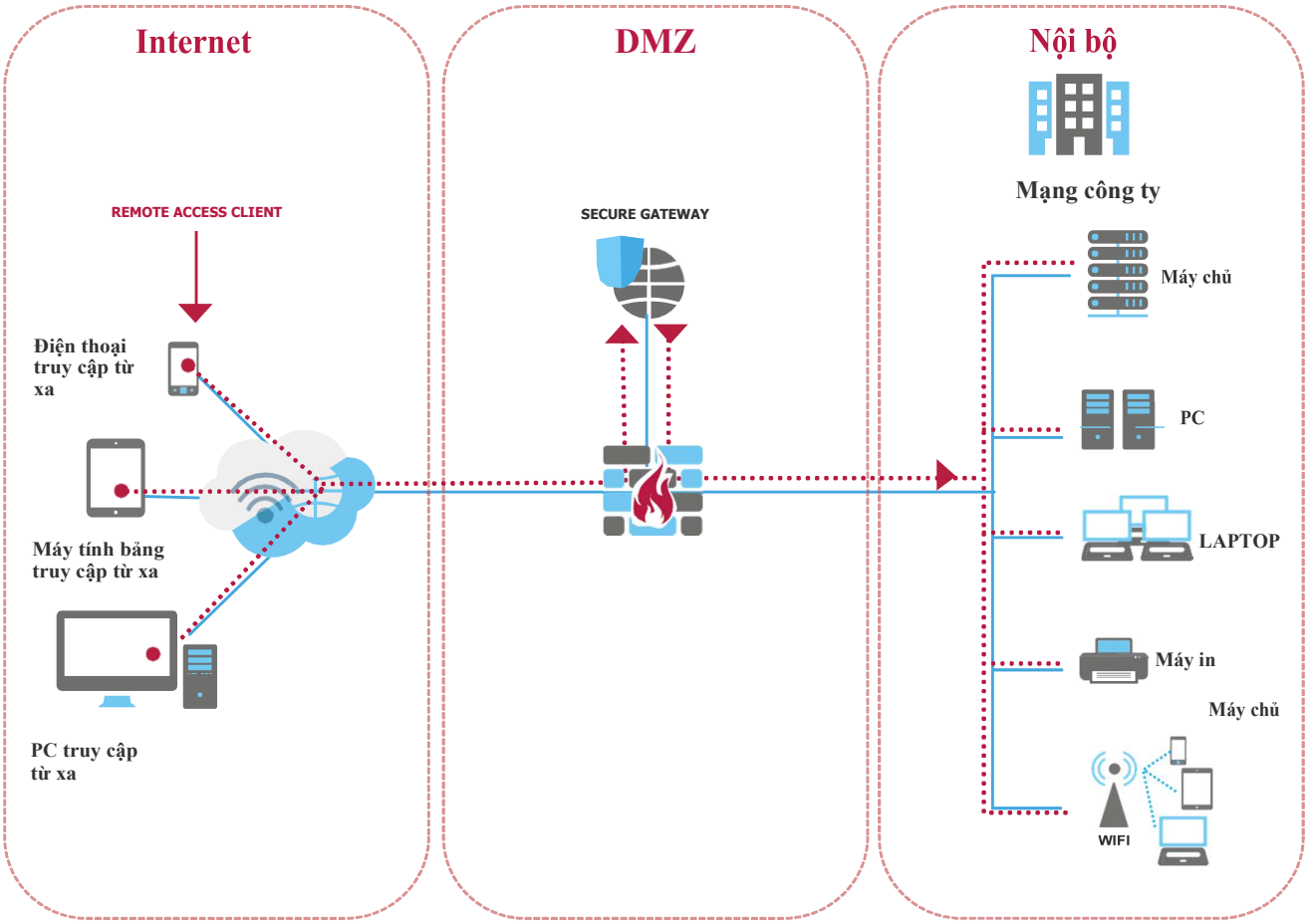
Ở phía client, người dùng sẽ sử dụng G/On Client chuyên dụng chỉ được sử dụng để kết nối với máy chủ cổng. Người dùng có quyền truy cập vào các ứng dụng dựa trên quy tắc cấp phép hoặc với tư cách thành viên nhóm Active Directory và không cần nhớ bất kỳ URL nào hoặc thông tin khác để truy cập các ứng dụng. G/On bao gồm các ứng dụng client cho RDP, Citrix, VNC, trình duyệt, truy cập tệp tin và nhiều ứng dụng khác.

Ở phía máy chủ, quản trị viên sẽ sử dụng bảng điều khiển trung tâm, chỉ bằng 1 cái nhìn, để quản lý toàn bộ môi trường G/On, gồm nhiều server cổng bảo mật.

G/On cung cấp dịch vụ xác thực 2 yếu tố lẫn nhau cho người dùng và thiết bị. Nếu được yêu cầu, nó có thể kết nối 1 người dùng đặc định với một thiết bị. Thực tế là **không có VPN nào được tạo ra** và **client không bao giờ là một phần của mạng công ty**, **không cần cấu hình địa chỉ TCP / IP trên client**. Người dùng có thể sử dụng các ứng dụng khác, như trình duyệt web, để truy cập tới các tài nguyên khác trên internet. Ngoài ra, người dùng có thể thiết lập vô số đường truyền G/On cùng lúc.

G/On khả dụng trên Windows, MacOS và Linux (có chọn lọc)

TIÊU CHÍ CHO GIẢI PHÁP TRUY CẬP TỪ XA



Mọi giải pháp bảo mật của Soliton đều được phát triển với tiêu chí:

- Xác thực hai chiều lẫn nhau giữa client và cổng kết nối, tạo nên một đường kết nối an toàn, bảo mật.
- Cổng kết nối bảo vệ mạng và máy chủ khỏi những cuộc tấn công mạng hay truy cập trái phép.
- Cổng kết nối cô lập client khỏi hệ thống mạng, do đó, thiết bị từ xa sẽ không tham gia trực tiếp vào mạng nội bộ.
- Cổng kết nối trao đổi dữ liệu với hệ thống mạng, cho phép truy cập vào tài nguyên nội bộ an toàn.
- Client truy cập từ xa có thể được cài đặt bởi người dùng đầu cuối, không cần quyền đặc biệt cho PC và Mac.
- Quyền truy cập của người dùng dựa trên các quy tắc cấp phép hoặc theo tư cách thành viên nhóm Active Directory; người dùng không cần ghi nhớ bất kỳ URL nào.

THÀNH PHẦN CỦA G/ON

Cổng kết nối an toàn- Secure Gateway: Ngăn không cho các máy chủ ứng dụng của công ty phải tiếp xúc với Internet.

- Dữ liệu trung chuyển giữa cổng và ứng dụng client từ xa luôn được mã hóa AES 256-bit , được chứng nhận FIPS 140.2.
- Cung cấp dịch vụ proxy và phân giải tên DNS trên mạng nội bộ để cung cấp đầy đủ chức năng cho các ứng dụng trên máy client.
- Cung cấp chức năng tự động cân bằng tải và dự phòng tự động , hoạt động với các sản phẩm cân bằng tải của bên thứ ba.
- Các cổng bổ sung được tạo dễ dàng trong vài giây bằng trình cài đặt Cổng.

G/On Client: Kết nối các ứng dụng trên máy khách với các tài nguyên bên trong mạng công ty mà không cần VPN. Sau khi xác thực hai yếu tố lẫn nhau, cổng máy chủ sẽ gửi một đối tượng menu tới máy khách có chứa cấu hình khởi động cho mỗi ứng dụng mà người dùng có thể sử dụng tại đó các thiết bị, vị trí và/ hoặc thời gian.

Các tính năng khác**:**

- Các ứng dụng không khả dụng sẽ không hiển thị và quyền truy cập được thực thi trong cổng, ngăn người dùng khởi động các ứng dụng không được phép hoặc nâng cấp quyền truy cập.
- G/On-client cũng cung cấp tính năng tự động khởi chạy các ứng dụng và đăng nhập một lần (SSO).
- Client có thể đóng gói tất cả lưu lượng truy cập trong HTTP và di chuyển qua các proxy mà vẫn giữ được tính bảo mật.
- Quản trị viên hoặc người dùng cuối có thể tạo ra ứng dụng Client G/On một cách dễ dàng nhờ Trình cài đặt ứng dụng G/On Client , và nó có sẵn cho Windows, MacOS và các bản phân phối Linux được hỗ trợ.

G/On USB Token:

Một mã thông báo(Token) dạng USB nhỏ với thẻ thông minh di động được tích hợp trong thẻ MicroSD. Người dùng cuối nhận được ứng dụng G/On với đầy đủ chức năng đã được đăng ký trước, hoặc chỉ cần trải qua một quy trình đăng ký đơn giản để kích hoạt ứng dụng G/On. Trong quá trình đăng ký, thẻ thông minh tạo ra một cặp khóa riêng tư/ công khai. Khóa công khai được sử dụng để xác thực thẻ thông minh, khóa cá nhân được bảo vệ bởi thẻ thông minh và không bao giờ có thể rời khỏi nó. Do đó, G/On USB-token có thể được nhận dạng duy nhất dựa trên cặp khóa riêng tư/ công khai của thẻ thông minh trong thời gian xác thực.

G/On Desktop Client:

Khởi chạy từ máy tính thay vì từ G/On USB Token, và sử dụng máy tính làm yếu tố xác thực thứ hai thay vì dùng thẻ thông minh USB. Ứng dụng này chỉ hỗ trợ cho Windows.

G/ON HỖ TRỢ MỘT SỐ TÍNH NĂNG CHÍNH NHƯ:

- **Không cần sử dụng VPN**: G/On tạo ra một đường truy cập tới ứng dụng nội bộ và sử dụng máy chủ DNS nội bộ. Secure Gateway ngăn cách máy tính truy cập từ xa với mạng nội bộ. Người dùng vẫn có thể sử dụng ứng dụng cá nhân trên máy tính của mình.

- **Lịch sử sử dụng:** SecureGateway ghi lại tất cả các nỗ lực truy cập bao gồm thông tin chi tiết về người dùng nào, khi nào và những tài nguyên nào được người dùng đó truy cập.

- **Bảng điều khiển quản lý trung tâm:** Cung cấp toàn quyền kiểm soát việc cài đặt, người dùng và cách sử dụng. Quản trị viên CNTT có thể kiểm soát quyền truy cập vào các ứng dụng khác, ngăn sao chép / dán / tải xuống tệp tin hoặc cho phép tải tệp tin xuống trong môi trường an toàn chuyên dụng.

- **Các proxy tích hợp cho Citrix và RDP:** G/On giao tiếp trực tiếp với các dịch vụ broker trên cả Citrix và RDP, vì vậy không cần bất kỳ thành phần front-end nào, chẳng hạn như NetScaler và RD Gateway. G/On-client cũng có thể bao gồm Citrix-và RDP-Client, trong trường hợp đó không cần phải cài đặt chúng trên máy tính từ xa.

- **Thân thiện với người dùng:** Không có thủ tục khởi động và đăng nhập phức tạp. Chỉ cần cắm G/On USB Token vào máy tính, khởi chạy Ứng dụng Client G/On trong USB, đăng nhập bằng thông tin đăng nhập AD và chọn các ứng dụng cần thiết. Đăng nhập một lần(Single-sign-on) đã được bao gồm và các ứng dụng hay được sử dụng nhất có thể tự động khởi động sau khi xác thực.

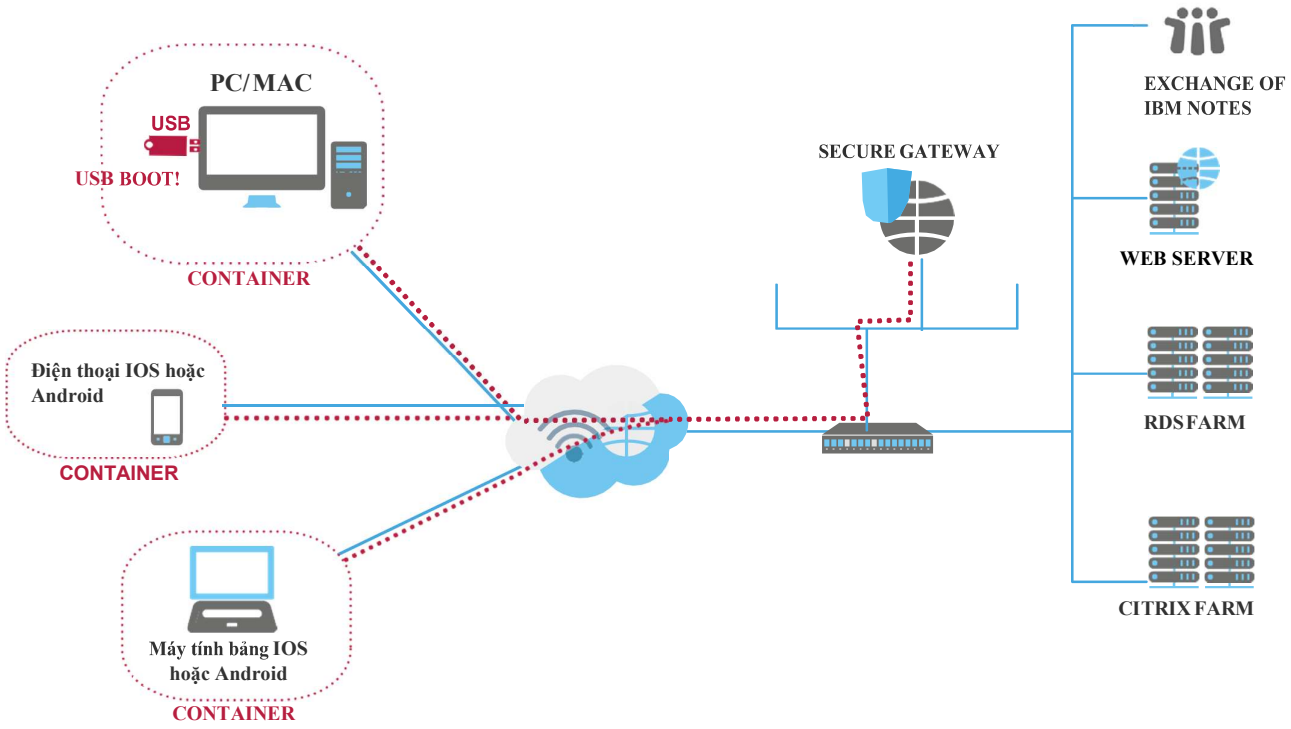
- **Không cần quản lý thiết bị:** G/On tách các ứng dụng nội bộ của công ty khỏi các ứng dụng cục bộ trên máy tính của người dùng cuối. Kết nối được bảo mật và máy tính của người dùng cuối không bao giờ được cấp bất kỳ quyền truy cập nào vào mạng nội bộ, vì tất cả các kết nối đều được ủy quyền thông qua SecureGateway.

Tùy chọn G/ON OS

G/On OS là một vùng chứa an toàn được thêm vào G/On để khóa toàn bộ ở phía máy khách. Các tính năng khác bao gồm:

- G/On OS là 1 hình ảnh Fedora Linux được thu nhỏ, được cài cứng (hardened), được khởi động trực tiếp vào bộ nhớ từ G/On USB Token. G/On OS không bao gồm driver để truy cập vào ổ cứng, vì vậy không có cách nào để lưu lại dữ liệu hoặc truyền dữ liệu ra từ máy tính được sử dụng.
- G/On OS có đầy đủ các tính năng với các ứng dụng client cho Citrix, RDP, VNC, trình duyệt và hơn thế nữa..
- G/On OS bị khóa để chỉ cho phép truy cập vào SecureGateway mà nó đã được đăng ký ban đầu.

CƠ SỞ HẠ TẦNG G/ON



THÔNG SỐ

SECUREGATEWAY

Nền tảng	Windows
Hệ điều hành	Windows Server 2008, 2008 R2, 2012, 2012 R2* và 2016
Số lượng người dùng	Lên đến ~ 2,000 người cho mỗi cổng (gateway)
Máy chủ xác thực được hỗ trợ	Active Directory, LDAP và tài khoản cục bộ
Nơi lưu log	File cục bộ

**Yêu cầu G/On Server từ 5.7 trở lên*

DATABASE (tùy chọn)

Nền tảng	Windows
Phiên bản hệ điều hành	Microsoft SQL server 2008, 2012, 2014, 2016 và 2017 (phiên bản 2012 trở về sau sẽ cần G/On server từ 5.7 trở lên)

G/ON CLIENT

Nền tảng	Windows, Mac OS và Linux
Phiên bản hệ điều hành	**Windows** 7, 8, 8.1 và 10 **Apple Mac OS** X 10.6 (Snow Leopard) tới OS X 10.13 (High Sierra) **Linux** Fedora 21 tới 27 với GTK+ GUI (64 bit)

G/ON TOKEN

Nền tảng	USB và Windows
Loại token	**G/On USB Token** với thẻ thông minh để chứng thực hai tầng **SoftToken** hoặc các loại USB từ 2 GB trở lên **Computer User Token** được cài trên nền tảng Windows

Về SOLITON

Soliton Systems có mục tiêu phát triển giải pháp nhằm đáp ứng nhu cầu của khách hàng một cách tiện lợi. Soliton hỗ trợ các công ty phát triển hệ thống quản lý bảo mật, bao gồm bảo mật mạng và truy cập từ xa vào mạng nội bộ hay ứng dụng đám mây. Các giải pháp của Soliton sẽ bảo vệ tài nguyên công ty khỏi những truy cập trái phép hay rò rỉ dữ liệu ngoài ý muốn.

Soliton®

EMEA office

Soliton Systems Europe N.V.

Jachthavenweg 109-A, 1081 KM Amsterdam, The Netherlands

+31 (0)20 280 6060 | emea@solitonsystems.com | www.solitonsystems.com

Đại lý ủy quyền duy nhất tại Việt Nam

Luvina Software JSC.

4F, tháp Hòa bình, 106 Hoàng Quốc Việt, Quận Cầu Giấy, Hà nội, Việt Nam

Tel: 024-3793 1103| support-gon@luvina.net | www.luvina.net

SOL200107