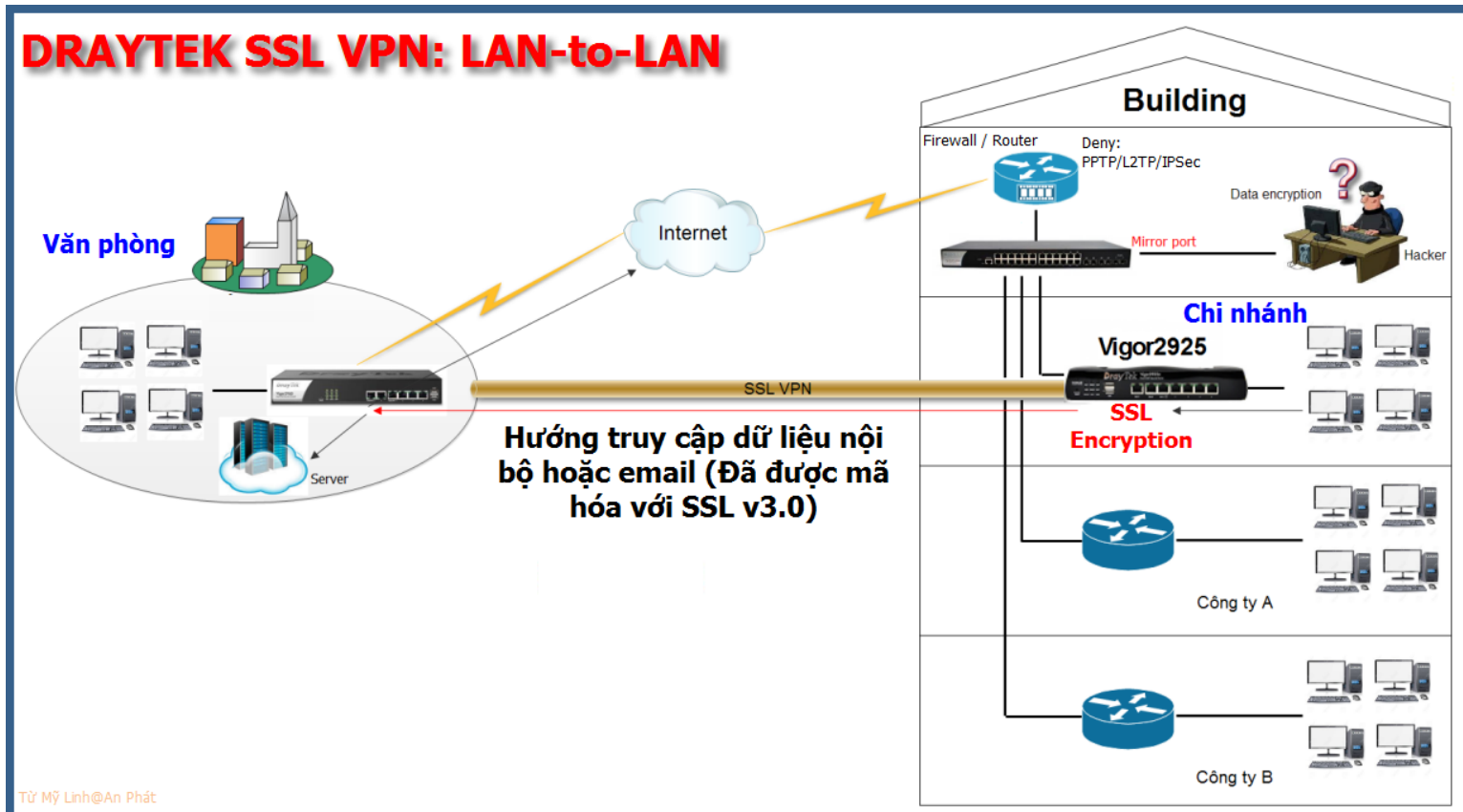


GIẢI PHÁP BẢO MẬT DỮ LIỆU VỚI SSL VPN LAN-to-LAN

DRAYTEK SSL VPN: LAN-to-LAN



Từ Mỹ Linh@An Phát

Hiện nay các Doanh nghiệp không ngừng mở rộng sản xuất kinh doanh vì thế việc kết nối dữ liệu từ xa liên tục và an toàn là một yêu cầu cấp thiết. Tuy nhiên không phải Doanh nghiệp nào cũng có thể chi trả chi phí thuê kênh riêng cho các kết nối nội bộ giữa Văn phòng và chi nhánh. **Để tiết kiệm chi phí thì VPN là giải pháp luôn được các Doanh nghiệp lựa chọn.** Ngoài việc tiết kiệm chi phí **VPN còn giúp cho Doanh nghiệp bảo mật dữ liệu quan trọng của mình bằng cách mã hóa dữ liệu** với giao thức IPSEC (Internet protocol security) và hiện nay là **SSL (Secure socket layer)**

Với Doanh nghiệp có văn phòng đặt tại các Tòa nhà và một số **Tòa nhà không cho phép kéo đường internet cáp quang riêng mà phải sử dụng chung hạ tầng mạng sẵn có tại Tòa nhà** (Tòa nhà thuê Internet từ ISP và cung cấp lại cho các công ty trong tòa nhà). Đây là trở ngại rất lớn và tiềm ẩn nguy cơ mất cắp dữ liệu:

- **Khi bạn sử dụng chung hạ tầng mạng** của Tòa nhà nghĩa là toàn bộ dữ liệu của bạn sẽ đi qua Swich, Router, Firewall của Tòa nhà trước khi tới nơi cần đến (Web Server, Mail

Server, ERP Server,..). **Như vậy hacker sẽ dễ dàng lấy được thông tin của bạn** chỉ với một port mirror trên Switch

- Khi **Router của Công ty nằm sau NAT device** của Tòa nhà (Firewall, Modem,...) sẽ rất **khó khăn khi thực hiện VPN với giao thức IPSEC** truyền thống và hoàn toàn phụ thuộc vào năng lực Pass-through VPN trên thiết bị của Tòa nhà

Thấy được những nhu cầu này của khách hàng, DrayTek đã nghiên cứu và đưa ra thị trường sản phẩm có **hỗ trợ chức năng SSL VPN LAN-to-LAN**. Để thực hiện kết nối SSL VPN LAN-to-LAN chúng ta **chỉ cần duy nhất một port TCP/443** và đây là port rất thông dụng được cho phép trong mọi trường hợp. Khi thiết lập VPN SSL Doanh nghiệp cũng sẽ an tâm hơn về vấn đề bảo mật dữ liệu.

Ưu điểm của SSL VPN

- Dễ dàng vượt tường lửa: Do sử dụng duy nhất 1 port TCP/443 để tạo VPN Tunnel. TCP/443 là port thông dụng luôn được các tường lửa cho phép đi qua.
- Không phụ thuộc vào khả năng PassThrough VPN của NAT Device (Trường hợp nằm sau NAT Device)
- Thích hợp khi tạo VPN LAN-to-LAN giữa 3G và ADSL/FTTH (3G là mạng đứng sau 1 NAT device của ISP nên nếu sử dụng PPTP hay IPsec sẽ gặp phải khó khăn)
- Bảo mật cao do sử dụng chuẩn SSL 3.0
- Băng thông VPN cao (Tùy model dao động từ 50 ~ 500Mbps)
- Hỗ trợ cả Host-to-LAN và LAN-to-LAN

Khuyết điểm duy nhất là SSL VPN LAN-to-LAN chỉ hỗ trợ **DrayTek -to-DrayTek**

Các model hiện tại đã hỗ trợ SSL VPN:

Vigor2860 (Firmware 3.8.1RC6)

Vigor2925 (Firmware 3.8.2RC3)

Vigor2960 (Firmware 1.1.0.1)

Vigor3900 (Firmware 1.1.0)

Hướng dẫn chi tiết tại: <http://www.anphat.vn/documentdetails.aspx?id=257>

Hoặc email về: hotro@anphat.vn

Điện thoại: 08-3925 3789