

GIẢI PHÁP ỨNG DỤNG

No.: 02-RA-A-V-B-101016-02

Chủ đề: Industrial Ethernet Bridge and Firewall (WALL IE_Helmholz)



I. Các tính năng của WALL IE

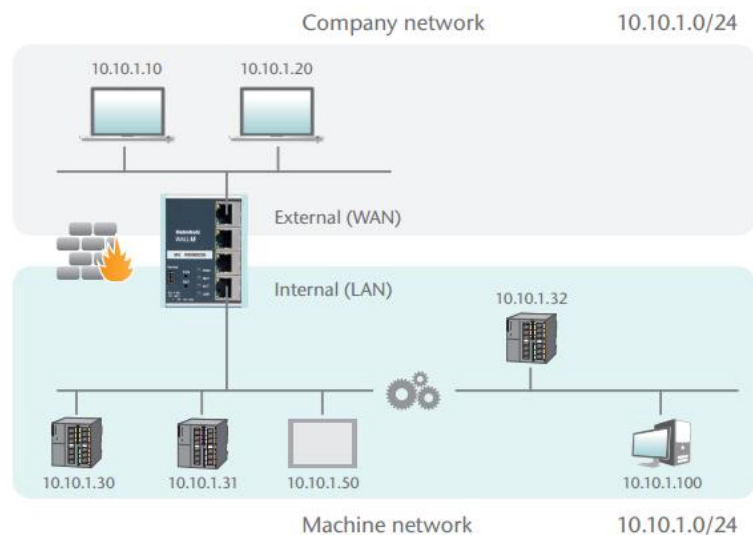
WALL IE là một *bridge and Firewall* (tường lửa) trong mạng công nghiệp. Thiết bị này được sử dụng để tích hợp các thiết bị điện tử động từ các lớp mạng khác nhau hoặc trong cùng một lớp mạng nhưng có thể giới hạn được khả năng truy cập vào thiết bị bên dưới thông qua “rule-điều kiện cho phép” được thiết lập trên Wallie, giúp tạo nên một mạng sản xuất tối ưu nhất.

Chức năng chính là *Bridge* và *NAT*

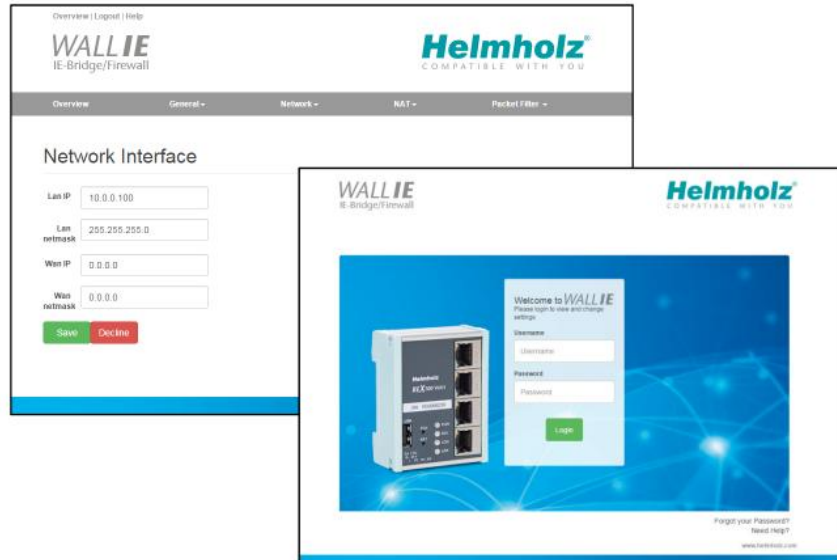
+ *Bridge*: Trong một lớp mạng chúng ta tạo một cầu phân cách, các thiết bị truy xuất lẫn nhau thông qua Port giao tiếp. Điều này giống như chúng ta muốn vào nhà của một ai đó thì cần người đó mở cửa cho phép ta vào.

- Chức năng Bridge mode

Với chức năng này Wallie cho phép lọc các gói tin từ nơi gửi đến nơi nhận (các thiết bị, máy móc bên dưới) theo điều kiện quy định đặt trước trong Wallie, khi đó mạng chúng ta như được cách ly thành 2 vùng riêng mà không cần sử dụng địa chỉ IP khác nhau.

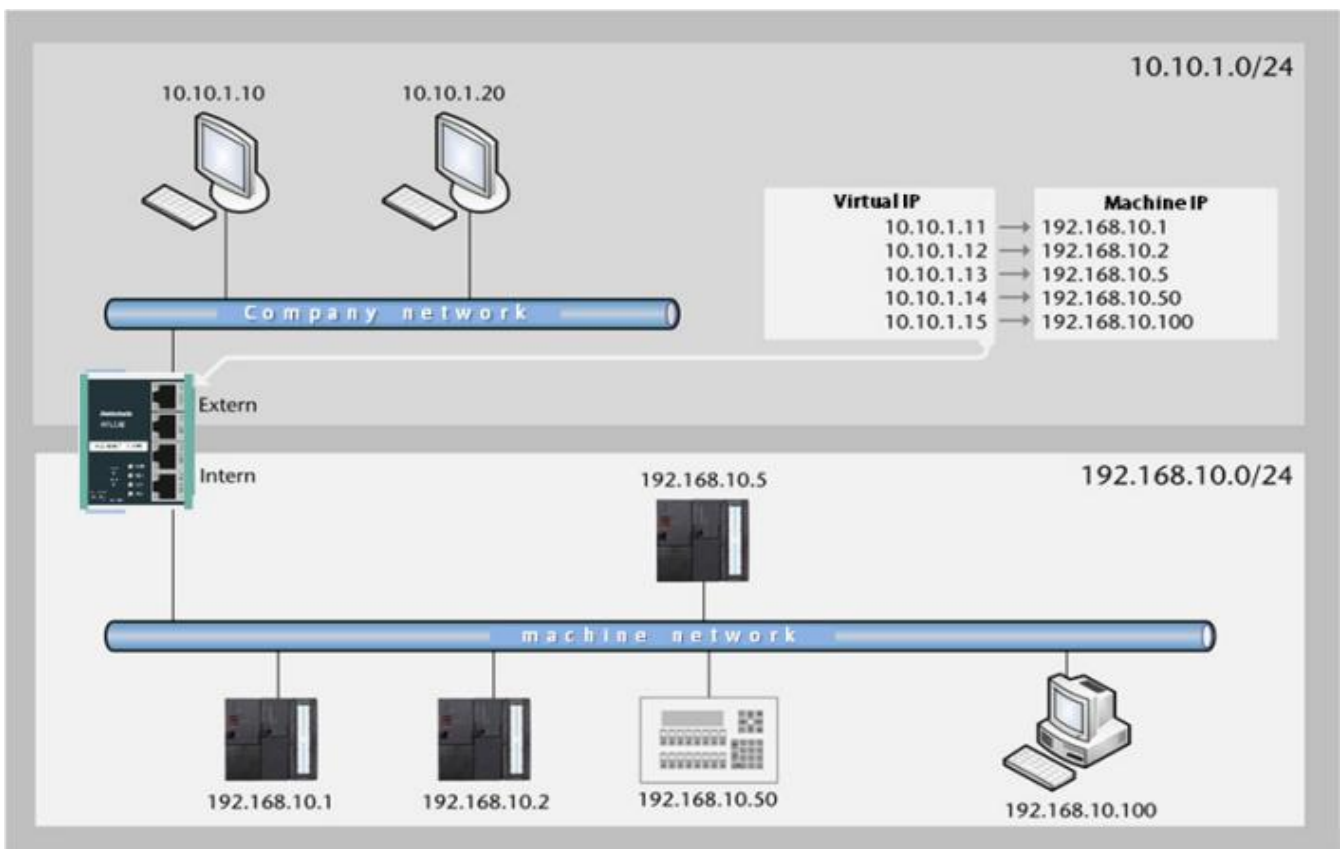


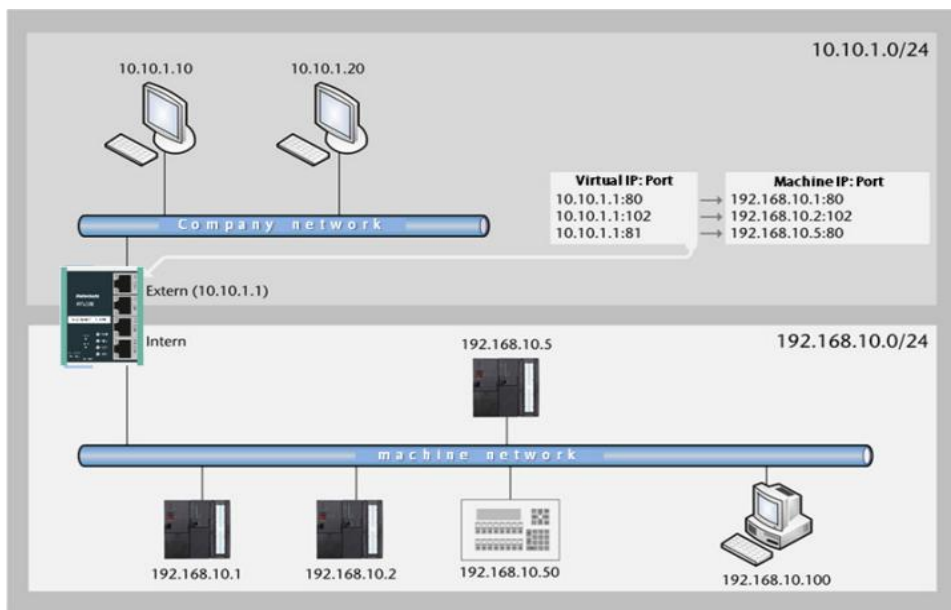
+ NAT: Trong một mạng, mỗi thiết bị có một địa chỉ IP riêng, khi đưa gói tin ra ngoài thông qua Wallie và sử dụng chức năng NAT thì địa chỉ IP đó sẽ được chuyển đổi sang địa chỉ IP khác để giao tiếp với các thành phần bên ngoài. Nếu bên ngoài gửi lại gói tin thì sẽ gửi đến địa chỉ bên ngoài đó và Wallie có nhiệm vụ đưa gói tin đến đúng địa chỉ máy bên trong.



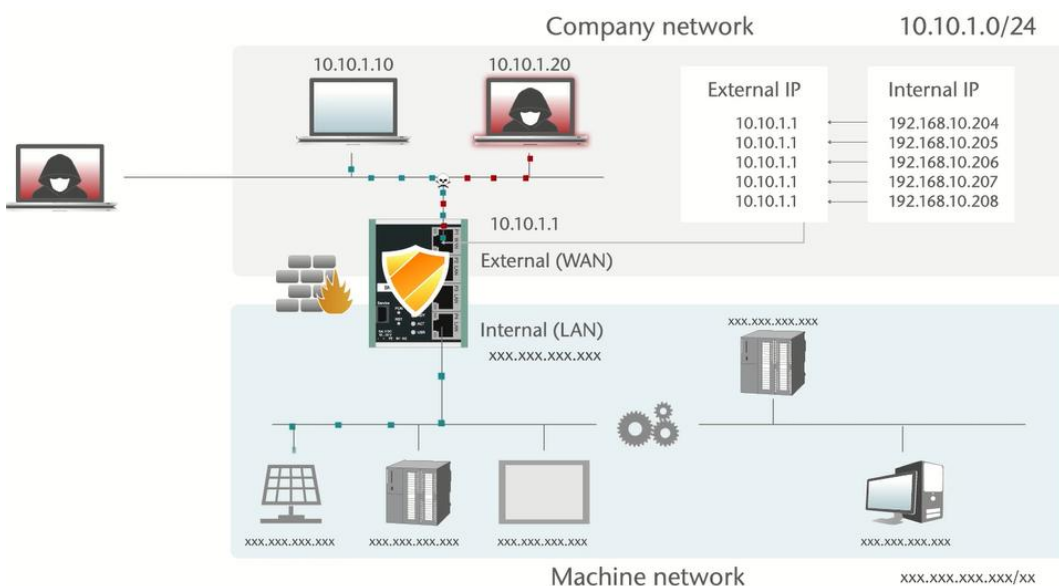
- Chức năng NAT

Nờ có tính năng NAT (bao gồm 1:1 NAT hay gọi Basic NAT, và NAT port) mà Wallie cho phép các thiết bị ở các lớp mạng khác nhau có thể liên lạc được với nhau thông qua cơ chế chuyển đổi IP, Port.





- Với tính năng lọc (filter) các gói data như trên thì tin tặc có tấn công vào cũng không thể thâm nhập được đến thiết bị. (các gói tin sẽ bị chặn bởi các "rules" hoặc nếu qua NAT thì tin tặc không biết được địa chỉ IP private của các thiết bị)



- **Chức năng lọc với MAC address:** Mỗi thành phần tham gia mạng có địa chỉ MAC duy nhất nên muốn hạn chế không cho truyền thông với thiết bị khác thì chúng ta có thể tạo một list sách các thiết bị được phép truyền thông nhau hoặc hoặc không được phép.

MAC Filtering:

Default MAC Policy: Whitelist Blacklist

| # | MAC | Interface | Comment | Status |
|---|-------------------|-----------|---|--|
| 0 | 14:DA:E9:AE:F6:68 | WAN | LAPTOP BINH | 💡 - |
| 1 | 24:EA:40:01:2D:0F | LAN | netLink, dien day du ca thanh phan MAC tham gia | 💡 - |

+