**Checklist for Security Configuration and Compliance**

**1. Yêu cầu chung**

**1.1: Đảm bảo sử dụng firmware, phần mềm và bản vá không có các lỗ hổng ATTT nghiêm trọng đã được công bố trong các CVE. Đảm bảo sử dụng firmware, phần mềm và bản vá kiểm tra định kỳ.**

**2. Cấu hình bảo mật lớp 1**

**2.1: Yêu cầu phải shutdown port không sử dụng.**

* **Mô tả: Shutdown tất cả các port không sử dụng trên thiết bị, chỉ bật lên khi có yêu cầu sử dụng.**

**3. Cấu hình bảo mật lớp 2**

**3.1: Yêu cầu không sử dụng vlan default.**

* **Mô tả: Bỏ cấu hình vlan default (thường là vlan 1) trên các interface.**

**3.2: Đối với mạng Office phải sử dụng các giải pháp chống tấn công lớp 2.**

* **3.2.1: Cấu hình một trong các giải pháp: static mapping địa chỉ IP – địa chỉ MAC, Arp Inspection, Port-security hoặc 802.1x.**
* **3.2.2: Cấu hình BPDU guard trên các port access.**
* **3.2.3: Cấu hình isolate người dùng để ngăn chặn việc các thiết bị kết nối ngang hàng (các port tới gateway không cấu hình isolate).**

**3.3: Mạng văn phòng sử dụng DHCP cho máy tính người dùng phải bật tính năng DHCP Snooping.**

* **Mô tả: Mạng văn phòng sử dụng DHCP cho máy tính người dùng phải bật tính năng DHCP Snooping.**

**4. Cấu hình bảo mật lớp 3**

**4.1: Yêu cầu bảo mật cho các giao thức lớp 3.**

* **4.1.1: Các giao thức dự phòng gateway (VRRP, HSRP, GLBP, NSRP...) phải cấu hình xác thực giữa các thiết bị.**
* **4.1.2: Các giao thức IGP (RIP/OSPF/ISIS...) phải thiết lập chuỗi xác thực có mã hóa giữa các thiết bị.**
* **4.1.3: BGP phải thiết lập chuỗi xác thực có mã hóa giữa các peer.**
* **4.1.4: Chuỗi xác thực cần có độ khó cao (tuân theo quy định, tiêu chuẩn của tổ chức/công ty/đơn vị). Ví dụ: có độ phức tạp bao gồm chữ in thường, in hoa, ký tự đặc biệt; chuỗi dài hơn 8 ký tự; không đặt các mật khẩu dễ đoán.**
* **4.1.5: Với các giao thức định tuyến động: Thực hiện chặn quảng bá thông tin định tuyến ra ngoài các port không cần thiết (port đấu xuống khách hàng, thiết bị đầu cuối...).**

**4.2: Yêu cầu cấu hình bảo mật cho các phiên eBGP với các đối tác, khách hàng bên ngoài.**

* **4.2.1: Chặn việc quảng bá/nhận quảng bá các dải IP không hợp lệ và không được định tuyến trên mạng Internet toàn cầu (các dải IP private, các dải IP dành riêng cho mục đích đặc biệt (nghiên cứu/dự phòng/kiểm thử/...), các dải IP nhỏ hơn subnet /24 với IPv4 và /48 với IPv6...).**
* **4.2.2: Giới hạn số lượng các BGP prefix nhận quảng bá từ đối tác/khách hàng.**
* **4.2.3: Chặn việc quảng bá bản tin BGP Update chứa thông tin private AS number ra các đối tác/khách hàng quốc tế.**
* **4.2.4: Trên các interface đấu nối sử dụng để thiết lập eBGP: Thực hiện filter TCP port 179 (chỉ cho phép các bản tin BGP đến từ địa chỉ BGP neighbor của đối tác/khách hàng, chặn tất cả các bản tin BGP đến từ địa chỉ IP khác).**

**4.3: Yêu cầu tách bảng định tuyến giữa lớp dịch vụ và lớp giám sát thông qua VRF riêng.**

* **Mô tả: Thiết bị switch layer 3, router có các interface đấu public phải tách bảng định tuyến giữa lớp dịch vụ và lớp giám sát thông qua VRF riêng cho lưu lượng OAM.**

**5. Cấu hình quản trị**

**5.1: Yêu cầu về sao lưu cấu hình.**

* **Mô tả: Lưu cấu hình trước khi tác động và định kỳ tối thiểu 01 lần/tuần (hoặc tuân theo chính sách của tổ chức/đơn vị). Lưu tối thiểu 02 bản gần nhất. Không lưu bản sao lưu trên máy tính cá nhân của quản trị viên.**

**5.2: Yêu cầu về quản lý tài khoản.**

* **5.2.1: Khuyến nghị sử dụng hệ thống AAA để quản lý tài khoản người dùng tập trung (xác thực, phân quyền, ghi lịch sử tác động). Tối đa 02 tài khoản quản trị local dùng cho trường hợp khẩn cấp. Xóa các tài khoản không còn sử dụng (các tài khoản của quản trị viên đã nghỉ việc hoặc không còn quản lí thiết bị).**
* **5.2.2: Quản trị viên phải sử dụng tài khoản được cấp riêng, phân quyền phù hợp trên local/AAA.**
* **5.2.3: Đổi mật khẩu mặc định các tài khoản local của thiết bị.**
* **5.2.4: Thiết lập chính sách mật khẩu mạnh cho các tài khoản trên local/AAA, tuân theo chính sách của tổ chức/đơn vị.**
  + **Yêu cầu có độ phức tạp bao gồm chữ in thường, in hoa, ký tự đặc biệt.**
  + **Mật khẩu dài hơn 8 ký tự.**
  + **Không đặt các mật khẩu dễ đoán.**
  + **Mật khẩu local trên thiết bị phải được cấu hình mã hóa hoặc ẩn đi trong file cấu hình.**
* **5.2.5: Cấu hình khóa tài khoản sau một số lần đăng nhập sai nhất định. Khuyến nghị nhỏ hơn 5 lần. Thời gian khóa tài khoản do đăng nhập sai. Khuyến nghị lớn hơn 5 phút.**

**5.3: Yêu cầu về kết nối quản trị.**

* **5.3.1: Khuyến nghị quản trị thiết bị qua Out-of-band MGMT hoặc sử dụng VLAN dành riêng.**
* **5.3.2: Quản trị thiết bị qua kết nối trực tiếp Console hoặc kết nối từ xa an toàn, có mã hóa (SSHv2, HTTPS...).**
* **5.3.3: Tắt các giao thức quản trị từ xa không an toàn (Telnet, HTTP...).**
* **5.3.4: Thời gian time-out của các phiên kết nối quản trị tối đa là 15 phút (hoặc tuân theo chính sách của tổ chức/đơn vị).**
* **5.3.5: Giới hạn chỉ cho phép quản trị từ các IP theo danh sách đăng ký.**

**6. Cấu hình log và giám sát**

**6.1: Yêu cầu cấu hình NTP.**

* **Mô tả: Đồng bộ thời gian theo tối thiểu 01 máy chủ thời gian (NTP server).**

**6.2: Yêu cầu cấu hình Log.**

* **Mô tả: Thiết bị phải được thiết lập bật chế độ ghi log và cấu hình lưu log tập trung.**

**6.3: Yêu cầu cấu hình SNMP.**

* **6.3.1: SNMP phiên bản v3.**
* **6.3.2: SNMP theo chế độ read-only.**
* **6.3.3: Xóa bỏ community string mặc định.**
* **6.3.4: Chỉ cho phép truy cập SNMP từ máy chủ giám sát.**