


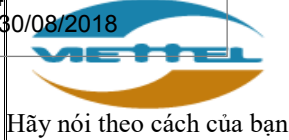


STT	Người ký	Đơn vị	Thời gian ký	Ý kiến
1	PHAM ANH ĐỨC	Phó Tổng giám đốc - Tổng công ty Mạng lưới Viettel	30/08/2018 14:18:09	
2	PHAN VIỆT CƯỜNG	Trưởng phòng - Phòng Công nghệ thông tin - Khối cơ quan TCT VTNET - Tổng công ty Mạng lưới Viettel	29/08/2018 14:53:30	

[illegible]

	Biên soạn	Kiểm tra	Phê duyệt
Chữ ký	 <b>Bùi Quang Huy</b>	 <b>Phan Việt Cường</b>	 <b>Phạm Anh Đức</b>



**HƯỚNG DẪN THIẾT LẬP AN TOÀN  
THÔNG TIN CHO HỆ ĐIỀU HÀNH  
MÁY CHỦ**

Ngày có hiệu lực: 01/9/2018

Ngày hết hiệu lực: 01/9/2019

Lần ban hành: 05

Trang: 2/71

## 1. Mục đích

Hướng dẫn chi tiết các bước cấu hình, thiết lập đảm bảo an toàn thông tin cho đối tượng hệ điều hành máy chủ, tuân thủ theo đúng Tiêu chuẩn số TC.VTQĐ.ANM.10.12 đã được Tập đoàn ban hành.

## 2. Phạm vi áp dụng và trách nhiệm các cá nhân, đơn vị

### 2.1. Phạm vi áp dụng

- Áp dụng cho tất cả hệ thống, thiết bị đang sử dụng hệ điều hành máy chủ Windows Server 2008/2012, Redhat 6.2, CentOS 6.4, IBM AIX, Solaris, SUSE, Dopro.
- Áp dụng cho tất cả đơn vị có nhiệm vụ quản lý hệ thống, thiết bị trên mạng lưới của Tổng Công ty.

### 2.2. Trách nhiệm và chế tài

- Trách nhiệm: Các đơn vị chủ trì và phối hợp có trách nhiệm thực hiện đúng theo hướng dẫn này và các quy trình, quy định, hướng dẫn liên quan.
- Chế tài: Đơn vị, cá nhân vi phạm theo trách nhiệm nêu trên thì tùy mức độ vi phạm sẽ phải chịu hình thức kỷ luật theo các quy định, chế tài xử phạt hiện hành hoặc theo quyết định của Hội đồng Kỷ luật Tập đoàn/TCT.

### 2.3. Người kiểm tra, giám sát

Bùi Quang Huy - Phòng Công nghệ Thông tin Tổng Công ty, email: HuyBQ4@viettel.com.vn, điện thoại: 0973579001.

## 3. Nguyên tắc cơ bản

Hướng dẫn xây dựng trên nguyên tắc đưa ra cách thức rà soát để phát hiện các lỗi gây mất an toàn thông tin đang tồn tại trên hệ thống, từ đó chỉ ra cách thức cấu hình, thiết lập để khắc phục lỗi, sau cùng là các bước để xác nhận lại kết quả thực hiện, đảm bảo lỗi đã được khắc phục.

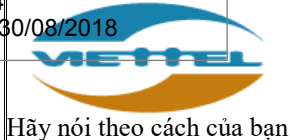
## 4. Tài liệu liên quan

Tiêu chuẩn an toàn thông tin cho hệ điều hành máy chủ có mã hiệu TC.VTQĐ.ANM.10.12.

## 5. Định nghĩa và viết tắt

- **ATTT:** An toàn thông tin.
- **OS:** Hệ điều hành.
- **B.CNTT TĐ:** Ban Công nghệ Thông tin - Tập đoàn.
- **TTANM:** Trung tâm An ninh mạng Viettel.
- **VTNet:** Tổng Công ty Mạng lưới Viettel.

## 6. Nội dung



## **HƯỚNG DẪN THIẾT LẬP CHÍNH SÁCH BẢO MẬT HỆ ĐIỀU HÀNH WINDOWS SERVER**

### **I. Nội dung hướng dẫn**

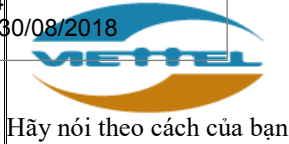
Hướng dẫn thiết lập an toàn cho hệ điều hành WINDOWS SERVER nhằm đảm bảo 8 tiêu chuẩn ATTT bao gồm:

- Cài đặt hệ điều hành và cập nhật bản vá.
- Xóa hoặc vô hiệu hóa các dịch vụ, ứng dụng, giao thức mạng không cần thiết.
- Thiết lập chính sách tài khoản.
- Thiết lập quản trị từ xa qua kênh truyền an toàn.
- Cài đặt và cấu hình firewall mềm
- Thiết lập chính sách quản lý log.
- Cài đặt phần mềm diệt virus.
- Cài đặt các phần mềm giám sát ATTT.

### **II. Chi tiết hướng dẫn**

#### **1. Cài đặt hệ điều hành và cập nhật bản vá.**

- Khi tiến hành cài đặt một hệ điều hành, một trong những yêu cầu đầu tiên phải thực hiện đó là cài đặt các bản vá hoặc upgrade version mới nhất nhằm tránh các lỗ hổng về bảo mật đã tồn tại trong các phiên bản cũ.
  - Với mỗi phiên bản hệ điều hành Windows Server yêu cầu nâng cấp lên phiên bản Service Pack mới nhất.
  - Đối với hệ điều hành Windows Server cài đặt mới, yêu cầu cài đặt phiên bản Windows Server 2008 R2 Service Pack 2 trở lên.
  - Hệ điều hành phải được cập nhật các bản vá security đã được Tập đoàn cảnh báo.
- Trup cập trang: <https://technet.microsoft.com/en-us/security/bulletin/>  
Thực hiện cập nhật bản vá mới nhất từ nhà phát triển cho hệ điều hành Windows Server tại đây.



Search by bulletin, KB, or CVE number OR Filter bulletins by product or component

Search Security Bulletins

Bulletins 1-15 of 1304

Date	Bulletin Number	KB Number	Title	Bulletin Rating
6/9/2015	MS15-064	3062157	Vulnerabilities in Microsoft Exchange Server Could Allow Elevation of Privilege	Important
6/9/2015	MS15-063	3063858	Vulnerability in Windows Kernel Could Allow Elevation of Privilege	Important
6/9/2015	MS15-062	3062577	Vulnerability in Active Directory Federation Services Could Allow Elevation of Privilege	Important
6/9/2015	MS15-061	3057839	Vulnerabilities in Windows Kernel-Mode Drivers Could Allow Elevation of Privilege	Important
6/9/2015	MS15-060	3059317	Vulnerability in Microsoft Common Controls Could Allow Remote Code Execution	Important
6/9/2015	MS15-059	3064949	Vulnerabilities in Microsoft Office Could Allow Remote Code Execution	Important
6/9/2015	MS15-057	3033890	Vulnerability in Windows Media Player Could Allow Remote Code Execution	Critical
6/9/2015	MS15-056	3058515	Cumulative Security Update for Internet Explorer	Critical
5/12/2015	MS15-055	3061518	Vulnerability in Schannel Could Allow Information Disclosure	Important
5/12/2015	MS15-054	3051768	Vulnerability in Microsoft Management Console File Format Could Allow Denial of Service	Important
5/12/2015	MS15-053	3057263	Vulnerabilities in JScript and VBScript Scripting Engines Could Allow Security Feature Bypass	Important
5/12/2015	MS15-052	3050514	Vulnerability in Windows Kernel Could Allow Security Feature Bypass	Important
5/12/2015	MS15-051	3057191	Vulnerabilities in Windows Kernel-Mode Drivers Could Allow Elevation of Privilege	Important

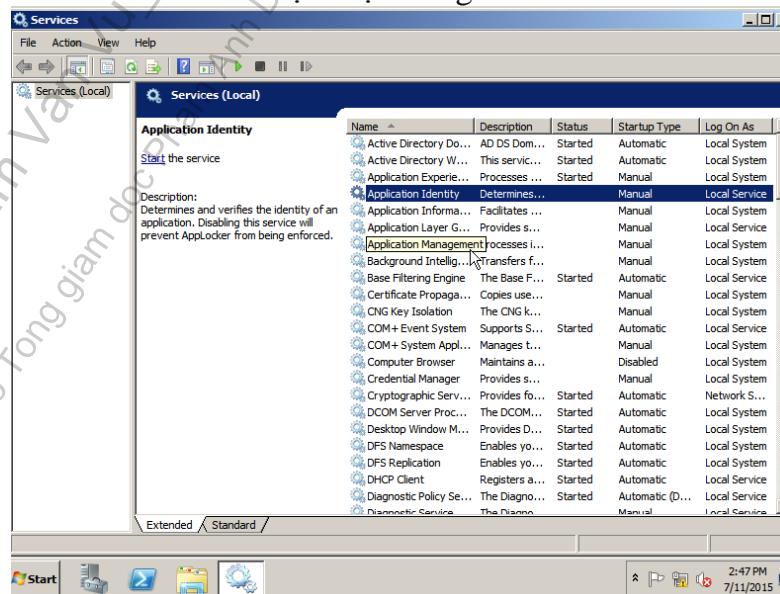
- Lưu ý: Phải tiến hành thử nghiệm trên hệ thống giả lập trước khi cập nhật bản vá và phải kiểm tra các lại dịch vụ của máy chủ sau khi thực hiện nâng cấp.

## 2. Xóa hoặc vô hiệu hóa các dịch vụ, ứng dụng, giao thức mạng không cần thiết.

- Trong thực tế, mỗi server (máy chủ) trong hệ thống sẽ đảm nhiệm một chức năng riêng biệt. Khi cài đặt hệ điều hành cho máy chủ, cần xóa hoặc disable tất cả các dịch vụ, ứng dụng, giao thức không cần thiết.

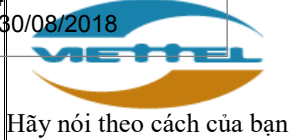
- Bước 1: Click chuột phải vào biểu tượng start của **Windows** => **Administrative Tools** => **Services**.

- Bước 2: Tìm và disabled các dịch vụ không cần thiết.



- Thông thường, một số dịch vụ, ứng dụng, giao thức sau nên được xóa hoặc disable nếu không sử dụng:

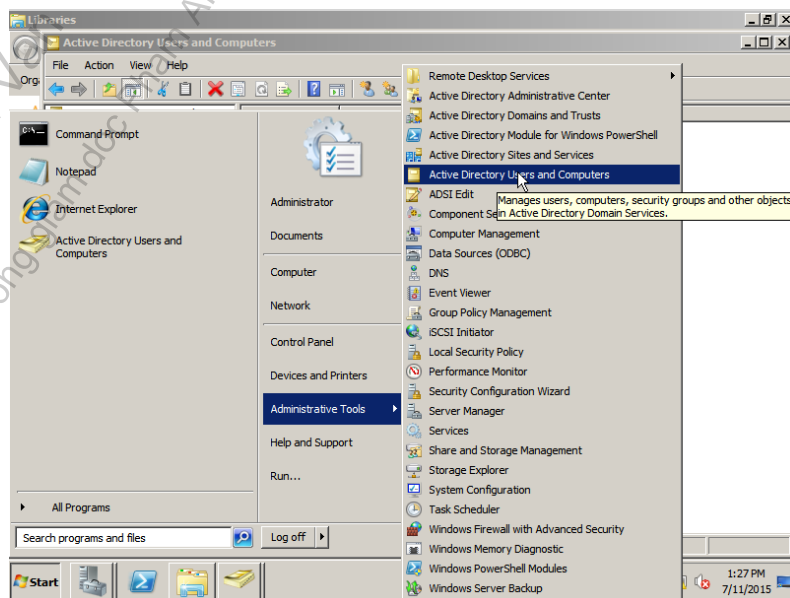
- Dịch vụ chia sẻ file và printer: NFS, FTP, NetBios,...

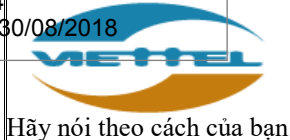


- Wireless networking.
- Chương trình hỗ trợ remote control hoặc remote access không an toàn: telnet.
- Directory services: LDAP, NIS.
- Webserver, webservices.
- Email services: smtp.
- Language compilers, libraries.
- System development tools.
- System and network management tools and utilities: SNMP.

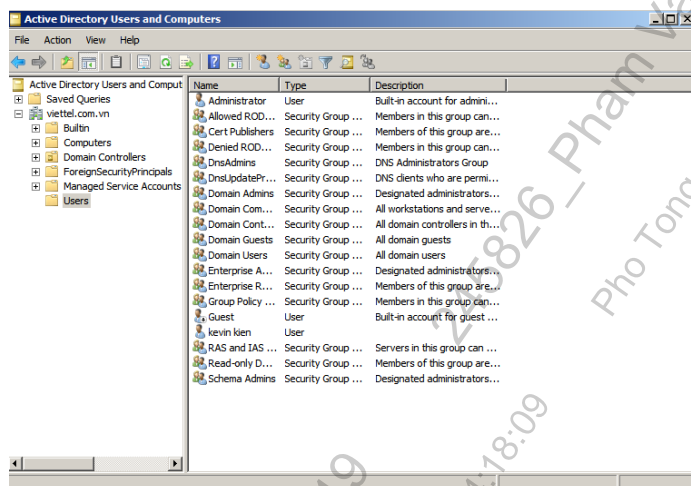
### 3. Thiết lập chính sách tài khoản.

- Các tài khoản mặc định của hệ thống, các tài khoản dễ đoán thường là mục tiêu tấn công, dò quét của các attacker. Mặc định hệ thống thường cung cấp các tài khoản như tài khoản guest, administrator... với những mật khẩu mặc định.
- Xóa hoặc vô hiệu hóa các tài khoản không sử dụng trên hệ thống:
  - o Kiểm tra tài khoản trên Local:
    - Bước 1: Click chuột phải vào My Computer => Manager => Configuration => Local User and group => Users/Groups.
    - Bước 2: Kiểm tra user nào không sử dụng xóa hoặc disable.
  - o Kiểm tra tài khoản trên máy domain controller:
    - Bước 1: Click chuột phải vào biểu tượng start của Windows => Administrative Tools => Active Directory Users and Computers.

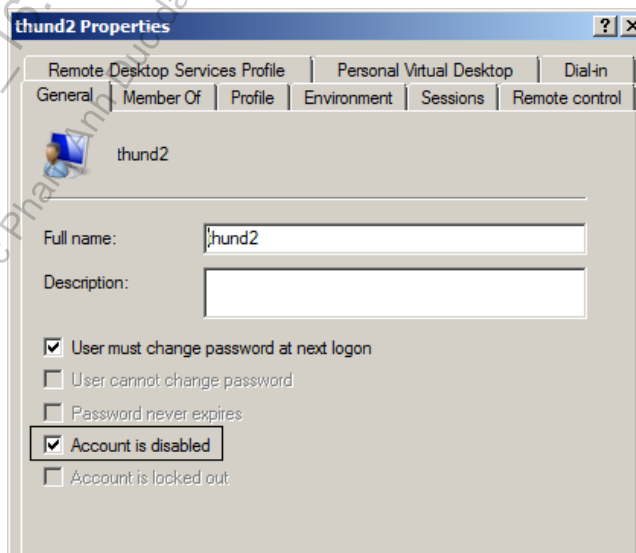




- Bước 2: Click vào User/Group. Xóa hoặc disable tài khoản không sử dụng.

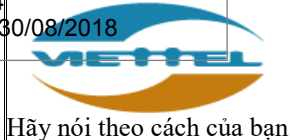


- Thay đổi tên, mật khẩu cho các tài khoản mặc định.
  - Thay đổi user, password trên máy Local: Vào Start => Programs => Administrative Tools => Server Manager Configuration => Configure => Local Users and Group => Users => Click chuột phải vào user => Properties => Account is disabled.

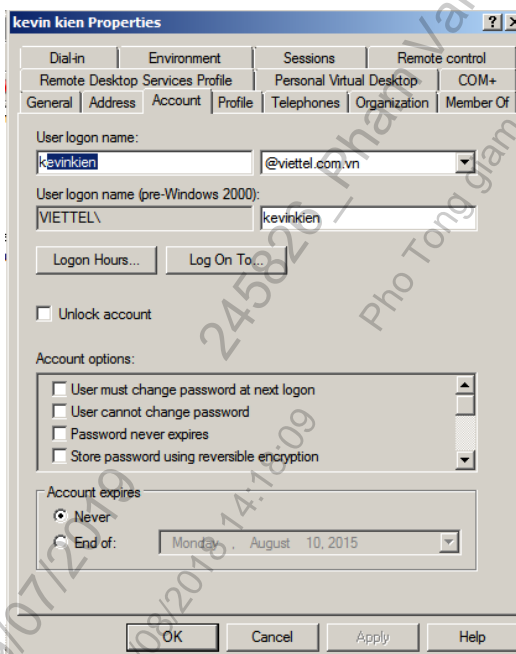


- Thay đổi tên, mật khẩu trên máy Domain Controller:
  - Bước 1: Click chuột phải vào biểu tượng start của Windows => Administrative Tools => Active Directory Users and Computers => User.

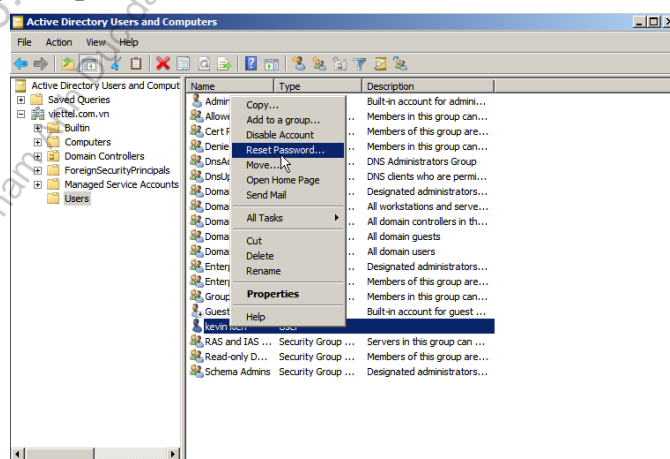




- Bước 2: Chọn tài khoản muốn thay đổi => Properties => Account.  
Thay đổi user muốn đổi.



Chuột phải vào user muốn thay đổi => Reset Password. Và thực hiện thay đổi password.



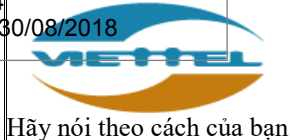
- Cấu hình chính sách mật khẩu cho tài khoản:

- Độ dài tối thiểu của mật khẩu phải lớn hơn hoặc bằng 8 ký tự.

- Bước 1: Click chuột phải vào biểu tượng start của Windows => Administrative Tools => Local Security Policy => Account Policies => Password Policy.
- Bước 2: Chọn *Minimum Password length* và đặt 8 ký tự.



Mã văn bản: HD.VTNet.CNTT.04/ATTT  
Số văn bản: 04-4  
Ngày ban hành: 30/08/2018



**TỔNG CÔNG TY MẠNG LƯỚI VIETTEL**

**HƯỚNG DẪN THIẾT LẬP AN TOÀN  
THÔNG TIN CHO HỆ ĐIỀU HÀNH  
MÁY CHỦ**

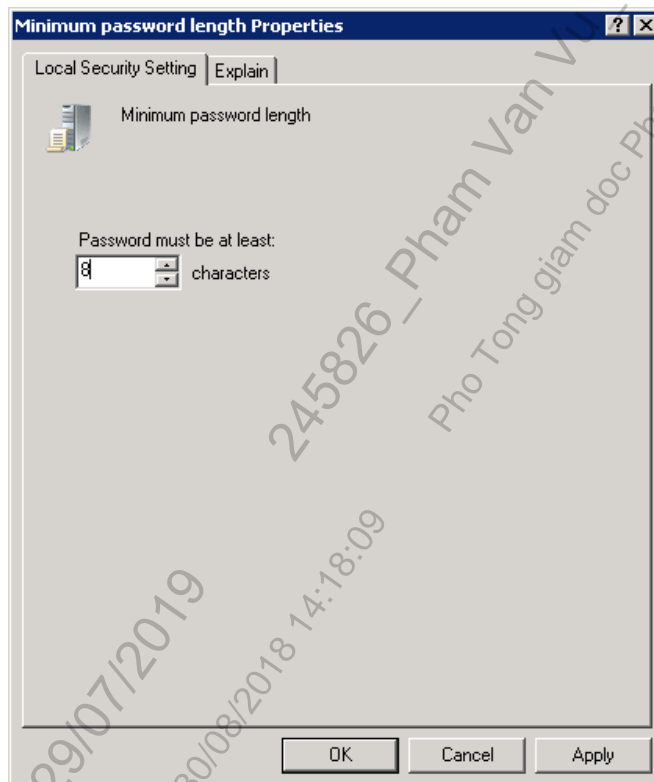
Mã hiệu: HD.VTNET.CNTT....

Ngày có hiệu lực: 01/9/2018

Ngày hết hiệu lực: 01/9/2019

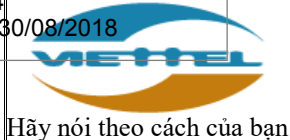
Lần ban hành: 05

Trang: 8/71



- Mật khẩu phải chứa ký tự viết hoa, viết thường, chữ số, ký tự đặc biệt.
  - Bước 1: Click chuột phải vào biểu tượng start của Windows > Administrative Tools => Local Security Policy => Account Policies => Password Policy.
  - Bước 2: Chọn *Password must meet complexity* và tích vào Enabled.

Mã văn bản: HD.VTNet.CNTT.04/ATTT  
Số văn bản: 04-4  
Ngày ban hành: 30/08/2018



**TỔNG CÔNG TY MẠNG LƯỚI VIETTEL**

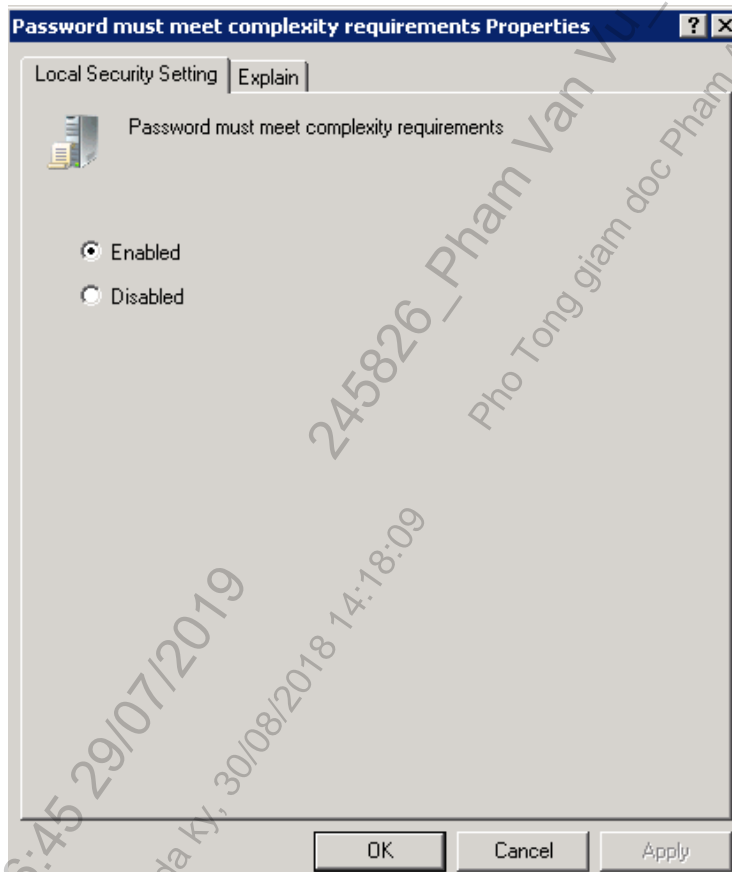
**HƯỚNG DẪN THIẾT LẬP AN TOÀN  
THÔNG TIN CHO HỆ ĐIỀU HÀNH  
MÁY CHỦ**

Mã hiệu: HD.VTNET.CNTT....

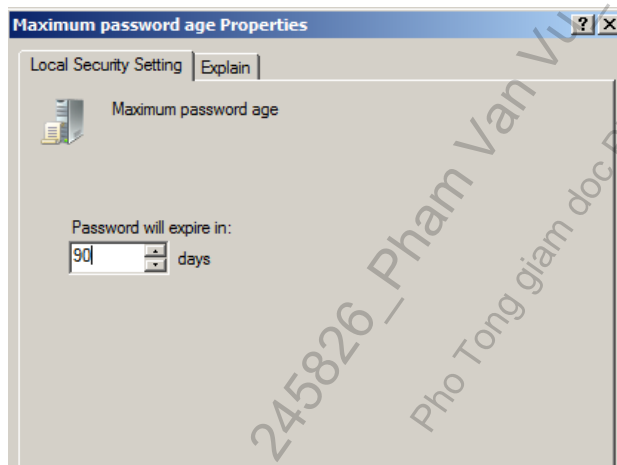
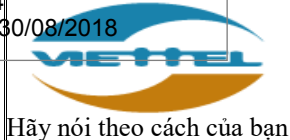
Ngày có hiệu lực: 01/9/2018  
Ngày hết hiệu lực: 01/9/2019

Lần ban hành: 05

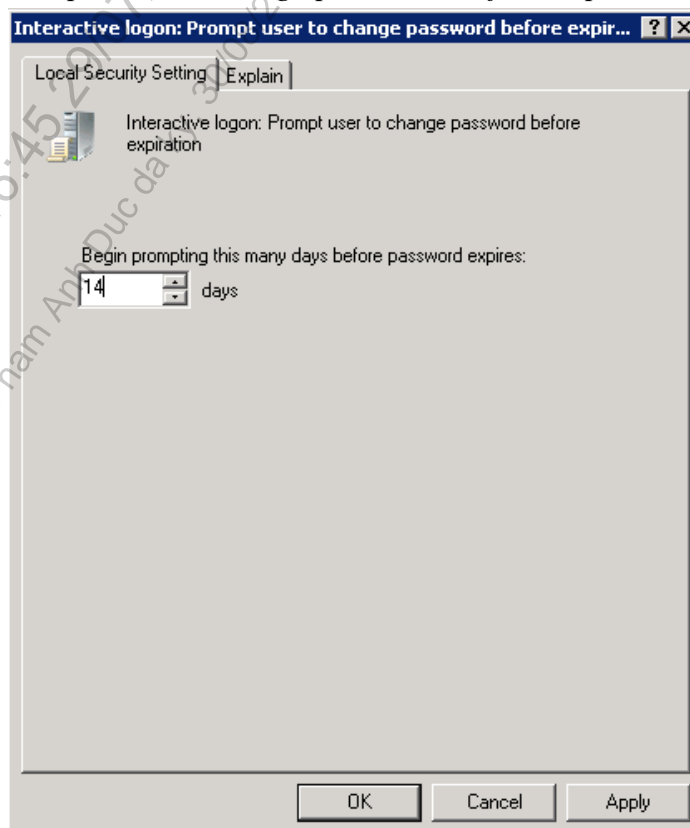
Trang: 9/71



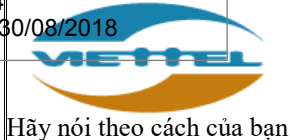
- Thời gian bắt buộc phải thay đổi mật khẩu đối với tài khoản người dùng (quantri, portal,...)
  - Bước 1: Click chuột phải vào biểu tượng start của Windows => Administrative Tools => Local Security Policy => Account Policies => Password Policy.
  - Bước 2: Chọn *Maximum Password Age* và đặt 90 ngày (với hệ thống public) hoặc 180 ngày (với hệ thống nội bộ).



- Bước 3: Cấu hình thông báo mật khẩu sắp hết hạn cho người dùng. Click chuột phải vào biểu tượng start của Windows => Administrative Tools => Local Security Policy => Local Policies => Security Options. Thiết lập giá trị cho cấu hình *Interactive logon: Prompt user to change password before expire* là 14.



- o Giới hạn mật khẩu mới không được trùng với mật khẩu gần nhất.



**HƯỚNG DẪN THIẾT LẬP AN TOÀN  
THÔNG TIN CHO HỆ ĐIỀU HÀNH  
MÁY CHỦ**

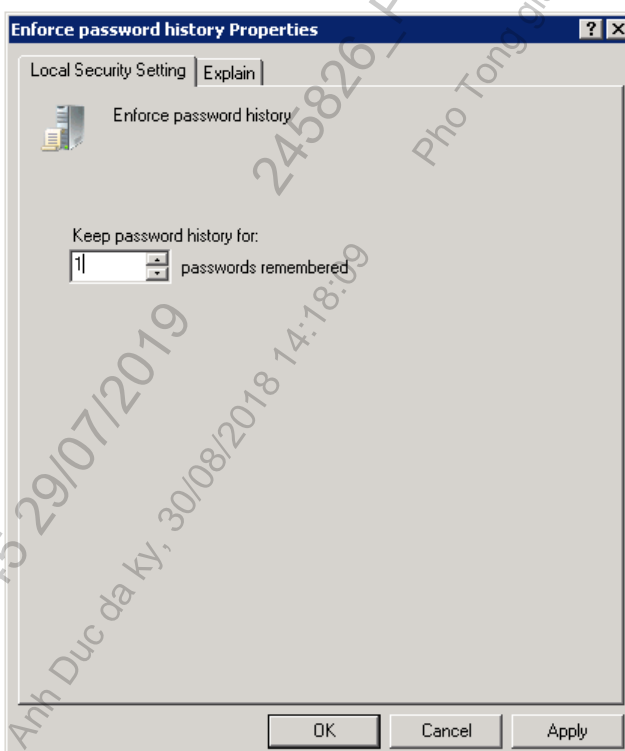
Ngày có hiệu lực: 01/9/2018

Ngày hết hiệu lực: 01/9/2019

Lần ban hành: 05

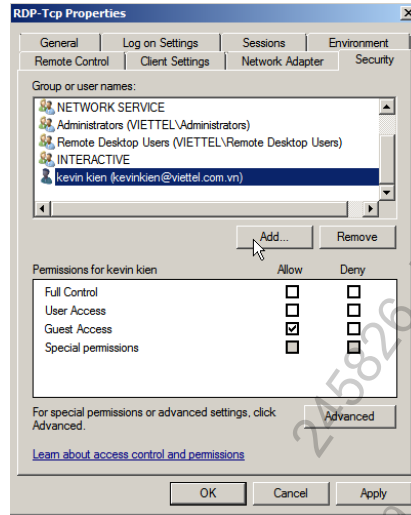
Trang: 11/71

- Bước 1: Click chuột phải vào biểu tượng start của Windows => Administrative Tools => Local Security Policy => Account Policies => Password Policy.
- Bước 2: Chọn *Enforce password history* và đặt giá trị là 02 (với hệ thống nội bộ) hoặc 05 (với hệ thống public).



#### **4. Quản trị từ xa qua kênh truyền an toàn.**

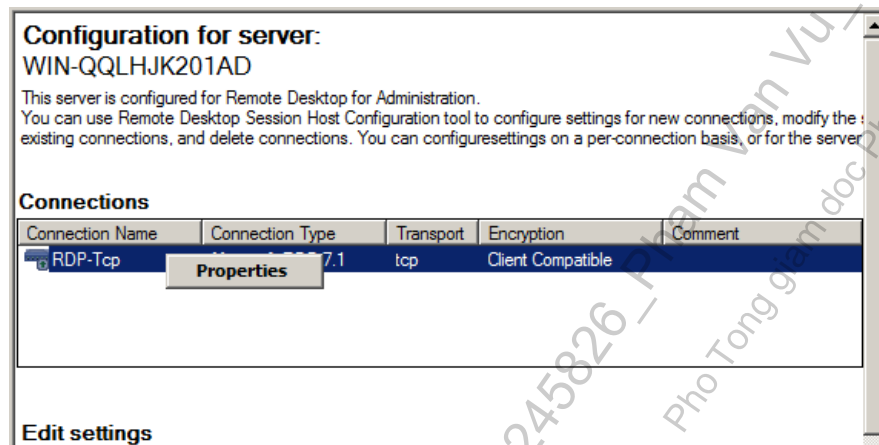
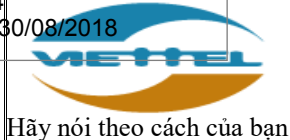
- Yêu cầu quản trị từ xa sử dụng kênh truyền an toàn, có mã hóa: Sử dụng ứng dụng Remote Desktop của Windows để quản trị từ xa.
- Cấu hình giới hạn tài khoản được phép sử dụng dịch vụ quản trị từ xa.
  - Bước 1: Chọn Start => Administrative Tools => Server Manager => Roles => Remote Desktop Services.
  - Bước 2: Chọn RD Session Host Configuration và click vào RDP-Tcp.
  - Bước 3: Chọn mục Security và add thêm user muốn cho remote.



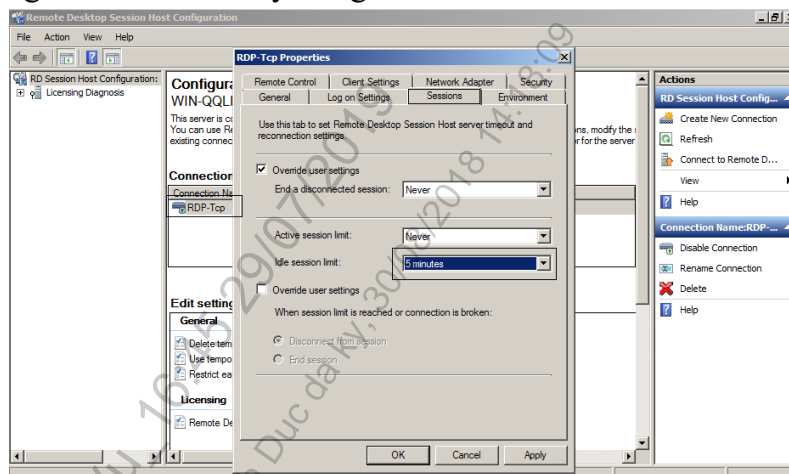
- Giới hạn số lần đăng nhập sai là 05 lần.
  - Bước 1: Click chuột phải vào biểu tượng start của Windows => Administrative Tools => Local Security Policy => Account Policies => Password Policy.
  - Bước 2: Chọn *Account lockout threshold* và thiết lập giá trị là 5, *Account lockout duration* thiết lập là 5 và *Reset account lockout counter after* thiết lập giá trị là 5.

Policy	Security Setting
Account lockout duration	5 minutes
Account lockout threshold	5 invalid logon attempts
Reset account lockout counter after	5 minutes

- Giới hạn thời gian tự động ngắt phiên khi không có hoạt động trong một khoảng thời gian là 5 phút.
  - Vào Start => Administrative Tools => Remote Desktop Services => Remote Desktop Session Host Configure. Click chuột phải vào RDP-TCP => Properties.



- Trong thẻ Sessions thay đổi giá trị Idle session limit:



## 5. Cài đặt và cấu hình firewall mềm.

Trên một server luôn có rất nhiều các dịch vụ đang chạy đồng thời, việc kiểm soát tất cả mọi truy cập vào ra trên hệ thống sẽ giúp hạn chế được các cuộc tấn công của attacker.

- Kích hoạt Windows Firewall: Run => services.msc => Chọn Windows Firewall => Chọn Automatic => Start.

Windows Error Rep...	Allows erro...	Manual	Local System
Windows Event Coll...	This servic...	Manual	Network S...
Windows Event Log	This servic...	Started	Automatic
Windows Firewall	Windows Fi...	Started	Automatic
Windows Font Cac...	Optimizes ...	Started	Automatic (D...

- Mặc định Windows Firewall cấm các kết nối vào và không cấm các kết nối ra đối với cả Domain Profile, Private Profile và Public Profile:



**TỔNG CÔNG TY MẠNG LƯỚI VIETTEL**

**HƯỚNG DẪN THIẾT LẬP AN TOÀN  
THÔNG TIN CHO HỆ ĐIỀU HÀNH  
MÁY CHỦ**

Mã hiệu: HD.VTNET.CNTT....

Ngày có hiệu lực: 01/9/2018

Ngày hết hiệu lực: 01/9/2019

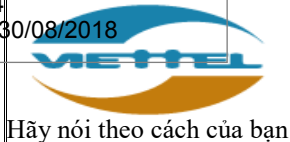
Lần ban hành: 05

Trang: 14/71

- Domain Profile: Cấu hình tường lửa được áp dụng khi máy tính kết nối với các máy khác trong cùng một domain.
- Private Profile: Cấu hình tường lửa được áp dụng khi máy tính kết nối với mạng riêng.
- Public Profile: Cấu hình tường lửa được áp dụng khi máy tính kết nối với mạng công cộng.
- Local IP: là địa chỉ trên máy chủ đang chấp nhận kết nối hoặc địa chỉ được sử dụng với tư cách là địa chỉ nguồn để gửi các kết nối gửi đi.
- Remote IP: là địa chỉ IP của máy chủ điều khiển xa mà máy chủ này đang muốn kết nối đến (trong kịch bản truy cập gửi đi), hoặc địa chỉ IP nguồn của máy tính đang muốn kết nối với máy chủ (trong trường hợp kịch bản truy cập gửi đến).
- Local Port: các cổng nội bộ trên máy chủ mà rule của tường lửa sử dụng. Nếu rule là Inbound Rules thì đây sẽ là cổng để máy chủ lắng nghe. Nếu rule là Outbound Rules thì đây sẽ là cổng nguồn để máy chủ sử dụng kết nối tới máy khác.
- Remote Port: đây là cổng điều khiển từ xa để sử dụng cho rule. Trong trường hợp rule kết nối gửi đi thì đây sẽ là cổng mà máy chủ kết nối với một máy tính khác. Trong trường hợp rule kết nối đến thì đây chính là cổng nguồn của máy tính muốn kết nối với máy chủ.



Mã văn bản: HD.VTNet.CNTT.04/ATTT  
Số văn bản: 04-4  
Ngày ban hành: 30/08/2018



Hãy nói theo cách của bạn

**TỔNG CÔNG TY MẠNG LƯỚI VIETTEL**

**HƯỚNG DẪN THIẾT LẬP AN TOÀN  
THÔNG TIN CHO HỆ ĐIỀU HÀNH  
MÁY CHỦ**

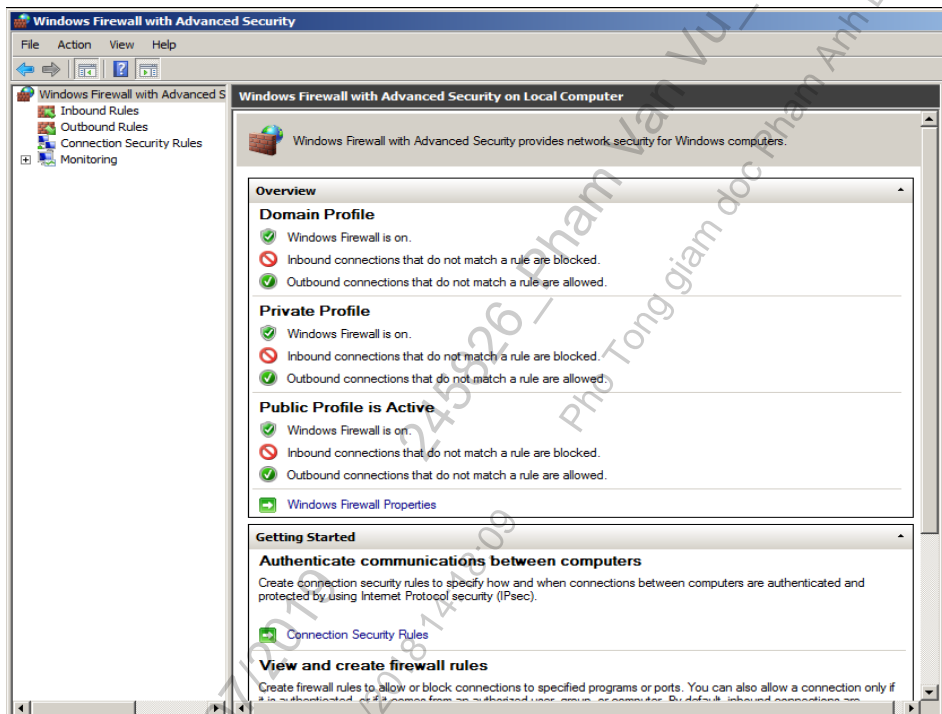
Mã hiệu: HD.VTNET.CNTT....

Ngày có hiệu lực: 01/9/2018

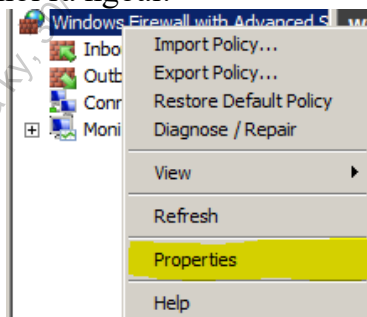
Ngày hết hiệu lực: 01/9/2019

Lần ban hành: 05

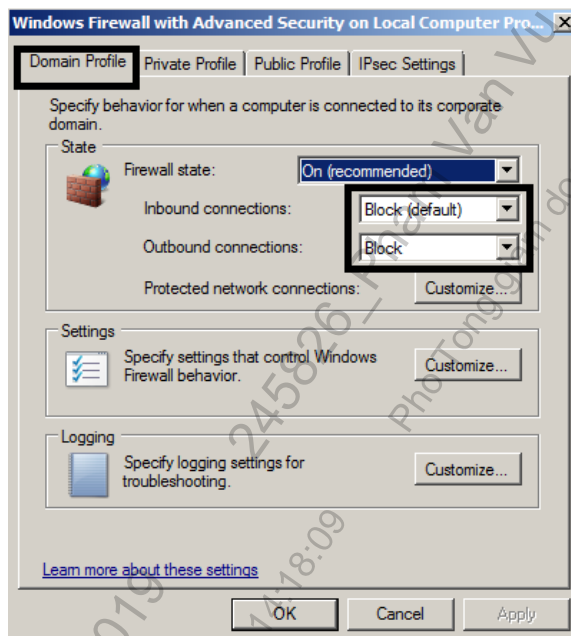
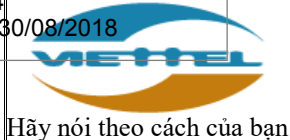
Trang: 15/71



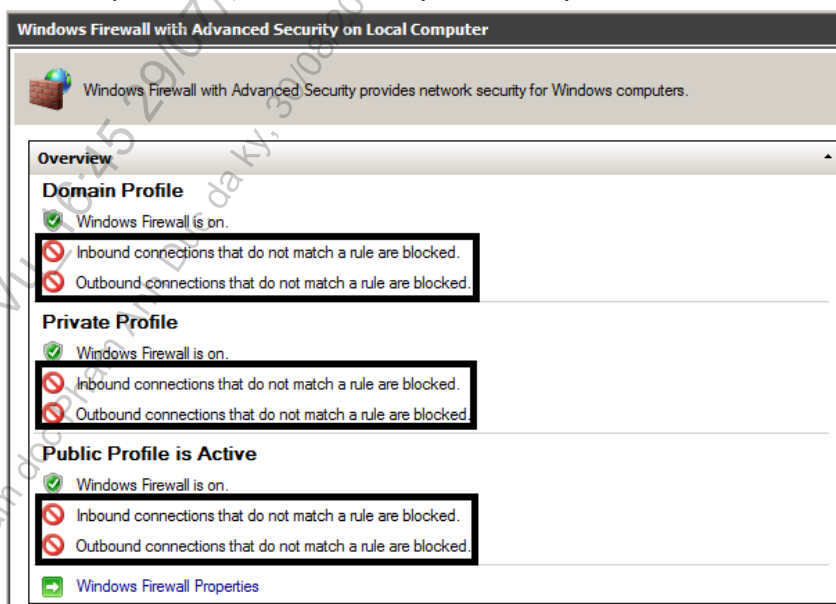
- Cấu hình block các kết nối ra ngoài:



Cấu hình Block Outbound Connection trong tab Domain Profile (làm tương tự đối với tab Private Profile và Public Profile).

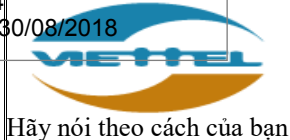


- Kiểm tra lại cấu hình xem đã được kích hoạt chưa:



- Thiết lập kết nối chiều ra/vào theo đặc quyền:
  - Thiết lập chính sách kết nối từ ngoài vào máy chủ (Inbound Rule): Click chọn Inbound Rule => New Rule...

Mã văn bản: HD.VTNet.CNTT.04/ATTT  
Số văn bản: 04-4  
Ngày ban hành: 30/08/2018



**TỔNG CÔNG TY MẠNG LƯỚI VIETTEL**

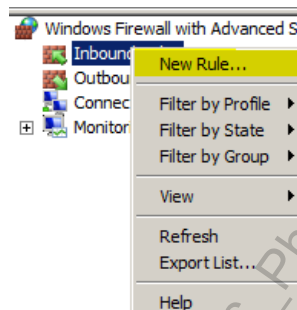
**HƯỚNG DẪN THIẾT LẬP AN TOÀN  
THÔNG TIN CHO HỆ ĐIỀU HÀNH  
MÁY CHỦ**

Mã hiệu: HD.VTNET.CNTT....

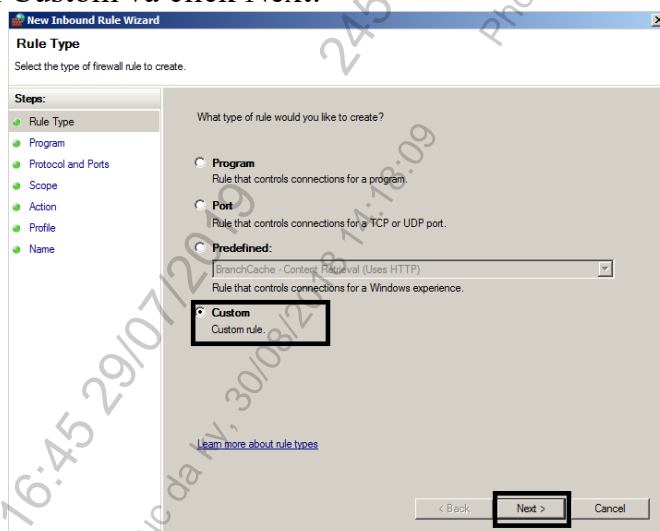
Ngày có hiệu lực: 01/9/2018  
Ngày hết hiệu lực: 01/9/2019

Lần ban hành: 05

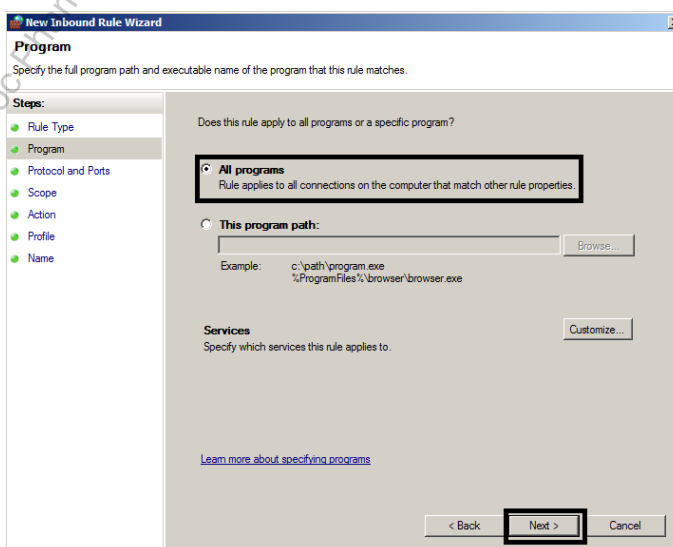
Trang: 17/71



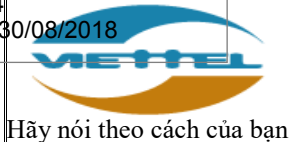
- Chọn Custom và click Next:



- Chọn chương trình kết nối => All Programs => Next.



Mã văn bản: HD.VTNet.CNTT.04/ATTT  
Số văn bản: 04-4  
Ngày ban hành: 30/08/2018



**TỔNG CÔNG TY MẠNG LƯỚI VIETTEL**

**HƯỚNG DẪN THIẾT LẬP AN TOÀN  
THÔNG TIN CHO HỆ ĐIỀU HÀNH  
MÁY CHỦ**

Mã hiệu: HD.VTNET.CNTT....

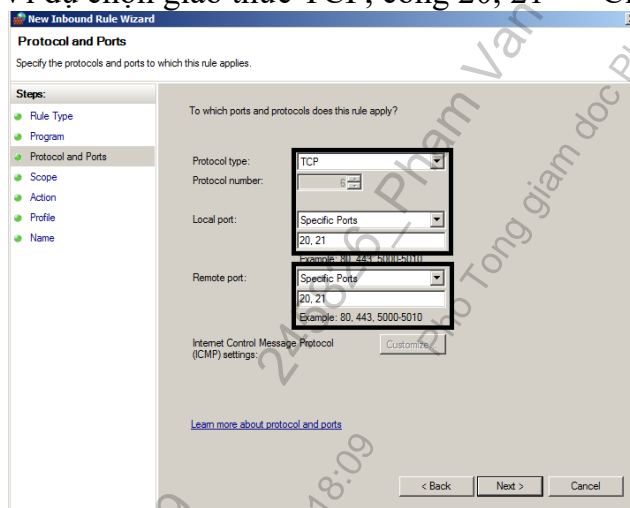
Ngày có hiệu lực: 01/9/2018

Ngày hết hiệu lực: 01/9/2019

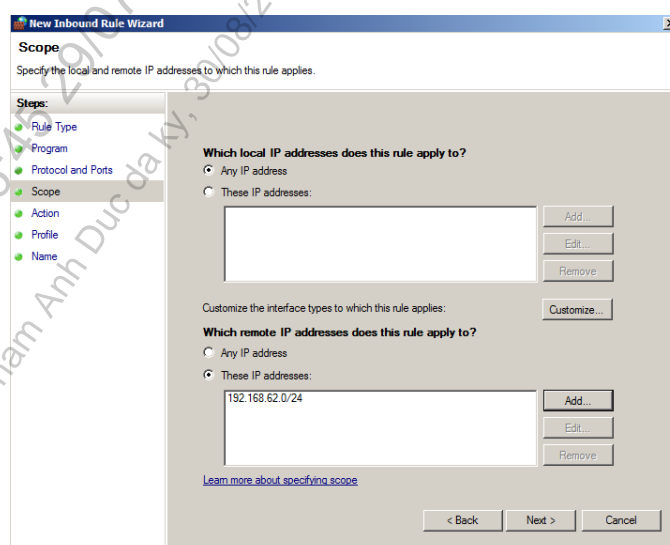
Lần ban hành: 05

Trang: 18/71

- Chọn giao thức và cổng tương ứng cần mở kết nối từ ngoài vào máy chủ. Ví dụ chọn giao thức TCP, cổng 20, 21 => Click Next.



- Thiết lập IP được phép kết nối => Click Next:



- Chọn Allow the connection => Click Next:

Mã văn bản: HD.VTNet.CNTT.04/ATTT  
 Số văn bản: 04-4  
 Ngày ban hành: 30/08/2018



**TỔNG CÔNG TY MẠNG LƯỚI VIETTEL**

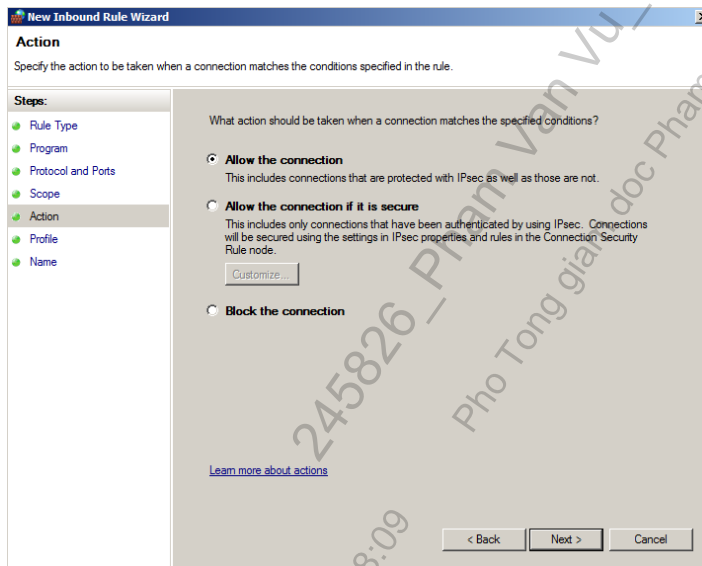
**HƯỚNG DẪN THIẾT LẬP AN TOÀN  
 THÔNG TIN CHO HỆ ĐIỀU HÀNH  
 MÁY CHỦ**

Mã hiệu: HD.VTNET.CNTT....

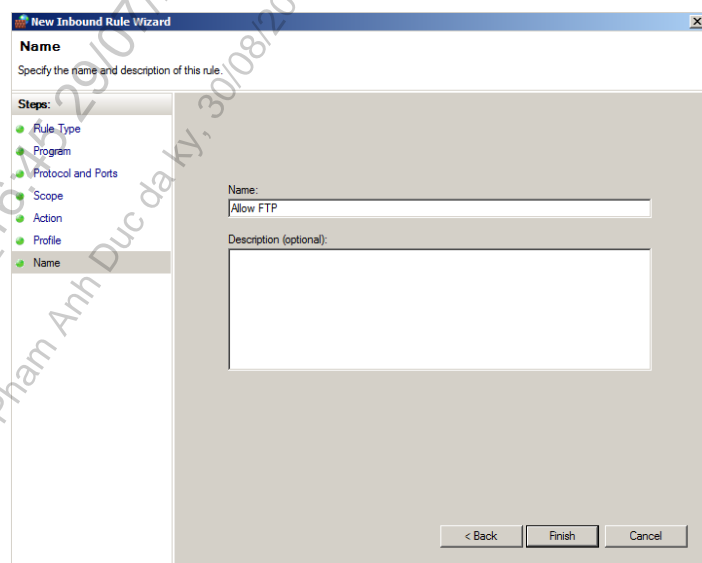
Ngày có hiệu lực: 01/9/2018  
 Ngày hết hiệu lực: 01/9/2019

Lần ban hành: 05

Trang: 19/71



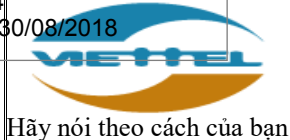
- Để mặc định => Next => Đặt tên cho Rule => Click Finish:



- Ta có được luật vừa tạo:

Inbound Rules						
Name	Group	Profile	Enabled	Action		
Allow FTP		All	Yes	Allow	N	
BranchCache Content Retrieval (HTTP-In)	BranchCache - Content Retrie...	All	No	Allow	N	
BranchCache Hosted Cache Server (HTTP-In)	BranchCache - Hosted Cache ...	All	No	Allow	N	
BranchCache Peer Discovery (WSD-In)	BranchCache - Peer Discovery...	All	No	Allow	N	
COM+ Network Access (DCOM-In)	COM+ Network Access	All	No	Allow	N	

- Thiết lập chính sách kết nối từ máy chủ ra ngoài (Outbound Rule): Cách thiết lập tương tự như trên.



Hãy nói theo cách của bạn

**TỔNG CÔNG TY MẠNG LƯỚI VIETTEL**

**HƯỚNG DẪN THIẾT LẬP AN TOÀN  
THÔNG TIN CHO HỆ ĐIỀU HÀNH  
MÁY CHỦ**

Mã hiệu: HD.VTNET.CNTT....

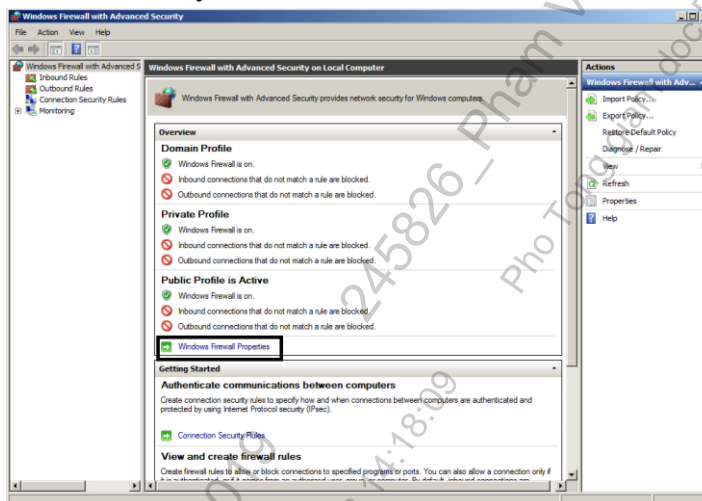
Ngày có hiệu lực: 01/9/2018

Ngày hết hiệu lực: 01/9/2019

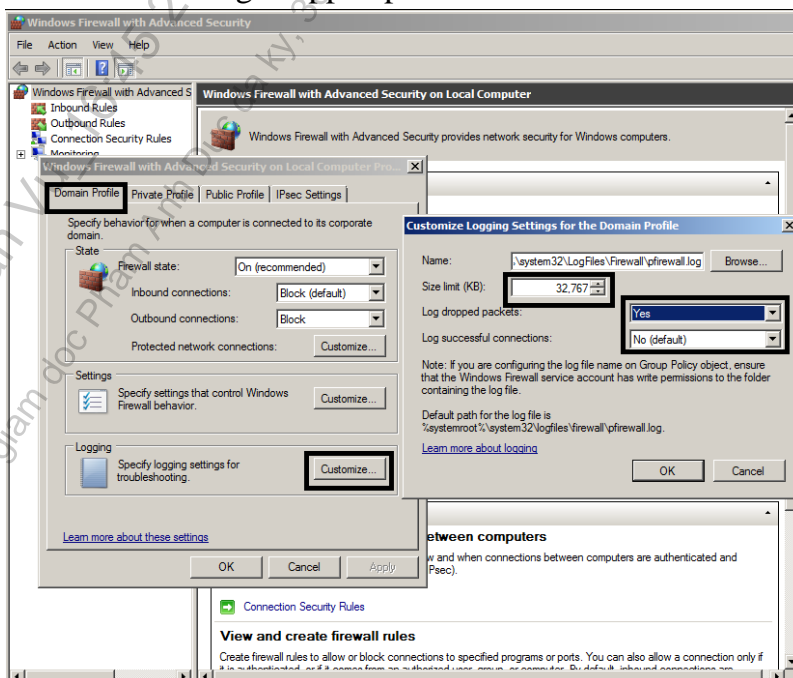
Lần ban hành: 05

Trang: 20/71

- Yêu cầu ghi log toàn bộ các gói tin vi phạm luật tường lửa.
  - Vào Start => Administrative Tools => Windows Firewall with Advanced Security.

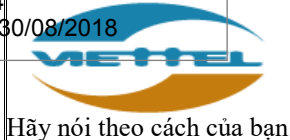


- Click Windows Firewall Properties => mở Customize... Logging của các tab Domain Profile, Private Profile và Public Profile => Click Yes cho Log dropped packets.



## 6. Thiết lập chính sách quản lý log.

- Ghi log các sự kiện đăng nhập vào máy chủ.



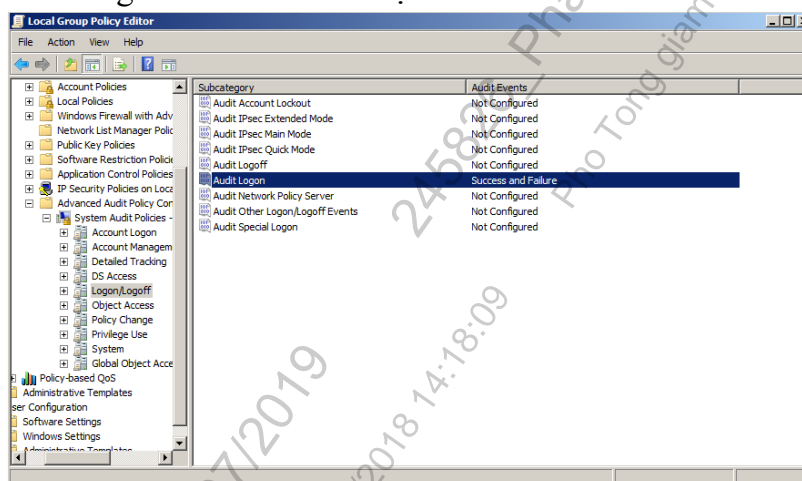
**HƯỚNG DẪN THIẾT LẬP AN TOÀN  
THÔNG TIN CHO HỆ ĐIỀU HÀNH  
MÁY CHỦ**

Ngày có hiệu lực: 01/9/2018  
Ngày hết hiệu lực: 01/9/2019

Lần ban hành: 05

Trang: 21/71

- Vào Run => gpedit.msc => Computer Configuration => Windows Setting => Security Setting => Advanced Audit Policy Configuration => System Audit Policy – Local Group Policy Object => Logon/logoff => Audit Logon => Configure the following audit event => Chọn Failure và Success.

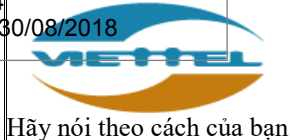


- Ghi log các sự kiện liên quan đến quản lý tài khoản và nhóm tài khoản.
  - Vào Run => gpedit.msc => Computer Configuration => Windows Setting => Security Setting => Advanced Audit Policy Configuration => System Audit Policy – Local Group Policy Object => Account Management.
  - Cấu hình như sau:
    - Audit Application Group Management => Chọn Success.
    - Audit Computer Account Management => Chọn Success.
    - Audit User Account Management => Chọn Success.

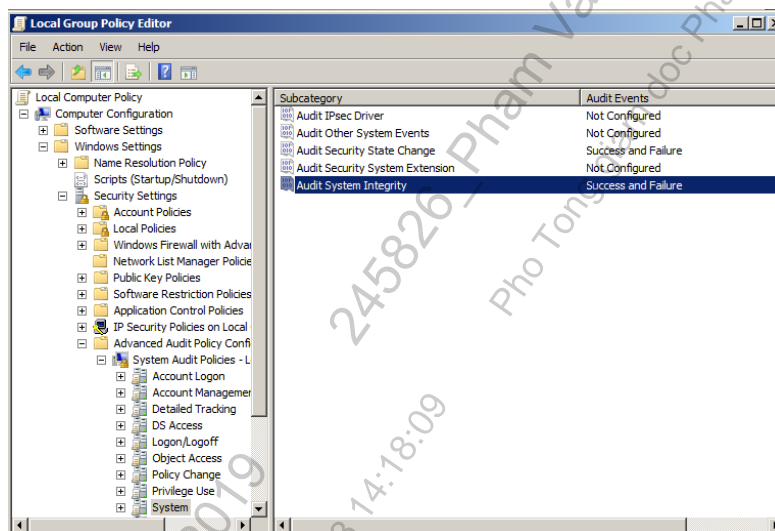
Subcategory	Audit Events
Audit Application Group Management	Success
Audit Computer Account Management	Success
Audit Distribution Group Management	Not Configured
Audit Other Account Management Events	Not Configured
Audit Security Group Management	Not Configured
Audit User Account Management	Success

- Ghi log những thay đổi trong “Security State Change” và “System Integrity”.
  - Vào Run => gpedit.msc => Computer Configuration => Windows Setting => Security Setting => Advanced Audit Policy Configuration => System Audit Policy – Local Group Policy Object => System:

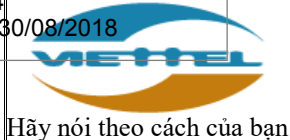




- Audit Security State Change => Chọn Failure và Success.
- Audit System Integrity => Chọn Failure và Success.



- Thiết lập kích cỡ và sao lưu file log Application, Security, System.
  - Vào Run => gpedit.msc => Computer Configuration => Administrative Templates => Windows Components => Event Log Service. Đối với cả 3 mục Application, Security, System thiết lập như sau:
    - Application => Maximum Log Size (KB) thiết lập kích cỡ 1024000 KB.
    - Security => Maximum Log Size (KB) thiết lập kích cỡ 1024000 KB.
    - System => Maximum Log Size (KB) thiết lập kích cỡ 1024000 KB.
    - Bật: Backup log automatically when full.



Hãy nói theo cách của bạn

## TỔNG CÔNG TY MẠNG LƯỚI VIETTEL

### HƯỚNG DẪN THIẾT LẬP AN TOÀN THÔNG TIN CHO HỆ ĐIỀU HÀNH MÁY CHỦ

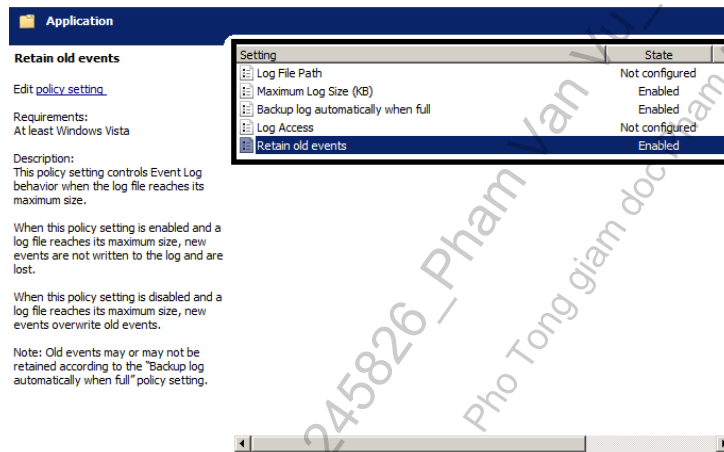
Mã hiệu: HD.VTNET.CNTT....

Ngày có hiệu lực: 01/9/2018

Ngày hết hiệu lực: 01/9/2019

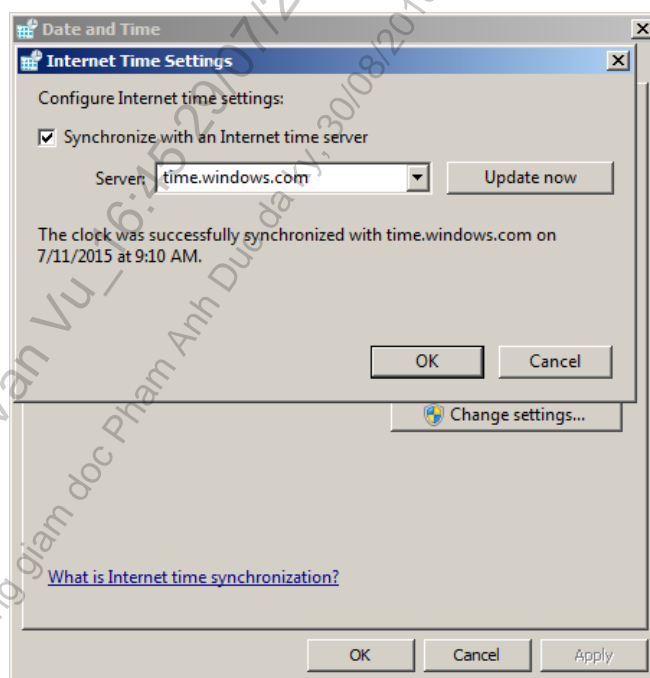
Lần ban hành: 05

Trang: 23/71



- Cấu hình đồng bộ thời gian cho hệ thống:

- Vào Start Menu => Control Panel => Date and Time => Internet Time => Change Setting => chọn “Synchronize with an Internet Time Server” => nhập địa chỉ Time Server => Update now.

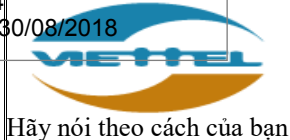


## 7. Cài đặt phần mềm diệt virus.

Yêu cầu cài đặt các phần mềm antiVirus nhằm ngăn ngừa, phát hiện các cuộc tấn công của attacker vào hệ thống. Trong phần này, phụ lục chi tiết hướng dẫn cấu hình phần mềm diệt virus Microsoft Security Essentials (MSE) theo các đầu mục của baseline.

- Yêu cầu sử dụng phần mềm diệt virus luôn ở chế độ bảo vệ.

Mã văn bản: HD.VTNet.CNTT.04/ATTT  
Số văn bản: 04-4  
Ngày ban hành: 30/08/2018



Hãy nói theo cách của bạn

**TỔNG CÔNG TY MẠNG LƯỚI VIETTEL**

**HƯỚNG DẪN THIẾT LẬP AN TOÀN  
THÔNG TIN CHO HỆ ĐIỀU HÀNH  
MÁY CHỦ**

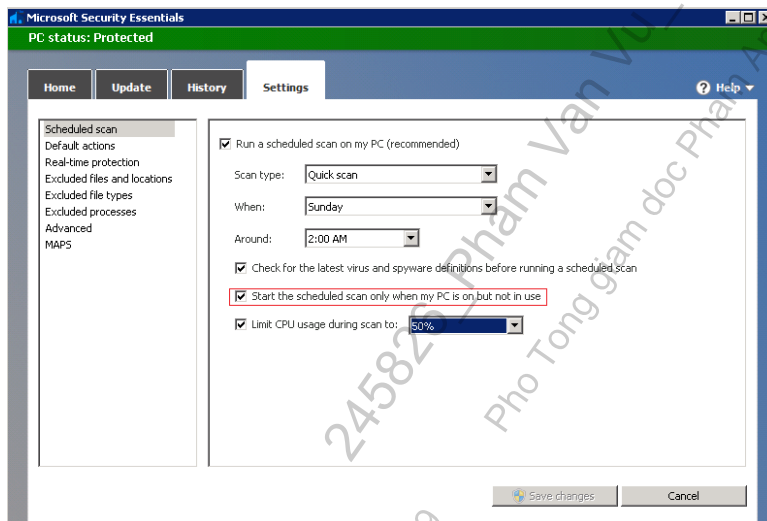
Mã hiệu: HD.VTNET.CNTT....

Ngày có hiệu lực: 01/9/2018

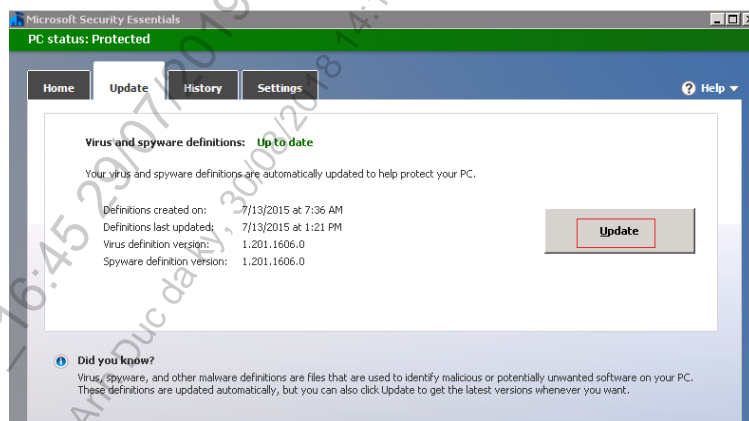
Ngày hết hiệu lực: 01/9/2019

Lần ban hành: 05

Trang: 24/71

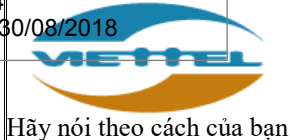


- Cập nhật các mẫu diệt virus mới hàng ngày.



- Quét toàn bộ máy chủ theo định kỳ tối thiểu 1 tháng 1 lần: Chỉ yêu cầu bắt buộc đối với các hệ thống public.

Mã văn bản: HD.VTNet.CNTT.04/ATTT  
Số văn bản: 04-4  
Ngày ban hành: 30/08/2018



Hãy nói theo cách của bạn

**TỔNG CÔNG TY MẠNG LƯỚI VIETTEL**

**HƯỚNG DẪN THIẾT LẬP AN TOÀN  
THÔNG TIN CHO HỆ ĐIỀU HÀNH  
MÁY CHỦ**

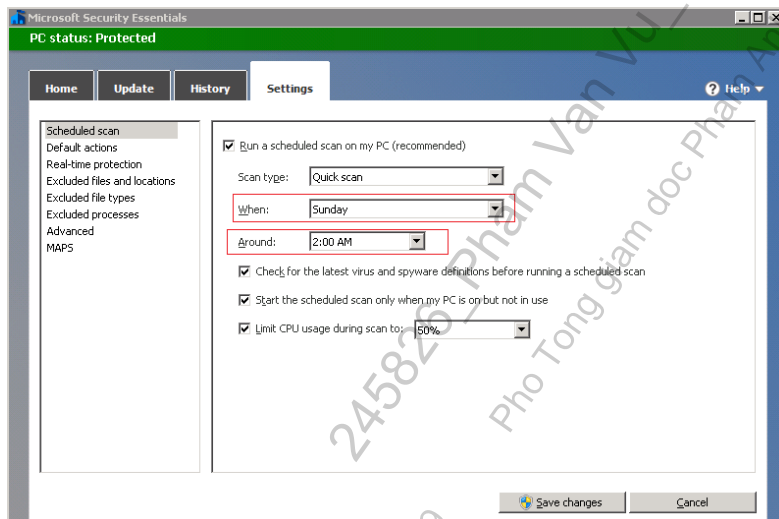
Mã hiệu: HD.VTNET.CNTT....

Ngày có hiệu lực: 01/9/2018

Ngày hết hiệu lực: 01/9/2019

Lần ban hành: 05

Trang: 25/71



## 8. Cài đặt các phần mềm giám sát ATTT

Yêu cầu cài đặt đầy đủ các phần mềm giám sát ATTT do TT.ANM cung cấp

- Phần mềm One Agent để hỗ trợ giám sát hành vi bất thường.
- Phần mềm Server Endpoint để hỗ trợ giám sát hành vi bất thường và vi phạm baseline.

Hướng dẫn cài đặt: [http://docs.sirc.viettel.com/guide/install\\_se\\_agent/](http://docs.sirc.viettel.com/guide/install_se_agent/)

- Phần mềm Filebeat hoặc WinlogBeat để hỗ trợ lấy log và event.

Hướng dẫn cài đặt: <http://docs.sirc.viettel.com/guide/LogAgent/>



## **HƯỚNG DẪN THIẾT LẬP CẤU HÌNH BẢO MẬT CHO HỆ ĐIỀU HÀNH CENTOS và REDHAT**

### **I. Nội dung hướng dẫn**

Hướng dẫn thiết lập an toàn cho hệ điều hành CENTOS/REDHAT nhằm đảm bảo 8 tiêu chuẩn ATTT bao gồm:

- Cài đặt và cập nhật bản vá cho hệ điều hành.
- Xóa hoặc vô hiệu hóa các dịch vụ, ứng dụng, giao thức mạng không cần thiết.
- Thiết lập chính sách tài khoản.
- Quản trị từ xa qua kênh truyền an toàn.
- Phân quyền tập tin và thư mục.
- Cài đặt và cấu hình firewall mềm.
- Thiết lập chính sách quản lý log.
- Cài đặt phần mềm giám sát ATTT.

### **II. Chi tiết hướng dẫn**

#### **1. Cài đặt và cập nhật bản vá cho hệ điều hành.**

- Cài đặt phiên bản mới nhất và cập nhật bản vá của hệ điều hành, không mắc các lỗi hỏng bảo mật đã được công bố.

- o Kiểm tra phiên bản kernel với lệnh: “uname -a”. Yêu cầu kernel phải được nâng cấp lên phiên bản mới nhất tính tới thời điểm cài đặt.

- o Trong trường hợp cập nhật bản vá, nâng cấp kernel:

- Trường hợp có kết nối Internet, thực hiện chạy lệnh sau để nâng cấp kernel

```
# yum upgrade kernel
```

- Trường hợp không có kết nối Internet, thực hiện chạy lệnh sau để tiến hành cài đặt:

- Bước 1: Cài đặt 1 máy ảo với hệ điều hành tương ứng với hệ điều hành cần nâng cấp kernel. *Chú ý máy ảo này phải có kết nối Internet.*

- Bước 2: Download toàn bộ các gói cần cài đặt nâng cấp kernel mà distro cung cấp về máy ảo:

```
# mkdir /opt/upgrade
```

```
# yum install yum-downloadonly -y
```

```
# yum install kernel -y --downloadonly --downloadaddir=/opt/upgrade
```



- Bước 3: Tải toàn bộ gói .rpm trong thư mục /opt/upgrade của máy tính lên máy chủ và thực hiện cài như cài gói .rpm như thông thường.

**Lưu ý:** Sau khi cài đặt xong cần khởi động lại máy chủ để hệ điều hành nhận kernel mới.

- Hệ điều hành phải được cập nhật các bản vá security đã được Tập đoàn cảnh báo.

## **2. Xóa hoặc vô hiệu hóa các dịch vụ, ứng dụng, giao thức mạng không cần thiết.**

- Trong thực tế, một server (máy chủ) trong hệ thống sẽ đảm nhiệm một chức năng riêng biệt. Khi cài đặt hệ điều hành cho server, cần xóa hoặc disable tất cả các dịch vụ, ứng dụng, giao thức không cần thiết.

- Bước 1: Liệt kê toàn bộ các gói tin với câu lệnh “yum list”, tìm kiếm các gói tin không cần thiết và thực hiện gỡ bỏ bằng cách sau:

```
# yum remove <package-name>
```

- Bước 2: Liệt kê các dịch vụ đang được chạy ở runlevel 3. Tìm kiếm và xóa bỏ các dịch vụ không cần thiết.

```
# chkconfig --list | grep '3:on'
```

*Tìm kiếm các dịch vụ chạy ở mức độ 3 không sử dụng, tiến hành tắt chúng bằng cách:*

```
# chkconfig <serviceName> off
```

- Bước 3: Kiểm tra các cổng đang mở trên hệ thống và các dịch vụ đang lắng nghe trên các cổng đó, tiến hành tắt các dịch vụ không cần thiết:

```
# netstat -tulpn
```

*Kiểm tra danh sách các dịch vụ không cần thiết, tiến hành tắt các dịch vụ:*

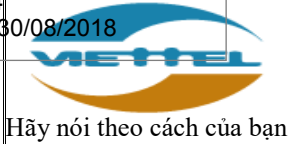
```
# service <serviceName> stop
```

## **3. Thiết lập chính sách tài khoản.**

- Xóa hoặc vô hiệu hóa các tài khoản không sử dụng trên hệ thống.

*Bước 1: Để tìm những tài khoản đang hoạt động trên hệ thống, ta sử dụng lệnh sau:*





**HƯỚNG DẪN THIẾT LẬP AN TOÀN  
THÔNG TIN CHO HỆ ĐIỀU HÀNH  
MÁY CHỦ**

Ngày có hiệu lực: 01/9/2018

Ngày hết hiệu lực: 01/9/2019

Lần ban hành: 05

Trang: 28/71

```
#cat /etc/passwd | grep /*sh$ | awk -F: '{print $1}'
```

*Bước 2: Kiểm tra xem trong danh sách tài khoản hiện ra xem tài khoản nào không sử dụng. Thực hiện xóa các tài khoản đó bằng lệnh sau:*

```
#userdel -r username
```

*Ví dụ: Trong danh sách có tài khoản user1 không sử dụng*

```
#userdel -r user1
```

- **Cấu hình chính sách mật khẩu cho tài khoản:**

- Độ dài tối thiểu của mật khẩu phải lớn hơn hoặc bằng 8 ký tự.

*Bước 1: Mở tập tin /etc/pam.d/system-auth*

```
#vi /etc/pam.d/system-auth
```

*Bước 2: Thêm hoặc cập nhật cấu hình sau trong tập tin cấu hình của PAM:*

```
password requisite pam_cracklib.so [các option trước đó] minlen=8
```

*Bước 3: Lưu lại tập tin cấu hình.*

- Mật khẩu phải chứa ký tự viết hoa, viết thường, chữ số, ký tự đặc biệt.

*Bước 1: Mở tập tin /etc/pam.d/system-auth*

```
#vi /etc/pam.d/system-auth
```

*Bước 2: Thêm hoặc cập nhật cấu hình sau trong tập tin cấu hình của PAM:*

```
password requisite pam_cracklib.so [các option trước đó] ucredit=-1
```

```
lcredit=-1 dcredit=-1 ocredit=-1
```

*Bước 3: Lưu lại tập tin cấu hình.*

- Thời gian bắt buộc phải thay đổi mật khẩu đối với các tài khoản người dùng (monitor, ossec, quantri,...): Thiết lập giá trị 90 ngày với hệ thống public và 180 ngày với hệ thống nội bộ. Ví dụ thiết lập với hệ thống public như sau:

*Mở tập tin /etc/login.defs, thay đổi tùy chọn PASS\_MAX\_DAYS, ví dụ:*

```
PASS_MAX_DAYS 90
```

*Với các tài khoản đã tồn tại, có thể sử dụng lệnh sau để thay đổi thời gian*





**HƯỚNG DẪN THIẾT LẬP AN TOÀN  
THÔNG TIN CHO HỆ ĐIỀU HÀNH  
MÁY CHỦ**

Ngày có hiệu lực: 01/9/2018

Ngày hết hiệu lực: 01/9/2019

Lần ban hành: 05

Trang: 29/71

*hết hạn mật khẩu:*

*#chage -M 90 username*

*Ví dụ, để thay đổi thời gian hết hạn mật khẩu cho tài khoản user1:*

*#chage -M 90 user1*

- Giới hạn mật khẩu mới không được trùng với mật khẩu gần nhất: Thiết lập giá trị là 2 với hệ thống nội bộ và 5 với hệ thống public. Ví dụ thiết lập cho hệ thống nội bộ như sau:

*Bước 1: Mở tập tin /etc/pam.d/system-auth*

*#vi /etc/pam.d/system-auth*

*Bước 2: Thêm hoặc cập nhật cấu hình thuộc tính remember của tùy chọn password sufficient trong tập tin cấu hình của PAM:*

*password sufficient pam\_unix.so [các option trước đó] remember=2*

*Bước 3: Lưu lại tập tin cấu hình.*

- Mã hóa mật khẩu sử dụng thuật toán mã hóa an toàn.

*Bước 1: Kiểm tra thuật toán mã hoá sử dụng:*

*#authconfig --test | grep hashing*

*password hashing algorithm is sha512*

*Bước 2: Nếu thuật toán mã hoá sử dụng không phải là sha512, thực hiện sửa đổi và kiểm tra lại:*

*#authconfig --passalgo=sha512 --update*

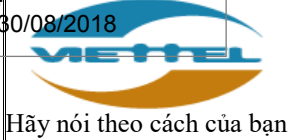
*#authconfig --test | grep hashing*

*password hashing algorithm is sha512*

#### **4. Quản trị từ xa qua kênh truyền an toàn.**

Để đảm bảo yêu cầu bảo mật cho hệ thống, tránh trường hợp thất thoát dữ liệu trên đường truyền khi quản trị hệ thống từ xa yêu cầu thiết lập và sử dụng các dịch vụ quản trị an toàn. Cụ thể nếu sử dụng SSH để quản trị cho Centos 6.x thì thực hiện các thiết lập sau như sau:

- Yêu cầu quản trị từ xa sử dụng kênh truyền an toàn, có mã hóa.



*Bước 1: Mở tập tin cấu hình /etc/ssh/sshd\_config:*

*#vi /etc/ssh/sshd\_config*

*Bước 2: Sửa lại tùy chọn Protocol như bên dưới:*

*Protocol 2*

*Bước 2: Lưu lại tập tin và khởi động lại dịch vụ ssh.*

- Cấu hình giới hạn tài khoản được phép sử dụng dịch vụ quản trị từ xa.

*Bước 1: Mở tập tin cấu hình /etc/ssh/sshd\_config*

*#vi /etc/ssh/sshd\_config*

*Bước 2: Thêm tùy chọn AllowUsers để cấu hình tài khoản được phép truy cập từ xa:*

*AllowUsers username*

*Ví dụ nếu muốn cho phép tài khoản sshuser được phép sử dụng dịch vụ truy cập từ xa, ta cấu hình như sau:*

*AllowUsers sshuser*

*Bước 3: Không cho phép tài khoản root đăng nhập quản trị từ xa.*

*PermitRootLogin no*

*Bước 3: Lưu lại cấu hình và khởi động lại dịch vụ ssh.*

- Giới hạn thời gian tự động ngắt phiên khi không có hoạt động trong một khoảng thời gian là 05 phút.

*Bước 1: Thêm nội dung sau vào cuối cấu hình file /etc/profile*

*TMOUT=300*

*readonly TMOUT*

*export TMOUT*

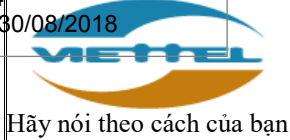
*Bước 2: Khởi động lại dịch vụ ssh*

## 5. Phân quyền tập tin và thư mục.

- Xác thực đường dẫn các biến môi trường PATH:

*Để kiểm tra đường dẫn PATH, ta dùng lệnh sau:*

*#echo \$PATH*



**HƯỚNG DẪN THIẾT LẬP AN TOÀN  
THÔNG TIN CHO HỆ ĐIỀU HÀNH  
MÁY CHỦ**

Ngày có hiệu lực: 01/9/2018  
Ngày hết hiệu lực: 01/9/2019

Lần ban hành: 05

Trang: 31/71

Ví dụ:

*PATH có chứa đường dẫn trống:*

*/usr/local/bin:/usr/sbin:/usr/bin:/sbin:/bin::*

*PATH có chứa đường dẫn tương đối:*

*/usr/local/bin:/usr/sbin:/usr/bin:/sbin:/bin:./src/bin*

*PATH có chứa đường dẫn nguy hiểm:*

*/usr/local/bin:/usr/sbin:/usr/bin:/sbin:/bin:./tmp*

- Thiết lập Cấu hình dịch vụ CRON.

*Bước 1: Thực hiện xóa File cron.deny:*

```
#rm /etc/cron.deny
```

*Bước 2: Thêm File cron.allow nếu hệ thống chưa có:*

```
#touch /etc/cron.allow
```

*Bước 3: Sửa file /etc/cron.allow, cập nhật hoặc thêm các tài khoản được phép sử dụng dịch vụ CRON:*

*User1*

*User2*

*...*

*Bước 4: Hạn chế quyền sửa các file cấu hình của CRON:*

```
#chown root:root /etc/crontab
```

```
#chmod 600 /etc/crontab
```

```
#chown -R root:root /etc/cron.hourly /etc/cron.daily /etc/cron.weekly  
/etc/cron.monthly /etc/cron.d
```

```
#chmod -R go-rwx /etc/cron.hourly /etc/cron.daily /etc/cron.weekly  
/etc/cron.monthly /etc/cron.d
```

## 6. Cài đặt và cấu hình firewall mềm.

- Yêu cầu sử dụng firewall mềm trên hệ thống.

*Kiểm tra chế độ của iptables trên hệ thống để chắc chắn chế độ 3 đang là*



**HƯỚNG DẪN THIẾT LẬP AN TOÀN  
THÔNG TIN CHO HỆ ĐIỀU HÀNH  
MÁY CHỦ**

Ngày có hiệu lực: 01/9/2018  
Ngày hết hiệu lực: 01/9/2019

Lần ban hành: 05

Trang: 32/71

*On (dịch vụ sẽ tự động khởi động cùng hệ điều hành):*

```
# chkconfig --list | grep iptables
```

*Kiểm tra trạng thái hiện tại của iptables:*

```
#service iptables status
```

- Cấu hình tường lửa mềm chỉ mở vừa đủ các kết nối vào/ra trên hệ thống.  
Sử dụng 2 lệnh chính sau:
  - iptables-save: lưu lại toàn bộ rule ra một file text có định dạng đặc biệt
  - iptables-restore: load rule từ file text đã lưu trước đó.

Cú pháp sử dụng:

- Lệnh iptables-save:

```
# iptables-save > /etc/iptables-save
```

Lưu ý: /etc/iptables-save là file lưu lệnh iptables, có thể thay đổi thành file bất kỳ.

- Lệnh iptables-restore:

```
# iptables-restore < /etc/iptables-save
```

Tất cả các rule trong file /etc/iptables-save sẽ được load và áp dụng vào iptables.

Ý nghĩa của file được lưu bởi lệnh iptables-save:

```
# Generated by iptables-save v1.4.7 on Fri Jul 10 22:34:12 2015
```

```
*filter
```

```
:INPUT ACCEPT [0:0]
```

```
:FORWARD ACCEPT [0:0]
```

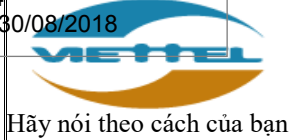
```
:OUTPUT ACCEPT [129895:7030615]
```

```
-A INPUT -m state --state RELATED,ESTABLISHED -j ACCEPT
```

```
-A INPUT -p udp -m state --state NEW -m udp --dport 123 -j ACCEPT
```

```
-A INPUT -p icmp -j ACCEPT
```

```
-A INPUT -i lo -j ACCEPT
```



**HƯỚNG DẪN THIẾT LẬP AN TOÀN  
THÔNG TIN CHO HỆ ĐIỀU HÀNH  
MÁY CHỦ**

Ngày có hiệu lực: 01/9/2018

Ngày hết hiệu lực: 01/9/2019

Lần ban hành: 05

Trang: 33/71

```
-A INPUT -p tcp -m state --state NEW -m tcp --dport 22 -j ACCEPT
-A INPUT -j REJECT --reject-with icmp-host-prohibited
-A FORWARD -j REJECT --reject-with icmp-host-prohibited
COMMIT
# Completed on Fri Jul 10 22:34:12 2015
```

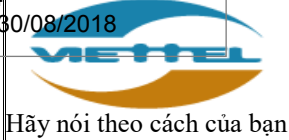
Trong đó:

- “\*filter”: Chỉ bắt đầu các rule của table filter, table dùng để viết các rule lọc gói tin.
- :INPUT ACCEPT [0:0]
  - INPUT: là chain của iptables, table filter có 3 chain là INPUT, OUTPUT, FORWARD. Trong đó INPUT là thời điểm gói tin đi vào hệ thống, OUTPUT là thời điểm gói tin đi ra hệ thống, còn FORWARD là thời điểm gói tin đi từ card mạng này sang card mạng khác.
  - ACCEPT: Chain policy của chain INPUT, OUTPUT và FORWARD. Ý nghĩa: Nếu gói tin sau khi được kiểm tra bởi tất cả các rule của iptables mà không có rule nào khớp thì sẽ được ACCEPT.
  - [0:0]: Số đầu tiên chỉ ra số lượng gói tin, số thứ 2 chỉ ra dung lượng của các gói tin. Đây là các thông số thống kê về các gói tin không khớp luật nào của iptables, và do đó được thực hiện Chain policy là ACCEPT.
- Các rule tiếp theo: Là rule lọc của iptables, sẽ áp dụng từ trên xuống dưới.
- COMMIT: Đánh dấu kết thúc bảng filter.

Cách sửa luật iptables:

Tạo một file có nội dung như sau, ví dụ là /etc/sysconfig/iptables:

```
# Firewall configuration written by system-config-firewall
# Manual customization of this file is not recommended.
```



**HƯỚNG DẪN THIẾT LẬP AN TOÀN  
THÔNG TIN CHO HỆ ĐIỀU HÀNH  
MÁY CHỦ**

Ngày có hiệu lực: 01/9/2018  
Ngày hết hiệu lực: 01/9/2019

Lần ban hành: 05

Trang: 34/71

*\*filter*

*:INPUT ACCEPT [0:0]*

*:FORWARD ACCEPT [0:0]*

*:OUTPUT ACCEPT [0:0]*

*### Cho phép các gói tin thuộc 1 kết nối đang tồn tại hoặc có liên quan đến 1 connection đang tồn tại đi vào, không cần kiểm tra ###*

*-A INPUT -m state --state ESTABLISHED,RELATED -j ACCEPT*

*-A OUTPUT -m state --state ESTABLISHED,RELATED -j ACCEPT*

*### Cho phép ping echo request đến server ###*

*-A INPUT -p icmp --icmp-type 8 -j ACCEPT*

*### Nhưng gói tin từ card mạng loopback thì không cần lọc ###*

*-A INPUT -i lo -j ACCEPT*

*### Thêm nhưng luật lọc chiều INPUT tại đây ###*

*# Ví dụ luật cho phép 1 IP hay 1 dải IP SSH đến server #*

*-A INPUT -m state --state NEW -s 192.168.1.190 -m tcp -p tcp --dport 22 -j ACCEPT*

*-A INPUT -m state --state NEW -s 192.168.2.0/24 -m tcp -p tcp --dport 22 -j ACCEPT*

*# Ví dụ luật cho phép HTTP #*

*-A INPUT -m state --state NEW -m tcp -p tcp --dport 80 -j ACCEPT*

*### Thêm các luật lọc chiều OUTPUT tại đây ###*

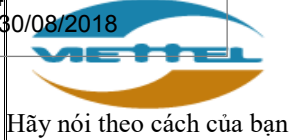
*### Chỉ khi server cần chủ động kết nối ra bên ngoài mới thêm luật tiếp theo ###*

*# Ví dụ luật cho phép server hiện tại ssh đến server 10.10.10.10 #*

*-A OUTPUT -m state --state NEW -d 10.10.10.10 -m tcp -p tcp --dport 22 -j ACCEPT*

*### Chặn toàn bộ các kết nối còn lại, ghi log trước khi chặn ###*





**HƯỚNG DẪN THIẾT LẬP AN TOÀN  
THÔNG TIN CHO HỆ ĐIỀU HÀNH  
MÁY CHỦ**

Ngày có hiệu lực: 01/9/2018

Ngày hết hiệu lực: 01/9/2019

Lần ban hành: 05

Trang: 35/71

```
-A INPUT -j LOG --log-level 4 --log-prefix "IPTABLES DROP"
-A FORWARD -j LOG --log-level 4 --log-prefix "IPTABLES DROP"
-A OUTPUT -j LOG --log-level 4 --log-prefix "IPTABLES DROP"
-A INPUT -j REJECT --reject-with icmp-host-prohibited
-A FORWARD -j REJECT --reject-with icmp-host-prohibited
-A OUTPUT -j REJECT --reject-with icmp-host-prohibited
COMMIT
```

Cách cấu hình để iptables nạp các rule khi server khởi động lại:

Thêm dòng sau vào cuối file /etc/rc.local:

```
iptables-restore < /etc/sysconfig/iptables
```

Cách tạm thời tắt tất cả các luật của iptables để troubleshoot:

Sử dụng các lệnh sau:

```
# iptables -F
# iptables -X
# iptables -P INPUT ACCEPT
# iptables -P OUTPUT ACCEPT
# iptables -P FORWARD ACCEPT
```

Ý nghĩa các lệnh:

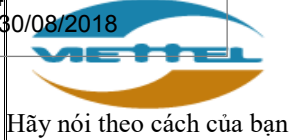
- Lệnh đầu tiên để xóa tất cả các rule trong tất cả các chain của iptables
- Lệnh thứ 2 xóa tất cả các chain do người dùng tự tạo
- Lệnh 3,4,5 thiết lập chain policy cho chain INPUT, OUTPUT, FORWARD là ACCEPT, khi đây server cho phép toàn bộ kết nối vào/ra server.

- Ghi log những bản ghi vào/ra không hợp lệ.

Lưu ý thêm các dòng sau vào file cấu hình iptables:

```
-A INPUT -j LOG --log-level 4 --log-prefix "IPTABLES DROP"
-A FORWARD -j LOG --log-level 4 --log-prefix "IPTABLES DROP"
```





***-A OUTPUT -j LOG --log-level 4 --log-prefix "IPTABLES DROP"***

## 7. Thiết lập chính sách quản lý log.

Ghi log các hành vi quan trọng của máy chủ: Yêu cầu thiết lập cấu hình ghi log tối thiểu các loại sau: message log, dmesg log, secure log.

Cấu hình rotate log tối đa là 1 lần/tháng.

- Bước 1: Cấu hình nội dung tập tin /etc/rsyslog.conf với nội dung sau:

```
$ModLoad imuxsock # provides support for local system logging (e.g. via  
logger command)  
$ModLoad imklog # provides kernel logging support (previously done  
by rklogd)  
$ActionFileDefaultTemplate RSYSLOG_TraditionalFileFormat  
$IncludeConfig /etc/rsyslog.d/*.conf  
*.info;mail.none;authpriv.none;cron.none  
authpriv.*  
mail.*  
cron.*  
*.emerg  
uucp,news.crit  
local7.*
```

- Bước 2: Cấu hình nội dung tập tin /etc/logrotate.conf với nội dung sau:

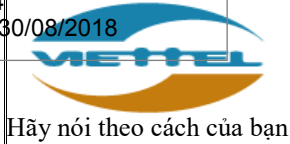
```
weekly  
rotate 12  
create  
dateext  
include /etc/logrotate.d  
/var/log/wtmp {
```



```
monthly
create 0664 root utmp
minsize 1M
rotate 3
}
/var/log/btmp {
missingok
monthly
create 0600 root utmp
rotate 3
}
```

- Bước 3: Cấu hình log cho các tập tin message log, syslog, kernel.log... như sau:

```
- Tạo tập tin syslog trong /etc/logrotate.d/
#vi /etc/logrotate.d/syslog
- Sửa nội dung tập tin thành:
/var/log/cron
/var/log/maillog
/var/log/messages
/var/log/secure
/var/log/spooler
{
sharedscripts
postrotate
/bin/kill -HUP `cat /var/run/syslogd.pid 2> /dev/null` 2> /dev/null
}
|| true
```



*endscript*

}

○ Bước 4: Khởi động lại dịch vụ log:

```
#/etc/init.d/rsyslog restart
```

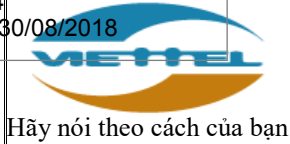
*Shutting down system logger:*

[ OK ]

*Starting system logger:*

[ OK ]

- Kiểm tra đảm bảo tất cả các sự kiện quan trọng đều được ghi lại log. Quản trị viên có thể phân nhóm các sự kiện và ghi ra thành các tập tin riêng biệt để thuận tiện trong việc theo dõi và giám sát.
- Trên CentOS 6.4, có 2 dịch vụ log được sử dụng, là syslog và rsyslog. Tuy nhiên syslog có nhiều hạn chế trong việc lưu trữ từ xa an toàn, do vậy rsyslog được khuyến nghị sử dụng.
- Cấu hình các sự kiện ghi log được lưu trong tập tin /etc/syslog.conf đối với syslog và /etc/rsyslog.conf đối với rsyslog.
- Syslog và rsyslog hỗ trợ nhiều loại log hệ thống với nhiều mức log, cụ thể như sau:
  - kern – kernel
  - user – log các ứng dụng của người dùng
  - mail/news/UUCP/cron – Email/NNTP/UUCP/cron
  - daemon – system daemons
  - auth – log liên quan tới xác thực người dùng
  - lpr – log liên quan đến dịch vụ in
  - mark – thêm timestamp vào dữ liệu log
  - local0-local7-8 log cho các tùy chọn kiểm tra, thanh tra
  - syslog – các log khác của dịch vụ syslog
  - authpriv – các log xác thực không thuộc hệ thống



- Log hệ điều hành có các mức: emerg, alert, crit, warning, notice, info, debug.
- Đồng bộ thời gian HĐH về máy chủ tập trung.

*Bước 1: Cài đặt:*

- Đối với máy chủ có kết nối Internet:

*# yum install ntp*

- Đối với máy chủ không có kết nối Internet:

*Download gói ntp dạng rpm: ntp-4.2.6p5-1.el6.centos*

*Copy gói cài đặt lên máy chủ, chuyển tới thư mục chứa tập tin và chạy lệnh:*

*#rpm -ivh {Tên tập tin}*

*Bước 2: Cấu hình dịch vụ NTP*

- Cấu hình dịch vụ ntpd luôn chạy khi khởi động máy chủ:

*#chkconfig ntpd on*

- Sửa tập tin cấu hình /etc/ntp.conf như sau:

*restrict default kod nomodify notrap nopeer noquery*

*restrict -6 default kod nomodify notrap nopeer noquery*

*restrict 127.0.0.1*

*restrict -6::1*

*server ntp-server*

- Đảm bảo file cấu hình ntp có cấu hình tham số server, trong đó tham số ntp-server là hostname hoặc địa chỉ IP của NTP server.

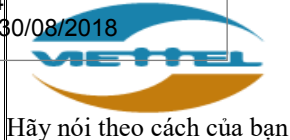
- Chạy dịch vụ ntpd và khởi động lại dịch vụ iptables bằng lệnh:

*#service ntpd start*

*#service iptables restart*

- Kiểm tra lại dịch vụ bằng lệnh:

*#netstat -tulpn | grep ntpd*



## 8. Cài đặt các phần mềm giám sát ATTT

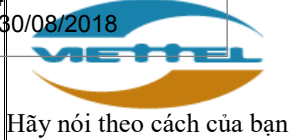
Yêu cầu cài đặt đầy đủ các phần mềm giám sát ATTT do TT.ANM cung cấp

- Phần mềm Server Endpoint để hỗ trợ giám sát hành vi bất thường và vi phạm baseline.

Hướng dẫn cài đặt: [http://docs.sirc.viettel.com/guide/install\\_se\\_agent/](http://docs.sirc.viettel.com/guide/install_se_agent/)

- Phần mềm Filebeat và OSSEC agent để hỗ trợ lấy log và event.

Hướng dẫn cài đặt: <http://docs.sirc.viettel.com/guide/LogAgent/>



## HƯỚNG DẪN THIẾT LẬP CẤU HÌNH BẢO MẬT CHO HỆ ĐIỀU HÀNH SOLARIS

### I. Nội dung hướng dẫn

Hướng dẫn thiết lập an toàn cho hệ điều hành SOLARIS nhằm đảm bảo 8 tiêu chuẩn ATTT bao gồm:

- Cài đặt và cập nhật bản vá cho hệ điều hành.
- Hệ thống chỉ chạy các phần mềm tối thiểu đúng với chức năng được thiết kế
- Thiết lập chính sách tài khoản.
- Quản trị từ xa qua kênh truyền an toàn.
- Phân quyền tập tin và thư mục.
- Cài đặt và cấu hình firewall mềm.
- Thiết lập chính sách quản lý log.
- Cài đặt phần mềm giám sát ATTT.

### II. Chi tiết hướng dẫn

#### 1. Cài đặt hệ điều hành và cập nhật bản vá.

##### **Yêu cầu khắc phục:**

- + Cài đặt phiên bản mới nhất tại khi cài đặt mới.
- + Cập nhật các bản vá lỗi cho hệ điều hành: Bao gồm các bản vá lỗ hổng bảo mật đã được công bố và các bản vá theo yêu cầu của Tập đoàn.

##### **Chú ý:**

- + Yêu cầu này chỉ áp dụng với các hệ thống đã mua bản quyền hệ điều hành Solaris.
- + Thực hiện backup hệ thống trước khi cập nhật bản vá để giảm thiểu rủi ro.

#### 2. Hệ thống chỉ chạy các phần mềm tối thiểu đúng với chức năng được thiết kế.

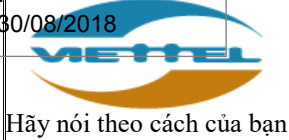
##### **Yêu cầu khắc phục:**

- + Cài đặt tối thiểu các phần mềm, dịch vụ theo đúng chức năng được thiết kế của server.
- + Gỡ bỏ hoặc vô hiệu hóa các gói dịch vụ không cần thiết, các gói dịch vụ lỗi thời có nguy cơ bị mất an toàn thông tin: Telnet, rcp, rsh, rlogin, nis, ftp...
- + Kiểm tra các dịch vụ đang chạy trên hệ điều hành. Nếu dịch vụ nào không cần thiết chạy thì thực hiện vô hiệu hóa hoặc xóa bỏ.

***Phương án 1: Vô hiệu hóa dịch vụ không cần thiết.***

***# svc -a***

***# svcadmin disable < Tên dịch vụ cần tắt >***



Ví dụ: # svcadmin disable network/telnet

**Phương án 2:** Gỡ bỏ dịch vụ không cần thiết.

# pkgrm <Tên gói cần xóa>

### 3. Thiết lập chính sách tài khoản.

#### 3.1. Xóa hoặc vô hiệu tất cả các tài khoản không sử dụng trên hệ thống.

- **Yêu cầu khắc phục:** Rà soát hệ thống, liệt kê những tài khoản đang hoạt động trên hệ thống rồi tìm và xóa hoặc vô hiệu những tài khoản không sử dụng ra khỏi hệ thống.

**Bước 1:** Để tìm những tài khoản đang hoạt động trên hệ thống, ta sử dụng lệnh sau:

```
# passwd -s -a | grep PS
```

**Bước 2:** Kiểm tra xem các tài khoản này tài khoản nào không sử dụng. Thực hiện 1 trong 2 phương án:

**Phương án 1:** Vô hiệu các tài khoản:

```
# passwd -l username
```

**Phương án 2:** Xóa tài khoản:

```
# userdel username
```

Ví dụ: Trong danh sách có tài khoản game không sử dụng

```
# userdel game
```

#### 3.2. Cấu hình chính sách mật khẩu cho tài khoản.

##### 3.2.1. Mật khẩu phải có độ dài tối thiểu 8 ký tự chứa ký tự viết hoa, viết thường, chữ số, ký tự đặc biệt.

- **Yêu cầu khắc phục:** Mật khẩu có độ dài tối thiểu 8 ký tự, đảm bảo phải bao gồm ký tự viết hoa, viết thường, chữ số, ký tự đặc biệt.

```
# chmod u+w /etc/default/passwd
```

```
# export EDITOR=vi
```

```
# vi /etc/default/passwd
```

```
PASSLENGTH=8
```

```
MINALPHA=1
```

```
chữ)
```

(yêu cầu mật khẩu phải có ít nhất 8 ký tự)

(yêu cầu mật khẩu phải có ít nhất 1 ký tự





HƯỚNG DẪN THIẾT LẬP AN TOÀN  
THÔNG TIN CHO HỆ ĐIỀU HÀNH  
MÁY CHỦ

Ngày có hiệu lực: 01/9/2018

Ngày hết hiệu lực: 01/9/2019

Lần ban hành: 05

Trang: 43/71

*MINDIGIT=1 (yêu cầu mật khẩu phải có ít nhất 1 ký tự số)*  
*MINSPECIAL=1 (yêu cầu mật khẩu phải có ít nhất 1 ký tự đặc biệt)*  
*MINUPPER=1 (yêu cầu mật khẩu phải có ít nhất 1 ký tự hoa)*  
*# chmod u-w /etc/default/passwd*

**Chú ý:** Nếu không có quyền sửa file /etc/default/passwd thì gõ lệnh sau để có quyền sửa file:

*# chmod u+w /etc/default/passwd*

### 3.2.2. Thời gian bắt buộc phải thay đổi mật khẩu người dùng.

- **Yêu cầu khắc phục:** đối với các tài khoản người dùng (monitor, ossec, quantri,...): thiết lập thời gian tối đa bắt buộc tối đa 3 tháng (90 ngày) với hệ thống public, 180 ngày với hệ thống nội bộ.

- Thay đổi giá trị MAXWEEKS=13 trong file /etc/default/passwd. Thực hiện như sau:

*# chmod u+w /etc/default/passwd*  
*# export EDITOR=vi*  
*# vi /etc/default/passwd*  
*MAXWEEKS=13*  
*# chmod u-w /etc/default/passwd*  
*# passwd -s -a | grep PS*  
*# passwd -x 91 <user\_name>*

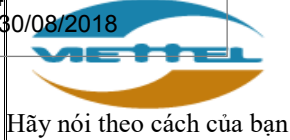
- **Chú ý:**

+ Trong file /etc/default/passwd không có tùy chọn MAXDAY=90 do vậy với tùy chọn MAXWEEKS=13 sẽ tương đương với thời hạn hết hạn mật khẩu là 91 ngày.

+ Câu lệnh passwd -s -a | grep PS có ý nghĩa liệt kê toàn bộ tài khoản có khả năng đăng nhập vào hệ thống. Một số tài khoản đang bị khóa hoặc không có quyền đăng nhập vào hệ thống sẽ không được liệt kê.

### 3.2.3. Giới hạn mật khẩu mới không được trùng với mật khẩu gần nhất.

- **Yêu cầu khắc phục:** Đối với mật khẩu người dùng, thiết lập bắt buộc mật khẩu mới phải không trùng với 5 mật khẩu gần nhất.



Thay đổi giá trị HISTORY=5 trong file /etc/default/passwd. Thực hiện như sau:

```
# chmod u+w /etc/default/passwd
# export EDITOR=vi
# vi /etc/default/passwd
HISTORY=5
```

### 3.2.4. Mật khẩu phải được lưu dưới dạng mã hóa sử dụng thuật toán băm SHA-512.

- **Yêu cầu khắc phục:** Kiểm tra và nâng cấp phương thức mã hóa mật khẩu, sử dụng thuật toán băm SHA-512.

Thực hiện 02 lệnh sau để đảm bảo hệ thống có hỗ trợ thuật toán băm sha-512.

```
# cat /etc/security/policy.conf | grep CRYPT_ALGORITHMS_ALLOW | grep -v ^#
```

Kết quả trả về : CRYPT\_ALGORITHMS\_ALLOW=1,2a,md5,5,6

```
# cat /etc/security/crypt.conf | grep crypt_sha512
```

Kết quả trả về : 6 crypt\_sha512.so.1

- Nếu kết quả trả về giống như ví dụ trên thì hệ điều hành có hỗ trợ mã hóa sha-512. Thực hiện các bước sau để thiết lập lưu password dưới dạng thuật toán băm sha-512:

Lưu password dưới dạng thuật toán băm sha-512. Thực hiện sửa hoặc thêm tùy chọn sau vào file /etc/security/policy.conf. Cụ thể:

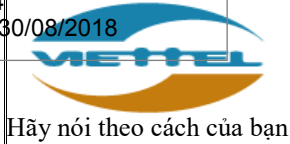
```
# export EDITOR=vi
# vi /etc/security/policy.conf
CRYPT_DEFAULT=6
```

#### - **Chú ý:**

- + Sau khi thiết lập tham số phải đăng nhập thử vào hệ thống. Nếu không đăng nhập được nghĩa là hệ thống không hỗ trợ thuật toán mã hóa SHA-512. Phải cấu hình tham số "CRYPT\_DEFAULT=MD5" nghĩa là sử dụng thuật toán MD5 để thay thế.
- + Với những tài khoản đang tồn tại trên hệ thống phải thực hiện các bước sau để chính sách được áp dụng:

#### 1. Liệt kê danh sách mật khẩu

```
# passwd -s -a | grep PS
```



2. Xóa mật khẩu cũ của tài khoản  
*# password -d username*
3. Đặt lại mật khẩu mới cho tài khoản  
*# passwd username*
4. Buộc người dùng phải đổi mật khẩu ở lần đăng nhập tiếp theo  
*# passwd -f username*

#### 4. Quản trị từ xa qua kênh truyền an toàn.

- **Yêu cầu khắc phục:** Để đảm bảo an toàn yêu cầu chỉ sử dụng công cụ quản trị từ xa có mã hóa đường truyền. Chỉ sử dụng SSH để quản trị máy chủ, khi sử dụng SSH cần thực hiện các thiết lập sau (*Yêu cầu khởi động lại dịch vụ SSH khi thiết lập xong cấu hình*):

##### 4.1. Yêu cầu quản trị từ xa sử dụng kênh truyền an toàn, có mã hóa.

**Chỉ cho phép sử dụng giao thức SSH version 2.**

Mở file cấu hình */etc/ssh/sshd\_config*, sửa lại tùy chọn:  
*Protocol 2*

**Cấu hình chỉ cho phép tài khoản người dùng được phép SSH.**

Mở file cấu hình */etc/ssh/sshd\_config*, thêm tùy chọn sau:  
*AllowUsers user1 user2*

**Không cho phép tài khoản root đăng nhập trực tiếp từ xa.**

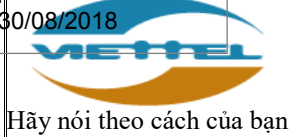
Mở file cấu hình */etc/ssh/sshd\_config*, sửa hoặc thêm tùy chọn sau:  
*PermitRootLogin no*

##### 4.2. Không cho phép tài khoản đăng nhập sai là 05 lần.

Mở file cấu hình */etc/default/login*, sửa hoặc thêm tùy chọn sau:  
*RETRIES=5*

##### 4.3. Thiết lập thời gian tự động ngắt phiên nếu phiên không có hoạt động trong 5 phút.

Mở file cấu hình */etc/profile*, thêm 3 dòng sau vào cuối file:



*TMOUT=300*

*readonly TMOUT*

*export TMOUT*

## 5. Phân quyền tệp tin và thư mục.

### 5.1. Biến môi trường \$PATH không được chứa các đường tương đối, đường dẫn bất thường, đường dẫn trống.

- **Yêu cầu khắc phục:** Kiểm tra biến môi trường PATH không được chứa các đường tương đối, đường dẫn bất thường, đường dẫn trống.

Để kiểm tra biến môi trường PATH, ta dùng lệnh sau:

```
# echo $PATH
```

Ví dụ:

PATH	chứa	đường	dẫn	trống:	PATH
/usr/local/bin:/usr/sbin:/usr/bin:/sbin:/bin:					

PATH	chứa	đường	dẫn	tương	đối:
/usr/local/bin:/usr/sbin:/usr/bin:/sbin:/bin:/src/bin					

PATH	chứa	đường	dẫn	nguy	hiểm:	/bin:/us:
/usr/local/bin:/usr/sbin:/usr/bin:/sbin:/bin:/tmp						

### 5.2. Thiết lập cấu hình dịch vụ CRON.

- **Yêu cầu khắc phục:**

+ Giới hạn tài khoản được phép chạy dịch vụ CRON bởi whitelist danh sách người dùng.

▪ Bước 1: Thực thi lệnh xóa file cron.deny:

```
# rm /etc/cron.d/cron.deny
```

▪ Bước 2: Thêm file cron.allow nếu hệ thống chưa có:

```
#touch /etc/cron.d/cron.allow
```

▪ Bước 3: Sửa file /etc/cron.allow, cập nhật hoặc thêm các tài khoản được phép sử dụng dịch vụ CRON:

User1

User2

...

+ Hạn chế quyền sửa các file cấu hình của CRON



```
# chown -R root:root /var/spool/cron/crontabs/  
# chmod -R 600 /var/spool/cron/crontabs/  
# chown -R root:root /etc/cron.d  
# chmod -R go-rwx /cron.d
```

## 6. Cấu hình tường lửa mềm.

### 6.1. Yêu cầu sử dụng tường lửa mềm trên hệ thống

- **Yêu cầu khắc phục:** Kiểm tra đảm bảo tường lửa mềm được bật.

```
# svcs -a | grep ipf  
online 10:06:55 svc:/network/ipfilter:default
```

- Nếu câu lệnh trả về có giá trị là "online" thì dịch vụ đang được bật, Ngược lại nghĩa là tường lửa chưa được bật. Và phải cấu hình rule và bật theo các mục bên dưới.

### 6.2. Giới hạn địa chỉ IP quản trị được phép truy cập đến máy chủ.

### 6.3. Cấu hình tường lửa mềm chỉ mở vừa đủ các kết nối vào/ra trên hệ thống.

- **Yêu cầu khắc phục:** Sử dụng tường lửa chỉ mở kết nối giới hạn.

- + Đối với hệ thống nội bộ:

- Chỉ mở vừa đủ các kết nối vào (Chiều INPUT).

- + Đối với hệ thống public:

- Yêu cầu mở vừa đủ các kết nối vào (Chiều INPUT).

- Yêu cầu mở vừa đủ các kết nối ra (Chiều OUTPUT).

- **Chú ý:** Người quản trị cần phải cấu hình tường lửa ở chế độ ghi log các gói tin trong vòng 1-2 tuần. Sau đó sẽ phân tích logs và thiết lập rule tương ứng. Thực hiện theo "Hướng dẫn cấu hình ipfilter cho Solaris".

### 6.4. Ghi log toàn bộ những bản tin vào ra không hợp lệ.

- **Yêu cầu khắc phục:** Ghi toàn bộ log vào/ra hệ thống không hợp lệ. Thực hiện theo "Hướng dẫn cấu hình ipfilter cho Solaris".

## 7. Thiết lập chính sách quản lý log.

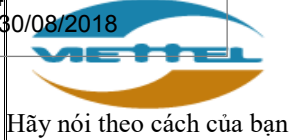
### 7.1. Ghi log mặc định của hệ điều hành.

- **Yêu cầu khắc phục:** Yêu cầu thiết lập cấu hình ghi log tối thiểu các loại sau: message log, dmesg log, secure log.

- Bước 1: Cấu hình log đăng nhập failed:

```
# export EDITOR=vi  
# vi /etc/default/login  
SYSLOG_FAILED_LOGINS=0
```





```
# touch /var/adm/authlog
```

- Bước 2: Thêm vào đầu file /etc/syslog.conf dòng sau:

```
# export EDITOR=vi  
# vi /etc/syslog.conf  
auth.notice;auth.crit;auth.info /var/adm/authlog
```

- Bước 3: Resart lại dịch vụ syslog:

```
# svcadm disable system/system-log  
# svcadm enable system/system-log
```

Kiểm tra lại trạng thái của dịch vụ system-log xem đã chắc chắn được bật chưa. Sử dụng câu lệnh sau:

```
# svcs system-log  
STATE      STIME      FMRI  
online      15:13:31   svc:/system/system-log:default
```

Nếu có STATE là "Online" nghĩa là dịch vụ đang hoạt động bình thường.

## 7.2. Cấu hình thời gian lưu log tối thiểu là 3 tháng.

- **Yêu cầu khắc phục:** Thiết lập cấu hình thời gian lưu log tối thiểu 03 tháng.

Mở file /etc/logadm.conf, kiểm tra cấu hình sẵn có và thêm vào cấu hình cho các file log /var/log/firewall, /var/adm/messages như sau:

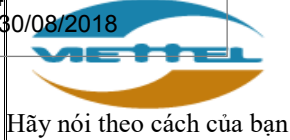
```
# export EDITOR=vi  
# vi /etc/logadm.conf  
/var/adm/messages -A 3m -C 10 -s 10m -z 0 -a 'kill -HUP `cat  
/var/run/syslog.pid`'  
/var/log/firewall -A 3m -C 10 -s 10m -z 0 -a 'kill -HUP `cat  
/var/run/syslog.pid`'
```

### Trong đó:

- A là số ngày tối đa lưu file logs đơn vị là "h" chỉ số giờ, "d" chỉ số ngày, "m" chỉ số tháng, "y" chỉ số năm.
- C là số file log cũ tối đa sẽ giữ lại.
- s là kích cỡ tối đa 1 file logs (ở đây là 10 MB).

**Chú ý:** Theo quy định của Tập đoàn thời gian tối thiểu lưu log là 3 tháng. Tuy nhiên nếu máy chủ hiện tại không đủ dung lượng ổ cứng để lưu log trong 3 tháng. Còn số này quản trị có thể thiết lập lại để phù hợp với thực tế tránh log đầy làm treo máy chủ.

- Bước 1: Kiểm tra lại kết quả



```
# logadm -V
```

- Bước 2: Kiểm tra logadm đã có trong crontab chưa

```
# crontab -l
```

- Nếu kết quả trả về chưa có dòng **"10 3 \* \* \* /usr/sbin/logadm"** thì thực hiện câu lệnh sau để thêm vào.

```
# export EDITOR=vi
```

```
# crontab -e
```

```
10 3 * * * /usr/sbin/logadm
```

- Bước 3: Thêm dòng bên dưới vào tệp tin **/etc/syslog.conf**

```
local0.debug /var/log/firewall
```

- Bước 4: Tạo file firewall bằng câu lệnh sau

```
# touch /var/log/firewall
```

```
# chmod 600 /var/log/firewall
```

- Bước 5: Restart lại dịch vụ syslog

```
# svcadm restart system-log
```

### 7.3. Đồng bộ thời gian HĐH về máy chủ tập trung.

- **Yêu cầu khắc phục:** Bật dịch vụ NTP để đồng bộ thời gian từ máy chủ thời gian chuẩn.

- + **Cách 1: Đồng bộ bằng dịch vụ ntp.**

- Bước 1: Tạo file **/etc/inet/ntp.conf**

```
# cp /etc/inet/ntp.client /etc/inet/ntp.conf
```

- Bước 2: Sửa file **/etc/inet/ntp.conf**

- Thay thế **multicastclient** **224.0.1.1**
- Bằng **server 192.168.181.50**

- Bước 3: Chạy dịch vụ ntpd và khởi động lại dịch vụ bằng lệnh:

```
# service disable network/ntp
```

```
# service enable network/ntp
```

Kiểm tra việc đồng bộ có thành công hay không, sử dụng lệnh:

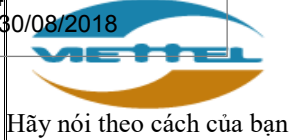
```
# ntpq -p
```

```
remote refid st t when poll reach delay offset disp
```

```
=====
```

```
=====
```





192.168.181.50 0.0.0.0 2 u 21 64 3 376.54 -71.105 7889.14

+ **Cách 2: Đồng bộ bằng crontab (Yêu cầu máy chủ phải cài đặt chương trình ntpdate).**

■ Bước 1: Sửa crontab của root.

```
# export EDITOR=vi
# crontab -e
# Bổ sung một crontab
*/5 * * * * ntpdate -u 192.168.181.50
```

## 8. Cài đặt các phần mềm giám sát ATTT

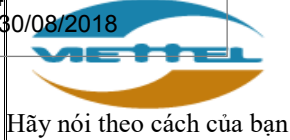
Yêu cầu cài đặt đầy đủ các phần mềm giám sát ATTT do TT.ANM cung cấp

- Phần mềm Server Endpoint để hỗ trợ giám sát hành vi bất thường và vi phạm baseline.

Hướng dẫn cài đặt: [http://docs.sirc.viettel.com/guide/install\\_se\\_agent/](http://docs.sirc.viettel.com/guide/install_se_agent/)

- Phần mềm Filebeat và OSSEC agent để hỗ trợ lấy log và event.

Hướng dẫn cài đặt: <http://docs.sirc.viettel.com/guide/LogAgent/>



## HƯỚNG DẪN THIẾT LẬP CẤU HÌNH BẢO MẬT CHO HỆ ĐIỀU HÀNH IBM AIX

### I. Nội dung hướng dẫn

Hướng dẫn thiết lập an toàn cho hệ điều hành IBM AIX nhằm đảm bảo 8 tiêu chuẩn ATTT bao gồm:

- Cài đặt và cập nhật bản vá cho hệ điều hành.
- Xóa hoặc vô hiệu hóa các dịch vụ, ứng dụng, giao thức mạng không cần thiết.
- Thiết lập chính sách tài khoản.
- Quản trị từ xa qua kênh truyền an toàn.
- Phân quyền tập tin và thư mục.
- Cài đặt và cấu hình firewall mềm.
- Thiết lập chính sách quản lý log.
- Cài đặt phần mềm giám sát ATTT.

### II. Chi tiết hướng dẫn

#### 1. Cài đặt hệ điều hành và cập nhật bản vá.

##### Yêu cầu:

- Cài đặt phiên bản mới nhất khi cài đặt mới.
- Cập nhật các bản vá lỗi cho hệ điều hành: Bao gồm các bản vá lỗ hổng bảo mật đã được công bố và các bản vá theo yêu cầu của Tập đoàn.

#### 2. Xóa hoặc vô hiệu hóa các dịch vụ, ứng dụng, giao thức mạng không cần thiết

##### Yêu cầu:

- Cài đặt tối thiểu các phần mềm, dịch vụ theo đúng chức năng được thiết kế của server.
- Gỡ bỏ hoặc vô hiệu hóa các gói dịch vụ không cần thiết, các gói dịch vụ lỗi thời có nguy cơ bị mất an toàn thông tin: Telnet, rcp, rsh, rlogin, nis, ftp...

##### Hướng dẫn:

- Bước 1: Xác định các dịch vụ đang hoạt động

```
# lssrc -a | grep active
```

- Bước 2: Xác định các dịch vụ thừa, không cần thiết để disable

```
# stopsrv -s <service>
```

- Nếu trong trường hợp dịch vụ là một trong những dịch vụ con của inetd thì thực hiện như sau:

```
# vi /etc/inetd.conf
```

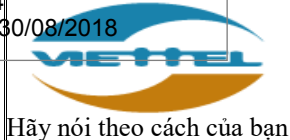
*Comment dòng bên dưới (thêm dấu # vào đầu dòng tương ứng với service), ví dụ :*

```
telnet stream tcp6 nowait root /usr/sbin/telnetd telnetd -a
```

*Restart lại dịch vụ inetd:*

```
# refresh -s inetd
```

#### 3. Thiết lập chính sách tài khoản



**HƯỚNG DẪN THIẾT LẬP AN TOÀN  
THÔNG TIN CHO HỆ ĐIỀU HÀNH  
MÁY CHỦ**

Ngày có hiệu lực: 01/9/2018

Ngày hết hiệu lực: 01/9/2019

Lần ban hành: 05

Trang: 52/71

- Xóa hoặc vô hiệu tất cả các tài khoản không sử dụng trên hệ thống
  - + Bước 1: Để tìm những tài khoản đang hoạt động trên hệ thống, ta sử dụng lệnh sau:

```
#lsuser ALL | awk '{print $1}'
```

- + Bước 2: Kiểm tra xem trong các tài khoản này tài khoản nào không sử dụng thì thực hiện khóa các tài khoản đó bằng lệnh sau:

```
#chuser account_locked=true <username>
```

- Cấu hình chính sách mật khẩu cho tài khoản

- + Mật khẩu phải có độ dài tối thiểu 8 ký tự, chứa ký tự viết hoa, viết thường, chữ số, ký tự đặc biệt

```
#vi /etc/security/user
    minalpha = 5 (yêu cầu mật khẩu có ít nhất 5 kí tự là chữ)
    minother = 3 (yêu cầu mật khẩu có ít nhất 3 kí tự đặc biệt)
    minlen = 8 (yêu cầu mật khẩu có ít nhất 8 ký tự)
```

- + Thời gian bắt buộc phải thay đổi mật khẩu người dùng: Thiết lập giá trị 90 ngày với hệ thống public và 180 ngày với hệ thống nội bộ.

Ví dụ thiết lập với hệ thống public: Thay đổi giá trị maxage = 13 và giá trị maxexpired = -1 trong file /etc/security/user. Thực hiện như sau:

```
#vi /etc/security/user
    maxage = 13
    maxexpired = -1
```

**Chú ý:** Trong file /etc/security/user, giá trị maxage = 13 (tuần) sẽ tương đương với thời hạn hết hạn mật khẩu là =< 90 ngày.

- + Giới hạn mật khẩu mới không được trùng với mật khẩu gần nhất: Thiết lập giá trị là 2 với hệ thống nội bộ và 5 với hệ thống public.

Ví dụ thiết lập cho hệ thống public: Thay đổi giá trị histsize = 5 trong file /etc/security/user. Thực hiện như sau:

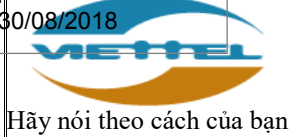
```
#vi /etc/security/user
    histsize = 5
```

- + Mã hóa mật khẩu sử dụng thuật toán mã hóa an toàn (SHA-512/MD5)

- Sử dụng lệnh sau để kiểm tra OS và TL (Technology Level):

```
#oslevel -r
<OS Ver>-<TL>-<SP>-<BUILD DATE>
```

- Nếu tham số TL>7 sẽ thực hiện các bước thiết lập mã hóa mật khẩu bằng SHA-512 bên dưới, nếu không ta bỏ qua. Ví dụ: #oslevel -r cho kết quả: 5300-02-07-2012. Tức là OS version=5.3, TL=2, build tuần thứ 07 của năm 2012, TL < 7 nên ta bỏ qua phần thiết lập mã hóa mật khẩu.
      - Nếu tham số TL>7, thực hiện lệnh sau để xem hệ điều hành có hỗ trợ thuật toán mã hóa SHA-512 hay không:



```
# cat /etc/security/pwddalgs.cfg | grep sha  
ssha512:
```

```
lpa_module = /usr/lib/security/ssh  
lpa_options = algorithm=sha512
```

- Nếu kết quả trả về xuất hiện như ví dụ trên thì hệ điều hành có hỗ trợ mã hóa SHA-512. Để thiết lập lưu mật khẩu dưới dạng mã hóa SHA-512, thêm tùy chọn sau vào file /etc/security/login.cfg. Cụ thể:

```
# vi /etc/security/login.cfg
```

Thêm hoặc sửa dòng như sau vào phần thiết lập (thường ở cuối file và có khoảng tab ở đầu dòng):

```
pwd_algorithm = ssha512
```

- Nếu hệ điều hành không hỗ trợ mã hóa SHA-512, sử dụng mã hóa MD5 để thay thế:

```
# vi /etc/security/login.cfg
```

Thêm hoặc sửa dòng như sau vào phần thiết lập (thường ở cuối file):

```
pwd_algorithm = smd5
```

- Với những tài khoản đang tồn tại trên hệ thống phải thực hiện các bước sau để cấu hình được áp dụng:

- Bước 1: Liệt kê các tài khoản đang tồn tại trên hệ thống

```
# lsuser ALL | awk '{print $1}'
```

- Bước 2: Buộc người dùng phải đổi mật khẩu ở lần đăng nhập tiếp theo, sử dụng lệnh

```
# pwdadm -f ADMCHG <username>
```

#### 4. Quản trị từ xa qua kênh truyền an toàn

Để đảm bảo yêu cầu bảo mật cho hệ thống, tránh trường hợp thất thoát dữ liệu trên đường truyền khi quản trị hệ thống từ xa yêu cầu thiết lập và sử dụng các dịch vụ quản trị an toàn. Cụ thể nếu sử dụng SSH để quản trị cho IBM AIX cần thực hiện các thiết lập sau (Yêu cầu khởi động lại dịch vụ SSH khi thiết lập xong cấu hình):

- Yêu cầu quản trị từ xa sử dụng kênh truyền an toàn, có mã hóa

Chỉ cho phép sử dụng giao thức SSH version 2:

```
Mở file cấu hình /etc/ssh/sshd_config, sửa lại tùy chọn:  
Protocol 2
```

- Cấu hình chỉ cho phép tài khoản người dùng được phép SSH:

```
Mở file cấu hình /etc/ssh/sshd_config, thêm tùy chọn sau:  
AllowUsers user1 user2
```

- Không cho phép tài khoản root đăng nhập trực tiếp từ xa

```
Mở file cấu hình /etc/ssh/sshd_config, sửa hoặc thêm tùy chọn sau:  
PermitRootLogin no
```

- Không cho phép tài khoản đăng nhập sai quá 05 lần:

```
Mở file cấu hình /etc/default/login, sửa hoặc thêm tùy chọn sau:
```



*RETRIES=5*

- Giới hạn thời gian tự động ngắt phiên khi không có hoạt động trong một khoảng thời gian là 5 phút:

*Mở file cấu hình /etc/profile, thêm 3 dòng sau vào cuối file:*

*TMOUT=300*

*readonly TMOUT*

*export TMOUT*

- Nếu hệ điều hành chưa cài OpenSSH, thực hiện theo hướng dẫn sau:

- + Tải gói cài đặt OpenSSL và OpenSSH:

- OpenSSL:

[https://www14.software.ibm.com/webapp/iwm/web/preLogin.do?source=ai\\_xbp](https://www14.software.ibm.com/webapp/iwm/web/preLogin.do?source=ai_xbp)

- OpenSSH: <http://sourceforge.net/projects/openssh-aix/files/>

- Lưu ý là chọn đúng phiên bản OpenSSL và OpenSSH tương ứng với phiên bản hệ điều hành, nếu không sẽ xảy ra lỗi khi cài đặt.

- + Cài đặt OpenSSL và OpenSSH:

- Đầu tiên là cài đặt OpenSSL

*# uncompress openssl-0.9.8.2500.tar.Z*

*# tar -xvf openssl-0.9.8.2500.tar*

*# cd openssl-0.9.8.2500*

*# smitty install*

- Chọn Install and Update Software => Install Software.

- Nhập '.' để chọn thư mục chứa file cài đặt là thư mục hiện tại.

- Di chuyển xuống "Accept new license agreements" và nhấn tab để đổi giá trị từ 'No' thành 'Yes'.

- Nhấn Enter để thực hiện quá trình cài đặt.

- Tương tự với OpenSSH:

*# uncompress openssh\_5.4p1.tar.Z*

*# tar -xvf openssh\_5.4p1.tar*

*# smitty install*

- Restart lại dịch vụ sshd sau khi cài đặt và cấu hình xong để các thiết lập có hiệu lực:

*# stopsrc -s sshd*

*# startsrc -s sshd*

## 5. Phân quyền tệp tin và thư mục

- Xác thực đường dẫn các biến môi trường PATH: Biến môi trường PATH không được chứa các đường dẫn tương đối, đường dẫn bất thường, đường dẫn trống:

*Để kiểm tra biến môi trường PATH, ta dùng lệnh sau:*

*# echo \$PATH*

*Ví dụ:*





HƯỚNG DẪN THIẾT LẬP AN TOÀN  
THÔNG TIN CHO HỆ ĐIỀU HÀNH  
MÁY CHỦ

Ngày có hiệu lực: 01/9/2018

Ngày hết hiệu lực: 01/9/2019

Lần ban hành: 05

Trang: 55/71

<i>PATH</i>	<i>chứa</i>	<i>đường</i>	<i>dẫn</i>	<i>trống:</i>	<i>PATH</i>
<i>/usr/local/bin:/usr/sbin:/usr/bin:/sbin:/bin::</i>					
<i>PATH</i>	<i>chứa</i>	<i>đường</i>	<i>dẫn</i>	<i>tương</i>	<i>đối:</i>
<i>/usr/local/bin:/usr/sbin:/usr/bin:/sbin:/bin:./src/bin</i>					
<i>PATH</i>	<i>chứa</i>	<i>đường</i>	<i>dẫn</i>	<i>nguy</i>	<i>hiểm:</i>
<i>/usr/local/bin:/usr/sbin:/usr/bin:/sbin:/bin:/tmp</i>					<i>/bin:/us:</i>

- Thiết lập cấu hình dịch vụ CRON

- + Giới hạn tài khoản được phép chạy dịch vụ CRON bởi whitelist danh sách người dùng:

- Bước 1: Thực thi lệnh xóa file cron.deny:

```
# rm /var/adm/cron/cron.deny
```

- Bước 2: Thêm file cron.allow nếu hệ thống chưa có:

```
# touch /var/adm/cron/cron.allow
```

- Bước 3: Sửa file /var/adm/cron/cron.allow, cập nhật hoặc thêm các tài khoản được phép sử dụng dịch vụ CRON:

```
User1
```

```
User2
```

```
...
```

- + Hạn chế quyền sửa các file cấu hình của CRON

```
# chown -R root:root /var/spool/cron/crontabs/  
# chmod -R 600 /var/spool/cron/crontabs/  
# chown -R root:root /var/adm/cron/  
# chmod -R go-rwx /cron.d
```

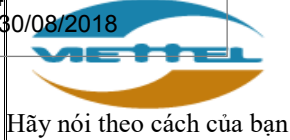
## 6. Cấu hình tường lửa mềm

- Yêu cầu sử dụng tường lửa mềm trên hệ thống.
- Cấu hình tường lửa mềm chỉ mở vừa đủ các kết nối vào/ra trên hệ thống: Đối với hệ thống nội bộ, chỉ mở vừa đủ các kết nối vào. Đối với hệ thống public, mở vừa đủ các kết nối vào/ra.

### Chú ý:

- + Người quản trị cần phải cấu hình tường lửa ở chế độ ghi log các gói tin trong vòng 1-2 tuần, sau đó sẽ phân tích log và thiết lập rule tương ứng.
- + Giải nghĩa 1 số lựa chọn trong quá trình thiết lập tường lửa trên hệ điều hành IBM AIX:

- **lsfilt:** Liệt kê các rule đang tồn tại
- **genfilt:** Tạo ra một rule mới, nếu câu lệnh không có option -n thì rule mới sẽ được thêm vào cuối của bảng
- **chfilt:** Sửa một rule đã tồn tại. Khi sử dụng lệnh này cần đưa cụ thể option -n tương ứng với ID của rule cần sửa. Rule có ID bằng 0,1,2 là các default rule và không thể sửa bằng lệnh này
- **rmfilt:** Xóa một rule tương ứng với ID đưa ra



- **mkfilt:** Câu lệnh dùng để active/deactive rules, enable/disable việc ghi log hoặc dùng để thay đổi default rule
- **-v:** IP version, giá trị là "4" hoặc "6"
- **-n:** Đưa ra số thứ tự của rule, nếu không đưa giá trị cụ thể cho lựa chọn này, rule sẽ mặc định gán vào cuối của tập luật
- **-a:** "action" của rule, giá trị "P" (permit) và "D" (deny)
- **-s:** Địa chỉ IP nguồn
- **-m:** Subnet mask IP nguồn
- **-d:** Địa chỉ IP đích
- **-M:** Subnet mask IP đích
- **-c:** Giao thức, giá trị là "udp", "icmp", "tcp", "tcp/ack", và "all"
- **-o:** Source port/ICMP, là các toán tử so sánh giá trị port nguồn. Giá trị là "lt" (less than: nhỏ hơn), "le" (less than or equal to: nhỏ hơn hoặc bằng), "gt" (greater than: lớn hơn), "ge" (greater than or equal to: lớn hơn hoặc bằng), "eq" (equal), "neq" (not equal) hoặc "any"
- **-O:** Destination port/ICMP, là các toán tử so sánh giá trị port đích. Giá trị là "lt" (less than: nhỏ hơn), "le" (less than or equal to: nhỏ hơn hoặc bằng), "gt" (greater than: lớn hơn), "ge" (greater than or equal to: lớn hơn hoặc bằng), "eq" (equal), "neq" (not equal) hoặc "any"
- **-p:** Source port/ICMP, giá trị port nguồn được dùng để so sánh. Giá trị 0 cho tất cả các port
- **-P:** Destination port/ICMP, giá trị port đích được dùng để so sánh. Giá trị 0 cho tất cả các port
- **-w:** Chỉ ra rule sẽ áp dụng cho chiều incoming (I), outgoing (O) hay cả 2 (B)
- **-l:** Ghi log, các giá trị là "Y" (yes) và "N" (no)
- **-i:** Interface, chỉ ra card mạng sẽ được áp dụng rule này. Giá trị "all" cho tất cả card mạng

+ Thiết lập cấu hình tường lửa:

- Bước 1: Thiết lập policy default:

- Xóa hết những rule đang tồn tại nếu có bằng lệnh:

```
# rmfilt -n all -v4
```

- Chỉnh sửa các policy default:

```
# smit ips4_start
```

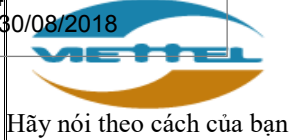
- Chú ý lựa chọn các giá trị:

- ✓ **Start IP Security:** Chọn Now and After Reboot để firewall có hiệu lực ngay lập tức và sau khi hệ thống reboot.

- ✓ **Deny All Non\_Secure IP Packets:** Chú ý chọn No, nếu chọn Yes thì có thể sẽ bị mất kết nối sau khi cấu hình.

- Sau đó nhấn Enter để khởi động tường lửa:





**HƯỚNG DẪN THIẾT LẬP AN TOÀN  
THÔNG TIN CHO HỆ ĐIỀU HÀNH  
MÁY CHỦ**

Ngày có hiệu lực: 01/9/2018

Ngày hết hiệu lực: 01/9/2019

Lần ban hành: 05

Trang: 57/71

- ✓ List các giá trị: F4, chọn giá trị sau đó Enter (bắt buộc phải thực hiện bước này để đảm bảo khởi động cho IPSecurity).
- ✓ Thoát ra bằng lệnh Esc+0.
- Liệt kê các rule mặc định:

```
# lsfilt -v4 -O
1/permit/0.0.0.0/0.0.0.0/0.0.0.0/0.0.0.0/no/udp/eq/4001/eq/4001
/both/both/no/all packets/0/all/0///Default Rule
2/** Dynamic filter placement rule for IKE tunnels **/no
0/permit/0.0.0.0/0.0.0.0/0.0.0.0/0.0.0.0/yes/all/any/0/any/0/both/
both/no/all packets/0/all/0///Default Rule
```

Chú ý 3 rule trên là mặc định, không nên thay đổi giá trị gì.

- Bước 2: Tạo một file có tên ruleIPSec.sh trong folder root/backup/<date>:

# vi /root/backup/<date>/ruleIPSec.sh

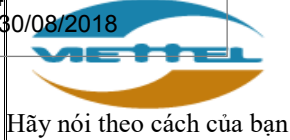
```
#!/bin/ksh
# Không thiết lập chặn các gói tin chiều vào tu loopback interface (lo0)
# Chu ý: Nếu thiết lập bao invalid interface "lo0" thì có thể bỏ qua câu
hình này
genfilt -v 4 -a P -s 0.0.0.0 -m 0.0.0.0 -d 0.0.0.0 -M 0.0.0.0 -c all -o any -p
0 -O any -P 0 -w B -l N -i lo0

# Không thiết lập chặn các gói tin chiều vào tu các internal interface
genfilt -v 4 -a P -s 0.0.0.0 -m 0.0.0.0 -d 0.0.0.0 -M 0.0.0.0 -c all -o any -p
0 -O any -P 0 -w B -l N -i en2

# Cho phép giao thức ICMP
genfilt -v 4 -a P -s 0.0.0.0 -m 0.0.0.0 -d 0.0.0.0 -M 0.0.0.0 -c icmp -o any
-p 0 -O any -P 0 -w I -l N -i en0
genfilt -v 4 -a P -s 0.0.0.0 -m 0.0.0.0 -d 0.0.0.0 -M 0.0.0.0 -c icmp -o any
-p 0 -O any -P 0 -w O -l N -i en0

# Cho phép server kết nối tới server khác qua cổng 22 (SSH)
genfilt -v 4 -a P -s 0.0.0.0 -m 0.0.0.0 -d 0.0.0.0 -M 0.0.0.0 -c tcp -o any -p
0 -O eq -P 22 -w O -l N -i en0
genfilt -v 4 -a P -s 0.0.0.0 -m 0.0.0.0 -d 0.0.0.0 -M 0.0.0.0 -c tcp/ack -o eq
-p 22 -O any -P 0 -w I -l N -i en0

# Cho quản trị IP 192.168.1.0/24 kết nối tới server qua SSH
genfilt -v 4 -a P -s 192.168.1.0 -m 255.255.255.0 -d 0.0.0.0 -M 0.0.0.0 -c
tcp -o any -p 0 -O eq -P 22 -w I -l N -i en0
genfilt -v 4 -a P -s 0.0.0.0 -m 0.0.0.0 -d 192.168.1.0 -M 255.255.255.0 -c
tcp/ack -o eq -p 22 -O any -P 0 -w O -l N -i en0
```



HƯỚNG DẪN THIẾT LẬP AN TOÀN  
THÔNG TIN CHO HỆ ĐIỀU HÀNH  
MÁY CHỦ

Ngày có hiệu lực: 01/9/2018  
Ngày hết hiệu lực: 01/9/2019

Lần ban hành: 05

Trang: 58/71

*# Cho phép giao thức HTTP và HTTPS*

```
genfilt -v 4 -a P -s 0.0.0.0 -m 0.0.0.0 -d 0.0.0.0 -M 0.0.0.0 -c tcp -o any -p  
0 -O eq -P 80 -w I -l N -i en0
```

```
genfilt -v 4 -a P -s 0.0.0.0 -m 0.0.0.0 -d 0.0.0.0 -M 0.0.0.0 -c tcp/ack -o  
any -p 0 -O eq -P 443 -w I -l N -i en0
```

```
genfilt -v 4 -a P -s 0.0.0.0 -m 0.0.0.0 -d 0.0.0.0 -M 0.0.0.0 -c tcp -o eq -p  
80 -O any -P 0 -w O -l N -i en0
```

```
genfilt -v 4 -a P -s 0.0.0.0 -m 0.0.0.0 -d 0.0.0.0 -M 0.0.0.0 -c tcp/ack -o eq  
-p 443 -O any -P 0 -w O -l N -i en0
```

*# Cho phép giao thức đồng bộ thời gian NTP*

```
genfilt -v 4 -a P -s 192.168.181.50 -m 255.255.255.255 -d 0.0.0.0 -M  
0.0.0.0 -c udp -o eq -p 123 -O eq -P 123 -w I -l N -i en0
```

```
genfilt -v 4 -a P -s 0.0.0.0 -m 0.0.0.0 -d 192.168.181.50 -M  
255.255.255.255 -c udp -o eq -p 123 -O eq -P 123 -w O -l N -i en0
```

*# Thiết lập ghi log và drop gói tin vi phạm*

```
genfilt -v 4 -a D -s 0.0.0.0 -m 0.0.0.0 -d 0.0.0.0 -M 0.0.0.0 -c all -o any -p  
0 -O any -P 0 -w I -l Y -i en0
```

• **Chú ý:**

- Tường lửa trên AIX không phải là tường lửa trạng thái do vậy muốn mở 1 kết nối thì cần phải mở cả chiều vào và chiều ra (xem ví dụ về rule mở cho phép telnet/ssh/http/https ở trên).
- Tường lửa trên AIX không cho phép mở 1 dải port ví dụ từ 1024-2098, nó chỉ cho phép mở các port >1024 hoặc <1024 hoặc =1024. Do vậy với các dịch vụ FTP server chạy ở chế độ passive cần phải cấu hình lại chạy ở chế độ active mới có thể hoạt động được.

• **Bước 3: Thực thi file ruleIPSec.sh như sau:**

```
# cd /root/backup/<date>  
# chmod +x ruleIPSec.sh  
# ./ruleIPSec.sh
```

• **Bước 4: Đưa các rule đã thiết lập vào thực thi:**

```
# mkfilt -v4 -u
```

• **Bước 5: Kiểm tra lại các rule đang active bằng lệnh sau:**

```
# lsfilt -v4 -O -a
```

• **Bước 6: Sau đó bắt đầu việc ghi log bằng lệnh:**

```
# mkfilt -v4 -g start
```

• **Lưu ý nếu muốn dừng việc ghi log thì dùng lệnh sau:**



```
# mkfilt -v4 -g stop
```

- + Ghi log toàn bộ những bản tin vào ra không hợp lệ: Thực hiện như hướng dẫn nêu trên.

## 7. Thiết lập chính sách quản lý log và đồng bộ thời gian

### Thiết lập log

- Ghi log mặc định của hệ điều hành: Yêu cầu thiết lập cấu hình ghi tối thiểu các loại sau: message log, dmesg log, secure log.

- + Bước 1: Tìm và sửa file /etc/syslog.conf tại dòng sau:

```
# vi /etc/syslog.conf
*.debug;local4.none;auth.none /var/log/syslog/syslog.out rotate size 4096k
files 12 time 1w compress
*.crit /var/log/syslog/syslog.out rotate size 4096k files 12 time 1w
compress
auth.debug /var/log/syslog/faillogin rotate size 4096k files 12 time
1w compress
```

- + Bước 2: Nếu chưa có file /var/log/syslog/syslog.out thì tạo ra bằng lệnh sau:

```
# mkdir /var/log/syslog
# touch /var/log/syslog/syslog.out
```

- + Bước 3: Khởi động lại dịch vụ syslog

```
# refresh -s syslogd
```

- + Bước 4: Kiểm tra lại /var/log/syslog/syslog.out để chắc chắn đã có log:

```
# tail -f /var/log/syslog/syslog.out
```

**Chú ý:** Theo quy định của Tập đoàn thời gian tối thiểu lưu log là 3 tháng. Tuy nhiên nếu máy chủ hiện tại không đủ dung lượng ổ cứng để lưu log trong 3 tháng thì quản trị có thể thiết lập lại để phù hợp với thực tế, tránh log đầy làm treo máy chủ.

- + Bước 5: Thực hiện ghi log tường lửa

```
# touch /var/log/firewall
```

- + Bước 6: Thêm dòng giá trị sau vào file /etc/syslog.conf.

```
local4.debug /var/log/firewall rotate size 4096k files 12 time 1w compress
```

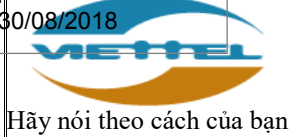
- + Bước 7: Khởi động lại dịch vụ syslog

```
# refresh -s syslogd
```

- + Bước 8: Kiểm tra trạng thái dịch vụ syslog, nếu ở trạng thái active tức là dịch vụ đã hoạt động.

```
# lssrc -a | grep log
syslogd      ras      168238      active
```

- Cấu hình rotate log:



Đối với hệ điều hành AIX cấu hình rotate log nằm trong file cấu hình /etc/syslog.conf như ở phần trên, tham số "**12 time 1w**" chỉ định log được rotate hàng tuần (1w) và lưu trữ 12 file log mới nhất (12 time):

```
# vi /etc/syslog.conf
*.debug;local4.none;auth.none /var/log/syslog/syslog.out rotate size 4096k files
12 time 1w compress
*.crit /var/log/syslog/syslog.out rotate size 4096k files 12 time 1w compress
auth.debug /var/log/syslog/faillogin rotate size 4096k files 12 time 1w compress
```

#### **Đồng bộ thời gian HĐH về máy chủ tập trung**

- Cách 1: Đồng bộ thời gian bằng dịch vụ NTP

- + Bước 1: Sửa file /etc/ntp.conf, đảm bảo đã có những dòng sau:

```
# vi /etc/ntp.conf
restrict default kod nomodify notrap nopeer noquery
restrict -6 default kod nomodify notrap nopeer noquery
restrict 127.0.0.1
restrict -6 ::1
```

Thêm dòng sau vào phía dưới dòng **#broadcastclient**  
**server 192.168.181.50 prefer**  
(Lưu ý: Dòng **driftfile** và **logfile** giữ nguyên)

- + Bước 2: Kiểm tra trạng thái dịch vụ ntpd:

```
# lssrc -a | grep xntp
xntpd tcpip 225286 active
```

- + Bước 3: Nếu dịch vụ xntpd chưa chạy thì dùng lệnh

```
# startsrc -s xntpd
```

- + Bước 4: Để dịch vụ tự khởi động khi reboot:

```
# vi /etc/rc.tcpip
Bỏ dấu # ở đầu dòng bên dưới để dịch vụ NTP khởi động cùng máy chủ sau
khi reboot.
start /usr/sbin/xntpd "$src_running"
```

- Cách 2: Đồng bộ bằng crontab (Yêu cầu máy chủ phải cài đặt chương trình ntpdate).

- + Bước 1: Sửa crontab của root

```
# export EDITOR=vi
# crontab -e
# Bổ sung một crontab
*/5 * * * * ntpdate -u 192.168.181.50
```

#### **8. Cài đặt các phần mềm giám sát ATTT**

Mã văn bản: HD.VTNet.CNTT.04/ATTT  
Số văn bản: 04-4  
Ngày ban hành: 30/08/2018



**TỔNG CÔNG TY MẠNG LƯỚI VIETTEL**

**HƯỚNG DẪN THIẾT LẬP AN TOÀN  
THÔNG TIN CHO HỆ ĐIỀU HÀNH  
MÁY CHỦ**

Mã hiệu: HD.VTNET.CNTT....

Ngày có hiệu lực: 01/9/2018

Ngày hết hiệu lực: 01/9/2019

Lần ban hành: 05

Trang: 61/71

Yêu cầu cài đặt đầy đủ các phần mềm giám sát ATTT do TT.ANM cung cấp

- Phần mềm Server Endpoint để hỗ trợ giám sát hành vi bất thường và vi phạm baseline.

Hướng dẫn cài đặt: [http://docs.sirc.viettel.com/guide/install\\_se\\_agent/](http://docs.sirc.viettel.com/guide/install_se_agent/)

- Phần mềm Filebeat và OSSEC agent để hỗ trợ lấy log và event.

Hướng dẫn cài đặt: <http://docs.sirc.viettel.com/guide/LogAgent/>



## HƯỚNG DẪN THIẾT LẬP CẤU HÌNH BẢO MẬT CHO HỆ ĐIỀU HÀNH SUSE

### I. Nội dung hướng dẫn

Hướng dẫn thiết lập an toàn cho hệ điều hành SUSE nhằm đảm bảo 8 tiêu chuẩn ATTT bao gồm:

- Cài đặt và cập nhật bản vá cho hệ điều hành.
- Xóa hoặc vô hiệu hóa các dịch vụ, ứng dụng, giao thức mạng không cần thiết.
- Thiết lập chính sách tài khoản.
- Quản trị từ xa qua kênh truyền an toàn.
- Phân quyền tập tin và thư mục.
- Cài đặt và cấu hình firewall mềm.
- Thiết lập chính sách quản lý log.
- Cài đặt phần mềm giám sát ATTT.

### II. Chi tiết hướng dẫn

#### 1. Cài đặt hệ điều hành và cập nhật bản vá.

##### Yêu cầu:

- Sử dụng phiên bản mới nhất của hệ điều hành khi cài đặt mới.
- Cập nhật các bản vá lỗi cho hệ điều hành: Bao gồm các bản vá lỗ hổng bảo mật đã được công bố và các bản vá theo yêu cầu của Tập đoàn.

##### Chú ý:

- Yêu cầu này chỉ áp dụng với các hệ thống đã mua bản quyền hệ điều hành SUSE.
- Thực hiện backup hệ thống trước khi cập nhật bản vá để giảm thiểu rủi ro.

#### 2. Xóa hoặc vô hiệu hóa các dịch vụ, ứng dụng, giao thức mạng không cần thiết

##### Yêu cầu:

- Cài đặt tối thiểu các phần mềm, dịch vụ theo đúng chức năng được thiết kế của server.
- Gỡ bỏ hoặc vô hiệu hóa các gói dịch vụ không cần thiết, các gói dịch vụ lỗi thời có nguy cơ bị mất an toàn thông tin: Telnet, rcp, rsh, rlogin, nis, ftp...

**Phương án 1:** Vô hiệu hóa dịch vụ không cần thiết.

**Bước 1:** Dừng dịch vụ

```
# service <Tên_service> stop
```

**Bước 2:** Tắt dịch vụ khởi động cùng hệ thống

```
# chkconfig <Tên_service> off
```

**Ví dụ:**

```
service telnetd stop
```

```
# chkconfig telnetd off
```

**Phương án 2:** Gỡ bỏ dịch vụ không cần thiết.

```
# yast --remove <Tên gói cần xóa>
```

#### 3. Thiết lập chính sách tài khoản





HƯỚNG DẪN THIẾT LẬP AN TOÀN  
THÔNG TIN CHO HỆ ĐIỀU HÀNH  
MÁY CHỦ

Ngày có hiệu lực: 01/9/2018

Ngày hết hiệu lực: 01/9/2019

Lần ban hành: 05

Trang: 63/71

- Xóa hoặc vô hiệu tất cả các tài khoản không sử dụng trên hệ thống

*Bước 1: Để tìm những tài khoản đang hoạt động trên hệ thống, ta sử dụng lệnh sau:*

```
# cat /etc/passwd | grep /*sh$ | awk -F: '{print $1}'
```

*Bước 2: Kiểm tra xem các tài khoản này tài khoản nào không sử dụng. Thực hiện 1 trong 2 phương án:*

**Phương án 1:** Vô hiệu các tài khoản:

```
# passwd -l <username>
```

**Phương án 2:** Xóa tài khoản:

```
# userdel <username>
```

*Ví dụ: Trong danh sách có tài khoản game không sử dụng*

```
# userdel game
```

- Cấu hình chính sách mật khẩu cho tài khoản

- + Mật khẩu phải có độ dài tối thiểu 8 ký tự chứa ký tự viết hoa, viết thường, chữ số, ký tự đặc biệt.

**Đối với SLES 11:**

```
# vi /etc/pam.d/common-password
```

*#Thực hiện thay thế các 2 cấu hình "password required pam\_cracklib.so..." và "password required pam\_pwhistory.so..." bằng 2 dòng sau:*

```
password required pam_cracklib.so dcredit=-1 ucredit=-1 lcredit=-1  
minlen=8 retry=5
```

```
password required pam_pwhistory.so use_authtok remember=3 retry=5
```

**Đối với SLES 10:**

```
# vi /etc/pam.d/common-password
```

*#Thực hiện thay thế các 2 cấu hình "password required pam\_cracklib.so..." và "password required pam\_pwcheck.so..." bằng 2 dòng sau:*

```
password required pam_cracklib.so dcredit=-1 ucredit=-1 lcredit=-1  
minlen=10 retry=5
```

```
password required pam_pwcheck.so nullok remember=3
```

**Đối với SLES 9:**

**Bước 1: Tạo mới file /etc/pam.d/common-password**

```
# touch /etc/pam.d/common-password
```

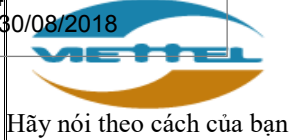
```
# vi /etc/pam.d/common-password
```

```
password required pam_pwcheck.so
```

```
password required pam_cracklib.so use_authtok retry=3 lcredit=-1  
ucredit=-1 dcredit=-1 ocredit=-1 minlen=8
```

```
password required pam_pwcheck.so remember=5 use_authtok
```





*use\_first\_pass*

*password required pam\_unix2.so nullok use\_authok use\_first\_pass*

**Bước 2: Sửa file /etc/pam.d/passwd**

# Mở file cấu hình /etc/pam.d/passwd và comment (#) hết các dòng bắt đầu bằng password sẵn có, sau đó thêm vào vị trí đó dòng sau: password

*include common-password*

*#vi /etc/pam.d/passwd*

*password include common-password*

- + Thời gian bắt buộc phải thay đổi mật khẩu người dùng: Thiết lập giá trị 90 ngày với hệ thống public và 180 ngày với hệ thống nội bộ.

Thay đổi giá trị PASS\_MAX\_DAYS trong file /etc/login.defs. Thực hiện như sau:

*# vi /etc/login.defs*

*PASS\_MAX\_DAYS 90*

*# cat /etc/passwd | grep /\*sh\$ | awk -F: '{print \$1}'*

*# chage -M 90 <user\_name>*

**Chú ý:** Câu lệnh *cat /etc/passwd | grep /\*sh\$ | awk -F: '{print \$1}'* có ý nghĩa liệt kê toàn bộ tài khoản có khả năng đăng nhập vào hệ thống. Một số tài khoản đang bị khóa hoặc không có quyền đăng nhập vào hệ thống sẽ không được liệt kê.

- + Giới hạn mật khẩu mới không được trùng với mật khẩu gần nhất: Thiết lập giá trị là 2 với hệ thống nội bộ và 5 với hệ thống public.

Thay đổi giá trị *remember* trong file /etc/pam.d/common-password. Thực hiện như sau:

**Đối với SLES 11:**

*# vi /etc/pam.d/common-password*

*password required pam\_pwhistory.so use\_authok remember=3  
retry=5*

**Đối với SLES 10:**

*# vi /etc/pam.d/common-password*

*password required pam\_pwcheck.so nullok remember=3*

**Đối với SLES 9:**

*# vi /etc/pam.d/common-password*

*password required pam\_pwcheck.so remember=5 use\_authok  
use\_first\_pass*

- + Mã hóa mật khẩu sử dụng thuật toán mã hóa an toàn (SHA-512)

- Thực hiện lệnh sau để đảm bảo hệ thống có hỗ trợ thuật toán SHA-512.

*# yast security set help*

Kết quả trả về: *passwd [ des md5 blowfish sha256 sha512 ]*



**HƯỚNG DẪN THIẾT LẬP AN TOÀN  
THÔNG TIN CHO HỆ ĐIỀU HÀNH  
MÁY CHỦ**

Ngày có hiệu lực: 01/9/2018

Ngày hết hiệu lực: 01/9/2019

Lần ban hành: 05

Trang: 65/71

*Password encryption method*

- Nếu kết quả trả về giống như trên thì hệ điều hành có hỗ trợ mã hóa SHA-512, thiết lập lưu password sử dụng SHA-512:

```
# yast security set passwd=sha512
```

- Chú ý:** Với những tài khoản đang tồn tại trên hệ thống phải thực hiện các bước sau để chính sách được áp dụng:

Đặt lại mật khẩu mới cho tài khoản

```
# passwd username
```

Buộc người dùng phải đổi mật khẩu ở lần đăng nhập tiếp theo

```
# passwd -f username
```

#### 4. Quản trị từ xa qua kênh truyền an toàn

Để đảm bảo yêu cầu bảo mật cho hệ thống, tránh trường hợp thất thoát dữ liệu trên đường truyền khi quản trị hệ thống từ xa yêu cầu thiết lập và sử dụng các dịch vụ quản trị an toàn. Cụ thể nếu sử dụng SSH để quản trị cho SUSE cần thực hiện các thiết lập sau (*Yêu cầu khởi động lại dịch vụ SSH khi thiết lập xong cấu hình*):

- Yêu cầu quản trị từ xa sử dụng kênh truyền an toàn, có mã hóa

Chỉ cho phép sử dụng giao thức SSH version 2.

Mở file cấu hình `/etc/ssh/sshd_config`, sửa lại tùy chọn:  
*Protocol 2*

- Cấu hình chỉ cho phép tài khoản người dùng được phép SSH

Mở file cấu hình `/etc/ssh/sshd_config`, thêm tùy chọn sau:  
*AllowUsers user1 user2*

- Không cho phép tài khoản root đăng nhập trực tiếp từ xa

Mở file cấu hình `/etc/ssh/sshd_config`, sửa hoặc thêm tùy chọn sau:  
*PermitRootLogin no*

- Không cho phép tài khoản đăng nhập sai quá 05 lần:

Mở file cấu hình `/etc/ssh/sshd_config`, sửa hoặc thêm tùy chọn sau:  
*MaxAuthTries 5*

- Giới hạn thời gian tự động ngắt phiên khi không có hoạt động trong một khoảng thời gian là 5 phút:

Mở file cấu hình `/etc/profile`, thêm 3 dòng sau vào cuối file:  
*TMOUT=300*  
*readonly TMOUT*  
*export TMOUT*

#### 5. Phân quyền tệp tin và thư mục

- Xác thực đường dẫn các biến môi trường PATH: Biến môi trường PATH không được chứa các đường dẫn tương đối, đường dẫn bất thường, đường dẫn trống:

Để kiểm tra biến môi trường PATH, ta dùng lệnh sau:

```
# echo $PATH
```

Ví dụ:



HƯỚNG DẪN THIẾT LẬP AN TOÀN  
THÔNG TIN CHO HỆ ĐIỀU HÀNH  
MÁY CHỦ

Ngày có hiệu lực: 01/9/2018

Ngày hết hiệu lực: 01/9/2019

Lần ban hành: 05

Trang: 66/71

<i>PATH</i>	<i>chứa</i>	<i>đường</i>	<i>dẫn</i>	<i>trống:</i>	<i>PATH</i>
<i>/usr/local/bin:/usr/sbin:/usr/bin:/sbin:/bin::</i>					
<i>PATH</i>	<i>chứa</i>	<i>đường</i>	<i>dẫn</i>	<i>tương</i>	<i>đổi:</i>
<i>/usr/local/bin:/usr/sbin:/usr/bin:/sbin:/bin:./src/bin</i>					
<i>PATH</i>	<i>chứa</i>	<i>đường</i>	<i>dẫn</i>	<i>nguy</i>	<i>hiểm:</i>
<i>/usr/local/bin:/usr/sbin:/usr/bin:/sbin:/bin:/tmp</i>					<i>/bin:/us:</i>

- Thiết lập cấu hình dịch vụ CRON

- + Giới hạn tài khoản được phép chạy dịch vụ CRON bởi whitelist danh sách người dùng:

- Bước 1: Thực thi lệnh xóa file cron.deny:

```
# rm /etc/cron.d/cron.deny
```

- Bước 2: Thêm file cron.allow nếu hệ thống chưa có:

```
#touch /etc/cron.d/cron.allow
```

- Bước 3: Sửa file /etc/cron.allow, cập nhật hoặc thêm các tài khoản được phép sử dụng dịch vụ CRON:

```
User1
```

```
User2
```

```
...
```

- + Hạn chế quyền sửa các file cấu hình của CRON

```
# chown -R root:root /var/spool/cron/crontabs/  
# chmod -R 600 /var/spool/cron/crontabs/  
# chown -R root:root /etc/cron.d  
#chmod -R go-rwx /cron.d
```

6. Cấu hình tường lửa mềm

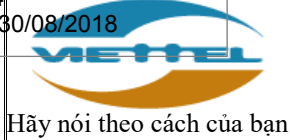
- Yêu cầu sử dụng tường lửa mềm trên hệ thống: Mặc định hệ điều hành SUSE sử dụng firewall SuSEfirewall2 tuy nhiên để dễ quản lý và thống nhất với CentOS/RHEL ta sẽ tắt SuSEfirewall2 và sử dụng iptables thay thế.

- + Bước 1: Tắt SuSEfirewall2 và không cho khởi động cùng hệ thống

```
# SuSEfirewall2 stop  
# SuSEfirewall2 off
```

- + Bước 2: Tạo file cấu hình /etc/sysconfig/iptables với nội dung như sau

```
*filter  
:INPUT ACCEPT [0:0]  
:FORWARD DROP [0:0]  
:OUTPUT ACCEPT [0:0]  
##### CẤU HÌNH CHẾU INPUT  
#####  
##### CẤU HÌNH CHẾU OUTPUT  
#####  
##### CẤU HÌNH CHẾU FORWARD
```



HƯỚNG DẪN THIẾT LẬP AN TOÀN  
THÔNG TIN CHO HỆ ĐIỀU HÀNH  
MÁY CHỦ

Ngày có hiệu lực: 01/9/2018

Ngày hết hiệu lực: 01/9/2019

Lần ban hành: 05

Trang: 67/71

#####  
COMMIT

+ Bước 3: Load các module cho iptables

- Kiểm tra xem module đã có hay chưa, dùng lệnh:  
# modprobe -l | grep conntrack\_ftp  
(Kết quả trả về có thể là nf\_conntrack\_ftp hoặc ip\_conntrack\_ftp tùy OS)
- Sau đó nếu có thì gõ lệnh sau để load module này lên:  
# modprobe ip\_conntrack\_ftp
- Kiểm tra lại bằng lệnh sau:  
# lsmod | grep conntrack\_ftp
- Cấu hình để load module trên khi hệ thống khởi động. Thêm vào cuối file /etc/init.d/boot.local dòng sau:  
modprobe ip\_conntrack\_ftp

+ Bước 4: Cấu hình load rule iptables khi khởi động

```
# Bổ sung dòng sau vào iptables
# crontab -e
@reboot /usr/sbin/iptables-restore < /etc/sysconfig/iptables
```

- Cấu hình tường lửa mềm chỉ mở vừa đủ các kết nối vào/ra trên hệ thống: Đối với hệ thống nội bộ, chỉ mở vừa đủ các kết nối vào. Đối với hệ thống public, mở vừa đủ các kết nối vào/ra.

**Chú ý:** Người quản trị cần phải cấu hình tường lửa ở chế độ ghi log các gói tin trong vòng 1-2 tuần. Sau đó sẽ phân tích log và thiết lập rule tương ứng.

+ Sử dụng 2 lệnh chính sau:

- iptables-save: Lưu lại toàn bộ rule ra một file text có định dạng đặc biệt
- iptables-restore: Load rule từ file text đã lưu trước đó.

+ Cú pháp sử dụng:

- Lệnh iptables-save:

```
# iptables-save > /etc/iptables-save
```

**Lưu ý:** /etc/iptables-save là file lưu lệnh iptables, có thể thay đổi thành file bất kỳ.

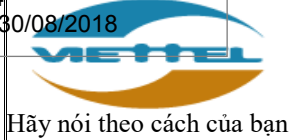
- Lệnh iptables-restore:

```
# iptables-restore < /etc/iptables-save
```

Tất cả các rule trong file /etc/iptables-save sẽ được load và áp dụng vào iptables.

+ Ý nghĩa của file được lưu bởi lệnh iptables-save:

```
# Generated by iptables-save v1.4.7 on Fri Jul 10 22:34:12 2015
*filter
:INPUT ACCEPT [0:0]
:FORWARD ACCEPT [0:0]
:OUTPUT ACCEPT [129895:7030615]
```



HƯỚNG DẪN THIẾT LẬP AN TOÀN  
THÔNG TIN CHO HỆ ĐIỀU HÀNH  
MÁY CHỦ

Ngày có hiệu lực: 01/9/2018

Ngày hết hiệu lực: 01/9/2019

Lần ban hành: 05

Trang: 68/71

```
-A INPUT -m state --state RELATED,ESTABLISHED -j ACCEPT
-A INPUT -p udp -m state --state NEW -m udp --dport 123 -j ACCEPT
-A INPUT -p icmp -j ACCEPT
-A INPUT -i lo -j ACCEPT
-A INPUT -p tcp -m state --state NEW -m tcp --dport 22 -j ACCEPT
-A INPUT -j REJECT --reject-with icmp-host-prohibited
-A FORWARD -j REJECT --reject-with icmp-host-prohibited
COMMIT
# Completed on Fri Jul 10 22:34:12 2015
```

Trong đó:

- “\*filter”: Chỉ bắt đầu các rule của table filter, table dùng để viết các rule lọc gói tin.
  - :INPUT ACCEPT [0:0]
    - INPUT: là chain của iptables, table filter có 3 chain là INPUT, OUTPUT, FORWARD. Trong đó INPUT là thời điểm gói tin đi vào hệ thống, OUTPUT là thời điểm gói tin đi ra hệ thống, còn FORWARD là thời điểm gói tin đi từ card mạng này sang card mạng khác.
    - ACCEPT: Chain policy của chain INPUT, OUTPUT và FORWARD. Ý nghĩa: Nếu gói tin sau khi được kiểm tra bởi tất cả các rule của iptables mà không có rule nào khớp thì sẽ được ACCEPT.
  - [0:0]: Số đầu tiên chỉ ra số lượng gói tin, số thứ 2 chỉ ra dung lượng của các gói tin. Đây là các thông số thống kê về các gói tin không khớp luật nào của iptables, và do đó được thực hiện chain policy là ACCEPT.
  - Các rule tiếp theo: Là rule lọc của iptables, sẽ áp dụng từ trên xuống dưới.
  - COMMIT: Đánh dấu kết thúc bảng filter.
- + Cách sửa rule của iptables: Để cấu hình thêm rule mới thực hiện sửa file /etc/sysconfig/iptables:

```
# Firewall configuration written by system-config-firewall
# Manual customization of this file is not recommended.
*filter
:INPUT ACCEPT [0:0]
:FORWARD ACCEPT [0:0]
:OUTPUT ACCEPT [0:0]
##### CẤU HÌNH CHÈU INPUT
#####
### Cho phép các gói tin thuộc 1 kết nối đang tồn tại hoặc có liên quan đến
1 connection đang tồn tại đi vào, không cần kiểm tra ###
-A INPUT -m state --state RELATED,ESTABLISHED -j ACCEPT
### Nhưng gói tin từ card mạng loopback thì không cần lọc ###
-A INPUT -i lo -j ACCEPT
```





HƯỚNG DẪN THIẾT LẬP AN TOÀN  
THÔNG TIN CHO HỆ ĐIỀU HÀNH  
MÁY CHỦ

Ngày có hiệu lực: 01/9/2018  
Ngày hết hiệu lực: 01/9/2019

Lần ban hành: 05

Trang: 69/71

### Cho phép ping echo request đến server ###

-A INPUT -p icmp --icmp-type any -j ACCEPT

# Ví dụ luật cho phép 1 IP hay 1 dải IP SSH đến server #

-A INPUT -m state --state NEW -s 192.168.1.190 -m tcp -p tcp --dport 22 -j ACCEPT

-A INPUT -m state --state NEW -s 192.168.2.0/24 -m tcp -p tcp --dport 22 -j ACCEPT

# Ví dụ luật cho phép HTTP #

-A INPUT -m state --state NEW -m tcp -p tcp --dport 80 -j ACCEPT

### Thêm các luật chiều INPUT tại đây ###

### Chặn toàn bộ các kết nối còn lại, ghi log trước khi chặn ###

-A INPUT -j LOG --log-level 4 --log-prefix "IPTABLES DROP INPUT "

-A INPUT -j REJECT --reject-with icmp-host-prohibited

##### CẤU HÌNH CHÈU OUTPUT  
#####

### Cho phép các gói tin thuộc 1 kết nối đang tồn tại hoặc có liên quan đến 1 connection đang tồn tại đi vào, không cần kiểm tra ###

-A OUTPUT -m state --state RELATED,ESTABLISHED -j ACCEPT

### Nhưng gói tin từ card mạng loopback thì không cần lọc ###

-A OUTPUT -o lo -j ACCEPT

### Cho phép ping ###

-A OUTPUT -p icmp --icmp-type any -j ACCEPT

# Ví dụ luật cho phép server hiện tại ssh đến server 10.10.10.10 #

-A OUTPUT -m state --state NEW -d 10.10.10.10 -m tcp -p tcp --dport 22 -j ACCEPT

### Thêm các luật lọc chiều OUTPUT tại đây

### Chỉ khi server cần chủ động kết nối ra bên ngoài mới thêm luật tiếp theo ###

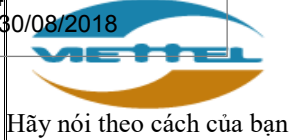
### Chặn toàn bộ các kết nối còn lại, ghi log trước khi chặn ###

-A OUTPUT -j LOG --log-level 4 --log-prefix "IPTABLES DROP OUTPUT "

-A OUTPUT -j REJECT --reject-with icmp-host-prohibited

##### CẤU HÌNH CHÈU FORWARD  
#####





```
-A FORWARD -j LOG --log-level 4 --log-prefix "IPTABLES DROP FORWARD "  
-A FORWARD -j REJECT --reject-with icmp-host-prohibited  
COMMIT
```

- + Cách cấu hình để iptables nạp các rule khi server khởi động lại:

```
Thêm dòng sau vào cuối file /etc/rc.local:  
iptables-restore < /etc/sysconfig/iptables
```

- + Cách tạm thời tắt tất cả các luật của iptables để troubleshoot:

```
Sử dụng các lệnh sau:  
# iptables -F  
# iptables -X  
# iptables -P INPUT ACCEPT  
# iptables -P OUTPUT ACCEPT  
# iptables -P FORWARD ACCEPT
```

- + Ý nghĩa các lệnh:

- Lệnh thứ nhất để xóa tất cả các rule trong tất cả các chain của iptables
- Lệnh thứ 2 xóa tất cả các chain do người dùng tự tạo
- Lệnh thứ 3, 4, 5 thiết lập chain policy cho chain INPUT, OUTPUT, FORWARD là ACCEPT, khi đây server cho phép toàn bộ kết nối vào/ra server.

- Ghi log những bản ghi không hợp lệ:

```
Thêm các dòng sau vào file cấu hình iptables:  
-A INPUT -j LOG --log-level 4 --log-prefix "IPTABLES DROP INPUT "  
-A FORWARD -j LOG --log-level 4 --log-prefix "IPTABLES DROP OUTPUT "  
-A OUTPUT -j LOG --log-level 4 --log-prefix "IPTABLES DROP FORWARD "
```

## 7. Thiết lập chính sách quản lý log

- Ghi log mặc định của hệ điều hành: Yêu cầu thiết lập cấu hình ghi tối thiểu các loại sau: message log, dmesg log, secure log (Mặc định Suse ghi log message và secure vào cùng file log /var/log/ message).

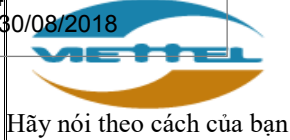
- + Bước 1: Cấu hình log sshd:

```
# vi /etc/ssh/sshd_config  
SyslogFacility AUTH
```

- + Bước 2: Cấu hình syslog

Với máy chủ sử dụng **syslog-ng** đảm bảo file /etc/syslog-ng/syslog-ng.conf có chứa dòng sau:

```
# vi /etc/syslog-ng/syslog-ng.conf  
filter f_iptables { facility(kern) and match("IN=") and match("OUT="); };  
filter f_messages { not facility(news, mail) and not filter(f_iptables); };  
destination messages { file("/var/log/messages"); };
```



HƯỚNG DẪN THIẾT LẬP AN TOÀN  
THÔNG TIN CHO HỆ ĐIỀU HÀNH  
MÁY CHỦ

Ngày có hiệu lực: 01/9/2018  
Ngày hết hiệu lực: 01/9/2019

Lần ban hành: 05

Trang: 71/71

```
log { source(src); filter(f_messages); destination(messages); };
```

- + Bước 3: Restart lại dịch vụ syslog-ng

```
# /etc/init.d/syslog stop  
# /etc/init.d/syslog start
```

- + Bước 4: Kiểm tra lại trạng thái của dịch vụ system-log xem đã chắc chắn được bật chưa, sử dụng câu lệnh sau:

```
# /etc/init.d/syslog status  
Checking for service syslog: running
```

Nếu có trạng thái là **"running"** nghĩa là dịch vụ đang hoạt động bình thường.

- Cấu hình thời gian lưu log tối thiểu là 3 tháng

- + Bước 1: Thiết lập trong file `/etc/logrotate.conf`. Mở file `/etc/logrotate.conf` thiết lập 2 giá trị là `"weekly"` và `"rotate 4"`

```
# vi /etc/logrotate.conf  
weekly  
rotate 12
```

Trong đó:

- `"weekly"`: Thực hiện rotate theo tuần.
- `"rotate 12"`: Thực hiện lưu trữ 12 tuần gần nhất tương đương 3 tháng.

- + Bước 2: Thiết lập trong file `/etc/logrotate.d/syslog`.

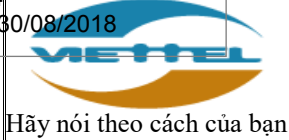
```
# vi /etc/logrotate.d/syslog  
/var/log/messages /var/log/firewall <các file log khác> {  
    daily                # rotate log hằng ngày  
    compress  
    dateext  
    rotate 90            # lưu log 90 ngày  
    missingok  
    notifempty  
    create 600 root root  
    sharedscripts  
    postrotate  
        /etc/init.d/syslog reload > /dev/null  
    endscript  
}
```

**Chú ý:** Theo quy định của Tập đoàn thời gian tối thiểu lưu log là 3 tháng, tuy nhiên nếu máy chủ hiện tại không đủ dung lượng ổ cứng để lưu log trong 3 tháng thì quản trị có thể thiết lập lại để phù hợp với thực tế tránh log đầy làm treo máy chủ.

**Đồng bộ thời gian HĐH về máy chủ tập trung**

- Cách 1: Đồng bộ bằng dịch vụ NTP

- + Bước 1: Sửa file `/etc/ntp.conf`



Thay thế server <ip\_address> bằng server 192.168.181.50

- + Bước 2: Chạy dịch vụ ntpd và khởi chạy cùng hệ điều hành bằng lệnh:

```
# service ntp start  
# chkconfig ntp on
```

- + Bước 3: Kiểm tra việc đồng bộ có thành công hay không, sử dụng lệnh:

```
# ntpq -p  
remote refid st t when poll reach delay offset jitter  
=====
```

*192.168.181.50	137.189.4.10	2	u	780	1024	377	1.866	-14.601	67.605
-----------------	--------------	---	---	-----	------	-----	-------	---------	--------

- Cách 2: Đồng bộ bằng crontab (Yêu cầu máy chủ phải cài đặt chương trình ntpdate).

- + Bước 1: Sửa crontab của root.

```
# crontab -e  
# Bổ sung một crontab  
*/5 * * * * ntpdate -u 192.168.181.50
```

## 8. Cài đặt các phần mềm giám sát ATTT

Yêu cầu cài đặt đầy đủ các phần mềm giám sát ATTT do TT.ANM cung cấp

- Phần mềm Server Endpoint để hỗ trợ giám sát hành vi bất thường và vi phạm baseline.

Hướng dẫn cài đặt: [http://docs.sirc.viettel.com/guide/install\\_se\\_agent/](http://docs.sirc.viettel.com/guide/install_se_agent/)

- Phần mềm Filebeat và OSSEC agent để hỗ trợ lấy log và event.

Hướng dẫn cài đặt: <http://docs.sirc.viettel.com/guide/LogAgent/>



## HƯỚNG DẪN THIẾT LẬP CẤU HÌNH BẢO MẬT CHO HỆ ĐIỀU HÀNH DOPRA

### I. Nội dung hướng dẫn

Hệ điều hành Dopra là hệ điều hành lõi Linux được Huawei xây dựng và sử dụng trong các hệ thống BSC/RNC. Để thực hiện hướng dẫn dưới, yêu cầu có SSH tool (putty), password của tài khoản root, lgnusr.

Hướng dẫn thiết lập an toàn cho hệ điều hành DOPRA nhằm đảm bảo 8 tiêu chuẩn ATTT bao gồm:

- Cài đặt và cập nhật bản vá cho hệ điều hành.
- Xóa hoặc vô hiệu hóa các dịch vụ, ứng dụng, giao thức mạng không cần thiết.
- Thiết lập chính sách tài khoản.
- Quản trị từ xa qua kênh truyền an toàn.
- Phân quyền tập tin và thư mục.
- Cài đặt và cấu hình firewall mềm.
- Thiết lập chính sách quản lý log.
- Cài đặt phần mềm giám sát ATTT.

### II. Chi tiết hướng dẫn

#### 1. Cài đặt hệ điều hành và cập nhật bản vá.

- Sử dụng phiên bản mới nhất của hệ điều hành khi cài đặt mới.
- Cập nhật các bản vá lỗi cho hệ điều hành: Bao gồm các bản vá lỗ hổng bảo mật đã được công bố và các bản vá theo yêu cầu của Tập đoàn.

**Chú ý:** Do Dopra là hệ điều hành đặc thù do đối tác phát triển riêng để chạy cho các tổng đài nên việc cập nhật bản vá phải có hợp đồng và hướng dẫn của đối tác để thực hiện.

#### 2. Xóa hoặc vô hiệu hóa các dịch vụ, ứng dụng, giao thức mạng không cần thiết

- Cài đặt tối thiểu các phần mềm, dịch vụ theo đúng chức năng được thiết kế của server.
- Gỡ bỏ hoặc vô hiệu hóa các gói dịch vụ không cần thiết, các gói dịch vụ lỗi thời có nguy cơ bị mất an toàn thông tin: Telnet, rcp, rsh, rlogin, nis, ftp...

*Vô hiệu hóa dịch vụ không cần thiết*

*Bước 1: Xác định thông tin về dịch vụ:*

```
# ps -e -o pid -o command | grep <tên_service>
```

*Xác định được PID tương ứng với dịch vụ cần tắt*

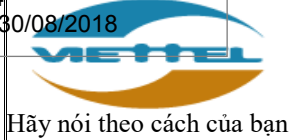
*Bước 2: Kill tiến trình dịch vụ*

```
# kill -9 PID
```

#### 3. Thiết lập chính sách tài khoản

- Xóa hoặc vô hiệu tất cả các tài khoản không sử dụng trên hệ thống

*Bước 1: Để tìm những tài khoản đang hoạt động trên hệ thống, ta sử dụng lệnh sau:*



```
# cat /etc/passwd | grep /*sh$ | awk -F: '{print $1}'
```

Bước 2: Để xóa 1 tài khoản "username" không sử dụng, ta dùng lệnh sau:

```
# userdel username
```

Hoặc

```
# passwd -l username
```

- Cấu hình chính sách mật khẩu cho tài khoản

- + Mật khẩu phải có độ dài tối thiểu 8 ký tự chứa ký tự viết hoa, viết thường, chữ số, ký tự đặc biệt.

Quản trị viên mở file cấu hình **/etc/pam.d/common-password** và cấu hình dòng có **pam\_cracklib.so** như sau (trên Dopro thường có sẵn dòng này, ta chỉ chỉnh sửa lại giá trị cho phù hợp):

```
password required pam_cracklib.so retry=3 lcredit=-1 ucredit=-1 dcredit=-1 ocredit=-1 minlen=8 uname_check enforce_root
```

- + Thời gian bắt buộc phải thay đổi mật khẩu người dùng: Thiết lập giá trị 90 ngày với hệ thống public và 180 ngày với hệ thống nội bộ.

Mở file **/etc/login.defs**, thay đổi tùy chọn như sau:

```
PASS_MAX_DAYS 90
```

```
PASS_MIN_LEN 8
```

```
PASS_WARN_AGE 7
```

Đối với các user đã tồn tại sẽ không bị ảnh hưởng bởi thiết lập trên, do đó thực hiện lệnh sau để thiết lập

```
# chage -M 90 <user người dùng >
```

- + Giới hạn mật khẩu mới không được trùng với mật khẩu gần nhất: Thiết lập giá trị là 2 với hệ thống nội bộ và 5 với hệ thống public.

Quản trị viên có thể sử dụng module **pam\_unix.so** của PAM để thiết lập số lần mật khẩu không được trùng lặp, cấu hình như sau:

Mở file cấu hình **/etc/pam.d/common-password** và cấu hình dòng có **pam\_unix.so** như sau (trên Dopro thường có sẵn dòng này, ta chỉ chỉnh sửa lại giá trị cho phù hợp):

```
password required pam_unix.so remember=5 [existing_options]
```

- + Mã hóa mật khẩu sử dụng thuật toán mã hóa an toàn (SHA-512)

Cấu hình để sử dụng loại thuật toán mã hóa tối ưu nhất mà hệ điều hành hỗ trợ.

- Kiểm tra điều kiện 1: Mở file **/etc/pam.d/common-password**, ở dòng **pam\_unix.so** có tham số **sha512** thì đảm bảo.
- Kiểm tra điều kiện 2: Mở file **/etc/shadow**:
  - User nào có ký hiệu **\$6\$** ngay sau thì đảm bảo.
  - User nào có dấu **!** hoặc **\*** sau tên là user bị lock → bỏ qua.
- Nếu không thỏa mãn 1 trong 2 điều kiện trên thì thực hiện như sau:

Mở file **/etc/default/passwd** và tìm dòng **comment** có dạng:





HƯỚNG DẪN THIẾT LẬP AN TOÀN  
THÔNG TIN CHO HỆ ĐIỀU HÀNH  
MÁY CHỦ

Ngày có hiệu lực: 01/9/2018

Ngày hết hiệu lực: 01/9/2019

Lần ban hành: 05

Trang: 75/71

# CRYPT={...}

Trong dấu ngoặc là các dạng mã hóa mà hệ điều hành hỗ trợ, nếu không có sha512 thì ta sẽ chỉ sử dụng md5, nếu có sha512 thì ta sẽ sử dụng loại mã hóa này.

Ví dụ chỉ sử dụng được md5, ta sẽ cấu hình như sau:

Bước 1: Mở file /etc/default/passwd, sửa lại giá trị tham số CRYPT như sau:

CRYPT=md5

Bước 2: Mở file /etc/pam.d/common-password và cấu hình dòng có pam\_unix.so như sau (trên Dopro thường có sẵn dòng này, ta chỉ chỉnh sửa lại giá trị cho phù hợp):

password sufficient pam\_unix [existing options] md5

#### 4. Sử dụng công cụ quản trị từ xa an toàn

Để đảm bảo yêu cầu bảo mật cho hệ thống, tránh trường hợp thất thoát dữ liệu trên đường truyền khi quản trị hệ thống từ xa yêu cầu thiết lập và sử dụng các dịch vụ quản trị an toàn. Cụ thể nếu sử dụng SSH để quản trị cho Dopro cần thực hiện các thiết lập sau:

- Yêu cầu quản trị từ xa sử dụng kênh truyền an toàn, có mã hóa  
Chỉ cho phép sử dụng giao thức SSH version 2.

Mở file cấu hình **/etc/ssh/sshd\_config**, sửa lại tùy chọn:  
Protocol 2

- Cấu hình chỉ cho phép tài khoản người dùng được phép SSH.

Mở file cấu hình **/etc/ssh/sshd\_config**, thêm tùy chọn sau:  
AllowUsers user1 user2

- Không cho phép tài khoản root đăng nhập trực tiếp từ xa.

Mở file cấu hình **/etc/ssh/sshd\_config**, sửa hoặc thêm tùy chọn sau:  
PermitRootLogin no

- Không cho phép tài khoản đăng nhập sai quá 05 lần.

- Giới hạn thời gian tự động ngắt phiên khi không có hoạt động trong một khoảng thời gian là 5 phút:

Mở file cấu hình **/etc/profile** và thêm 3 dòng sau vào cuối file:  
TMOUT=300  
readonly TMOUT  
export TMOUT

#### 5. Phân quyền tệp tin và thư mục

- Xác thực đường dẫn các biến môi trường PATH: Biến môi trường PATH không được chứa các đường dẫn tương đối, đường dẫn bất thường, đường dẫn trống:

Để kiểm tra đường dẫn PATH, ta dùng lệnh sau:

# echo \$PATH

Kiểm tra lại toàn bộ đường dẫn trong biến PATH xem có đường dẫn nào là





HƯỚNG DẪN THIẾT LẬP AN TOÀN  
THÔNG TIN CHO HỆ ĐIỀU HÀNH  
MÁY CHỦ

Ngày có hiệu lực: 01/9/2018

Ngày hết hiệu lực: 01/9/2019

Lần ban hành: 05

Trang: 76/71

*đường dẫn trống hoặc đường tương đối không.*

*Ví dụ của đường dẫn tuyệt đối (không cần phải thiết lập nữa):*

*/bin:/usr/bin:/sbin:/usr/sbin*

- Thiết lập cấu hình dịch vụ CRON
  - + Giới hạn tài khoản được phép chạy dịch vụ CRON bởi whitelist danh sách người dùng.
  - + Hạn chế quyền sửa các file cấu hình của CRON.

*Bước 1: Thực hiện xóa file cron.deny, nếu không có thì bỏ qua, thực hiện*

*Bước 2*

*# rm /etc/cron.deny*

*Bước 2: Thêm file cron.allow nếu hệ thống chưa có*

*# touch /etc/cron.allow*

*Bước 3: Sửa file /etc/cron.allow, cập nhật thêm các tài khoản được phép sử dụng dịch vụ CRON:*

*User1*

*User2*

*...*

*Bước 4: Hạn chế quyền sửa file cấu hình của dịch vụ CRON:*

*# chown root:root /etc/crontab*

*# chmod 600 /etc/crontab*

*# chown -R root:root /etc/cron.d /etc/cron.daily*

*# chmod -R go-rwx /etc/cron.d /etc/cron.daily*

## 6. Cấu hình tường lửa mềm

- Yêu cầu sử dụng tường lửa mềm trên hệ thống: Kiểm tra đảm bảo tường lửa mềm được bật:

*Sử dụng lệnh sau để kiểm tra:*

*# iptables -L -nv*

- Cấu hình tường lửa mềm chỉ mở vừa đủ các kết nối vào/ra trên hệ thống: Đối với hệ thống nội bộ, chỉ mở vừa đủ các kết nối vào. Đối với hệ thống public, mở vừa đủ các kết nối vào/ra.

**Chú ý:** Người quản trị cần phải cấu hình tường lửa ở chế độ ghi log các gói tin trong vòng 1-2 tuần. Sau đó sẽ phân tích log và thiết lập rule tương ứng.

*Bước 1: Tạo script để thiết lập tường lửa mềm*

*# mkdir /root*

*# cd /root*

*# touch iptables.sh*

*# vi iptables.sh*

*Trong file iptables.sh phải có các rule cần thiết cho quản trị và dịch vụ.*

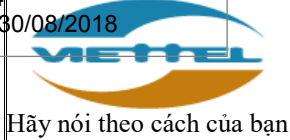
*Ví dụ các file rule như sau:*

*#####Phan rule khong thay doi#####*



```
iptables -F
iptables -P INPUT ACCEPT
iptables -P OUTPUT ACCEPT
iptables -P FORWARD ACCEPT
iptables -A INPUT -m state --state ESTABLISHED,RELATED -j ACCEPT
iptables -A INPUT -p icmp -j ACCEPT
iptables -A INPUT -i lo -j ACCEPT
iptables -A OUTPUT -j ACCEPT
#####TTDD
iptables -A INPUT -p tcp --dport 20 -s 10.61.128.0/24 -j ACCEPT
iptables -A INPUT -p tcp --dport 21 -s 10.61.128.0/24 -j ACCEPT
iptables -A INPUT -p tcp --dport 22 -s 10.61.128.0/24 -j ACCEPT
iptables -A INPUT -p tcp --dport 80 -s 10.61.128.0/24 -j ACCEPT
iptables -A INPUT -p tcp --dport 443 -s 10.61.128.0/24 -j ACCEPT
iptables -A INPUT -p tcp --dport 1024:65535 -s 10.61.128.0/24 -j ACCEPT
#####XLSC,DHVT
iptables -A INPUT -p tcp --dport 20 -s 192.168.252.0/24 -j ACCEPT
iptables -A INPUT -p tcp --dport 21 -s 192.168.252.0/24 -j ACCEPT
iptables -A INPUT -p tcp --dport 22 -s 192.168.252.0/24 -j ACCEPT
iptables -A INPUT -p tcp --dport 80 -s 192.168.252.0/24 -j ACCEPT
iptables -A INPUT -p tcp --dport 443 -s 192.168.252.0/24 -j ACCEPT
iptables -A INPUT -p tcp --dport 6088 -s 192.168.252.0/24 -j ACCEPT
iptables -A INPUT -p tcp --dport 8088 -s 192.168.252.0/24 -j ACCEPT
#####KTKV1
iptables -A INPUT -p tcp --dport 20 -s 192.168.173.0/24 -j ACCEPT
iptables -A INPUT -p tcp --dport 21 -s 192.168.173.0/24 -j ACCEPT
#####Phan rule khong doi#####
iptables -A INPUT -j LOG --log-level 4 --log-prefix "REJECT INPUT
IPTABLES: "
iptables -A FORWARD -j LOG --log-level 4 --log-prefix "REJECT FORWARD
IPTABLES: "
iptables -A INPUT -j REJECT --reject-with icmp-host-prohibited
iptables -A FORWARD -j REJECT --reject-with icmp-host-prohibited
#####Ket thuc rule #####
Bước 2:
Cấp quyền cho file:
# chmod u+x /root/iptables.sh
Bước 3:
Chạy file để thiết lập firewall mềm
#./iptables.sh
```

Ghi log những bản ghi không hợp lệ



Đảm bảo trong rule có các dòng sau:

```
iptables -A INPUT -j LOG --log-level 4 --log-prefix "REJECT INPUT  
IPTABLES: "  
iptables -A FORWARD -j LOG --log-level 4 --log-prefix "REJECT FORWARD  
IPTABLES: "
```

## 7. Thiết lập chính sách quản lý log

- Ghi log mặc định của hệ điều hành: Yêu cầu thiết lập cấu hình ghi tối thiểu các loại sau: message log, dmesg log, secure log → Mặc định hệ điều hành đã có syslog hoạt động và ghi đủ message log, dmesg log, secure log. Trong trường hợp syslog không hoạt động, đề nghị liên hệ đối tác để có phương pháp xử lý.

Cách kiểm tra syslog có hoạt động hay không:

```
# ps -ef | grep syslog | grep -v grep
```

Nếu không có dòng nào thì nghĩa là syslog đang không hoạt động.

- Cấu hình thời gian lưu log tối thiểu là 3 tháng

Bước 1: Mở file /etc/logrotate.conf, sửa các thông số về giá trị như sau:

weekly

rotate 12

create

dateext (thêm vào trước dòng include /etc/logrotate.d)

Bước 2: Mở các file trong thư mục /etc/logrotate.d, sửa các thông số về giá trị như sau:

maxage 365

rotate 99

create 600 root root

size +4096k

Ở file wtmp: thêm một dòng create 600 root root vào sau missingok

**Chú ý:** Theo quy định của Tập đoàn thời gian tối thiểu lưu log là 3 tháng, tuy nhiên nếu máy chủ hiện tại không đủ dung lượng ổ cứng để lưu log trong 3 tháng thì quản trị có thể thiết lập lại để phù hợp với thực tế tránh log đầy làm treo máy chủ.

## Đồng bộ thời gian hệ điều hành về máy chủ tập trung

Không cần thiết lập vì BSC/RNC đồng bộ từ hệ thống M2000.

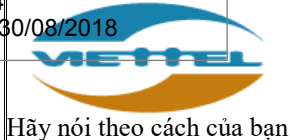
## 8. Cài đặt các phần mềm giám sát ATTT

Yêu cầu cài đặt đầy đủ các phần mềm giám sát ATTT do TT.ANM cung cấp

- Phần mềm Server Endpoint để hỗ trợ giám sát hành vi bất thường và vi phạm baseline.

Hướng dẫn cài đặt: [http://docs.sirc.viettel.com/guide/install\\_se\\_agent/](http://docs.sirc.viettel.com/guide/install_se_agent/)

- Phần mềm Filebeat và OSSEC agent để hỗ trợ lấy log và event.



Hướng dẫn cài đặt: <http://docs.sirc.viettel.com/guide/LogAgent/>

**PHỤ LỤC**  
**DANH SÁCH CÁC PHẦN MỀM GIÁM SÁT ATTT CẦN CÀI ĐẶT**

	<b>Server Endpoint</b>	<b>Filebeat</b>	<b>Winlogbeat</b>	<b>OSSEC</b>	<b>OneAgent</b>
<b>CentOS/RHEL 4X</b>	M			M	
<b>CentOS/RHEL 5X</b>	M			M	
<b>CentOS/RHEL 6.X/7.X</b>	M	M			
<b>Oracle Enterprise Linux 6/7 with RHEL Kernel only</b>	M	M			
<b>Ubuntu 14.04</b>	M	M			
<b>Ubuntu 16.04</b>	M	M			
<b>SuSE Enterprise 10/11</b>	M			M	
<b>SLES 11 SP4/12</b>	M	M			
<b>Debian 7.x/8.x</b>	M	M			
<b>Windows Server 2003</b>	M			M	
<b>Windows Server 2008/R2</b>	M	M	M		M
<b>Windows Server 2012/R2</b>	M	M	M		M
<b>OSX 10.12</b>		M			
<b>Sun Solaris 10 Intel</b>	M			M	
<b>Sun Solaris SPARC/SmartOS</b>				M	
<b>AIX</b>				M	
<b>Windows 7</b>					M
<b>Windows 8</b>					M
<b>Windows 8.1</b>					M
<b>Windows 10</b>					M
<b>Ubuntu Desktop 12.x</b>					M
<b>Ubuntu Desktop 14.x</b>					M
<b>Ubuntu Desktop 16.x</b>					M