Cài đặt tường lửa (Firewall) (SoPhos UTM9 thông qua máy ảo Vmware)

Piller	Dashboard for Friday, May 10, 2024 1	4:34:5	19
Im	🕏 demo	0	Interface
Definitions Users	Model: ASG Software		all
Interfaces & Routing	Subscriptions: Base Functionality		eth1
Network Services	Metwork Protection		eth2
Network Protection	Webierver Erotection		cors
Web Protection	Uptime: Od 0h 10m		A0
Email Protection	The Managine Information	•	Ŷ
Advanced Protection	Eirmanna varsion: 0.719.5	-	121703
Wireless Protection	1 Update(s) available for installation		9 Cu
Webserver Protection	Pattern version: 239578		O Fire
RED Management	Last check: 8 minutes ago		O Wel
Site to site VPN	Resource Usage	0	O Net
Remote Access	СРИ 🖸 👘	1	O SM
Logging & Reporting	RAM [1] 10% of 4.3 G8		O RE

đầu tiên trong hệ thống. Dưới đây là một số lợi ích khi sử dụng tường lửa cho doanh nghiệp: liệu.

vấn đề pháp lý.

vụ phân tán (DDoS). Nó cũng giúp phát hiện phần mềm độc hại và virus. Giám sát hoạt động mạng: Tường lửa giám sát toàn bộ các hoạt động đăng nhập và truy cập vào hệ thống mạng

Trong Phần nội dung này ta tìm hiểu cách cài đặt tường lửa (Firewall) (SoPhos UTM9 thông qua máy ảo Vmware)

Name	Туре	State	Link	In	Out	C
Ul Interfaces Internal Joused Joused Joused	Ethernet	Up	Up	28.7 kbit 28.7 kbit	42.31	dbit idbit
Botnet/cc is disable	ofection ommand-and- ed	control tr	affic de	etection	0 Indirectional ()	. O
nt System Con	figuration					
all is active wi sion Preventio	th 5 rules In is inactive					
Filtering is ina ork Visibility i Proxy is inac Proxy is inac	ctive s inactive tive tive					
	2152					

- Tường lửa (firewall) là một phần quan trọng trong bảo mật mạng của doanh nghiệp và thường được coi là tuyến phòng thủ
- Bảo vệ dữ liệu và thông tin: Tường lửa giúp bảo vệ dữ liệu và thông tin của khách hàng, giảm thiếu nguy cơ mất mát dữ
- Tuân thủ quy định bảo mật: Sử dụng tường lửa giúp doanh nghiệp tuân thủ các quy định bảo mật và bảo vệ mạng khỏi các
- Ngăn chặn cuộc tấn công: Tường lửa phát hiện và ngăn chặn các cuộc tấn công như từ chối dịch vụ (DoS) và từ chối dịch
- Lọc nội dung truy cập: Tường lửa có khả năng lọc nội dung truy cập, ngăn chặn các luồng thông tin không mong muốn.





Link tải file utm9 tại đây : https://www.sophos.com/en-us/support/downloads

	X & C D D L	≡
volved over the last 12 months. Read the report		5
rtners 🗙 About 🌱 Support 🜱	Q ()	
? Get help now. >		Zele
		+
		-
		•
truet Sonhoe		0
and suprios		-
any other		
y provider.		
Learn More		
xpert >		
ile utm9.iso tại địa chi	l help you	
am/		

sophos.com/en-us

SOPHOS

Services & Products *

Solutions *

Sophos Support

\$ XA Discover how ransomware and its business impacts have evolved over the last 12 months. Read the report Q \oplus Support ^ About Y Partners * **Product Support Get Help** ources Support Portal ? Sophos Community Forums ? ids and Updates 🔌 Im Support Packages Sophos Firewall mentation Partner Care Support **Technical Training** Sophos Endpoint > Tech Support Techvids - Training Videos Sophos Cloud Sophos Status Page Sophos Central

Sophos Email ?

Support Portal

See How 🕑

Speak with an expert >

Tại Tab Resources ta click vào download and update

cybersecurity provider.

Submit a Threat

Learn More



Tiếp đến ta click vào mục UTM Downloads

Downloads	Firewall Installers	UTM Downloads
9.719-3.1		
Sophos UTM		
Platform: UTM v9 hardware appliance		
Size : 1.3 GB		
9.719-3.1		
Sophos UTM		
Platform: UTM v9 software appliance		
Size: 1.3 GB		

Ta Click vào Download như hình, Sophos yêu cần đăng ký thông, sau đó sohops sẽ gởi link để Download





Tiếp đến ta cần cài máy ảo Vmware Xem hướng dẫn tại search google



Ta click vào khởi tạo máy ảo mới làm như hình

			1
			<u> </u>
Nizard			
stem Installation			
is like a physical computer; it needs an operating you install the quest operating system?			
able			
file (iso):			
e iso sophos utm 9\asg-9.718-5.1.i Browsel			
rating system later.			
< Back Next > Cancel			



Chọn Linux và click tab Next



Đặt tên & chọn nơi lưu cho máy ảo và click next

Library ×	My Computer × My Computer		
 Windows Server 2 Windows 10 x64 Kali linux kali linux 2024 Sophos 	Name Kali linux kali linux 2024 Sophos Windows 10 x64 Windows Server 2025	Status Powered Powered Powered	off New Virtual Machine Wizz Name the Virtual Machine Virtual r Virtual Machine L Sophos Location C:\Use The def Folder: New f Make New Fold
< >			

Như hình tôi chọn lưu vào ổ đĩa D và click vào <mark>next</mark>





Lựa chọn tích vào ô như hình rồi click vào next

	• []
ne Wizard X	
acity	
you want this disk to be?	
hard disk is stored as one or more files on the host lisk. These file(s) start small and become larger as you add d data to your vertual machine.	
or Other Linux 6 Jernel 64-bit: 8 GB	
ac a cincle file	
ito multiple files	
makes it easier to move the virtual machine to another	
y reduce performance with very large disks.	
< Back Next > Cancel	



Tại đây ta phân bổ phần cứng cho máy ảo



Ta Phân bổ core CPU, Ram, ổ đĩa và các phần cứng mở rộng khác

				1			
			×				
				T			
sors	12	1.24					
er of processors:	2	2					
er of cores per processor:	1	-0					
processor cores:	2						
zation engine	10.11/01/1						
tualize Intel VT-x/EPT or A tualize CPU performance c	MD-V/RVI punters						
rtualize IOMMU (IO memory	management	unit)					
		Gancal					
J. avaiiduse	OK	Cancel	Help				



Tại mục use iso image file : Ta Browse đến file iso vừa tải



Hình này cho thêm card mạng và cấu hình nat cho card mạng

	×		
S			
ed			
at power on			
inection			
: Connected directly to the physical network			
icate physical network connection state			
sed to share the host's IP address			
ly: A private network shared with the host			
- Specific virtual notwork			
iment:			
OK Cancel	Help		
			and the second se



Ta có thể thêm nhiều card mạng ảo



Như hình ta thấy tôi thêm 4 card mạng ảo cho Sophos và Click OK

6	X My Computer	phos utm9.7 ×	
Type here to sea			
My Computer	I sophos utm9.	7	
Windows Ser	/eri	schioa	
Windows 10 >	164	tings	
L Kali linux 202		unga	
Sophos	• Dovices		
C sophos utm9.	7	12 CP	
		4,5 00	
	Hard Dick (SCSI)	50 GR	
		Jucino file Ev@bb	
	S Network Adapter	Bridged (Autom	
	Network Adapter 2	Host-only	
	Network Adapter 3	Host-only	
	Network Adapter 4	Host-only	
	USB Controller	Present	
	di Sound Card	Auto detect	
	Display	Auto detect	
	ing Display	Auto detect	
	▼ Description		
	Type here to enter a descrip	ption of this virtual	
	machine.		
			 Virtual Machine Details
			State: Po
			Configuration file: D. Hardware compatibility: We
			Primary IP address: Ne

Tiếp đến ta click vào mục Power on this virtual machine



owered off \sophos utm9.7\sophos utm9.7.vmx orkstation 17.5.x virtual machine etwork information is not available



Tiến trình này đang khởi động máy ảo

Mare[®]

Press F2 to enter SETUP, F12 for Network Boot, ESC for Boot Menu

The host-only adapter driver does not seem to be running. If you have not rebooted the host since installing the host-only network adapter, you need to do so before you can use this support. Otherwise, check the system Event Log for an explanation of why service VMnetAdapter did not startup properly. Virtual device 'Ethernet1' will start disconnected.



Quá trình cài đặt bắt đầu

1.692552] pcieport 0000:00:18.6: Signaling PME through PCIe PME interrupt 1.692651] pcieport 0000:00:18.7: Signaling PME through PCIe PME interrupt 1.746046] Serial: 8250/16550 driver, 4 ports, IRQ sharing enabled 1.747451] Linux agpgart interface v0.103 1.747500] agpgart-intel 0000:00:00.0: Intel 440BX Chipset 1.747975] agpgart-intel 0000:00:00.0: AGP aperture is 256M @ 0×0 1.751906) usbcore: registered new interface driver usbserial 1.7520381 usbcore: registered new interface driver usbserial_generic 1.752215] usbserial: USB Serial support registered for generic 1.7525061 i8042: PNP: PS/2 Controller [PNP0303:KBC, PNP0f13:MOUS1 at 0x60,0x 1.753176] serio: i8042 KBD port at 0×60,0×64 irq 1 1.753227] serio: i8042 AUX port at 0×60,0×64 irq 12 1.7537651 mousedev: PS/2 mouse device common for all mice 1.754362] hidraw: raw HID events driver (C) Jiri Kosina

1.769318] drivers/rtc/hctosys.c: unable to open rtc device (rtc0) 1.776197] Freeing unused kernel memory: 408K (804ca000 - 80530000)



Quá trình cài đặt đang kiểm tra card mạng



Chọn ngôn ngữ bàn phim







Lựa chọn card mạng để kết nối

t	Admin I	ntei	face		
				1 1 102	
10	u will u	seal	to acce	ss th	e webhamin
e	PRO/1000	MT	Single	Port	Adapter
e	PRO/1000	MT	Single	Port	Adapter
а	PRO/1000	MT	Single	Port	Adapter
в	PRO/1000	MT	Single	Port	Adapter
			10 C		1172
	45 28	amer	ally ZHo	Int	

Ta có thể đặt lại IP để đăng nhập vào phần quản lý

work Confi	guration	1		
dministrat	ive netw	ork interfac	2:	
2.168.0	-			
5.255.255.	8			
content de la content		(optional)		
k> <next></next>	<canc< td=""><td>el></td><td></td><td></td></canc<>	el>		
_				

Ta nên đặt lớp mạng theo ip router nhà cung cấp

juration	
ive network interface:	
(optional)	
<cancel></cancel>	

Xem tiến trình cài đặt bao gồm 7 bước

ut∕output erre	or Sophos	UTM (9.7	
Formatting (Si 75% ition	tep 2/7)		
<mark>«Cant</mark>			
View log <f:< td=""><td>1> Help</td><td></td><td></td></f:<>	1> Help		

Xem tiến trình cài đặt đến bước 6

Quá Trình cài đã thành công

Ta click vào tab Reboot như hình

ophos UTM 9.7
ished
USB device, connect the ace to your local network ing the Reboot button.
n user interface and
ort>
0117
le l p

Booting 'Sophos UTM 9.7 (3.12.74-0.434058663.g1ba2494.rb7-smp64)'

root (hd0,0)
Filesystem type is ext2fs, partition type 0x83
kernel /boot/vmlinuz-3.12.74-0.434058663.g1ba2494.rb7-smp64 root=/dev/disk/by-l
abel/root vga=791 rootflags=data=ordered splash=silent
[Linux-bzImage, setup=0x3c00, size=0x2bb490]
initrd /boot/initrd-3.12.74-0.434058663.g1ba2494.rb7-smp64

Tiến Trình đang khởi động

Tiến trình đang load vào giao diện Sophos utm9.7

192.168.0.101 login: _

Như hình Hệ thống Sophos yêu cầu đăng nhập

Kiểm tra ip vừa rồi ta add vào như hình

6	-)		×								
ne and the opera	ating system	m boots up	, click "I Fi	nished Installing".				I Finish	ed Installing	Help	
						1			ti Fili Fili d	a 131.	

Đăng Nhập Vào phần Quản Lý Sophos thông qua địa chỉ IP và thêm port 4444

							ال	,
		☆	3	<u>ن</u>	≡J	٢	₹	=
								R.
								4
								4
								6
i là kết nối riêng tư								
inh cấp thông tin của bạn từ 192.168.0.101 (ví								
neu mem								
								-
của Cốc Cốc, hãy <u>bật chế độ bảo vệ tăng</u>								
Quay lại trang an toàn								
đá là 192 168 0 101 : chứng chỉ bảo mật của								
r tính của bạn tin cậy. Điều này có thể do định								
ối của bạn.								
								•

Balance -	Dashboard for Friday, May 10, 20	24 14:34:5	7								
Im	S demo	0	Interface	Name	Туре	State	Link	In	Out 🕥		
etinitions & Users	Model: ASG Software License ID: 000000		all eth0	All Interfaces	Ethernet	Up	Up	28.7 kbit	42.3 kbit		
terfaces & Routing	Subscriptions: Base Functional	ty	eth1	Unused	11201221110221	1.72	1.11.11				
etwork Services	Network Protects	00	eth2 eth3	Unused Unused							
etwork Protection	Wireless Prote	stion	13017	19/18/01/							
eb Protection	Uptime: 0d 0h 10m		Advanced Threat Protection								
mail Protection	Wareion Information	0	Ŷ	Botnet/co is disable	ommand-and- id	control t	raffic de	rtection	O Hosty		
dvanced Protection	Einmeara varsion: 0 718.5	~									
ireless Protection	1 Update(s) available for installati	Current System Configuration									
ebserver Protection	Pattern version: 239578	Intrusion Prevention is inactive									
ED Management	Last check. o minutes by	10	Ø Web	Filtering is ina	ctive	1111					
te-to-site VPN	Resource Usage	0	O Network Visibility is inactive								
emote Access	CPU O 0%		SMTP Proxy is inactive POP3 Proxy is inactive RED is inactive								
ogging & Reporting	RAM [1] = 10% of 4.3 G	B									
upport	Data Disk 📟 🧮 8% of 14.9 Gi	в	Ø Wire	less Protection	n is inactive						
πο ασ			Site-	to-Site VPN is	inactive						
	Firewalls 70 sectors filesed		O Web	Application Fi	naceve	s.					
	IPS: 0 attacks blocked		Sophos UTM Manager is not configured								
	Antivirus: 0 items blocked	Antivirus: 0 items blocked		Sophos Mobile Control is inactive							
	Antispam: 0 emails blocked Antispyware: 0 items blocked		() HA/	Cluster is inacti	ve						
	Web Filter: 0 URLs filtered		O Anti	virus is inactive	E						
	WAF: 0 attacks blocked	Antispam is inactive									

Giao Diện Tường lửa (Fireware) SoPhos