

# SETUP: Please turn on both VMs and login as root.

🤏 vm1 - VMware Workstation 12 Player (Non-commercial use only) –		×	🤏 vm2 - VMware Workstation 12 Player (Non-commercial use only)	- 🗆 🗙
Player 🕶 📕 💌 🛱 🔯	*		Player 🕶 📕 🕶 🛱 🛱	« 📰
Man 10:19 vml (Not later?			Mon 10:19 vm2 Not interform	
CentOS		>	CentOS	

SETUP: Make sure that the VMs have the correct IPs as below:

- VM1: 192.168.1.1 | 255.255.255.0
- VM2: 192.168.1.2 | 255.255.255.0

SETUP: Ensure that you can ping the other VMs from all VMs as per below:-

	root@localhost:~	- 0	×
File Edit View Search Terr	ninal Help		
<pre>[root@localhost ~]# ping PING 192.168.1.1 (192.168 64 bytes from 192.168.1.1 64 bytes from 192.168.1.1 64 bytes from 192.168.1.1 64 bytes from 192.168.1.1 64 bytes from 192.168.1.1 72 [1]+ Stopped [root@localhost ~]# ping PING 192.168.1.2 (192.168 64 bytes from 192.168.1.2 64 bytes from 192.168.1.2 64 bytes from 192.168.1.2 64 bytes from 192.168.1.2 64 bytes from 192.168.1.2 72 [2]+ Stopped [root@localhost ~]#</pre>	<pre>192.168.1.1 3.1.1) 56(84) bytes of data. : icmp_seq=1 ttl=64 time=0.470 ms : icmp_seq=2 ttl=64 time=0.170 ms : icmp_seq=3 ttl=64 time=0.224 ms : icmp_seq=4 ttl=64 time=2.51 ms : icmp_seq=5 ttl=64 time=0.173 ms ping 192.168.1.1 192.168.1.2 3.1.2) 56(84) bytes of data. 2: icmp_seq=1 ttl=64 time=0.048 ms 2: icmp_seq=3 ttl=64 time=0.050 ms ping 192.168.1.2 </pre>		

SETUP: Open Wireshark in vm2 and start capturing on the interface.

	Ca	pturing from eno167	77736 [Wireshark 1.10.14	(Git Rev Unknow	n from unkno	wn)]		• ×
File I	Edit View Go C	apture Analyze Sta	itistics Telephony Tools Inte	ernals Help				
0	۵ 🔳 🛋	(  🖪 🗎 🗙	C   Q 🔄 🗞 🖏			1	-   🏹	×
Filter:	:		<ul> <li>Expression</li> </ul>	on Clear Apply	Save			
No.	Time	Source	Destination	Protoco	Length Info			
	1 0.000000000	192,168,1,2	192.168.1.1	ICMP	98 Echo	(ping)	request	id=0x2
	2 0.000069717	192.168.1.1	192.168.1.2	ICMP	98 Echo	(ping)	reply	id=0x2
	3 1.001017431	192.168.1.2	192.168.1.1	ICMP	98 Echo	(ping)	request	id=0x2
	4 1.001062278	192.168.1.1	192.168.1.2	ICMP	98 Echo	(ping)	reply	id=0x2
	5 2.001819086	192.168.1.2	192.168.1.1	ICMP	98 Echo	(ping)	request	id=0x2
	6 2.001863189	192.168.1.1	192.168.1.2	ICMP	98 Echo	(ping)	reply	id=0x2
	7 3.002651637	192.168.1.2	192.168.1.1	ICMP	98 Echo	(ping)	request	id=0x2
	8 3.002701291	192.168.1.1	192.168.1.2	ICMP	98 Echo	(ping)	reply	id=0x2
_						-		

 Frame 1: 98 bytes on wire (784 bits), 98 bytes captured (784 bits) on interface 0

 Ethernet II, Src: Vmware\_46:7e:45 (00:0c:29:46:7e:45), Dst: Vmware\_ee:f5:ce (00:0c:29:ee:f5:ce)

 Internet Protocol Version 4, Src: 192.168.1.2 (192.168.1.2), Dst: 192.168.1.1 (192.168.1.1)

 Internet Control Message Protocol

## STEP: Start the terminal in both VMs.

🎕 vm1 - VMware Workstation 12 Player (Non-commercial use only) —	I		×	📽 vm2 - VMware Workstation 12 Player (Non-commercial use only) – 🗆 🗙
Player 🔻 📕 💌 🖶 🛄 🔯		<b>«</b>		Player 🕶 📙 🖛 🛱 🖾 🧶 🐻
S Applications ▼ Places ▼ Places ▼				Applications  Places  Places
File Edit View Search Terminal Help [root@localhost -]#	-		×	Capturing from eno16777736 [Wireshark 1.10.14 (Git Rev Unknown from unknown)] × File Edit View Go Capture Analyze Statistics Telephony Tools Internals Help root@localhost.* × File Edit View Search Terminal Help Fite:
0020 01 01 08 00 ad e2 2d 30 00 01 fd ad 02 57 00 00			Ť	S eno16777736: <live capture="" default<="" in="" no="" packets="" profile:="" prog="" td=""></live>

STEP: Install Libreswan (already done for you) in both VMs.

[root@vm2 ~]# yum install liberswan

Step: Initialize a new database. If a db already exist use rm /etc/ipsec.d/\*db to remove and then initialize a new one on both VMs.

[root@vm2 ~]# ipsec initnss Initializing NSS database See 'man pluto' if you want to protect the NSS datab ase with a password

STEP: Check if IPSEC service is running on both VMs.

[root@vm2 ~]#

root@vm2:~ \*
File Edit View Search Terminal Help
[root@vm2 ~]# systemctl status ipsec
• ipsec.service - Internet Key Exchange (IKE) Protoc
ol Daemon for IPsec
Loaded: loaded (/usr/lib/systemd/system/ipsec.ser
vice; disabled; vendor preset: disabled)
Active: inactive (dead)
[root@vm2 ~]#

STEP: Start IPSEC Service on both VMs.

[root@vm2 ~]# systemctl start ipsec
[root@vm2 ~]#

STEP: Check the status again on both VMs.

[root@vm2 ~]# systemctl status ipsec • ipsec.service - Internet Key Exchange (IKE) Protoc ol Daemon for IPsec Loaded: loaded (/usr/lib/systemd/system/ipsec.ser vice; disabled; vendor preset: disabled) Active: active (running) since Sun 2016-03-27 23: 27:49 EDT; 29s ago Process: 4638 ExecStartPre=/usr/sbin/ipsec --check nflog (code=exited, status=0/SUCCESS) Process: 4633 ExecStartPre=/usr/sbin/ipsec --check nss (code=exited. status=0/SUCCESS)

STEP: Important to add IPSEC to start on startup on both VMs.

[root@vm2 ~]# systemctl enable ipsec Created symlink from /etc/systemd/system/multi-user. target.wants/ipsec.service to /usr/lib/systemd/syste m/ipsec.service. [root@vm2 ~]#

## ! IMPORTANT INFO !

We are implementing HOST – to – HOST IPSEC VPN Tunnel

The two hosts are refered to as "left" and "right".

We are going to use vm1 as the "left".

And vm2 as "right".

STEP: Generate an rsa key for VM1 (left) as per below: -

# ipsec newhostkey --configdir /etc/ipsec.d \

--output /etc/ipsec.d/www.example.com.secrets

# ipsec showhostkey --left



## STEP: Generate rsa key for VM2 as per below: -

# ipsec newhostkey --configdir /etc/ipsec.d \

--output /etc/ipsec.d/www.example.com.secrets

## # ipsec showhostkey -right

🤏 vm2 - VMware Workstation 12 Player (Non-commercial use only)	
Player 🕶 📔 💌 🖨 🖂 🔯	
Activities >- Terminal - Sun 2	3:4
root@	vm2
File Edit View Search Terminal Help	
<pre>[root@vm2 ~]# ipsec newhostkeyconfigdir /etc/ipsec.d \</pre>	:ret 1+Q/ 1g5t :iUC )o1r =GzS

STEP: Create a new IPSEC config file using for favorite editor in both VMs: -

# nano /etc/ipsec.d/my\_host-to-host.conf

```
[root@vm2 ipsec.d]# nano /etc/ipsec.d/my_host-to-host.conf
[root@vm2 ipsec.d]#
```

STEP: In the config file we can place the IPSEC configuration info as below in both VMs: -

### conn mytunnel

leftid=@west.example.com

left=192.1.2.23

leftrsasigkey={Paste rsa key for left as generate above}

rightid=@east.example.com

right=192.1.2.45

rightrsasigkey={Paste rsa key for right as generate above}

authby=rsasig

# load and initiate automatically

```
auto=start
```





STEP: On both VMs add the tunnel that we created: -

# # ipsec auto --add mytunnel

🧠 vm2 - VMware Workstation 12 Player (Non-commercial use only)	9 <u>00</u> 9			×
Player 🕶 📔 🕶 🛱 🖂 🔯			<b>«</b> [	1
♦ Activities Yerminal  Mon 00:03		<b>(</b> 0)	С	۲
root@vm2:/etc/ipsec.d		×		
File Edit View Search Terminal Help				
<pre>[root@vm2 ipsec.d]# ipsec autoadd mytunnel 002 "mytunnel": deleting connection 002 added connection description "mytunnel" [root@vm2 ipsec.d]#</pre>				
🚳 vm1 - VMware Workstation 12 Player (Non-commercial use only) — [		×		
Player ▼   🚺 ▼ 🖧 🛱 🔯	*			
Applications  Places  Mon 00:04	4) Č	) - (		
root@localhost:* -	•	×		
File Edit View Search Terminal Help				
002 "mytunnel": deleting connection 002 added connection description "mytunnel" [root@localhost ~]#				
STEP: On any "ONE" of the VM turn on the connection: -				
# ipsec autoup mytunnel				
[root@vm2 ipsec.d]# ipsec autoup mytunnel 002 "mytunnel" #4: initiating Main Mode				
104 "mytunnel" #4: STATE_MAIN_I1: initiate 003 "mytunnel" #4: received Vendor ID payload [Dead Peer Detect				
ion] 003 "mytunnel" #4: received Vendor ID payload [FRAGMENTATION]				
003 "mytunnel" #4: received Vendor ID payload [RFC 3947] 002 "mytunnel" #4: enabling possible NAT-traversal with method				
RFC 3947 (NAT-Traversal) 002 "mytuppel" #4: trapsition from state STATE MAIN I1 to state				
STATE_MAIN_I2				
003 "mytunnel" #4: NAT-Traversal: Result using RFC 3947 (NAT-Tr	L X « ■ c.d X rtunnel mel" Mon 00:04 ■ ● O ~ . ■ X (Dead Peer Detect [FRAGMENTATION] [RFC 3947] rsal with method _MAIN_I1 to state Decting MR2 RFC 3947 (NAT-Tr MAIN_I2 to state			
002 "mytunnel" #4: transition from state STATE_MAIN_I2 to state				
108 "mytunnel" #4: STATE_MAIN_I3: sent MI3, expecting MR3				
003 "mytunnel" #4: received Vendor ID payload [CAN-IKEv2]				

IMPORTANT: In Wireshark on VM2 you will see ISAKMP connection packets establishing the IPSEC tunnel. Please ensure that you stop once you see these packets and explore them.

The second second second second	100 L 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1			200	~
" Kali-Linux-2016.1-vm-i686 - VMwa	re Workstation 12 Player (Non-	-commercial u	se only) —		X
Player •   🚺 • 🛱 🛱 🔯					*
Applications 🔻 Places 🔻	🙋 Wireshark 🔻	Mon 00:12	,# 1 ×	<ul> <li>(i)</li> </ul>	•
		*eth1		00	0
File Edit View Go Capture	Analyze Statistics Tel	ephony Wi	reless Tools Help		-
		24 🕈			
📕 Apply a display filter <ctrl- <="" td=""><td>&gt;</td><td></td><td>Expre</td><td>ssion</td><td>+</td></ctrl->	>		Expre	ssion	+
No. Tim Source	Destination	Protocol I	.engtl Info		-
119 5… Vmware_95:8a:50	Vmware_23:8d:df	ARP	42 192.168.20.254 is at 00:0c:29:95:8	a:50	
120 5 192.168.20.1	192.168.10.1	ISAKMP	834 Identity Protection (Main Mode)		
121 5 192.168.10.1	192.168.20.1	ISAKMP	186 Identity Protection (Main Mode)		
122 5 192.168.20.1	192.168.10.1	ISAKMP	398 Identity Protection (Main Mode)		
123 5 192.168.10.1	192.168.20.1	ISAKMP	398 Identity Protection (Main Mode)		
124 5 192.168.20.1	192.168.10.1	ISAKMP	598 Identity Protection (Main Mode)		
125 5 192.168.10.1	192.168.20.1	ISAKMP	566 Identity Protection (Main Mode)		
126 5 192.168.20.1	192.168.10.1	ISAKMP	518 Quick Mode		
127 5 192.168.10.1	192.168.20.1	ISAKMP	438 Quick Mode		
128 5 192.168.20.1	192.168.10.1	ISAKMP	102 Quick Mode		
129 5 Vmware_23:8d:df	Vmware_95:8a:50	ARP	60 Who has 192.168.20.254? Tell 192.10	68.20.1	
130 5… Vmware_95:8a:50	Vmware_23:8d:df	ARP	42 192.168.20.254 is at 00:0c:29:95:8	a:50	E
131 5 192.168.10.1	192,168,20,1	ISAKMP	518 Quick Mode		
132 5 192.168.20.1	192.168.10.1	ISAKMP	438 Quick Mode		
133 5 192.168.10.1	192.168.20.1	ISAKMP	102 Quick Mode		
134 5 Vmware_95:8a:50	Vmware_23:8d:df	ARP	42 Who has 192.168.20.1? Tell 192.168	.20.254	
135 5 Vmware_23:8d:df	Vmware_95:8a:50	ARP	60 192.168.20.1 1s at 00:0c:29:23:8d:0	df	-
					F
Erome 1, CO buter on Lire /	(480 bits) co butos os	stured (490	hite) en interfese 0		in the second second
Ethorpot TT Src: \/muoro 23	(480 bits), 60 bytes ca	df) Det:	(mularo OF: 20:E0 (00:00:20:0F: 20:E0)		
<pre>&gt; Ethernet II, Sit. Viiware_20</pre>	(request)	.ur), bst.	vmwale_95.68.50 (00.00.29.95.68.50)		
Address Resolution Frotocol	(Tequest)				
0000 00 0c 29 95 8a 50 00 0c	29 23 8d df 08 06 00	01)	*** )#******		
0010 08 00 06 04 00 01 00 0c	29 23 80 df c0 a8 14	01	n exe - 2年 exerce a		
0020 00 00 00 00 00 00 C0 a8	14 Te 00 00 00 00 00		and a state of the		
0030 00 00 00 00 00 00 00		2.4.4.4.4	Carla Carla Ala		

STEP: Ping from either VM1 or VM2 and you can observe the ESP encrypted packets:

Applica	ations	<u>/</u> iew <u>G</u> o	laces ▼	Wireshar Analyze <u>S</u> t	k ▼ Ca atistics	Mon 00:12 pturing from Telephony V	2 n eth1 Vireless Ic	pols <u>H</u> e	elp ⊕	, <b>*</b>	1	/	•) (	0
Appl	yad	splay filte	er <ctrl-></ctrl->		• •				•			Expre	ssion	
_	Tim	Source		Destinati	on	Protoco	Lengt Info		_					
-	1 0	192,168	.10.1	192.168	20.1	ESP	166 ESP	(SPI=0	x7179c	f80)				1
	2 0	192.168	.20.1	192.168.	10.1	ESP	166 ESP	(SPI=0	xe63f8(	Dae)				
	3 1	192.168	.10.1	192.168.	20.1	ESP	166 ESP	(SPI=0	x7179c	f80)				
	4 1	192.168	.20.1	192.168.	10.1	ESP	166 ESP	(SPI=0	xe63f80	Dae)				
	5 2	192.168	.10.1	192.168.	20.1	ESP	166 ESP	(SPI=0	x7179c	f80)				
	6 2	192.168	.20.1	192.168.	10.1	ESP	166 ESP	(SPI=0	xe63f80	Dae)				
	7 3	192.168	.10.1	192.168.	20.1	ESP	166 ESP	(SPI=0	x7179C	f80)				
	8 3	192.168	.20.1	192.168.	10.1	ESP	166 ESP	(SPI=0	xe63f8(	Dae)				
Fram	e 1:	166 byte	s on wire (	1328 bits),	166 byt	es captured	(1328 bits	) on in	terfac	e 0				
Ethe Inte Enca	rnet rnet psula	II, Src: Protocol ting Sec	Vmware_95: Version 4, urity Paylo	8a:50 (00:0 Src: 192.1 ad	C:29:95: 68.10.1,	8a:50), Dst: Dst: 192.16	Vmware_23 8.20.1	:8d:df	(00:0c	:29:2	3:8d:df)			
00 0 10 0 20 1	00 0c 00 98	29 23 8 7f 34 4 71 79 c	d df 00 0c 0 00 3f 32 f 80 00 00	29 95 8a 5 1c ad c0 a 00 08 71 5	0 08 00 8 0a 01 b 49 08	45 00)# c0 a84 5c c9qv	)P. @.?2 	.E.						

STEP: you can use setkey -D in both VMs to view the Security Association DB as below:-

```
root@vm2:~/Downloads
                                                                      ×
File Edit View Search Terminal Help
[root@vm2 Downloads]# setkey -D
192.168.10.1 192.168.20.1
       esp mode=tunnel spi=3752158016(0xdfa56340) regid=16401(0x00004011
       E: aes-cbc 5ec6772e d4fd2dc1 20de531f 9f687dc5
       A: hmac-shal 9a6984f8 bb1fe028 5b6d59cf 2c5b1061 f53e9de3
       seq=0x00000000 replay=32 flags=0x00000000 state=mature
       created: Mar 28 00:52:22 2016 current: Mar 28 00:52:39 2016
       diff: 17(s) hard: 0(s)
                                       soft: 0(s)
       last:
                                       hard: O(s)
                                                      soft: O(s)
       current: 0(bytes)
                             hard: O(bytes) soft: O(bytes)
       allocated: 0 hard: 0 soft: 0
       sadb seg=1 pid=8721 refcnt=0
192.168.20.1 192.168.10.1
       esp mode=tunnel spi=1696336313(0x651c09b9) regid=16401(0x00004011
)
       E: aes-cbc 52a767f6 49f6d115 6fcd4f55 8a58cda4
       A: hmac-shal 7deace3e b11e8342 0479448a e96cadb0 40c59197
       seq=0x00000000 replay=32 flags=0x00000000 state=mature
       created: Mar 28 00:52:22 2016 current: Mar 28 00:52:39 2016
                                       soft: O(s)
       diff: 17(s)
                     hard: O(s)
                                       hard: O(s)
       last:
                                                      soft: O(s)
       current: 0(bytes)
                              hard: O(bytes) soft: O(bytes)
       allocated: 0 hard: 0 soft: 0
```

Links:-

IP SEC Tools:-

http://ipsec-tools.sourceforge.net/

How to use IPSEC Tools:-

http://www.mad-hacking.net/documentation/linux/networking/ipsec/installation.xml

libreswan:-

https://libreswan.org/

Oakley:-

https://tools.ietf.org/html/rfc2412