

Secure data from MITM (Man in the Middle Attack) with SSTP Mikrotik

MuM Kuta, Bali 2019

MY PROFILE



Haris Hardiansyah

- Mahasiswa Universitas Bina Insani , Bekasi
- Network Engineer – Poltek Citra Widya Edukasi , Cibitung

- Ig : @haris_pc
- Email : harishardiansyah94@gmail.com

PROFILE POLITEKNIK CITRA WIDYA EDUKASI

- Program (Diploma 4)
 - Teknologi Produksi Tanaman Perkebunan
- Program (Diploma 3)
 - Manajemen Logistik
 - Teknologi Pengolahan Kelapa Sawit
 - Budidaya Perkebunan Kelapa Sawit

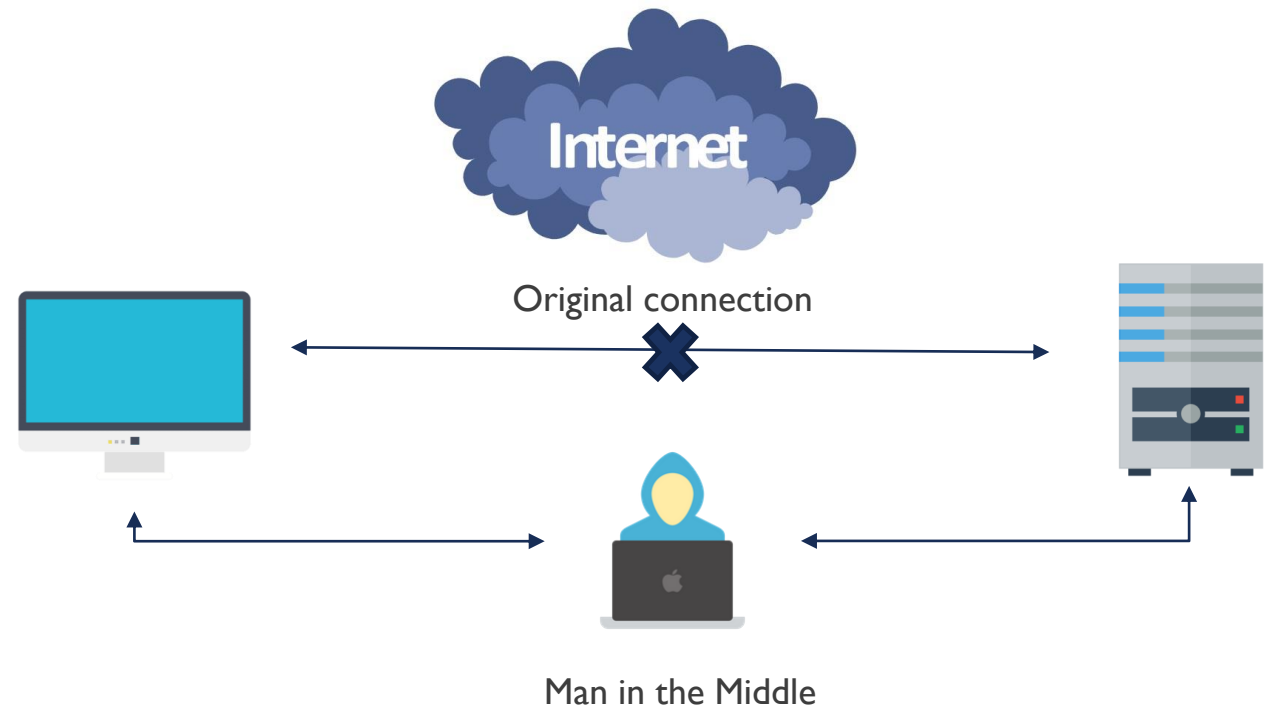


NETWORK TRAINING POLTEK CWE



MITM (MAN IN THE MIDDLE ATTACK)

- Suatu serangan yg berada diantara posisi client dan server
- MITM biasanya terjadi karena kelalaian dalam proses otentikasi oleh pengguna.

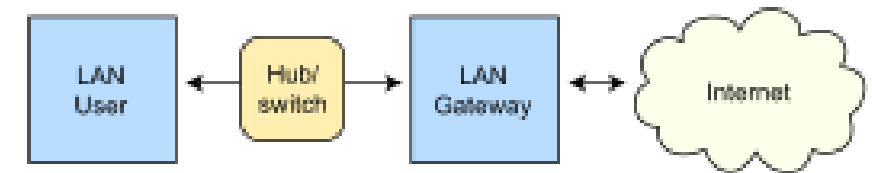


WHAT ATTACKED ?

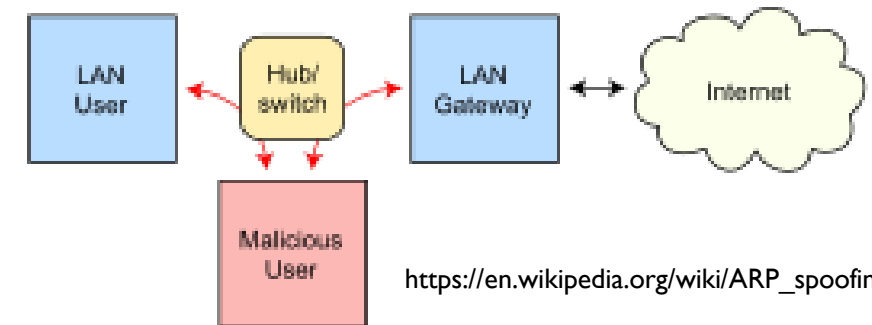
■ ARP

Mengirimkan pesan ARP palsu kepada client, penyerang akan mengambil frame data lalu memodifikasinya dan mengirim ke user (Arp Spoofing)

Routing under normal operation



Routing subject to ARP cache poisoning



https://en.wikipedia.org/wiki/ARP_spoofing



Solution?

WHAT IS SSTP

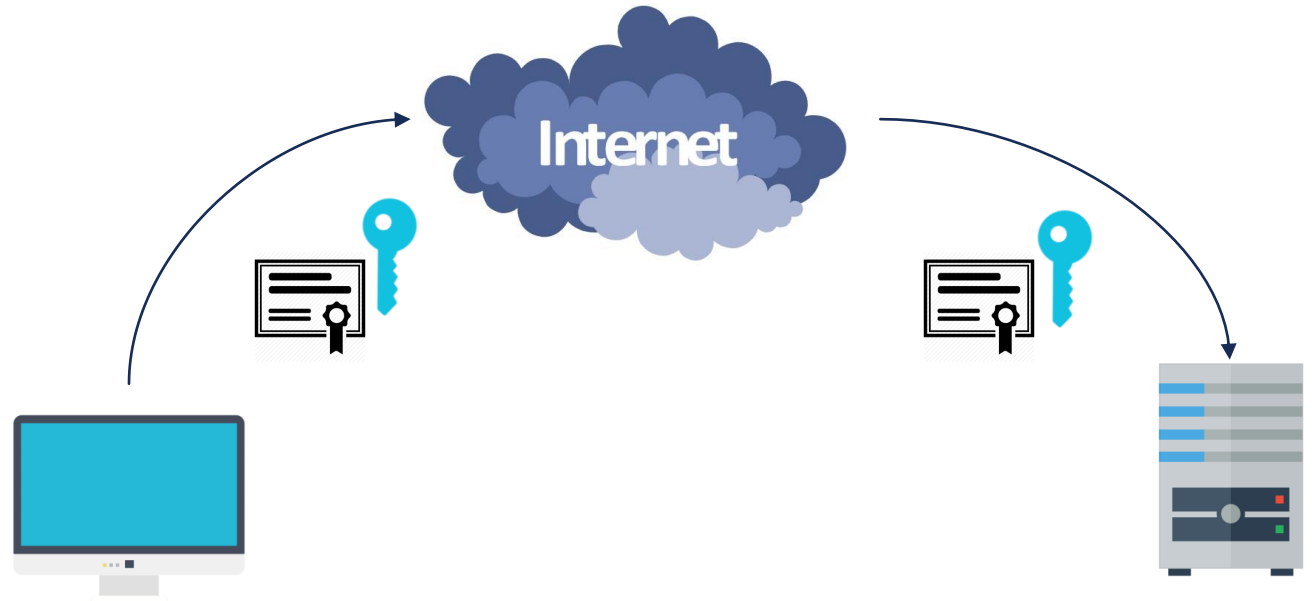
- Secure Socket Tunneling Protocol (SSTP)



- SSL memvalidasi sertifikat server.
- Memungkinkan server untuk memeriksa apakah koneksi aman.

TLS / SSL

- Transport Layer Security (TLS) , Secure Socket Layer (SSL)
- Protokol SSL / TLS menggunakan kriptografi public-key dan sertifikat publik key, yg digunakan untuk memastikan identitas dari pihak yang dimaksud.



■ TLS / SSL

- **Enkripsi**
- **Otentikasi**
- **Integritas**
- **Kriptografi security**

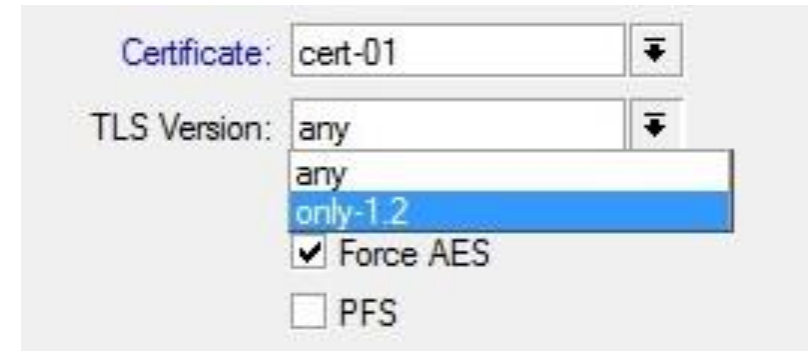


SSTP - TLS 1.2 VERSION

- Protokol ini menyediakan autentikasi akhir dan privasi komunikasi di Internet menggunakan cryptography.

Langkah dasar TLS / SSL

- Negosiasi
- *Public key, encryption-based-key, dan certificate-based authentication*
- Symmetric - Asymmetric cryptography



Certificate: cert-01

TLS Version: any

any

only-1.2

☒ Force AES

☐ PFS

- RouterOS mengimpor sertifikat CA dan mengaktifkan opsi verifikasi-server-sertifikat. Dalam skenario ini, serangan Man-in-the-Middle tidak dimungkinkan.

Certificate: cert-01

TLS Version: any

☒ Verify Client Certificate

☒ Force AES

☐ PFS

SSTP Server



Certificate: cert_export_cert-01.crt_0

TLS Version: any

☒ Verify Server Certificate

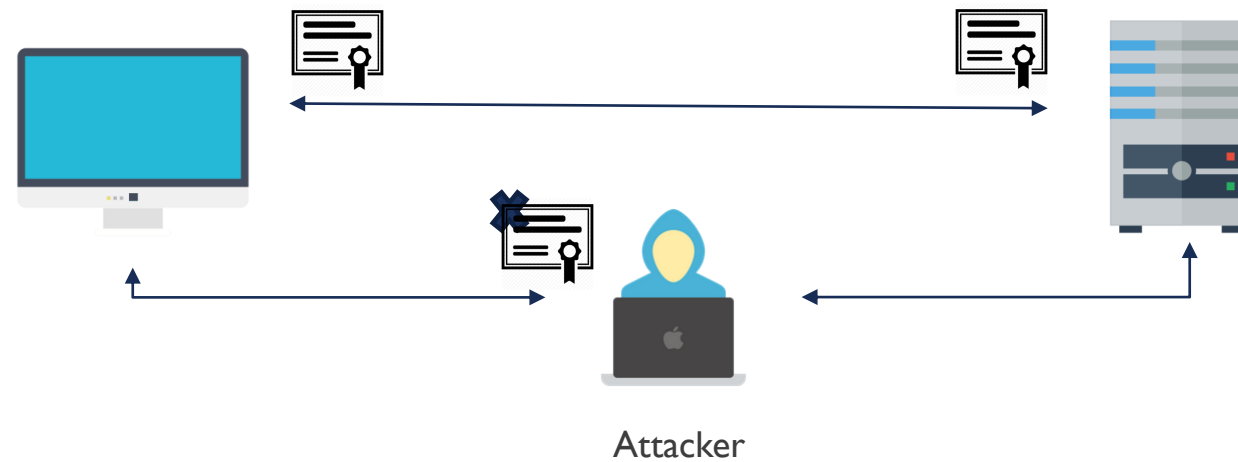
☐ Verify Server Address From Certificate

☐ PFS

SSTP Client

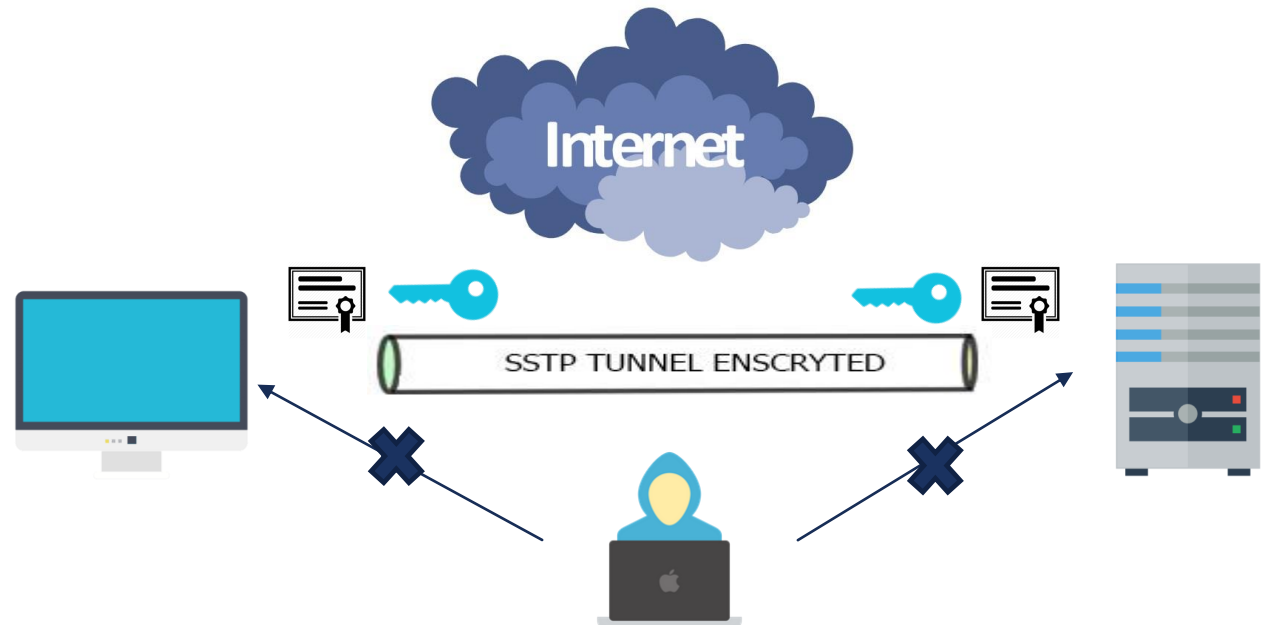
- Configuration requirements are:

- Sertifikat di server dan klien
- Opsi verifikasi diaktifkan di server dan klien



- Ini tidak hanya dilakukan dengan username dan password, tetapi pada client-server juga diautentikasi menggunakan sertifikat server.

this means that the servers to check if both channels are secure.



WHY SSTP ?

	<u>OpenVPN</u>	PPTP	L2TP/IPsec	SSTP	IKEv2/IPSec
Encryption	160-bit, 256-bit	128-bit	256-bit	256-bit	256-bit
Security	Very high	Weak	High security (might be weakened by NSA)	High	High
Speed	Fast	Speedy, due to low encryption	Medium, due to double encapsulation	Fast	Very fast
Stability	Very stable	Very stable	Stable	Very stable	Very stable
Compatibility	Strong desktop support, but mobile could be improved. Requires third-party software.	Strong Windows desktop support.	Multiple device and platform support.	Windows-platform, but works on other Linux distributions.	Limited platform support beyond Windows and Blackberry
Final Word	Most recommended choice. Fast and secure.	Native on Windows. Weak security. Useful for geo-restricted content.	Versatile and secure. A decent alternative to OpenVPN.	Faster and more secure alternative to PPTP and L2TP.	Secure, stable, and mobile-

<https://thebestvpn.com/ppp-l2tp-openvpn-sstp-ikev2-protocols/>

NOT USE IPSEC?

IPsec VPNs vs. SSL VPNs

FEATURES	IPsec VPN	SSL VPN
 Network layers	Operates at Layer 3	Operates at Layers 4-7
 Connectivity	Connects remote hosts to entire networks	Connects users to specific apps and services
 Applications	Can support all IP-based applications	Best for email, file sharing and browser-based apps
 Gateway location	Gateway usually implemented on the firewall	Gateway typically deployed behind the firewall
 Security/control	Broad access creates security concerns	More granular controls require more management
 Endpoints	Requires host-based clients	Browser-based, with optional thin client

"TLS menjaga konteks antara pengirim dan penerima dan pembaruan yang menyatakan (seperti nomor urut)"

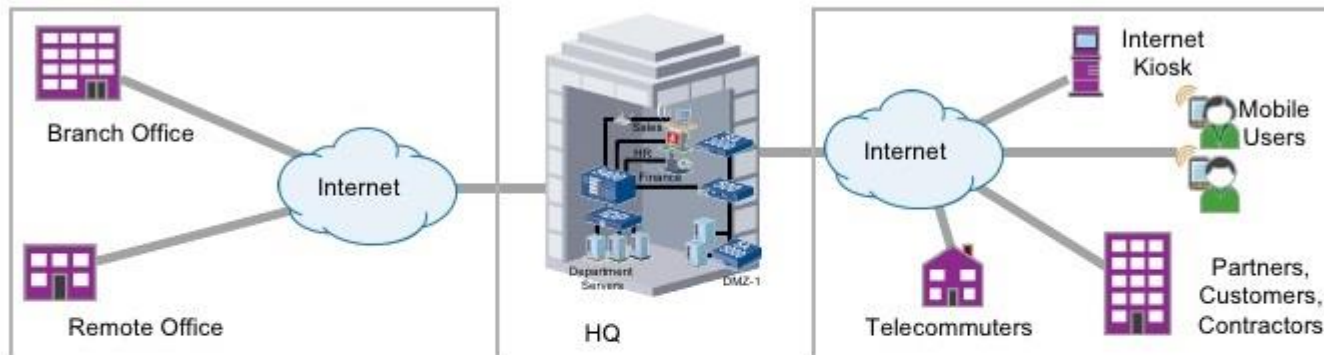
"Dengan IPsec, semua itu perlu dibuat eksplisit (karena tidak ada jaminan bahwa penerima akan mendapatkan paket yang sama dalam urutan yang sama dengan yang dikirim pengirim)"

IPsec VPNs vs. SSL VPNs

FEATURES	IPsec VPN	SSL VPN
 Network layers	Operates at Layer 3	Operates at Layers 4-7
 Connectivity	Connects remote hosts to entire networks	Connects users to specific apps and services
 Applications	Can support all IP-based applications	Best for email, file sharing and browser-based apps
 Gateway location	Gateway usually implemented on the firewall	Gateway typically deployed behind the firewall
 Security/control	Broad access creates security concerns	More granular controls require more management
 Endpoints	Requires host-based clients	Browser-based, with optional thin client

- SSL VPN that operates through a web browser will usually be able to manage connections faster than ip sec.
- SSTP support mobile connection, IPSEC not support

IPSEC VPN VS. SSL VPN



IPSec VPN
Remote/Branch Office Deployments
Fixed Site-to-Site
Managed Endpoints
Layer 3 Network Access
IP to IP Control
Access from Managed, Trusted Networks

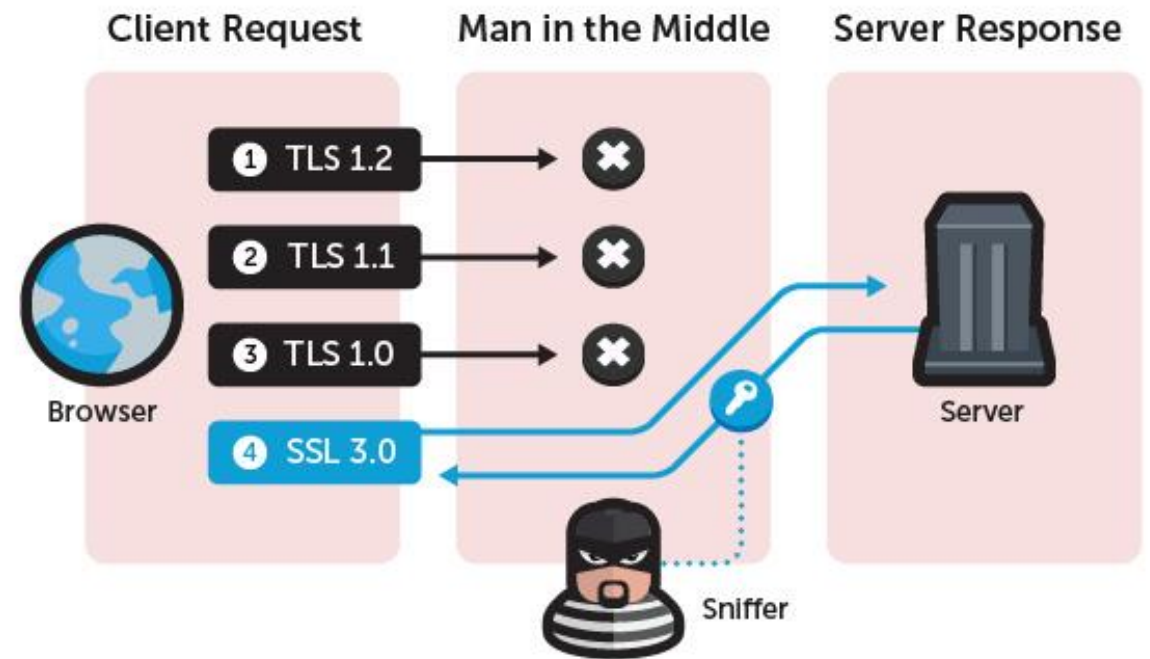
SSL VPN
Employee Remote Access
Telecommuters
Mobile Users
Partner Extranets
Mobile or Fixed
Managed or Unmanaged Endpoints
Access Control Per Application
User to Application Control
Access allowed from Unmanaged and Untrusted networks as well

- Network administrators who operate VPNs tend to find client management a lot easier and less time-consuming with SSL than with IPsec.

- SSTP uses TLS 1.2

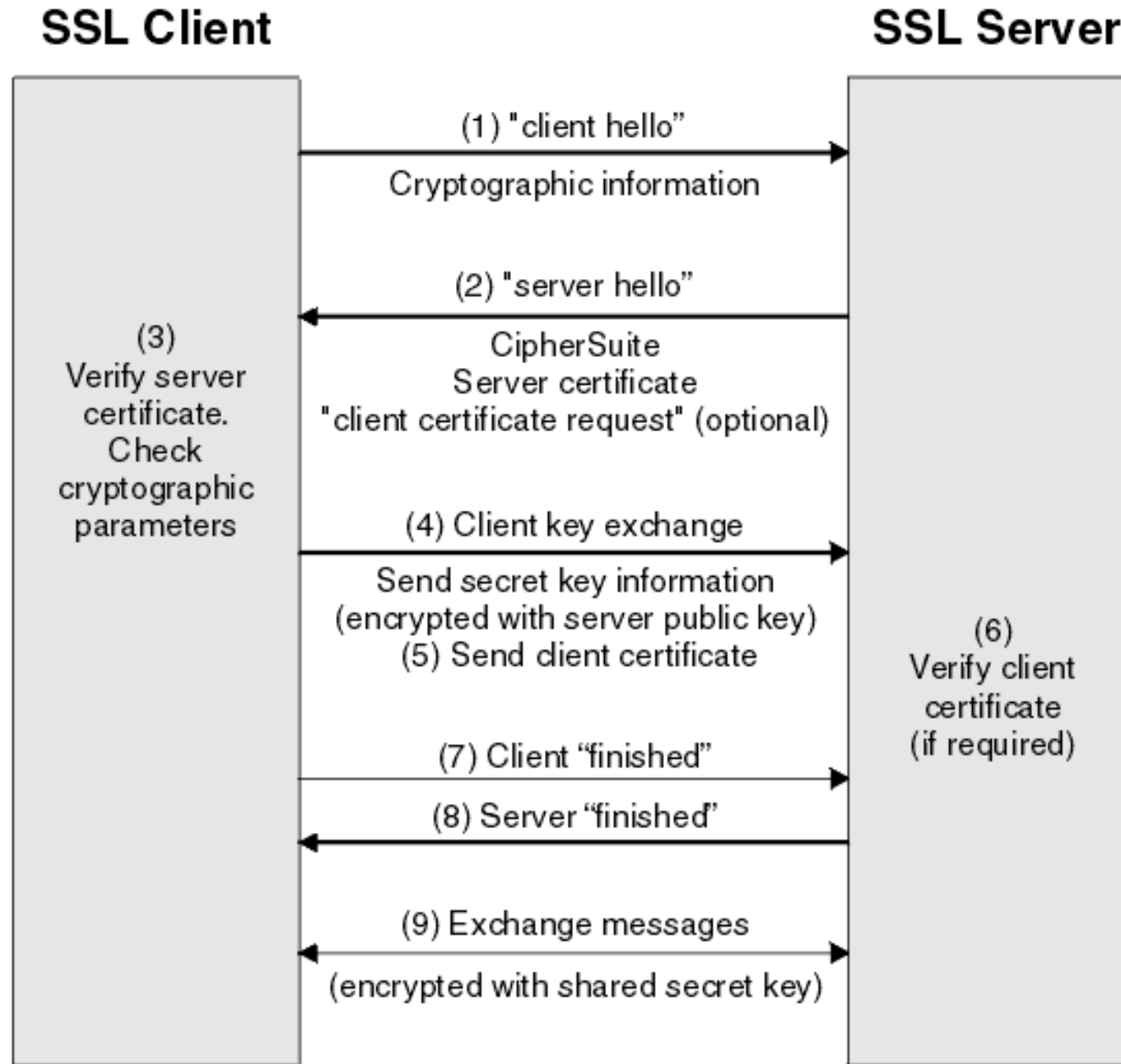
- Server & Client Certificate

Publik key
Disertifikasi oleh Sertifikat
dengan Kepercayaan dari
client.



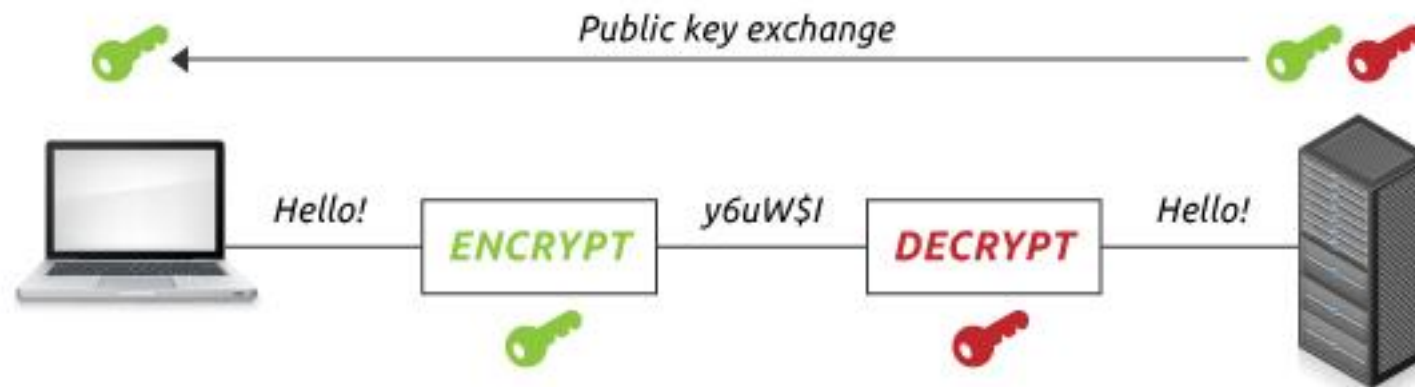
<https://blog.trendmicro.com/trendlabs-security-intelligence/poodle-vulnerability-puts-online-transactions-at-risk/>

PROSES HANDSHAKE SSL/TLS



ASYMMETRIC

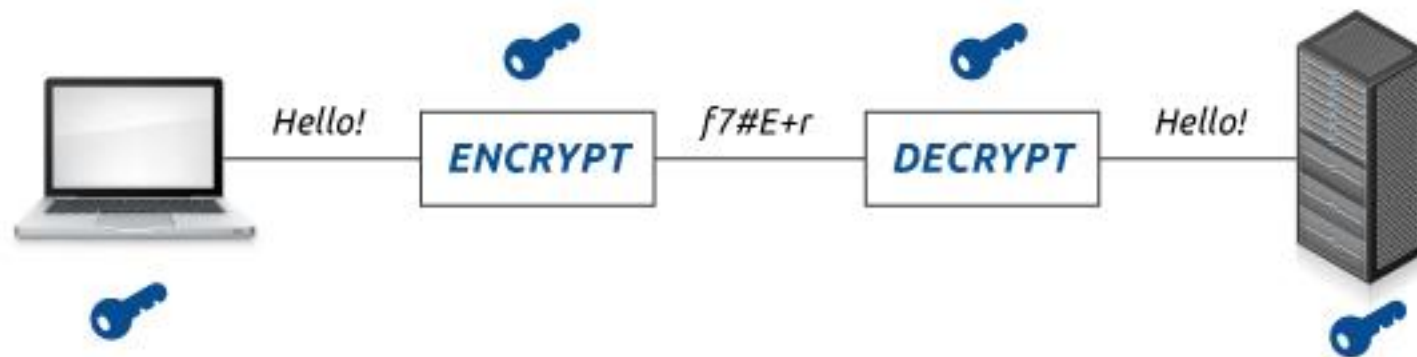
- SSTP It uses 2048 bit encryption and authentication certificates.



<https://www.digicert.com/ssl-cryptography.htm>

Enkripsi asimetris (atau kriptografi kunci publik)
menggunakan kunci terpisah untuk enkripsi dan dekripsi

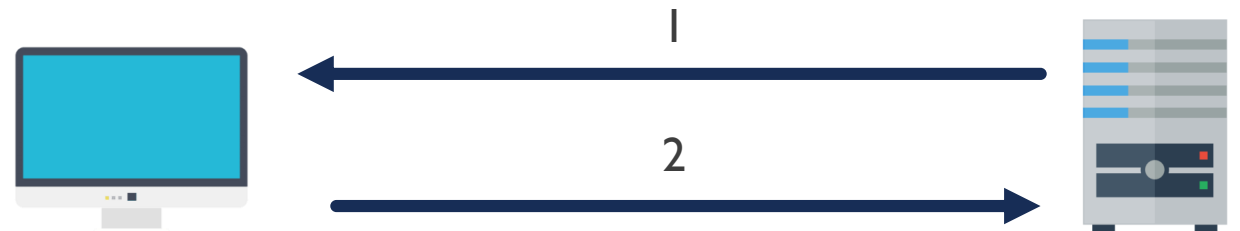
SYMMETRIC



Enkripsi simetris (atau enkripsi kunci yang dibagikan sebelumnya) menggunakan kunci tunggal untuk mengenkripsi dan mendekripsi data.

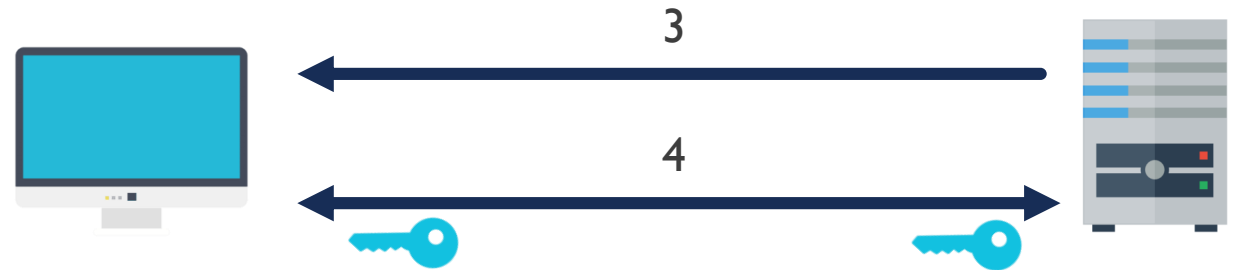
HOW SSL USES ASYMMETRIC AND SYMMETRIC

- Server mengirimkan salinan kunci publik asimetrisnya.
- Browser membuat kunci sesi simetris dan mengenkripsinya dengan kunci publik asimetris server. Kemudian mengirimkannya ke server.

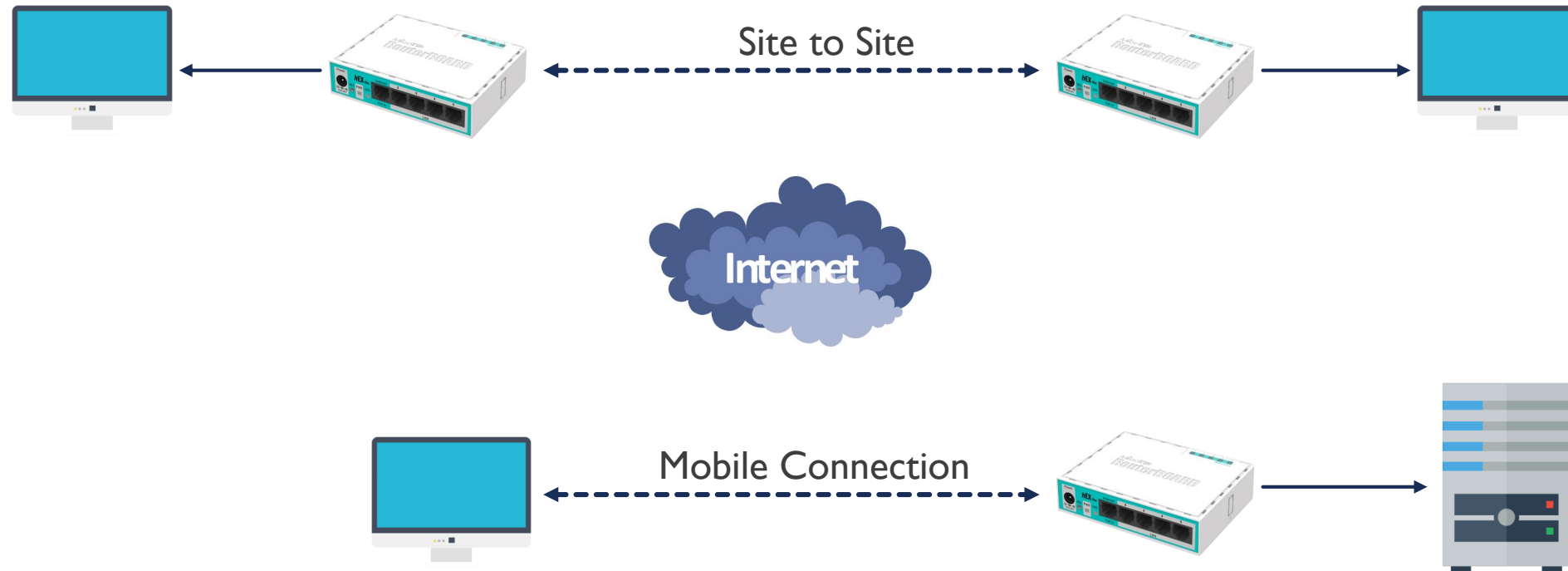


- Server dan Browser sekarang mengenkripsi dan mendekripsi semua data yang dikirimkan dengan kunci sesi

“This allows for a secure channel because the browser and the server know the session key”

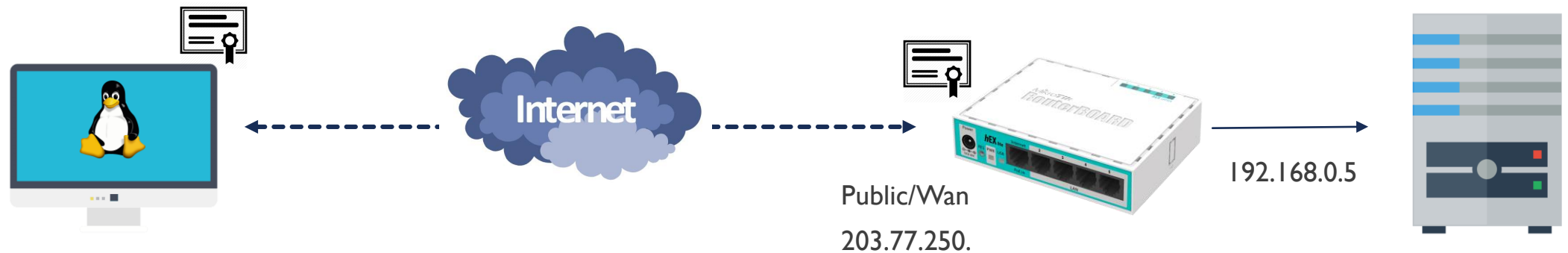


TOPOLOGI

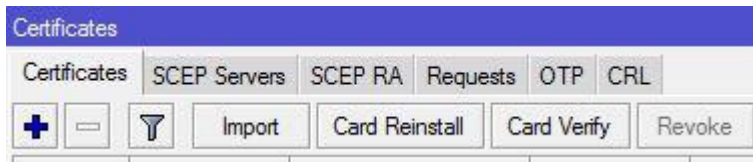


SSTP CLIENT ON LINUX

- Currently, SSTP clients exist in Windows Vista, Windows 7, Windows 8, Linux and RouterOS.



CONFIG MOBILE CONNECTION



■ Membuat Certificate

Disini kita akan membuat 3 Certificate

1. CA Template
2. Server
3. Client

A screenshot of the 'New Certificate' dialog box. The dialog has a blue title bar and three tabs: 'General', 'Key Usage', and 'Status'. The 'General' tab is selected. It contains several input fields: 'Name' (set to 'cert-01'), 'Issuer' (empty), 'Country' (set to 'ID'), 'State' (set to 'Jawa Barat'), 'Locality' (set to 'Bekasi'), 'Organization' (set to 'CWE'), 'Unit' (set to 'Support'), 'Common Name' (set to '203.77.250.'), 'Subject Alt. Name' (set to 'IP'), 'Key Size' (set to '2048'), and 'Days Valid' (set to '365'). On the right side of the dialog is a vertical stack of buttons: 'OK', 'Cancel', 'Apply', 'Copy', 'Remove', 'Sign', 'Sign via SCEP', 'Import', 'Card Reinstall', 'Card Verify', 'Set CA Passphrase', 'Export', and 'Revoke'. At the bottom of the dialog is a row of labels: 'private key', 'crl', 'authority', 'expired', 'smart card key', and 'trusted'.

- Key Usage
 - TLS Server & Client

The screenshot shows the 'New Certificate' dialog box with the 'Key Usage' tab selected. The dialog has three tabs: 'General', 'Key Usage', and 'Status'. The 'Key Usage' tab contains a list of checkboxes for various key uses. The 'Key Usage' label is followed by a list of checkboxes arranged in two columns. The first column includes 'digital signature', 'key encipherment', 'key agreement', 'crl sign', 'decipher only', 'server gated crypto', 'timestamp', 'ipsec tunnel', 'email protect', and 'tls client'. The second column includes 'content commitment', 'data encipherment', 'key cert. sign', 'encipher only', 'dvcs', 'ocsp sign', 'ipsec user', 'ipsec end system', 'code sign', and 'tls server'. The 'tls client' and 'tls server' checkboxes are checked. To the right of the checkbox list is a vertical stack of buttons: 'OK', 'Cancel', 'Apply', 'Copy', 'Remove', 'Sign', 'Sign via SCEP', 'Import', 'Card Reinstall', 'Card Verify', 'Set CA Passphrase', 'Export', and 'Revoke'. At the bottom of the dialog, there is a row of labels: 'private key', 'crl', 'authority', 'expired', 'smart card key', and 'trusted'.

Key Usage	Checked
digital signature	Yes
key encipherment	Yes
key agreement	No
crl sign	Yes
decipher only	No
server gated crypto	No
timestamp	No
ipsec tunnel	No
email protect	No
tls client	Yes
content commitment	No
data encipherment	Yes
key cert. sign	Yes
encipher only	No
dvcs	No
ocsp sign	No
ipsec user	No
ipsec end system	No
code sign	No
tls server	Yes

- Lakukan settingan yg sama , yang membedakan hanya common name dan name nya saja

New Certificate

General Key Usage Status

Name: server

Issuer:

Country: ID

State: Jawa Barat

Locality: Bekasi

Organization: CWE

Unit: Support

Common Name: server

Subject Alt. Name: IP

Key Size: 2048

Days Valid: 365

OK
Cancel
Apply
Copy
Remove
Sign
Sign via SCEP
Import
Card Reinstall
Card Verify
Set CA Passphrase
Export
Revoke

private key crl authority expired smart card key trusted

- Kita tanda tangani (self-signed) server dan client nya dan jangan lupa trusted

```

Terminal
[?] Gives the list of available commands
command [?] Gives help on the command and list of arguments

[Tab] Completes the command/word. If the input is ambiguous,
a second [Tab] gives possible options

/ Move up to base level
.. Move up one level
/command Use command at the base level
[haris_pc@CWE] > certificate sign cert1 ca-crl-host=203.77.250. name=cert-01
progress: done
[haris_pc@CWE] > certificate sign cert-server ca=cert-01 name=server
no such item
[haris_pc@CWE] > certificate sign ce ca=cert-01 name=server
"cert - client" "cert - server" cert-01
[haris_pc@CWE] > certificate sign "cert - server" ca=cert-01 name=server
progress: done
[haris_pc@CWE] > certificate sign "cert - client" ca=cert-01 name=client
progress: done
[haris_pc@CWE] > certificate set cli
client locality
[haris_pc@CWE] > certificate set client trusted=yes
[haris_pc@CWE] > certificate set server trusted=yes
[haris_pc@CWE] >

```

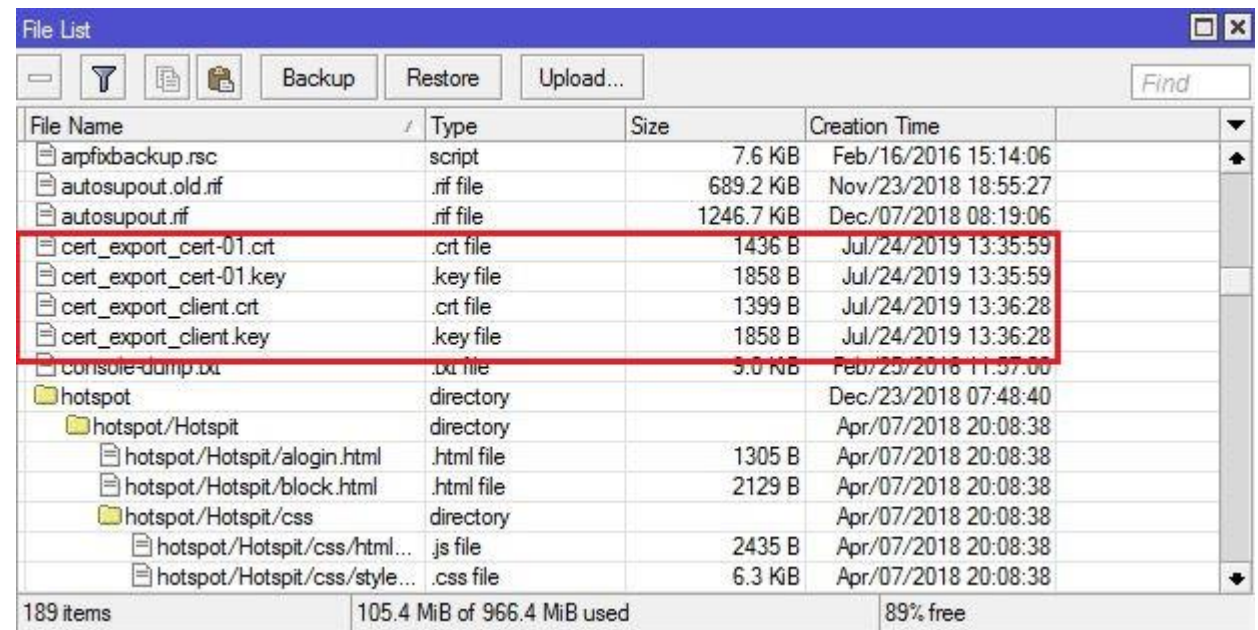
Certificates
Certificates SCEP Servers SCEP RA Requests OTP CRL
+ - Import Card Reinstall Card Verify Revoke Create Cert. Request Settings Find

	Name	Issuer	Common Name	Subject Alt. N...	Key Size	Days Valid	Trusted	SCEP U
KA	server		server	unknown:::	2048	365	no	
KA	client		client	unknown:::	2048	365	no	
KLAT	cert-01		203.77.250.	unknown:::	2048	365	yes	

Terminal
MMM MMM III KKK KKK RRR RRR OOOOOO TTT III KKK KKK
MikroTik RouterOS 6.44.3 (c) 1999-2019 http://www.mikrotik.com/
[?] Gives the list of available commands
command [?] Gives help on the command and list of arguments
[Tab] Completes the command/word. If the input is ambiguous,
a second [Tab] gives possible options
/ Move up to base level
.. Move up one level
/command Use command at the base level
[haris_pc@CWE] > certificate sign cert1 ca-crl-host=203.77.250. name=cert-01
progress: done
[haris_pc@CWE] > certificate sign cert-server ca=cert-01 name=server
no such item
[haris_pc@CWE] > certificate sign ce ca=cert-01 name=server
"cert - client" "cert - server" cert-01
[haris_pc@CWE] > certificate sign "cert - server" ca=cert-01 name=server
progress: done
[haris_pc@CWE] > certificate sign "cert - client" ca=cert-01 name=client
progress: done
[haris_pc@CWE] >

- Export certificate untuk nanti di pindahkan ke client

```
[haris_pc@CWE] > certificate export-certificate cert-01 export-passphrase=admin123  
[haris_pc@CWE] > certificate export-certificate client export-passphrase=admin123  
[haris_pc@CWE] >
```



File List

Backup Restore Upload... Find

File Name	Type	Size	Creation Time
arpfixbackup.rsc	script	7.6 KB	Feb/16/2016 15:14:06
autosupout.old.rif	.rif file	689.2 KB	Nov/23/2018 18:55:27
autosupout.rif	.rif file	1246.7 KB	Dec/07/2018 08:19:06
cert_export_cert-01.crt	.crt file	1436 B	Jul/24/2019 13:35:59
cert_export_cert-01.key	key file	1858 B	Jul/24/2019 13:35:59
cert_export_client.crt	.crt file	1399 B	Jul/24/2019 13:36:28
cert_export_client.key	key file	1858 B	Jul/24/2019 13:36:28
console-dump.txt	.txt file	5.0 KB	Feb/25/2018 11:37:00
hotspot	directory		Dec/23/2018 07:48:40
hotspot/Hotspot	directory		Apr/07/2018 20:08:38
hotspot/Hotspot/login.html	.html file	1305 B	Apr/07/2018 20:08:38
hotspot/Hotspot/block.html	.html file	2129 B	Apr/07/2018 20:08:38
hotspot/Hotspot/css	directory		Apr/07/2018 20:08:38
hotspot/Hotspot/css/html...	.js file	2435 B	Apr/07/2018 20:08:38
hotspot/Hotspot/css/style...	.css file	6.3 KB	Apr/07/2018 20:08:38

189 items 105.4 MiB of 966.4 MiB used 89% free

- Aktifkan SSTP Server dan buat secret untuk akses login client

TLS/SSL validates server certificate.

The screenshot shows the 'PPP Secret <haris>' window. The 'Name' field is 'haris', 'Password' is masked with '***', 'Service' is 'sstp', 'Caller ID' is empty, and 'Profile' is 'default-encryption'. Below these are fields for 'Local Address' (10.10.10.1) and 'Remote Address' (10.10.10.2), a 'Routes' dropdown, 'Limit Bytes In' and 'Limit Bytes Out' dropdowns, and a 'Last Logged Out' field. On the right side, there are buttons for 'OK', 'Cancel', 'Apply', 'Disable', 'Comment', 'Copy', and 'Remove'. At the bottom, the status is 'enabled'.

The screenshot shows the 'SSTP Server' window. The 'Enabled' checkbox is checked. The 'Port' is 443, 'Max MTU' is 1500, and 'Max MRU' is 1500. The 'MRRU' dropdown is empty. The 'Keepalive Timeout' is 60. The 'Default Profile' is 'default-encryption'. Under 'Authentication', 'mschap2', 'mschap1', 'chap', and 'pap' are all checked. The 'Certificate' dropdown is set to 'cert-01'. The 'TLS Version' dropdown is open, showing 'any', 'only-1.2' (which is highlighted), and 'Force AES' (checked). The 'PFS' checkbox is unchecked. On the right side, there are buttons for 'OK', 'Cancel', and 'Apply'.

- Disini kita pilih TLS version 1.2

- Sekarang kita aktifkan VPN connection nya

Hardware

DSL
Ethernet
InfiniBand
Mobile Broadband
Wi-Fi
WiMAX

Virtual

Bond
Bridge
VLAN

VPN

Point-to-Point Tunneling Protocol (PPTP)
Secure Socket Tunneling Protocol (SSTP)

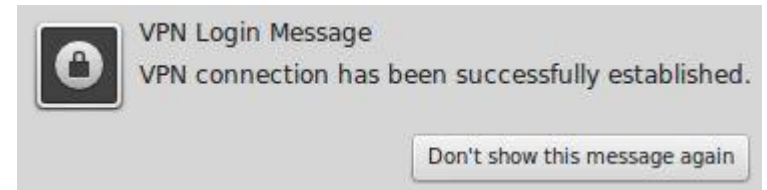
Import a saved VPN configuration...

- Buat koneksi vpn baru



CONNECTED ON LINUX

- Jika VPN berhasil terhubung ke SSTP Server , coba test ping ke ip public router
- Dan coba ping ke ip private yang ada di router



```
Terminal
haris@haris-Mint ~ $ ifconfig
eth0      Link encap:Ethernet  HWaddr 08:00:27:b0:a2:74
          inet addr:192.168.43.190  Bcast:192.168.43.255  Mask:255.255.255.0

Terminal
haris@haris-Mint ~ $ ping 203.77.250.194
PING 203.77.250.194 (203.77.250.194) 56(84) bytes of data.
64 bytes from 203.77.250.194: icmp_seq=1 ttl=55 time=58.7 ms
64 bytes from 203.77.250.194: icmp_seq=2 ttl=55 time=32.0 ms
64 bytes from 203.77.250.194: icmp_seq=3 ttl=55 time=27.1 ms
^C
--- 203.77.250.194 ping statistics ---
3 packets transmitted, 3 received, 0% packet loss, time 2005ms
rtt min/avg/max/mdev = 27.114/39.289/58.742/13.901 ms
haris@haris-Mint ~ $ ping 192.168.0.5
PING 192.168.0.5 (192.168.0.5) 56(84) bytes of data.
64 bytes from 192.168.0.5: icmp_seq=1 ttl=127 time=48.0 ms
64 bytes from 192.168.0.5: icmp_seq=2 ttl=127 time=46.7 ms
^C
```

CONNECTED ON MIKROTIK

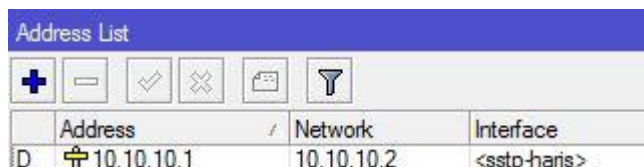
- Cek apakah user sudah terhubung pada server di **“Active Connections”**



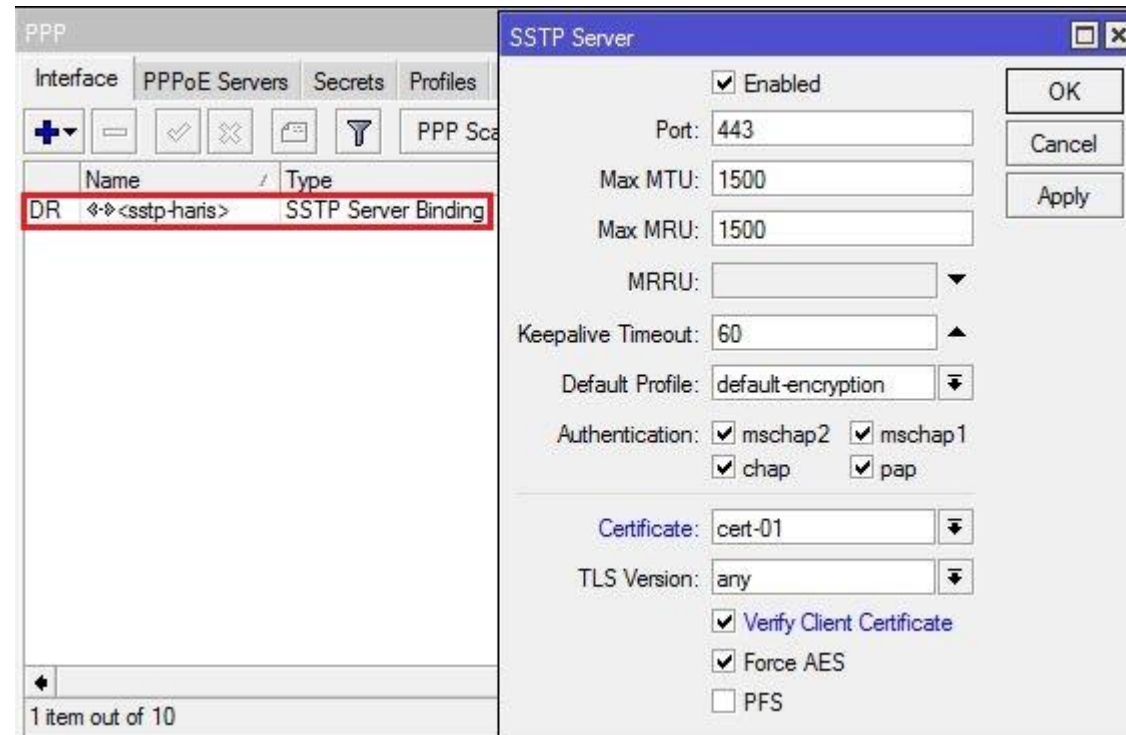
PPP						
Interface PPPoE Servers Secrets Profiles Active Connections L2TP Secrets						
Name / Service Caller ID Encoding Address Uptime						
L	hris	sstp	128.0.1.12	AES256-CBC	10.10.10.2	00:00:10

- Jika user terhubung pada server , maka di menu interface akan muncul

- IP yang di dapatkan otomatis

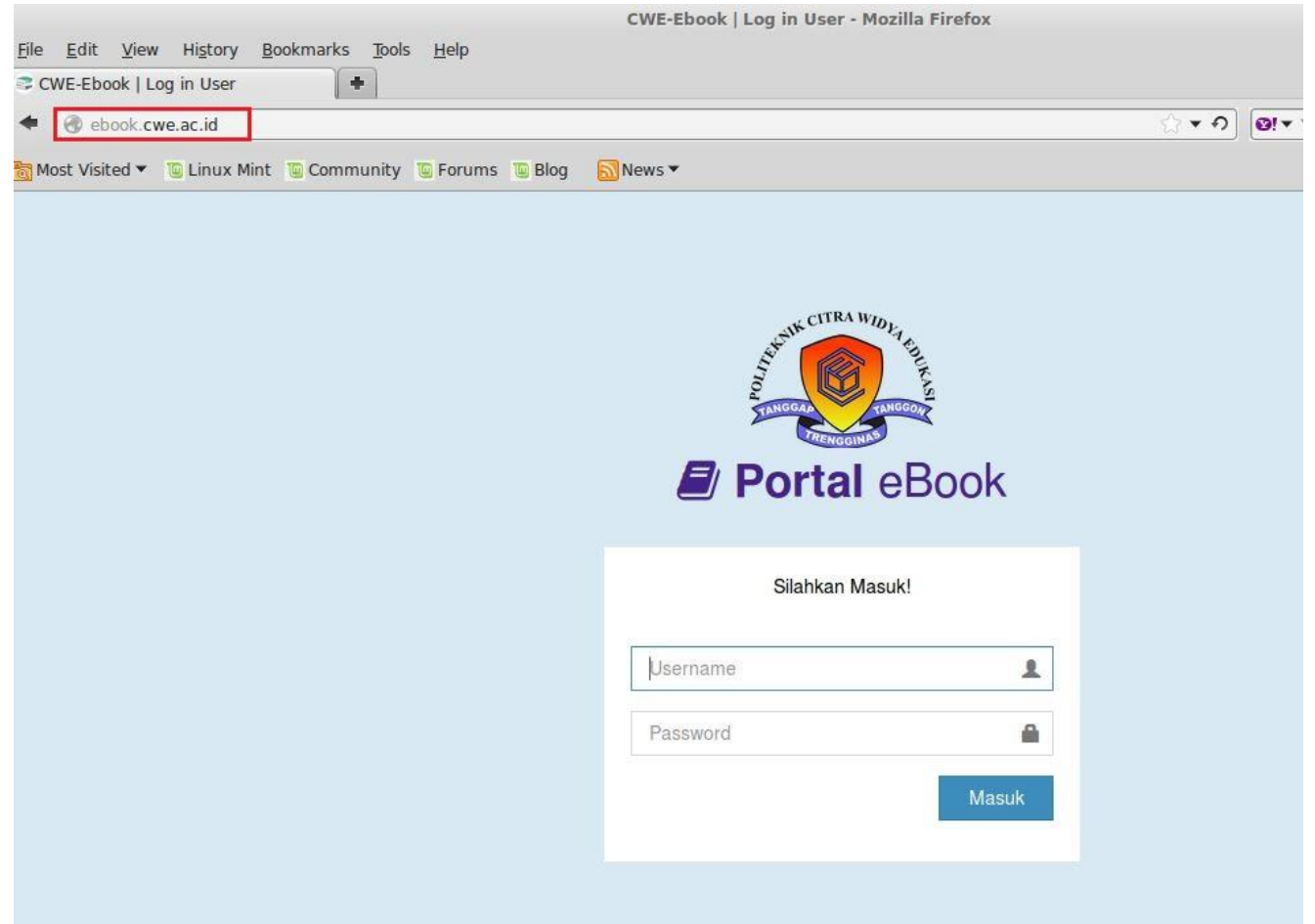
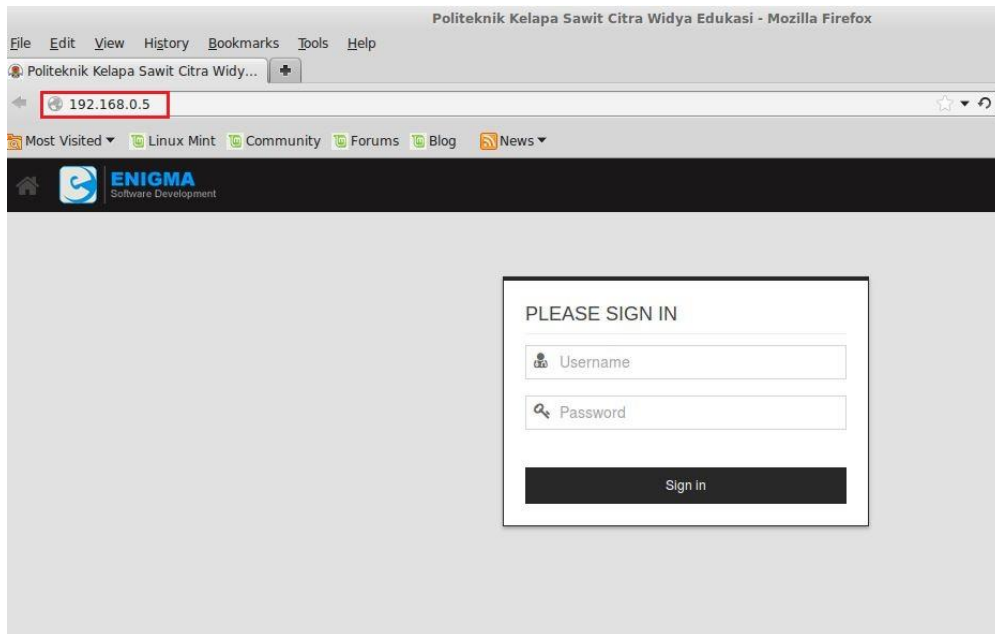


Address List			
Address Network Interface			
D	10.10.10.1	10.10.10.2	<sstp-haris>



PPP		SSTP Server	
Interface PPPoE Servers Secrets Profiles PPP Sca		Enabled	
Name / Type		Port:	443
DR <<sstp-haris>		Max MTU:	1500
SSTP Server Binding		Max MRU:	1500
		MRRU:	
		Keepalive Timeout:	60
		Default Profile:	default-encryption
		Authentication:	☒ mschap2 ☒ mschap1
			☒ chap ☒ pap
		Certificate:	cert-01
		TLS Version:	any
		☒ Verify Client Certificate	
		☒ Force AES	
		☐ PFS	

- Disini saya mencoba mengakses salah satu web server yg saya setting dengan ip local yaitu 192.168.0.5



EXAMPLE SITE TO SITE

PPP

Interface PPPoE Servers Secrets Profiles Active Connections L2TP Secrets

+ - ✓ ✗ [Icon] [Icon] [Icon] [Icon] [Icon] [Icon] [Icon] [Icon] [Icon] [Icon] Find

Name	Type	Actual MTU	L2 MTU	Tx	Rx	Tx Packet (p/s)	Rx
DR <-> <sstp-ff>	SSTP Server Binding	1500		0 bps	0 bps	0	0

SSTP Server

☒ Enabled

Port: 443

Max MTU: 1500

Max MRU: 1500

MRRU: [Dropdown]

Keepalive Timeout: 60

Default Profile: default-encryption

Authentication: ☒ mschap2 ☒ mschap1
☒ chap ☒ pap

Certificate: cert1

TLS Version: only-1.2

☒ Verify Client Certificate
☐ Force AES
☐ PFS

OK Cancel Apply

Interface <<sstp-ff>>

General Status Traffic

Last Link Down Time: [Field]

Last Link Up Time: Jul/30/2019 10:14:45

Link Downs: 0

Uptime: 00:52:29

User: ff

Caller ID: 103.75.54.33

Encoding: RC4

MTU: 1500

MRU: 1500

Local Address: 10.10.10.1

Remote Address: 10.10.10.2

OK Copy Remove Torch

dynamic enabled running slave Status: connected

Capturing from Ethernet

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

Apply a display filter ... <Ctrl-/> Expression...

No.	Time	Source	Destination	Protocol	Length	Info
99	12.299727	fe80::795e:613:4111...	ff02::1:3	LLMNR	95	Standard query 0xcd1c ANY DESKTOP-2QPQM2B
98	12.158905	fe80::795e:613:4111...	ff02::16	ICMPv6	90	Multicast Listener Report Message v2
95	11.892599	fe80::795e:613:4111...	ff02::1:3	LLMNR	95	Standard query 0xcd1c ANY DESKTOP-2QPQM2B
93	11.888993	fe80::795e:613:4111...	ff02::16	ICMPv6	90	Multicast Listener Report Message v2
91	11.888444	fe80::795e:613:4111...	ff02::16	ICMPv6	90	Multicast Listener Report Message v2
88	11.886326	fe80::795e:613:4111...	ff02::16	ICMPv6	90	Multicast Listener Report Message v2
86	11.859930	fe80::795e:613:4111...	ff02::16	ICMPv6	90	Multicast Listener Report Message v2
112	12.857891	WistronI_2b:62:b7	Routerbo_78:ee:09	ARP	42	192.168.1.254 is at f0:de:f1:2b:62:b7
402	34.790562	Routerbo_78:ee:09	LLDP_Multicast	LLDP	144	TTL = 120 SysName = tes Sstp Client SysDesc = MikroTik RouterOS 6.44.3 ...
401	34.790562	Routerbo_78:ee:09	CDP/VTP/DTP/PAGP/UDLD	CDP	111	Device ID: tes Sstp Client Port ID: ether3
111	12.857857	Routerbo_78:ee:09	WistronI 2b:62:b7	ARP	60	Who has 192.168.1.254? Tell 192.168.1.1
352	27.372940	77.88.21.119	192.168.1.254	TLSv1.2	624	Application Data
351	27.358989	77.88.21.119	192.168.1.254	TCP	60	443 → 50528 [ACK] Seq=1711 Ack=4557 Win=335 Len=0
300	21.720834	77.88.21.119	192.168.1.254	TCP	60	[TCP Keep-Alive ACK] 443 → 50528 [ACK] Seq=1711 Ack=3418 Win=326 Len=0
78	11.501864	77.88.21.119	192.168.1.254	TLSv1.2	624	Application Data
24	4.257210	77.88.21.119	192.168.1.254	TLSv1.2	624	Application Data
2	0.223150	77.88.21.119	192.168.1.254	TLSv1.2	624	Application Data
359	28.164272	74.125.24.95	192.168.1.254	TLSv1.2	93	Application Data
252	19.971641	74.125.200.95	192.168.1.254	TCP	60	443 → 50397 [ACK] Seq=649 Ack=123 Win=266 Len=0
246	19.947163	74.125.200.95	192.168.1.254	TLSv1.2	93	Application Data

Version: 1
TTL: 120 seconds
Checksum: 0x3e1e [correct]
[Checksum Status: Good]

- > Device ID: tes Sstp Client
- > Port ID: ether3
- > Capabilities
- > Software Version
- > Platform: MikroTik

```
0000 01 00 0c cc cc cc 64 d1 54 78 ee 09 00 50 aa aa  ....d..Tx...P..
0010 03 00 00 0c 20 00 01 78 3e 1e 00 01 00 13 74 65  ....x>.....te
0020 73 20 53 53 54 50 20 43 6c 69 65 6e 74 00 03 00  s Sstp C lient...
0030 0a 65 74 68 65 72 33 00 04 00 08 00 00 00 01 00  .ether3...
0040 05 00 13 36 2e 34 34 2e 33 20 28 73 74 61 62 6c  ...6.44. 3 (stabl
0050 65 29 00 06 00 0c 4d 69 6b 72 6f 54 69 6b     e)....Mi kroTik
```

THE CONCLUSION IS

- SSL dan IPSec keduanya memiliki silsilah keamanan yang kuat dengan kecepatan throughput, keamanan, dan kemudahan penggunaan yang sebanding untuk sebagian besar pelanggan layanan VPN komersial.
- Sstp bisa menjadi alternatif yang mudah diimplementasikan untuk mencegah MITM, Otentikasi dengan sertifikat akan membuatnya aman
- Jadi, keduanya memiliki pro dan kontra, sehingga tidak boleh dilihat sebagai lebih baik atau lebih buruk tetapi lebih seperti alat yang digunakan untuk menyelesaikan pekerjaan.

REFERENCE

wiki.mikrotik.com

blogs.akamai.com

thebestvpn.com

mikrotik.co.id

digicert.com

searchsecurity.techtarget.com

PERTANYAAN ?

?

THANK YOU

- Mikrotik & MuM Bali 2019
- Politeknik Citra Widya Edukasi
- Fullstack Team
- NBH Team

CONTACT



haris_pc



089529128403



harishardiansyah94@gmail.com