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

MY PROFILE

Haris Hardiansyah

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

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

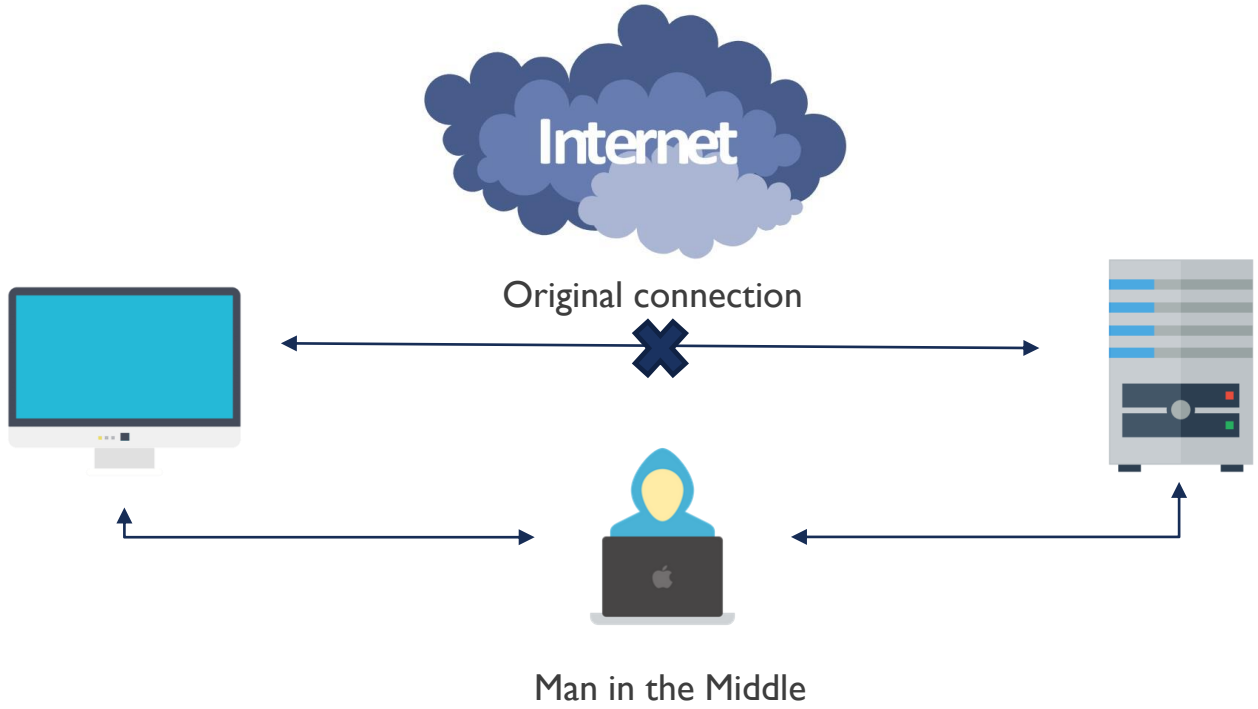
PROFILE POLITEKNIK CITRA WIDYA EDUKASI

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

NETWORK TRAINING POLTEK CWE

MITM (MAN IN THE MIDDLE ATTACK)

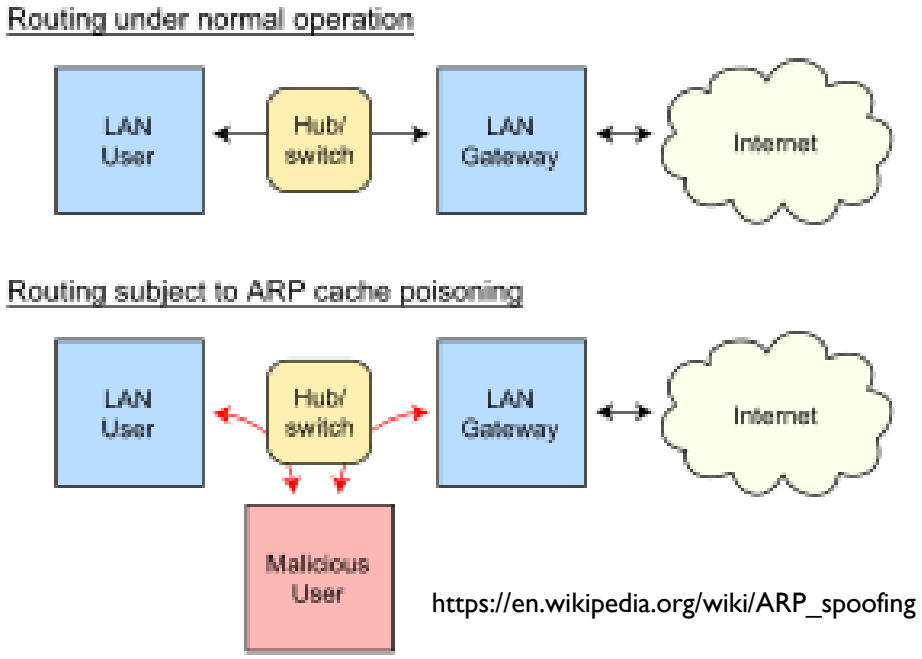
- Suatu serangan yg berada diantara posisi client dan server
- MITM biasanya terjadi karena kelalaian dalam proses otentikasi oleh pengguna.



WHAT ATTACKED ?

- ARP

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



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

Solution?

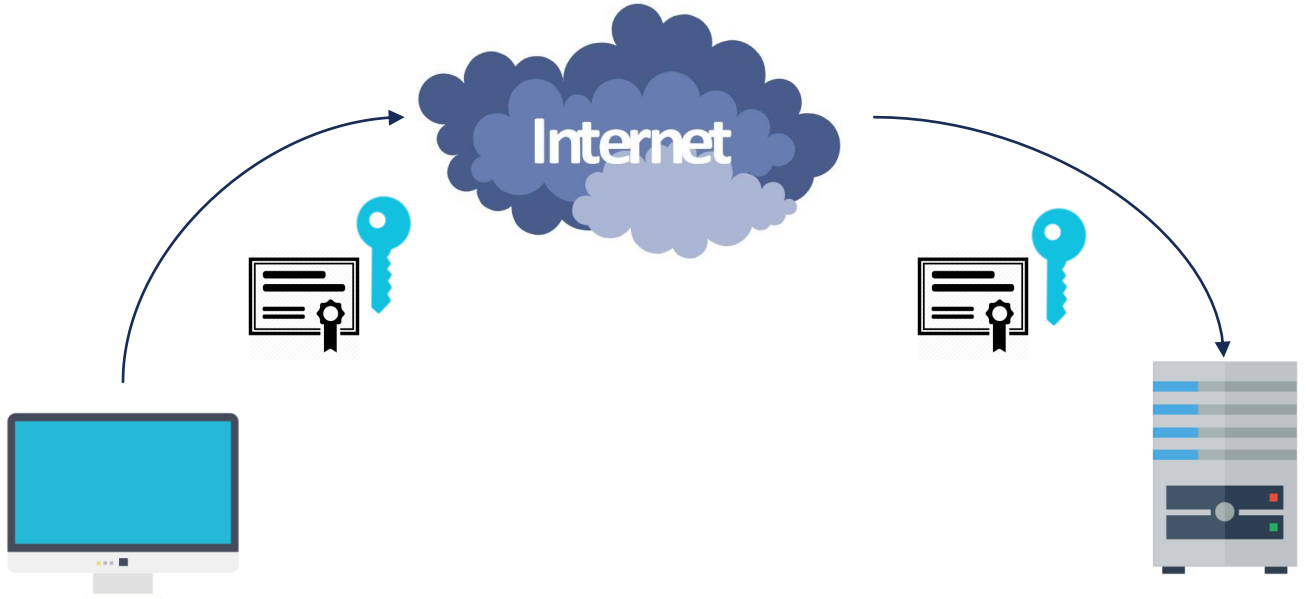
WHAT IS SSTP

- 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.



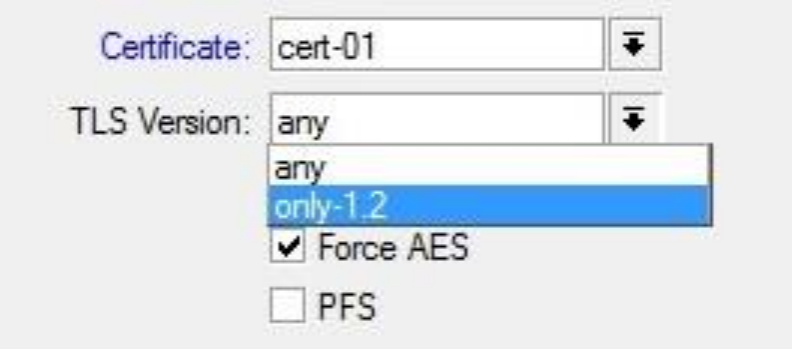
- TLS / SSL
  - **Enkripsi**
  - **Otentikasi**
  - **Integritas**
  - **Kriptografi security**

SSTP - TLS 1.2 VERSION

- Protokol ini menyediakan authentikasi 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

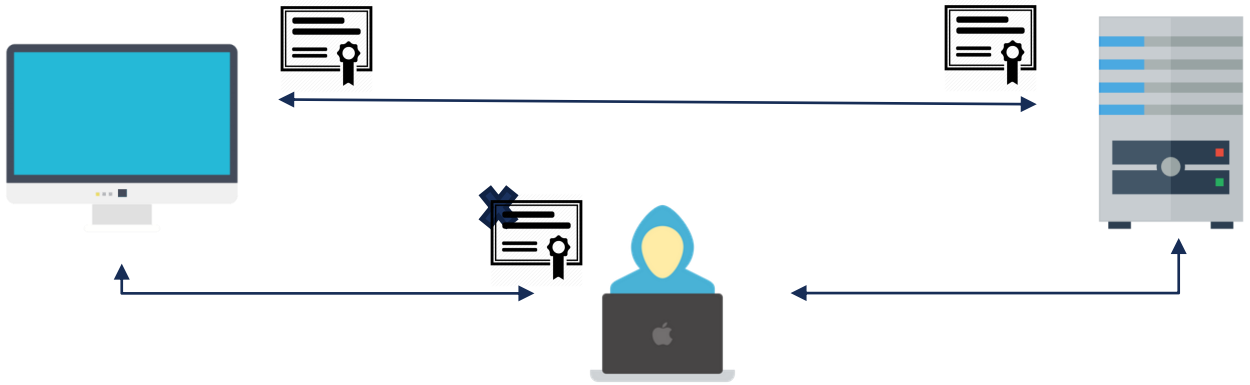


- RouterOS mengimpor sertifikat CA dan mengaktifkan opsi verifikasi-server-sertifikat. Dalam skenario ini, serangan Man-in-the-Middle tidak dimungkinkan.

SSTP Server

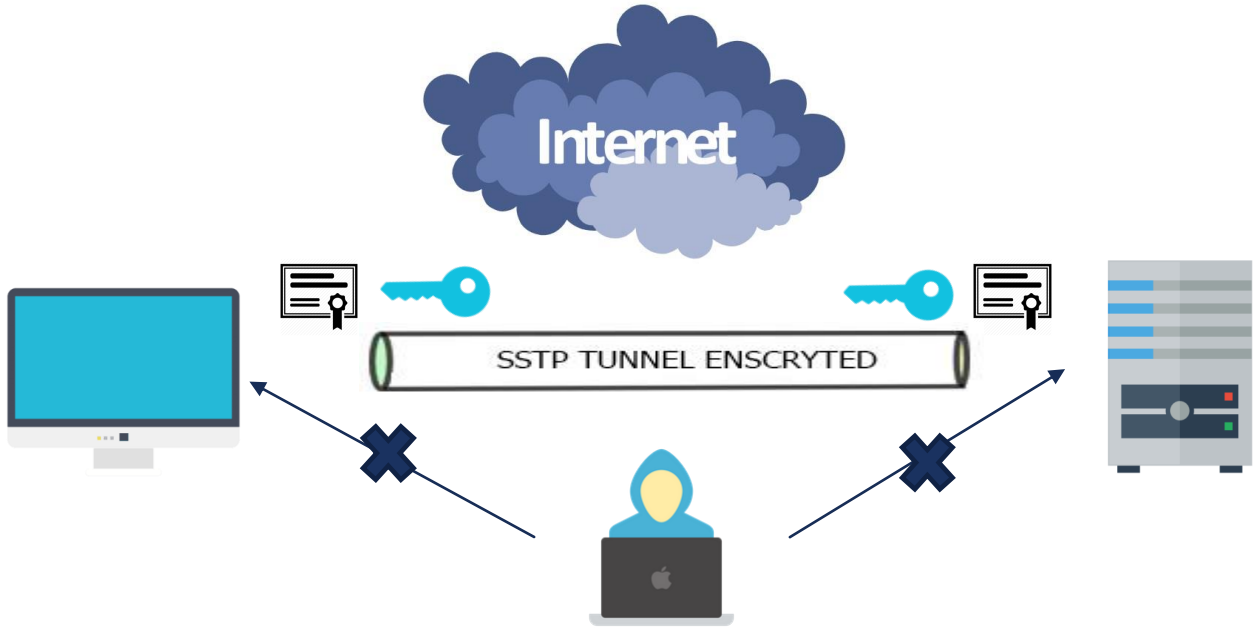
SSTP Client

- 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.

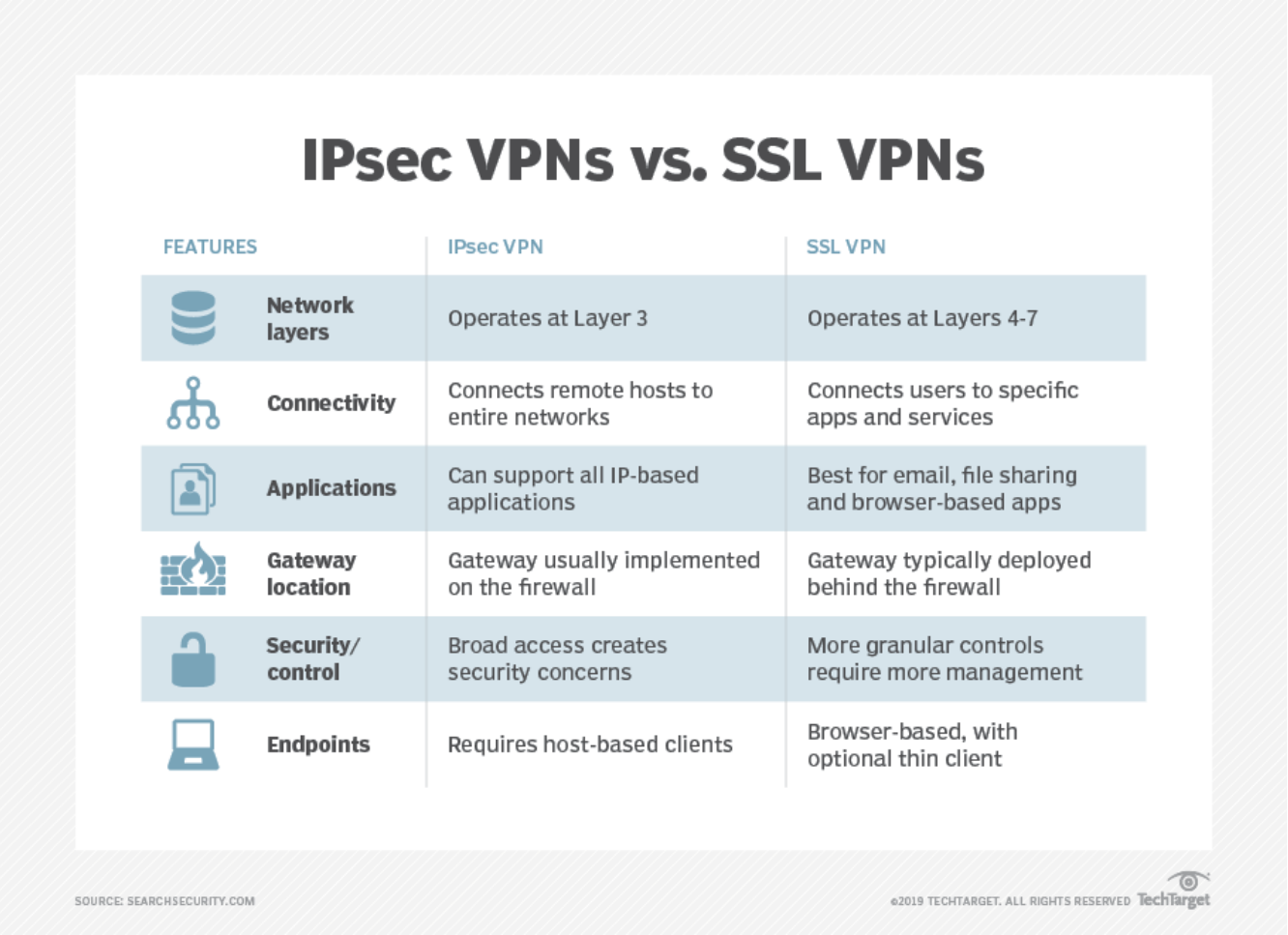


WHY SSTP ?

	OpenVPN	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/pptp-l2tp-openvpn-sstp-ikev2-protocols/

NOT USE IPSEC?



IPsec VPNs vs. SSL VPNs

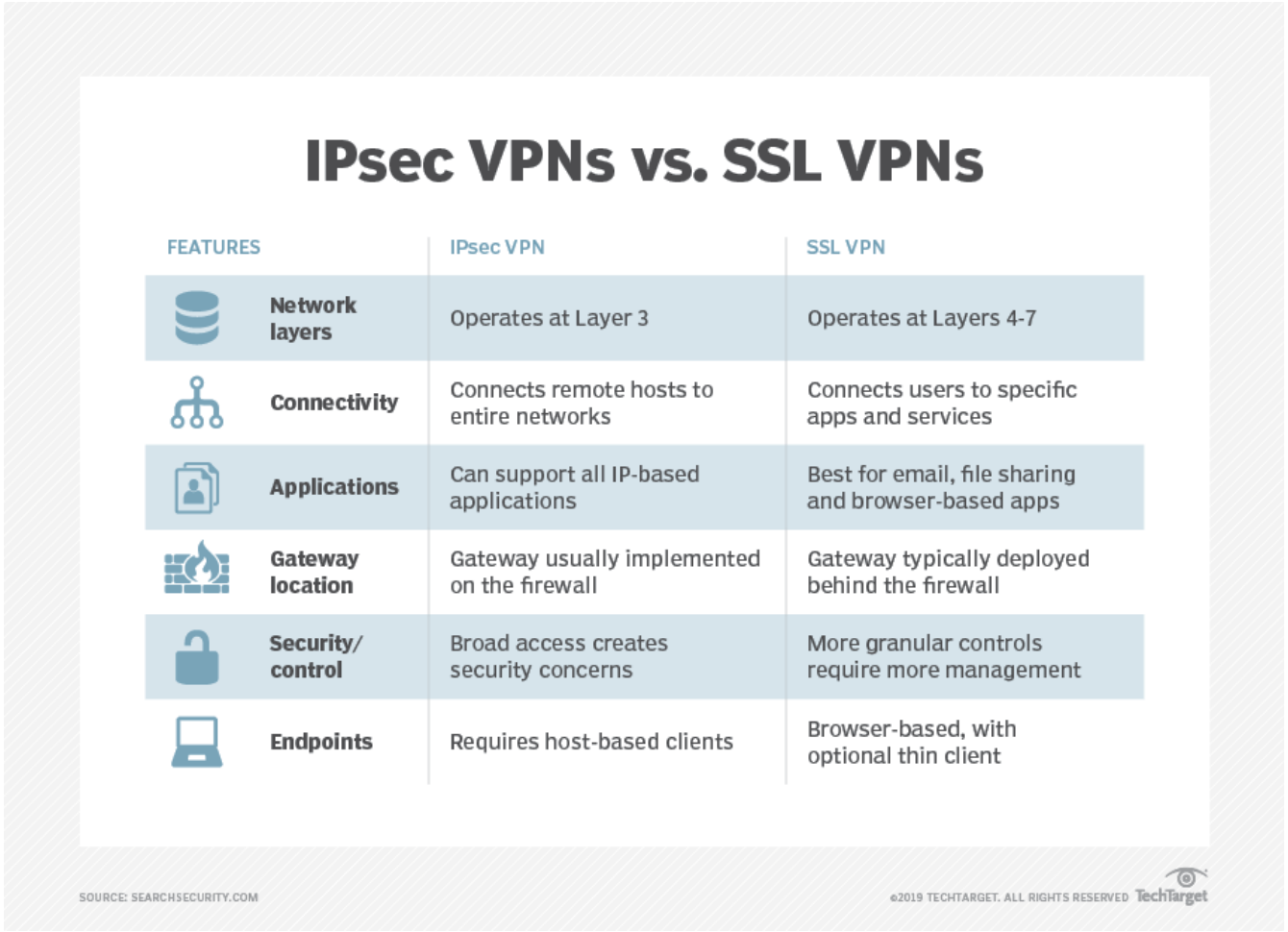
FEATURES	IPsec VPN	SSL VPN
Network layers	Operates at Layer 3	Operates at Layers 4-7
Connectivity	Connects remote hosts to entire networks	Connects users to specific apps and services
Applications	Can support all IP-based applications	Best for email, file sharing and browser-based apps
Gateway location	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

SOURCE: SEARCHSECURITY.COM

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

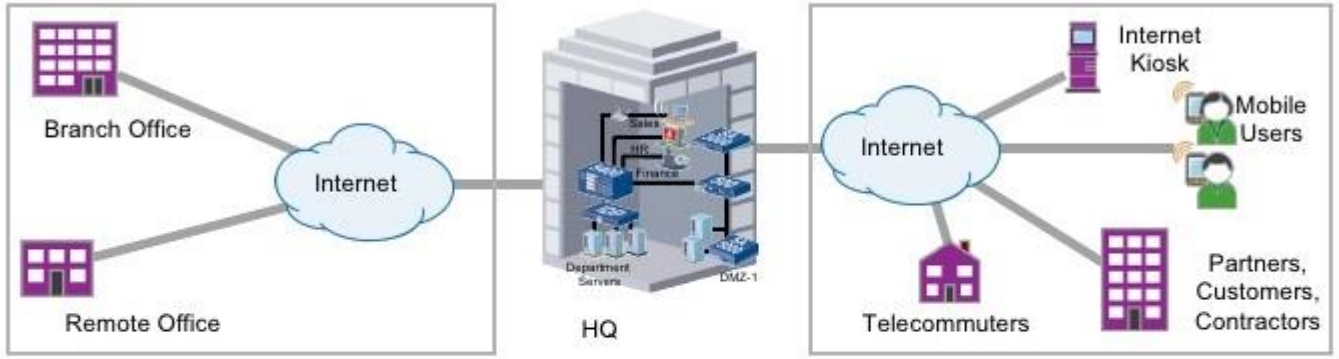
"Dengan IPsec, semua itu perlu dibuat eksplisit (karena tidak ada jaminan bahwa penerima akan mendapatkan paket yang sama dalam urutan yang sama dengan yang dikirim pengirim)"

https://searchsecurity.techtarget.com/tip/IPSec-VPN-vs-SSL-VPN-Comparing-respective-VPN-security-risks



- 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



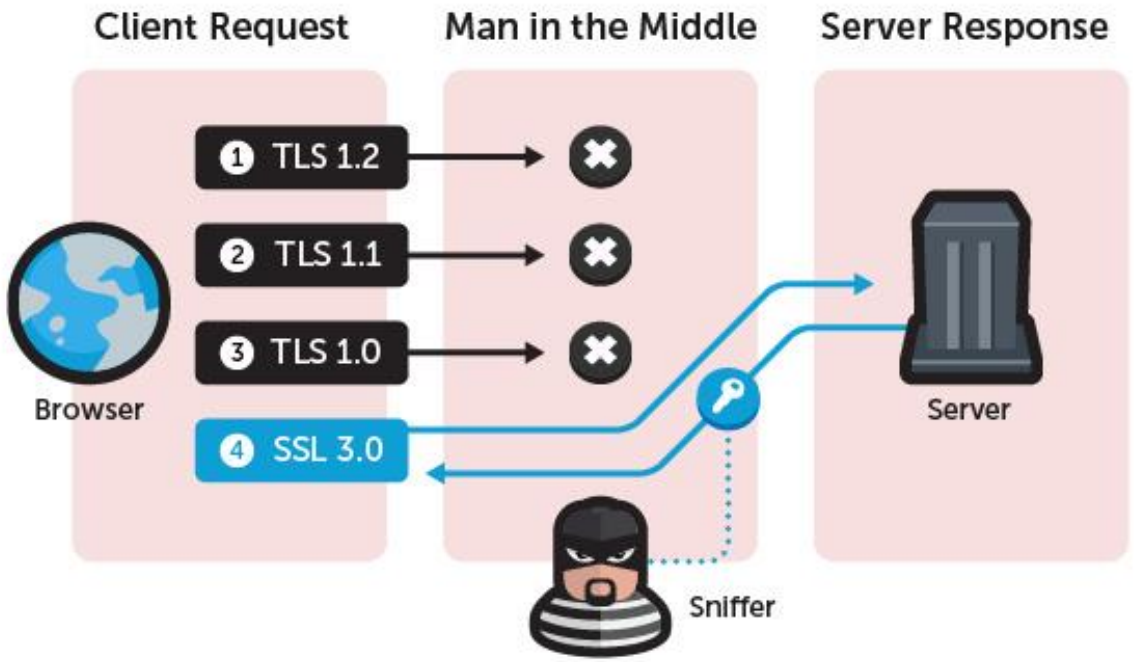
IPSec VPN
Remote/Branch Office Deployments
Fixed Site-to-Site
Managed Endpoints
Layer 3 Network Access
IP to IP Control
Access from Managed, Trusted Networks

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.

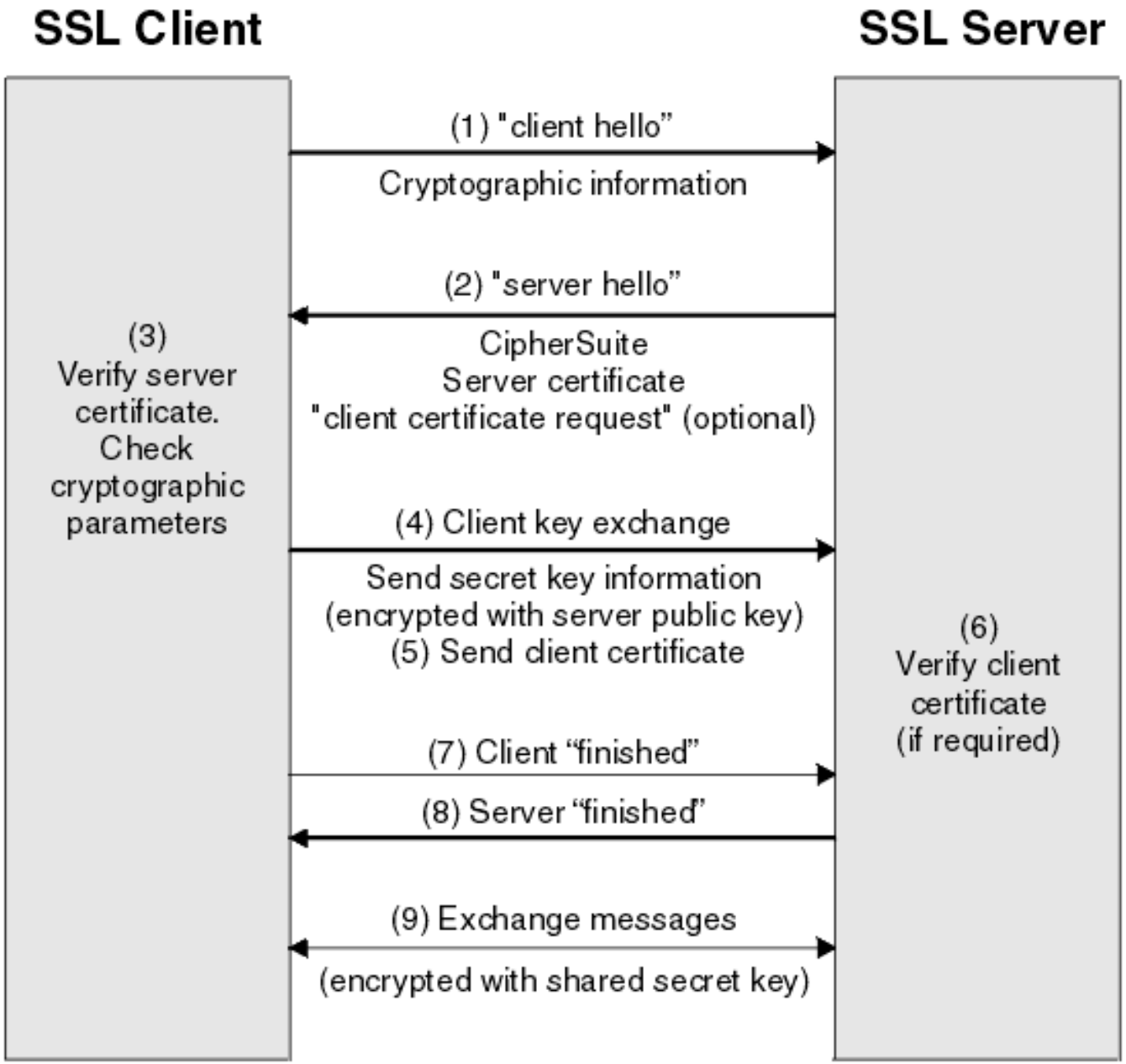
- SSTP uses TLS 1.2
  - Server & Client Certificate

    Publik key Disertifikasi oleh Sertifikat dengan Kepercayaan dari client.



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

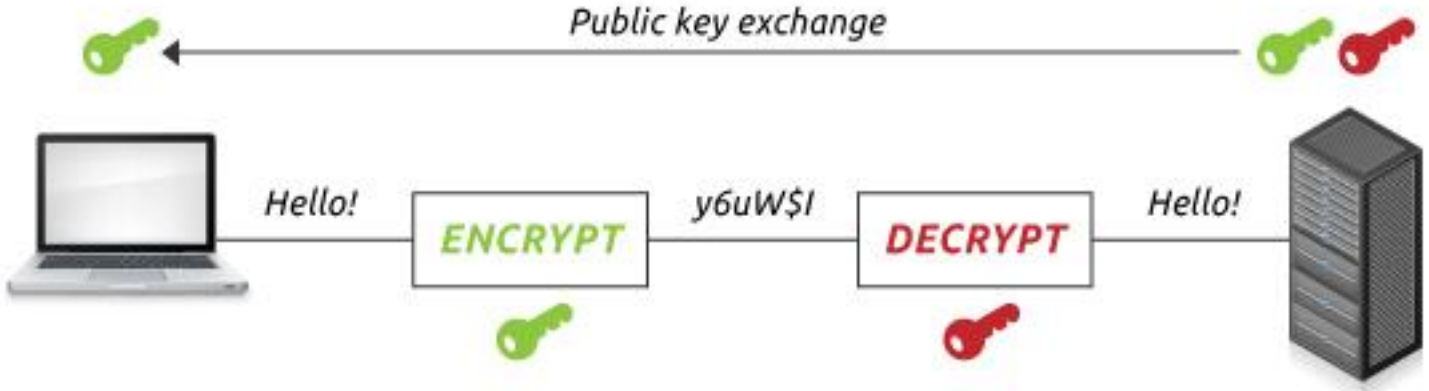
PROSES HANDSHAKE SSL/TLS



https://www.ibm.com/support/knowledgecenter/en/SSFKSJ_7.1.0/com.ibm.mq.doc/sy10660_.htm

ASYMMETRIC

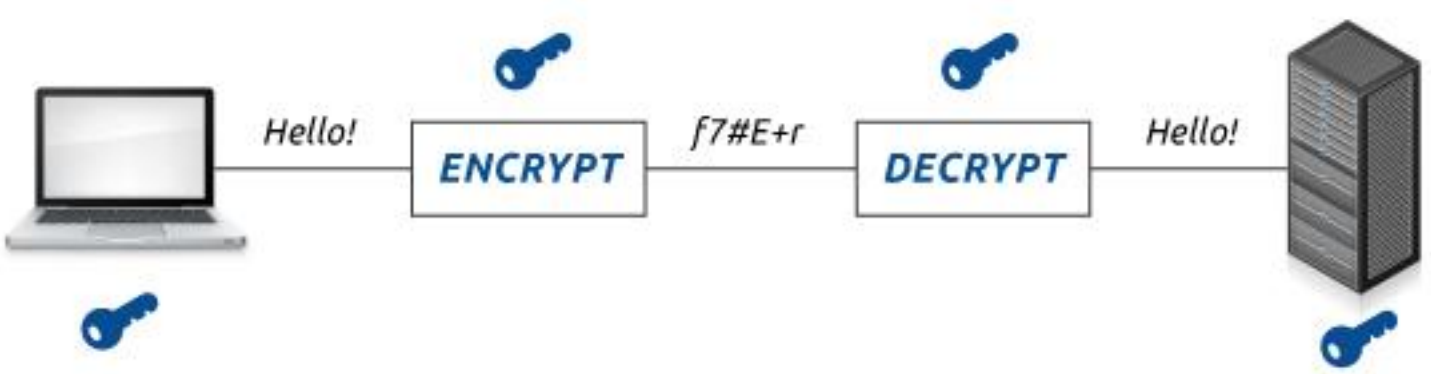
- SSTP It uses 2048 bit encryption and authentication certificates.



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

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

SYMMETRIC

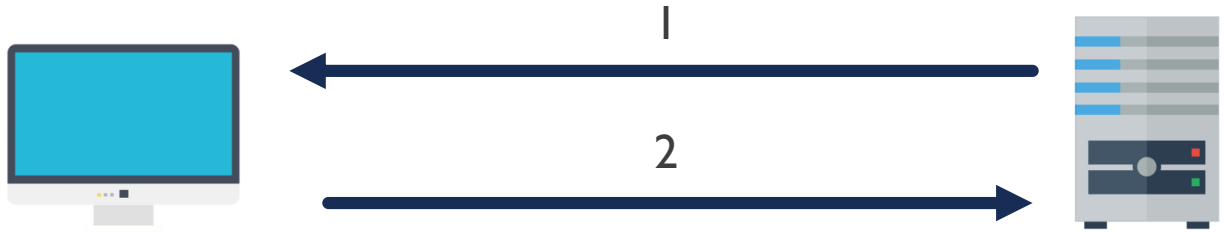


Enkripsi simetris (atau enkripsi kunci yang dibagikan sebelumnya) menggunakan kunci tunggal untuk mengenkripsi dan mendekripsi data.

HOW SSL USES ASYMMETRIC AND SYMMETRIC

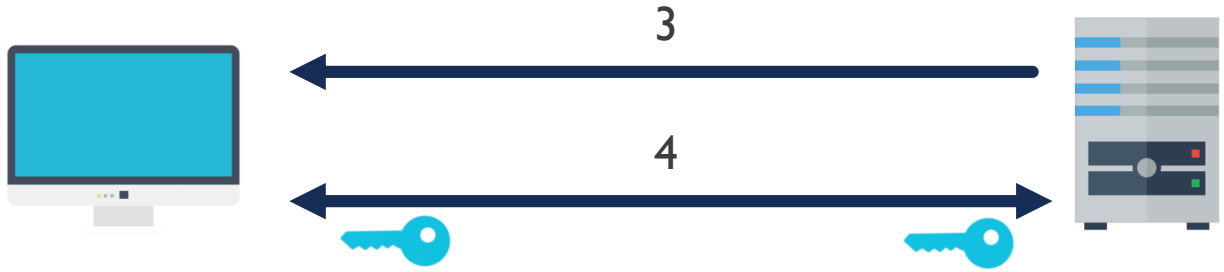
- Server mengirimkan salinan kunci publik asimetrisnya.

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

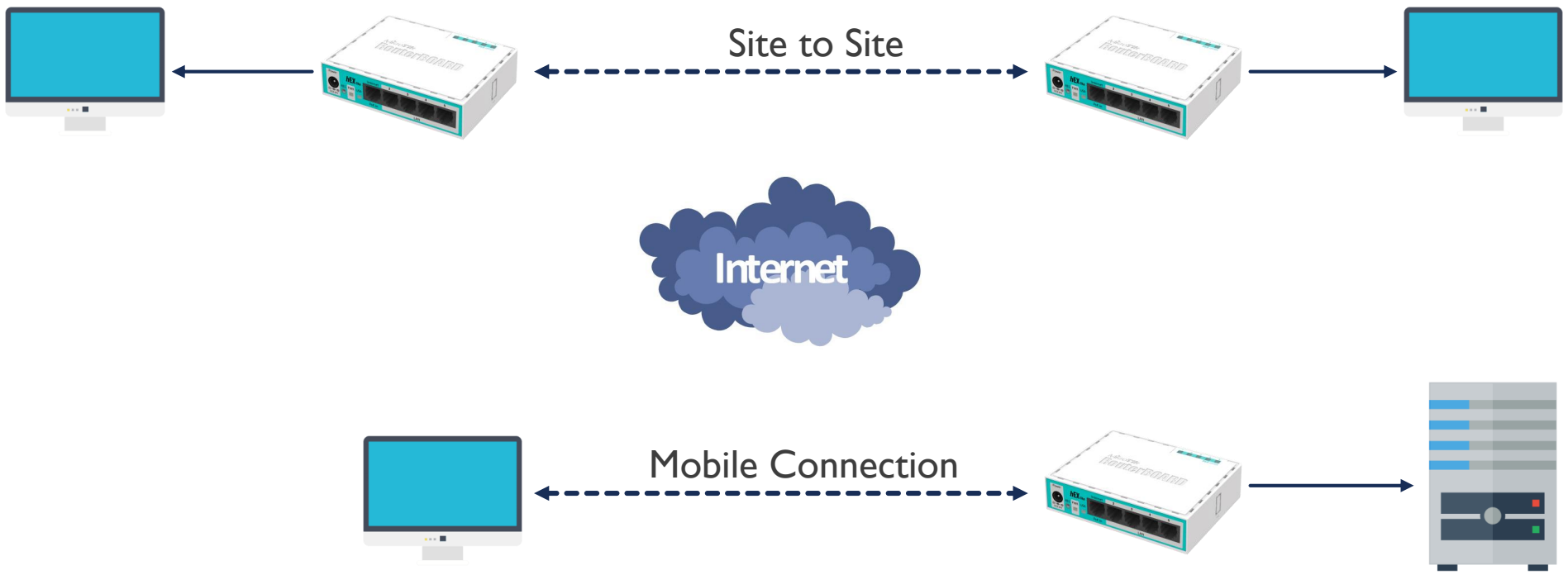


- Server dan Browser sekarang mengenkripsi dan mendekripsi semua data yang dikirimkan dengan kunci sesi

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

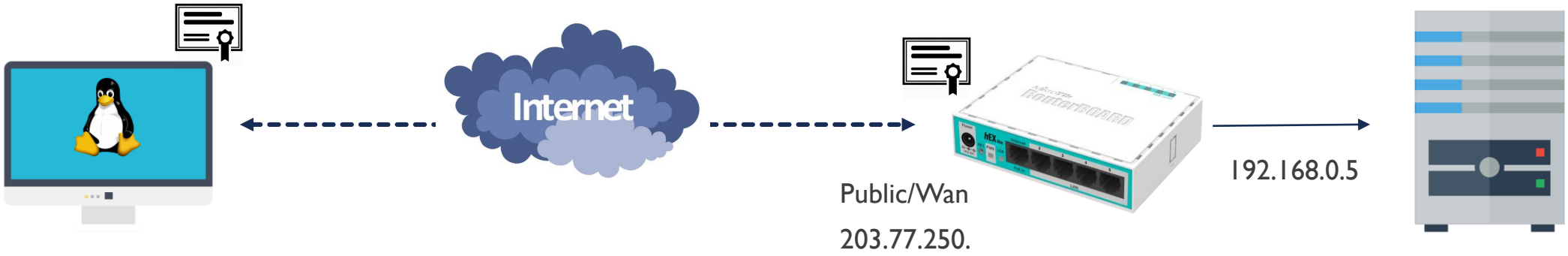


TOPOLOGI

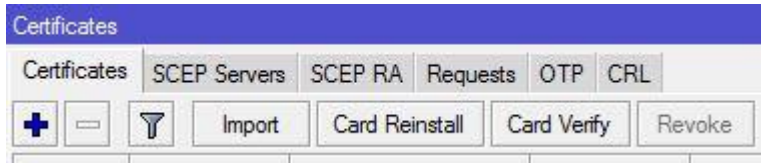


SSTP CLIENT ON LINUX

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



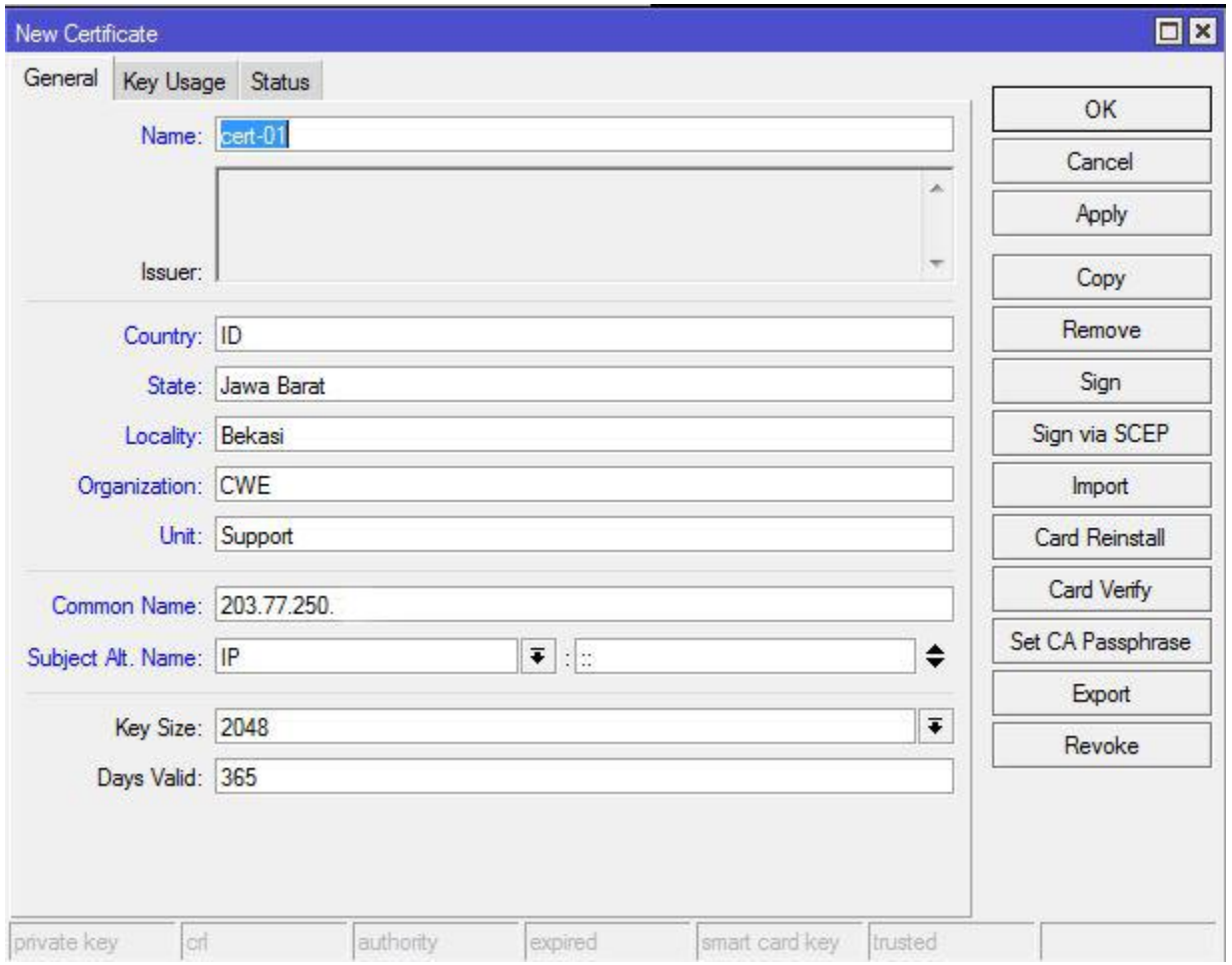
CONFIG MOBILE CONNECTION



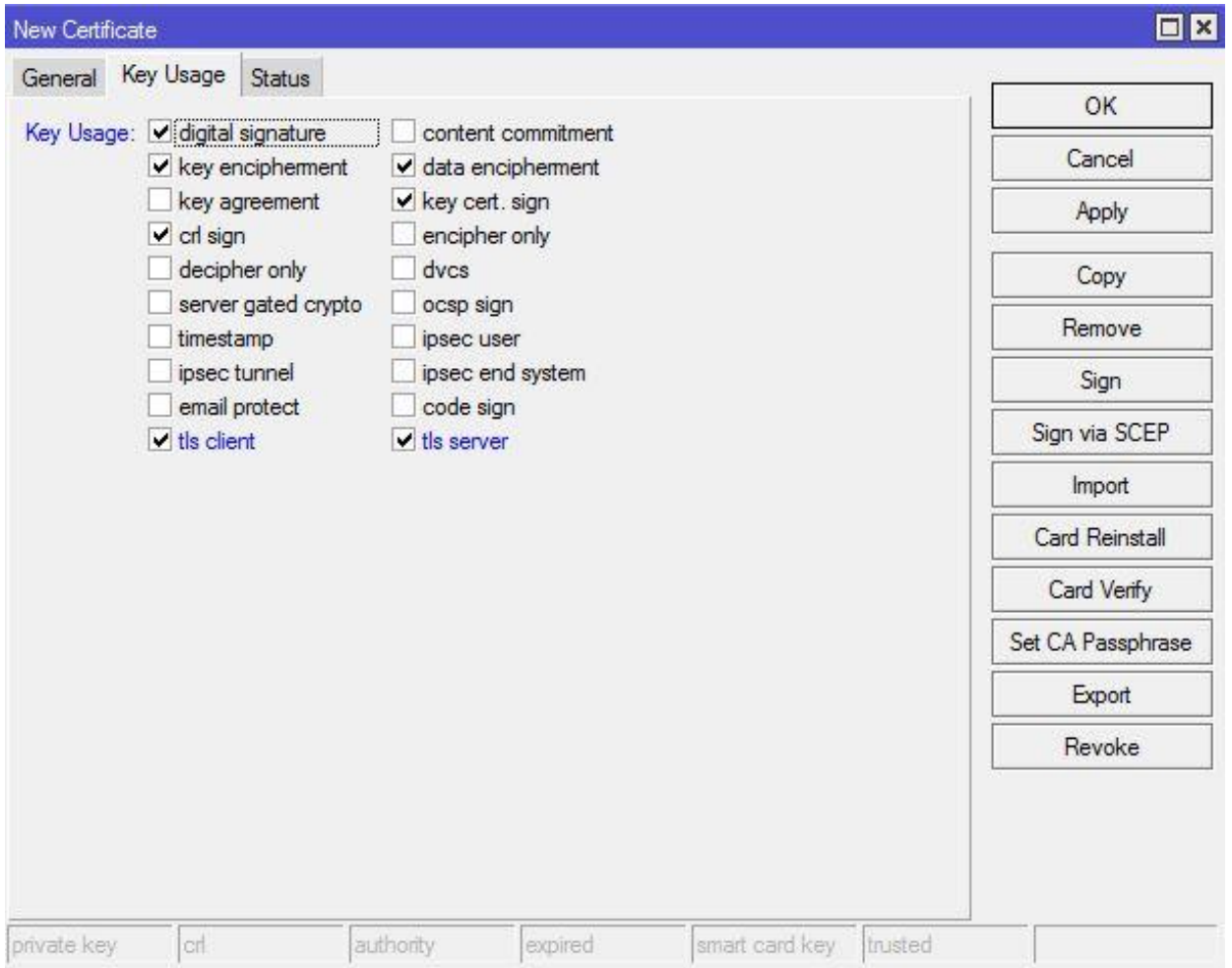
- Membuat Certificate

Disini kita akan membuat 3 Certificate

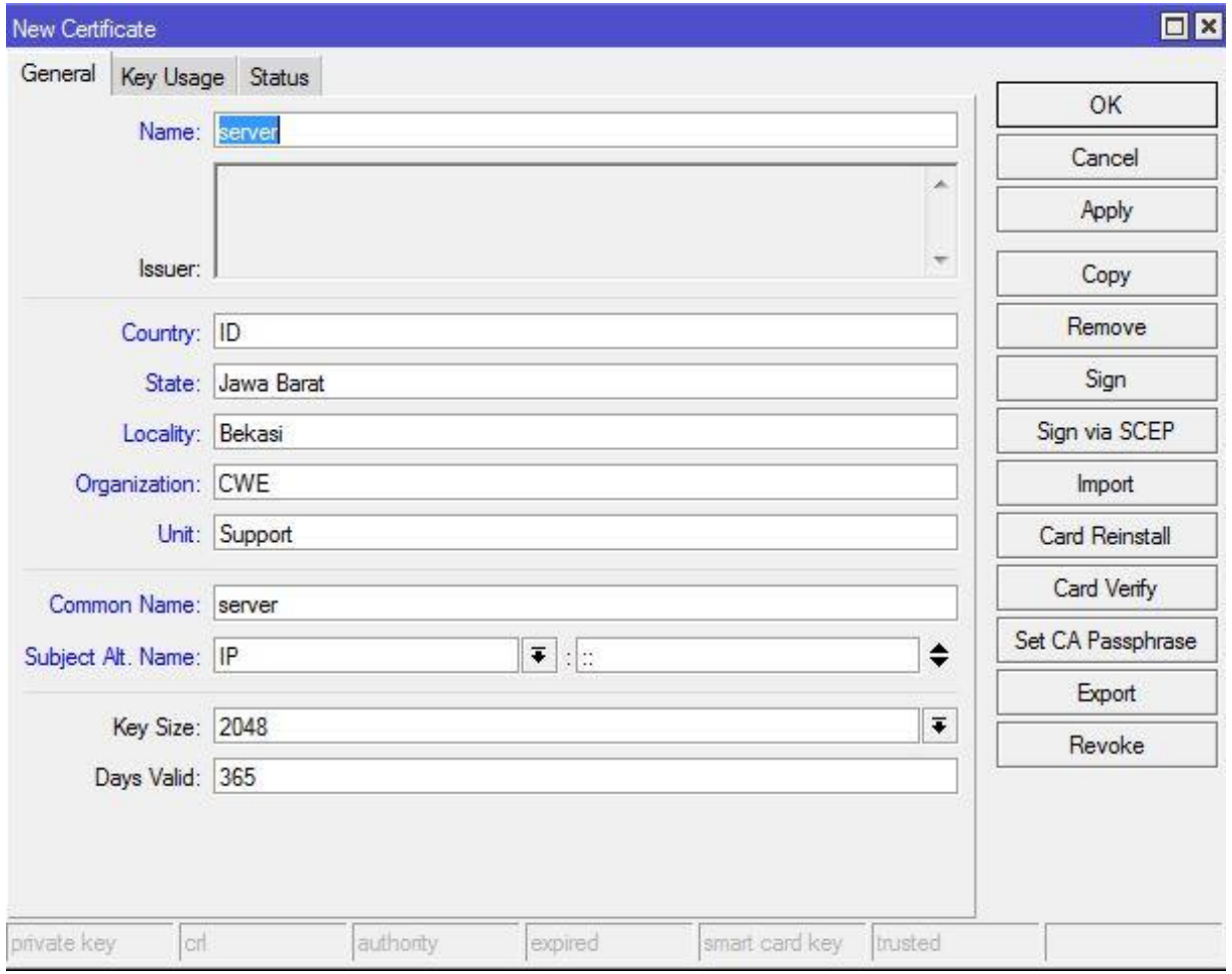
1. CA Template
2. Server
3. Client



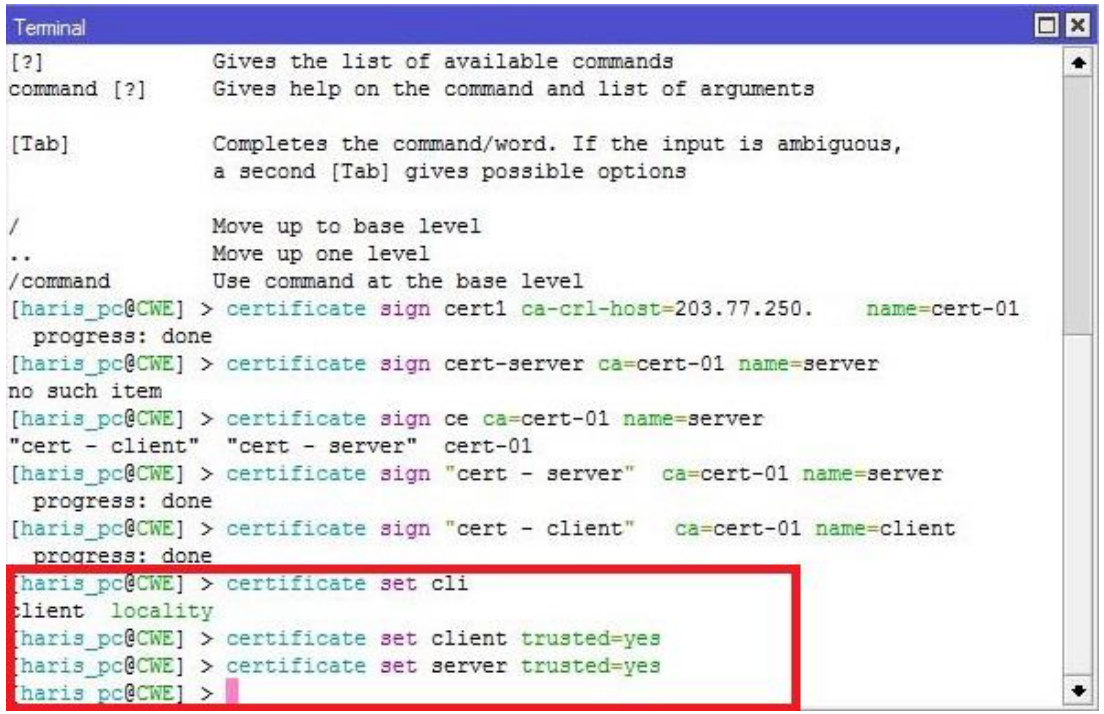
- Key Usage
  - TLS Server & Client

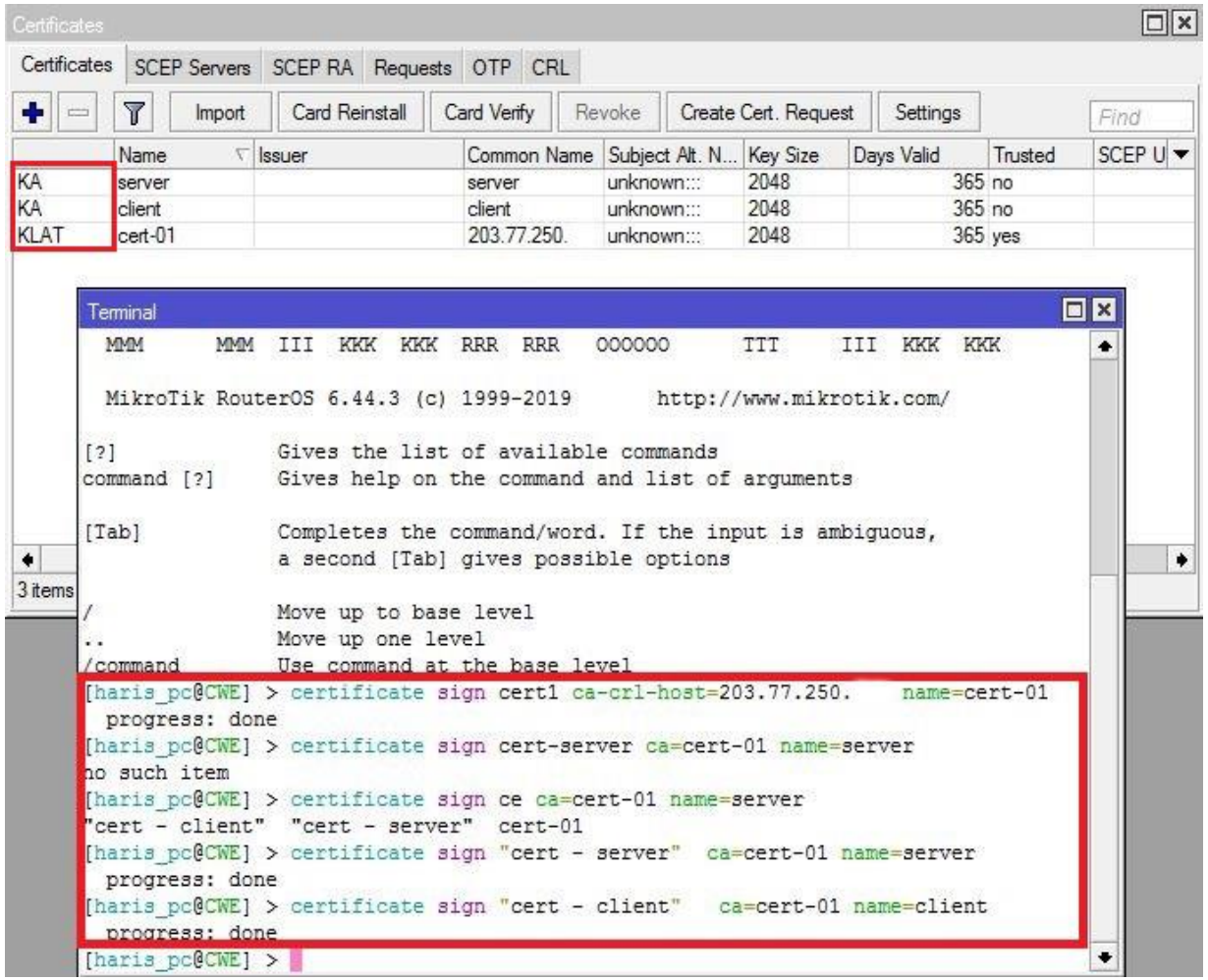


- Lakukan settingan yg sama , yang membedakan hanya common name dan name nya saja



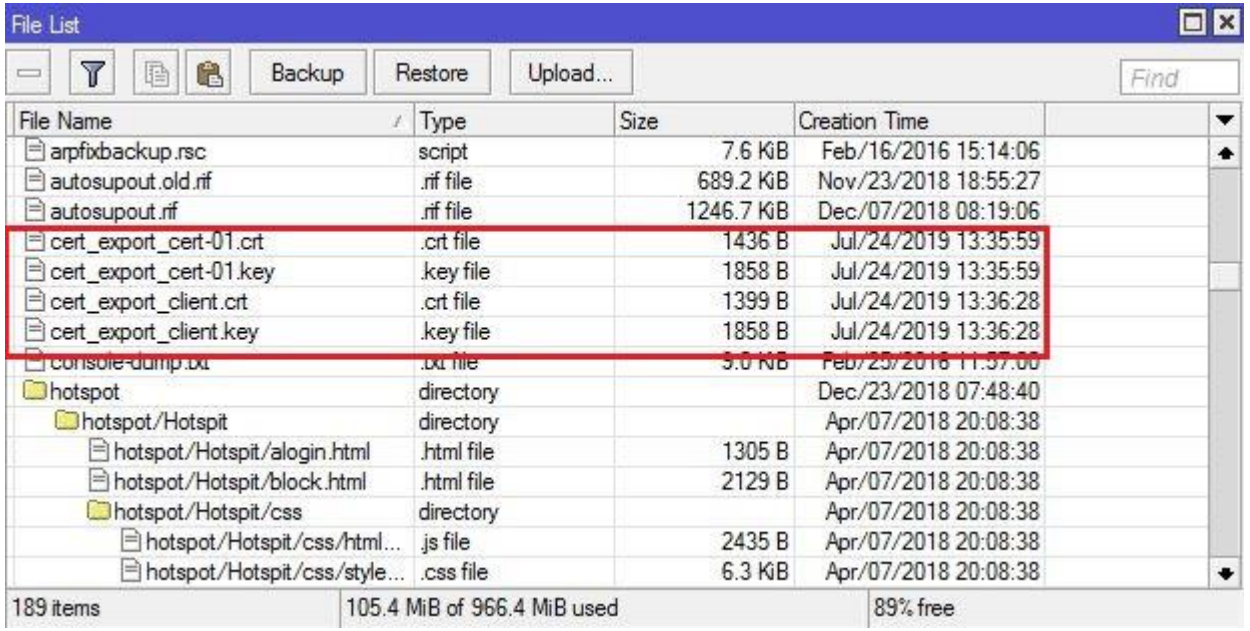
- Kita tanda tangani (sel-signed) server dan client nya dan jangan lupa trusted





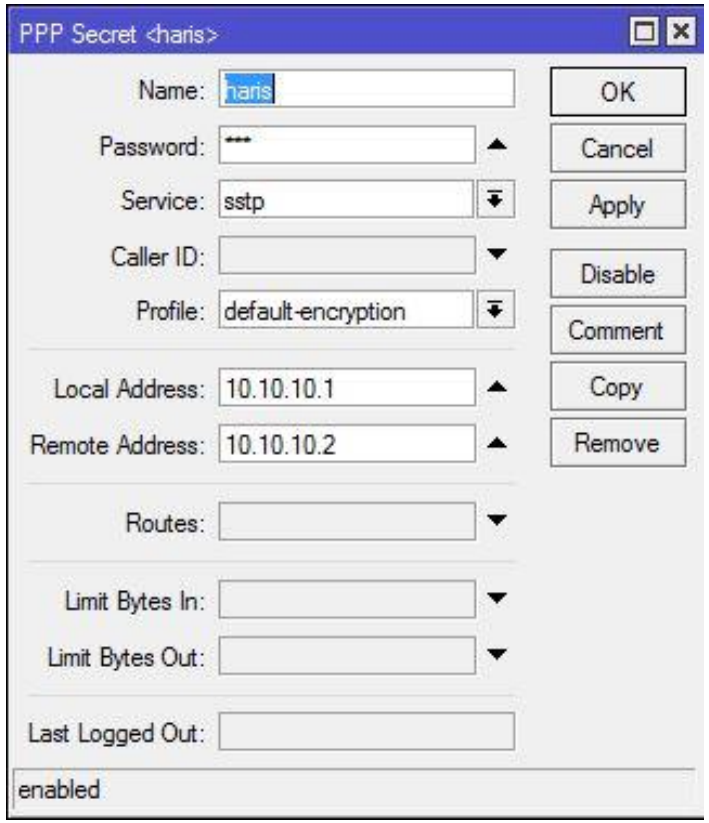
- Export certificate untuk nanti di pindahkan ke client

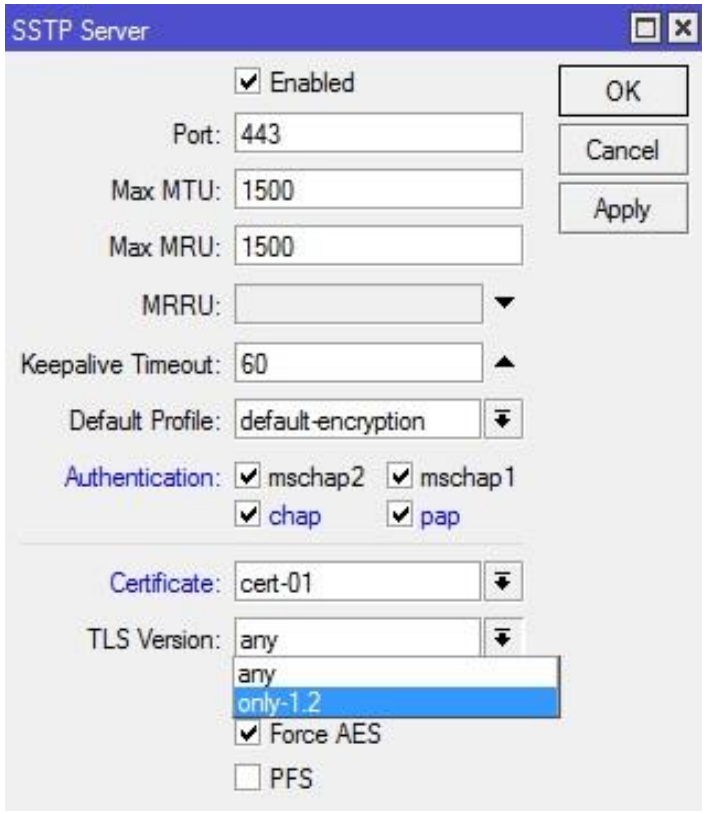
```
[haris_pc@CWE] > certificate export-certificate cert-01 export-passphrase=admin123

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

[haris_pc@CWE] >
```



- Aktifkan SSTP Server dan buat secret untuk akses login client

TLS/SSL validates server certificate.





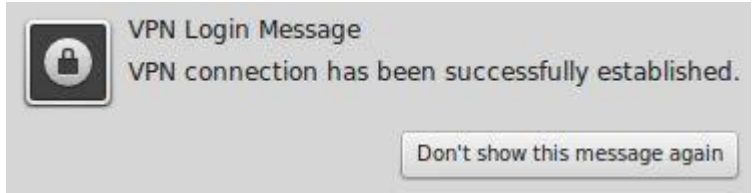
- Disini kita pilih TLS version 1.2

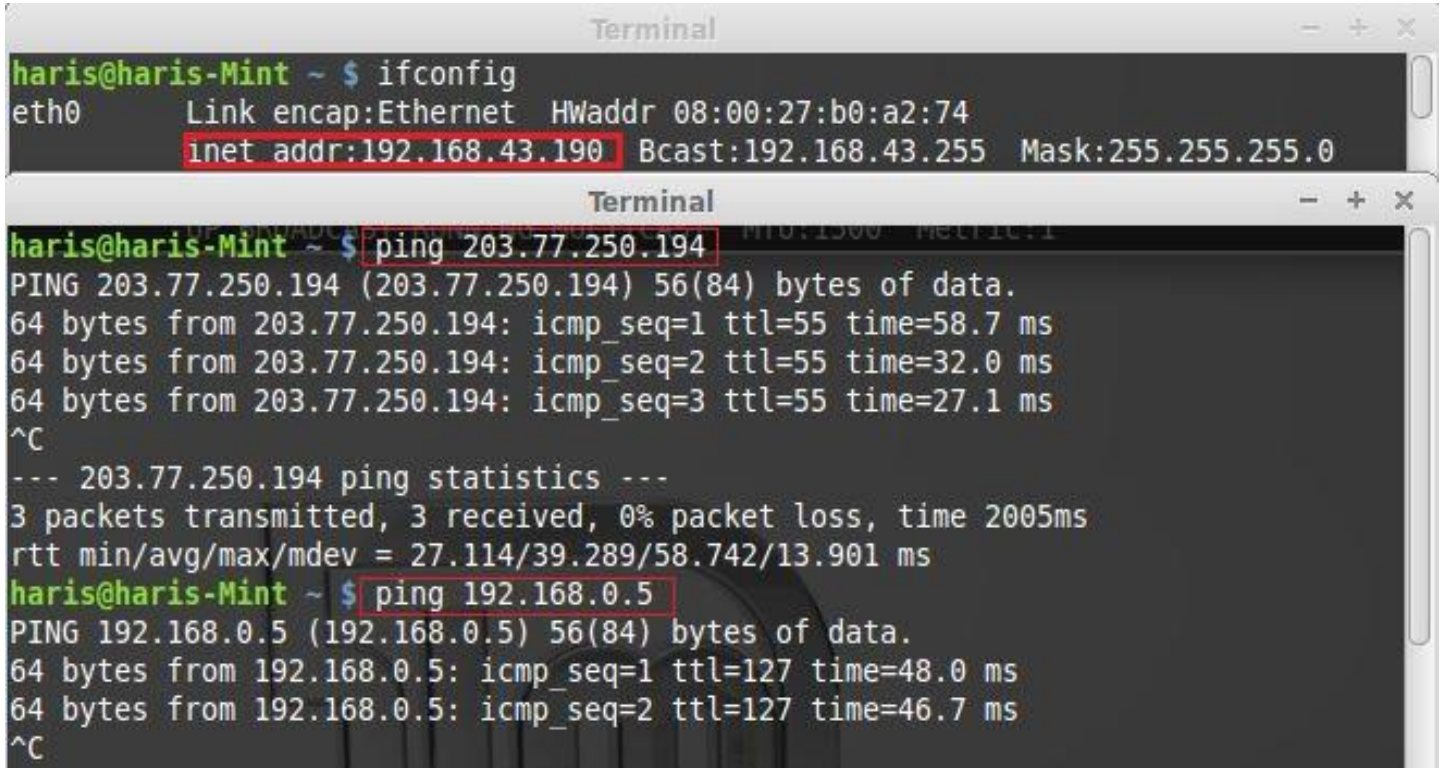
- Sekarang kita aktifkan VPN connection nya

- 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

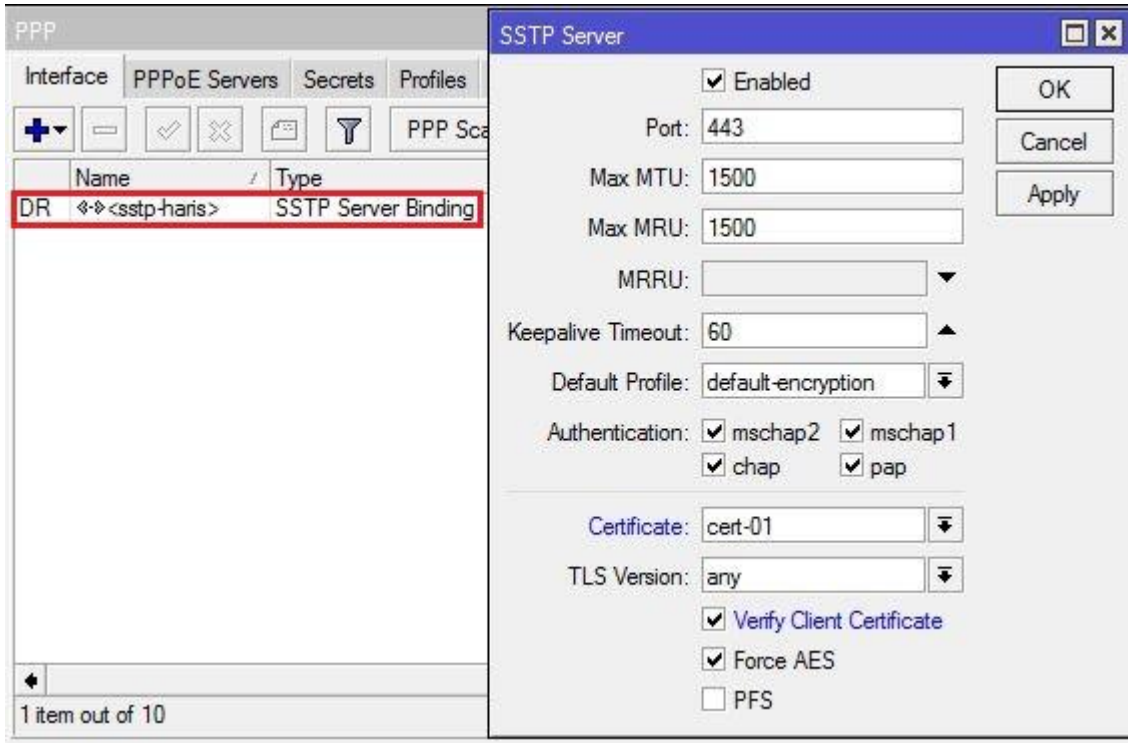




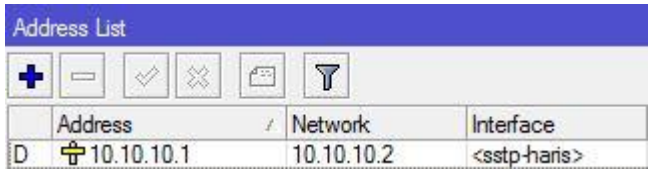
CONNECTED ON MIKROTIK

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

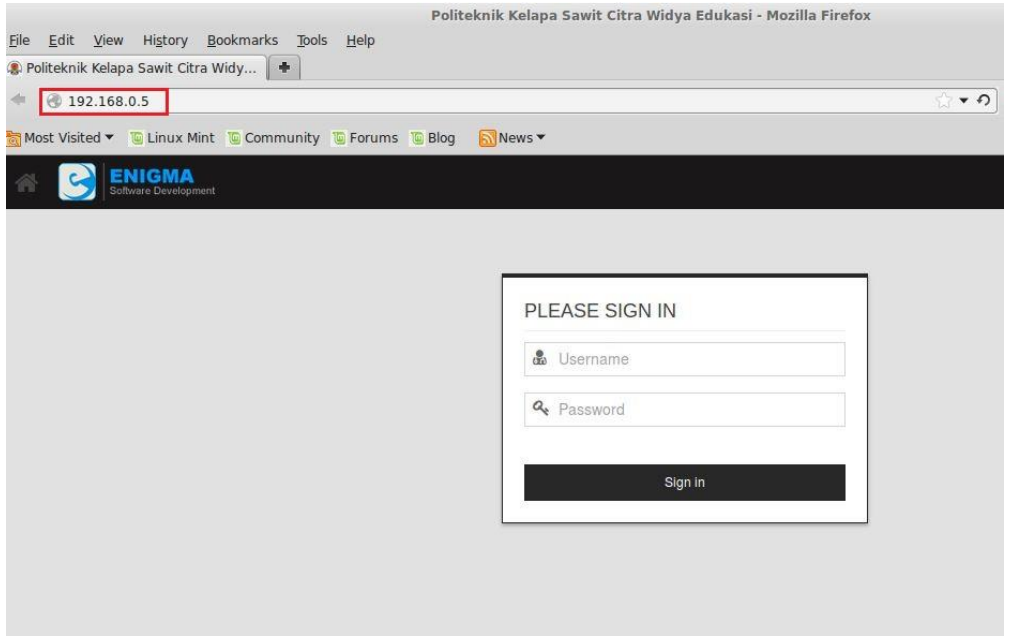
- Jika user terhubung pada server , maka di menu interface akan muncul

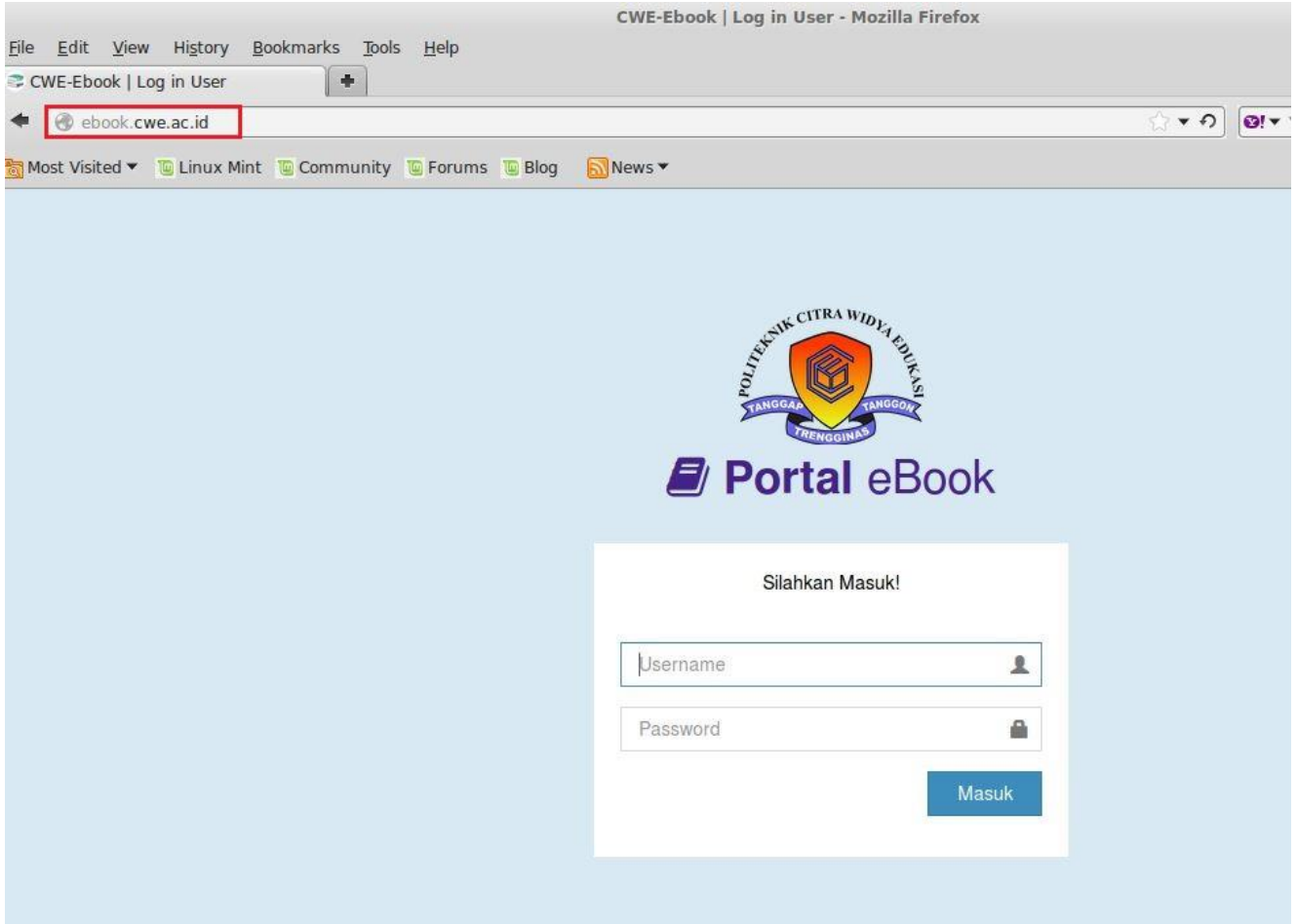


- IP yang di dapatkan otomatis

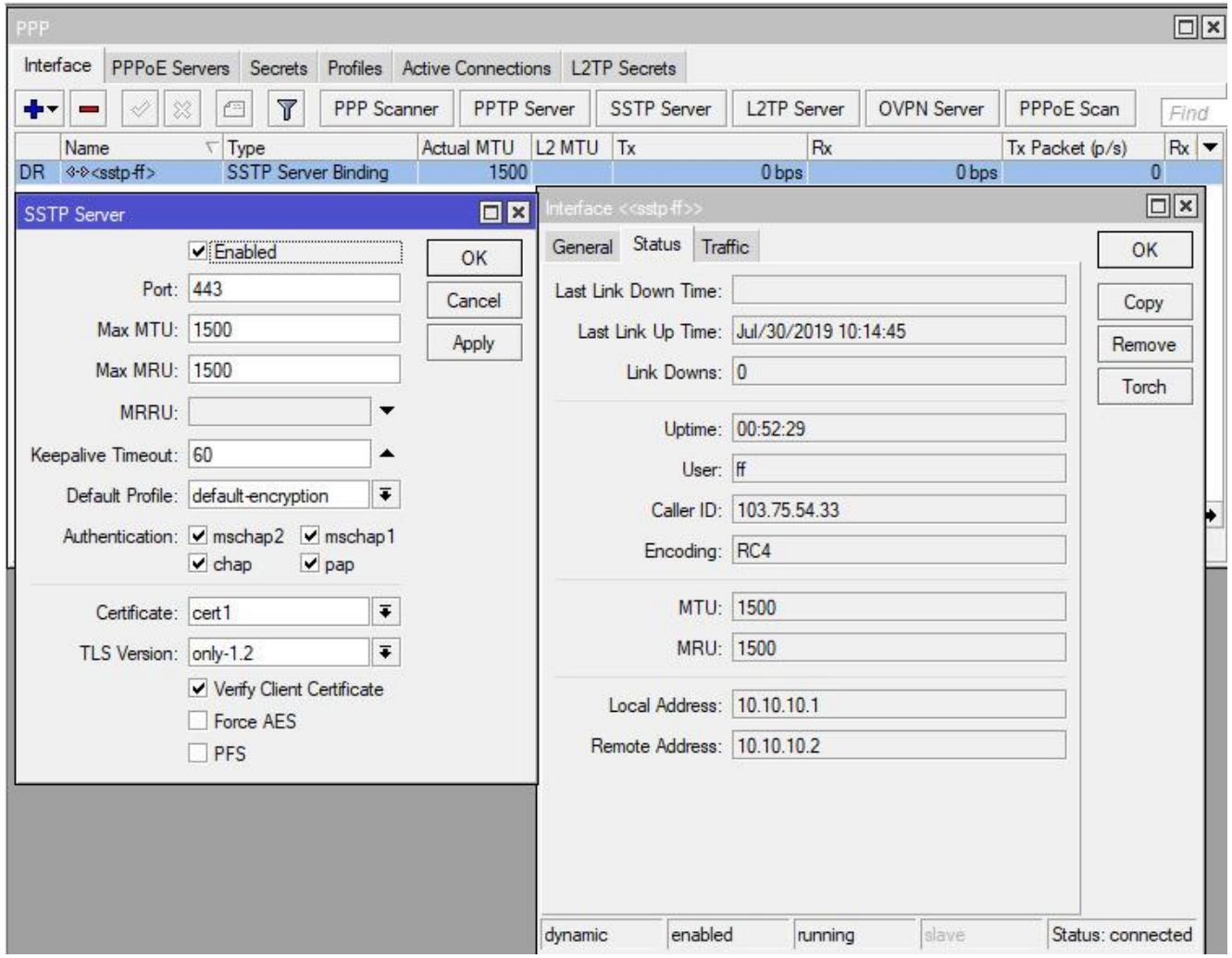


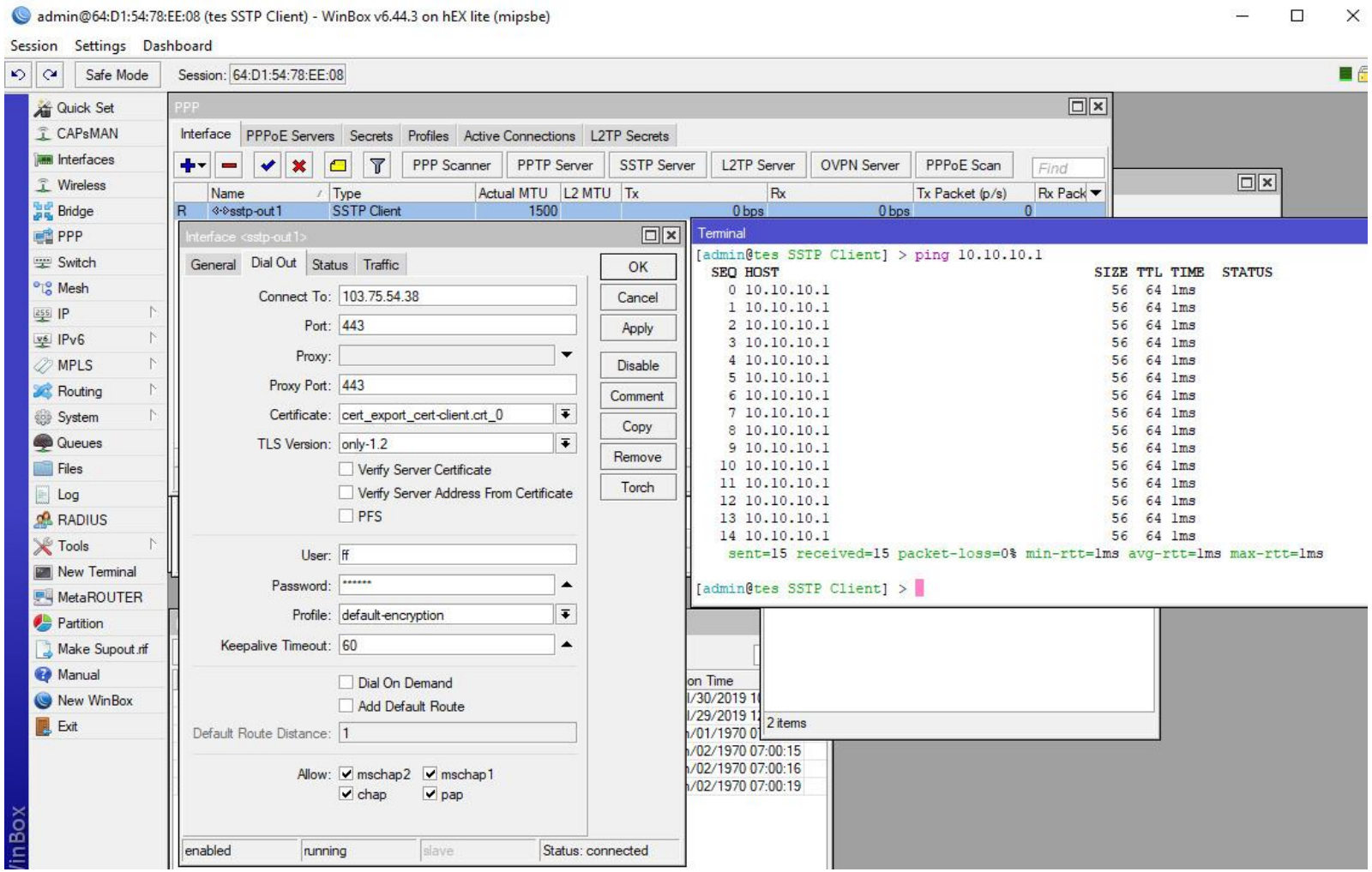
- Disini saya mencoba mengakses salah satu web server yg saya setting dengan ip local yaitu 192.168.0.5

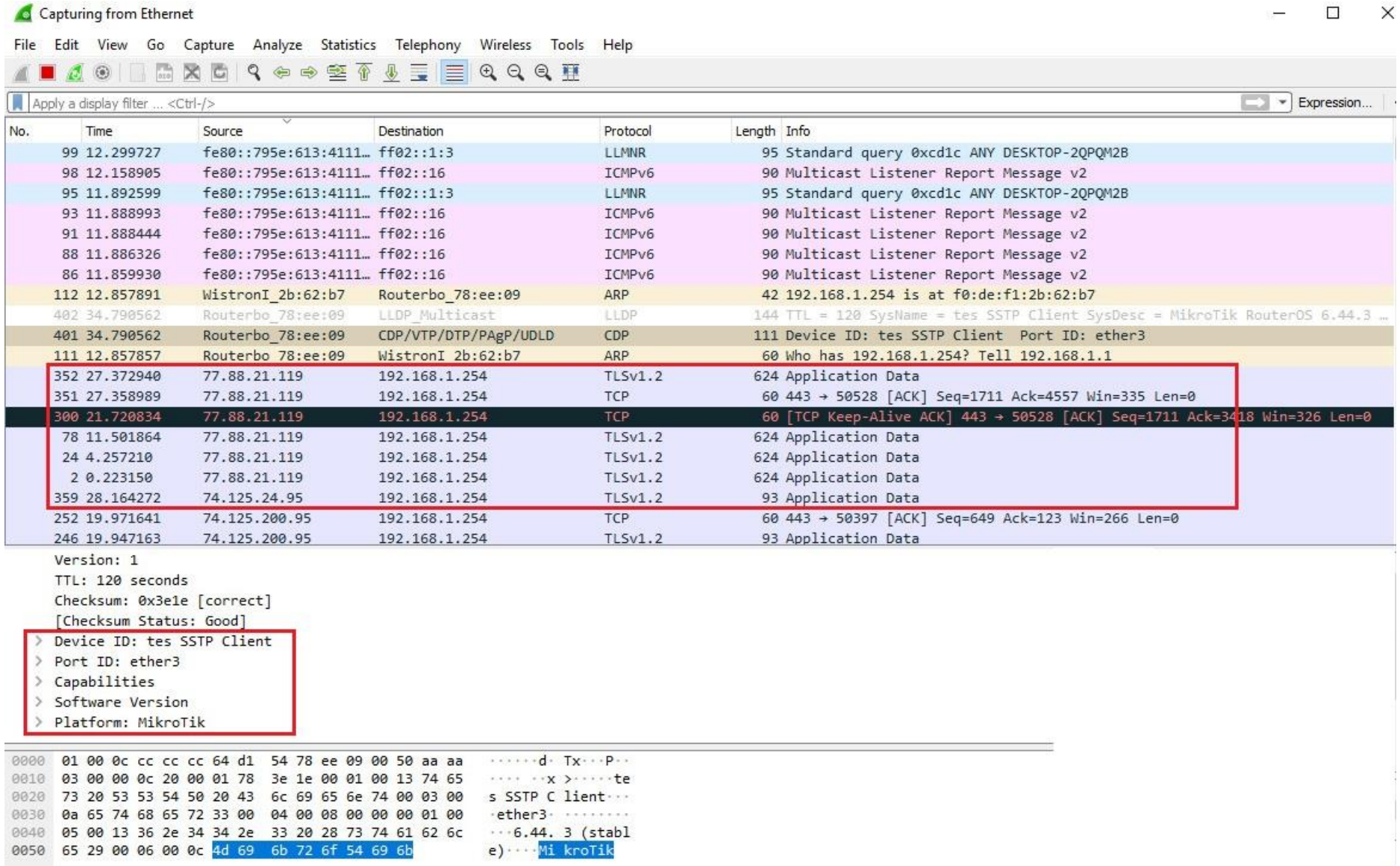




EXAMPLE SITE TO SITE




admin@64:D1:54:78:EE:08 (tes SSTP Client) - WinBox v6.44.3 on hEX lite (mipsbe)
Session Settings Dashboard
Safe Mode
Session: 64:D1:54:78:EE:08
Quick Set
CAPsMAN
Interfaces
Wireless
Bridge
PPP
Switch
Mesh
IP
IPv6
MPLS
Routing
System
Queues
Files
Log
RADIUS
Tools
New Terminal
MetaROUTER
Partition
Make Supout.rif
Manual
New WinBox
Exit
PPP
Interface
PPPoE Servers
Secrets
Profiles
Active Connections
L2TP Secrets
PPP Scanner
PPTP Server
SSTP Server
L2TP Server
OVPN Server
PPPoE Scan
Find
Name
Type
Actual MTU
L2 MTU
Tx
Rx
Tx Packet (p/s)
Rx Pack
R
sstp-out1
SSTP Client
1500
0 bps
0 bps
0
Interface <sstp-out1>
General
Dial Out
Status
Traffic
OK
Cancel
Apply
Disable
Comment
Copy
Remove
Torch
Connect To: 103.75.54.38
Port: 443
Proxy:
Proxy Port: 443
Certificate: cert_export_cert-client.crt_0
TLS Version: only-1.2
Verify Server Certificate
Verify Server Address From Certificate
PFS
User: ff
Password: ******
Profile: default-encryption
Keepalive Timeout: 60
Dial On Demand
Add Default Route
Default Route Distance: 1
Allow: mschap2 mschap1 chap pap
enabled
running
slave
Status: connected
Terminal
[admin@tes SSTP Client] > ping 10.10.10.1
SEQ HOST SIZE TTL TIME STATUS
0 10.10.10.1 56 64 1ms
1 10.10.10.1 56 64 1ms
2 10.10.10.1 56 64 1ms
3 10.10.10.1 56 64 1ms
4 10.10.10.1 56 64 1ms
5 10.10.10.1 56 64 1ms
6 10.10.10.1 56 64 1ms
7 10.10.10.1 56 64 1ms
8 10.10.10.1 56 64 1ms
9 10.10.10.1 56 64 1ms
10 10.10.10.1 56 64 1ms
11 10.10.10.1 56 64 1ms
12 10.10.10.1 56 64 1ms
13 10.10.10.1 56 64 1ms
14 10.10.10.1 56 64 1ms
sent=15 received=15 packet-loss=0% min-rtt=1ms avg-rtt=1ms max-rtt=1ms
[admin@tes SSTP Client] >
on Time
/30/2019 1
/29/2019 1
/01/1970 0
/02/1970 07:00:15
/02/1970 07:00:16
/02/1970 07:00:19
2 items
WinBox


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
0010 03 00 00 0c 20 00 01 78 3e 1e 00 01 00 13 74 65
0020 73 20 53 53 54 50 20 43 6c 69 65 6e 74 00 03 00
0030 0a 65 74 68 65 72 33 00 04 00 08 00 00 00 01 00
0040 05 00 13 36 2e 34 34 2e 33 20 28 73 74 61 62 6c
0050 65 29 00 06 00 0c 4d 69 6b 72 6f 54 69 6b

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

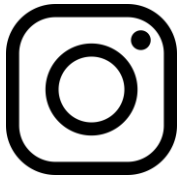
PERTANYAAN ?

?

THANK YOU

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

CONTACT



haris_pc

089529128403

harishardiansyah94@gmail.com