SANGFOR WANO Exchange Acceleration Guide

SANGFOR Technologies Co., Ltd.

Nov 2015

WANO Exchange Acceleration Guide

1. Backgroud

1.1 Protocol support

Protocol	Status
SMTP	Y
POP	Y
TLS/SSL	Y
MAPI	Y

1.2 Exchange version support

Server / Outlook	2003	2007	2010	2013	2016
2003	Y	Y	Y	Y	N
2007	Y	Y	Y	Y	N
2010	Y	Y	Y	Y	N
2013	Y	Y	Y	Y	N
2016	N	N	N	N	N
365	N	N	N	N	N

(This Explain from latest version 9.1R1, Nov.2015)

1.3 Things that customer need to prepare

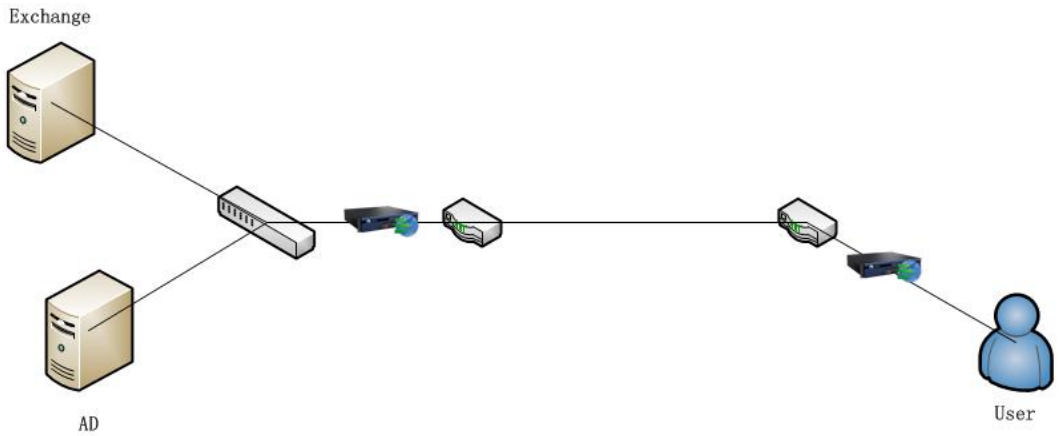
According to the following scenarios, there is(are) 1-3 things need customer to prepare:

1. WANO use administrator account to join domain
2. Create a domain user for WANO and use this account delegate Exchange server ExchangeMDB service
3. Import Exchange CA to WANO

Make sure customer prepare the above things in advance!

2. Exchange Scenarios

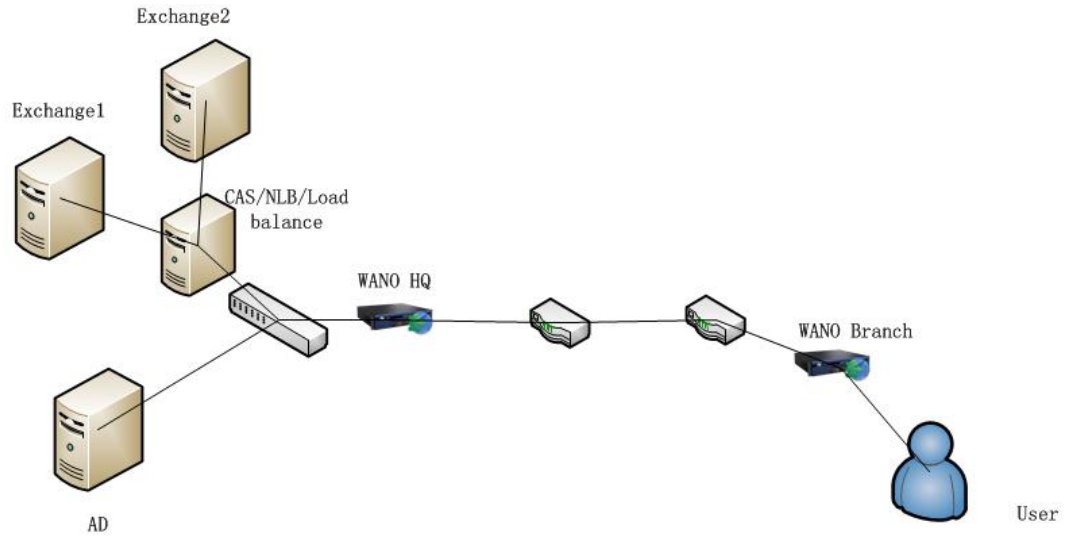
Scenario 1 : Single Domain/ Centralized AD server/ Centralized Exchange server/ Single Exchange server



Scenarios	Single Domain/ Centralized AD server/ Centralized Exchange server/ Single Exchange server
Version requested	9.1SP1 or above

Item	Email protocol enabled	WANO configuration
1	SMTP/POP3	Enable SMTP/POP3 Proxy
2	SMTP/POP3 over SSL	1. Import Exchange server certificate to WANO, configure certificate IP as Exchange server IP, configure port as 0 2. Enable SMTP/POP3 Proxy
3	MAPI	1. WANO join domain 2. Create a domain user for WANO and use this account delegate Exchange server ExchangeMDB service 3. Sync WANO time zone/date/time with AD, keep time differ in 30s, and then use delegation mode in exchange proxy. 4. Outlook anywhere need to import Exchange server certificate to WANO , configure certificate IP as Exchange sever IP, configure port as 0
4	WebMail	1. Import Exchange server certificate to WANO 2. Enable SSL proxy

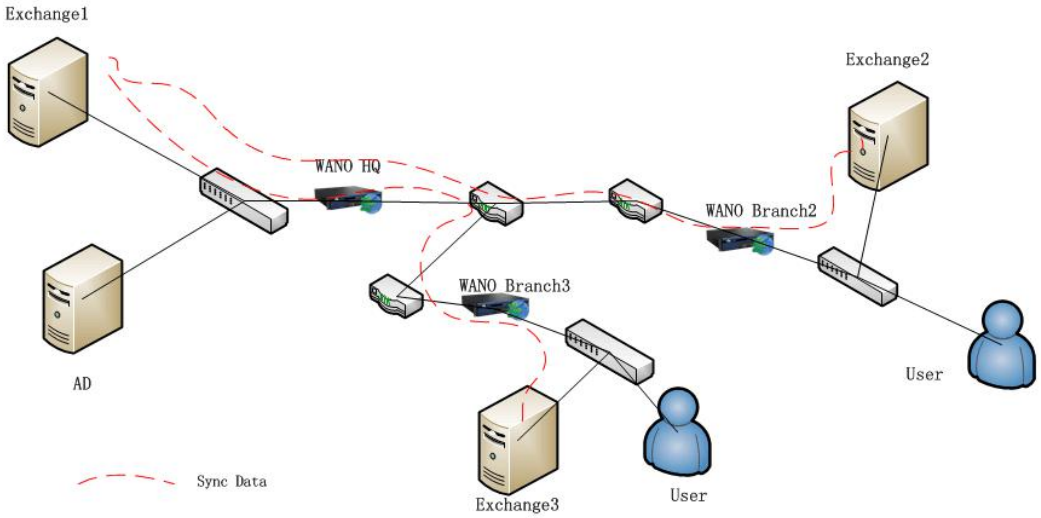
Scenario 2 : Single Domain/ Centralized AD server/ Centralized Exchange server / Exchange server cluster



Scenarios	Single Domain/ Centralized AD server/ Centralized Exchange server / Exchange server cluster
Version requested	9.1R1/9.3 or above

Item	Email protocol enabled	WANO configuration
1	SMTP/POP3	Enable SMTP/POP3 Proxy
2	SMTP/POP3 over SSL	1. Import Exchange server certificate to WANO, configure certificate IP as Exchange server IP, configure port as 0 2. Enable SMTP/POP3 Proxy
3	MAPI	1. WANO join Domain 2. Create a domain user for WANO and use this account delegate all Exchange server ExchangeMDB service 3. Sync WANO time zone/date/time with AD, keep time differ in 30s, and then use delegation mode in exchange proxy. 4.outlookanywhere need to import Exchange server certificate to WANO ,configure certificate IP as Cluster IP,configure port as 0
4	WebMail	1. Import Exchange server certificate to WANO , Certificate IP set Cluster IP, port set 0 2. Enable SSL proxy

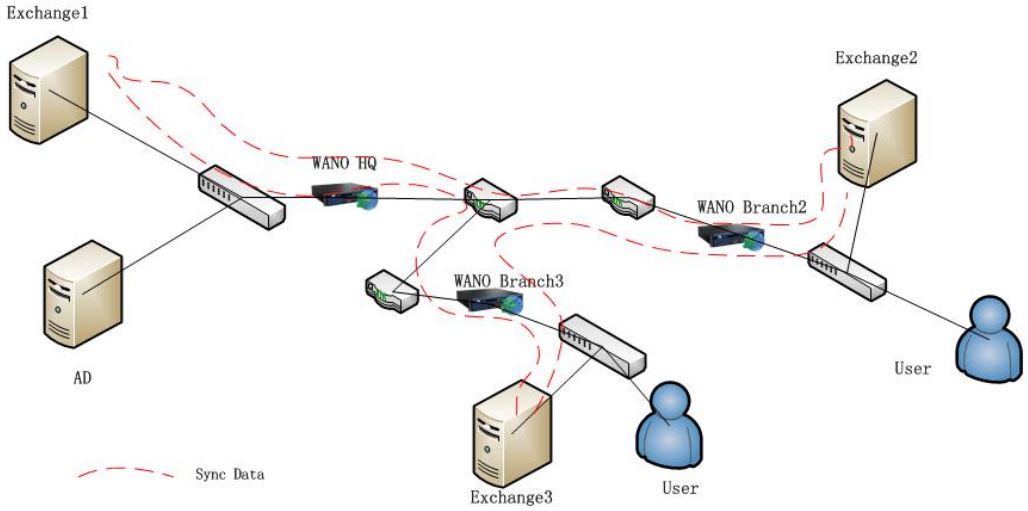
Scenario 3 : Single Domain/ Centralized AD server/ Distributed Exchange server / Single Exchange server ①



Scenarios	Single Domain/ Centralized AD server/ Distributed Exchange server / Single Exchange server① (Each Exchange server communicate and sync to each other directly)
Version requested	9.1R1 or above

Item	**Email protocol enabled**	**WANO configuration**
1	SMTP/POP3	Enable SMTP/POP3 proxy
2	SMTP/POP3 over SSL	1. Import Exchange1 certificate to WANO HQ, configure Certificate IP as Exchange 1 server IP, configure port as 0 2. Import Exchange2 certificate to WANO Branch2, configure certificate IP as Exchange2 IP, configure port as 0 3. Import Exchange3 certificate to WANO Branch3, configure certificate IP as Exchange3 IP, configure port as 0 4. Enable SMTP/POP3 proxy
3	MAPI	N/A
4	WebMail	N/A

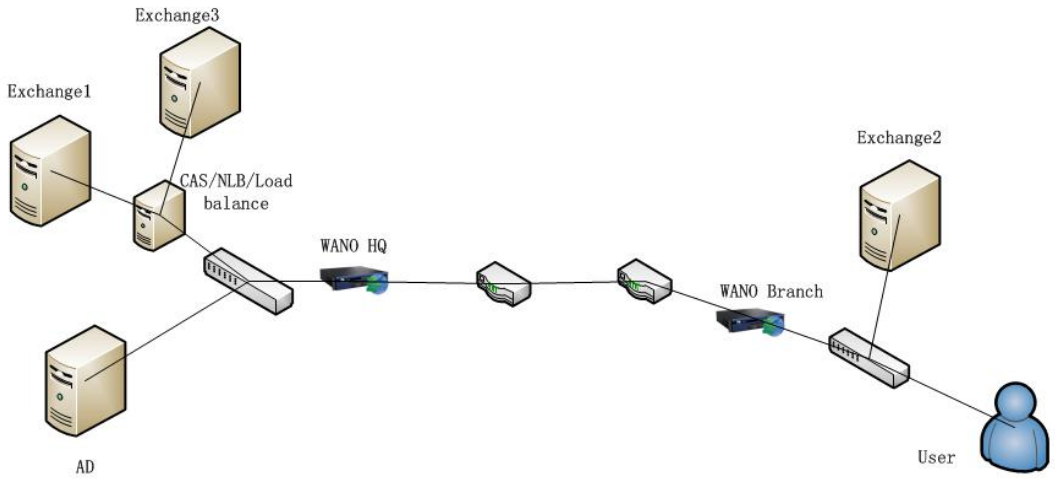
Scenario 4 : Single Domain/ Centralized AD server/ Distributed Exchange server / Single Exchange server ②



Scenarios	Multi site/ Single Domain/ Single AD/ Single Exchange (All branch exchange sync to HQ exchange ,then HQ exchange sync to other Exchange servers)
Version requested	9.1R1 or above

Item	**Email protocol enabled**	**WANO configuration**
1	SMTP/POP3	Enable SMTP/POP3 proxy
2	SMTP/POP3 over SSL	1. Import Exchange1 certificate to WANO HQ, configure certificate IP as Exchange1 IP, configure port as 0 2. Import Exchange2 certificate to WANO Branch2, configure certificate IP as Exchange2 IP, configure port as 0 3. Import Exchange3 certificate to WANO Branch3, configure certificate IP as Exchange3 IP, configure port as 0 4. Enable SMTP/POP3 proxy
3	MAPI	N/A
4	WebMail	N/A

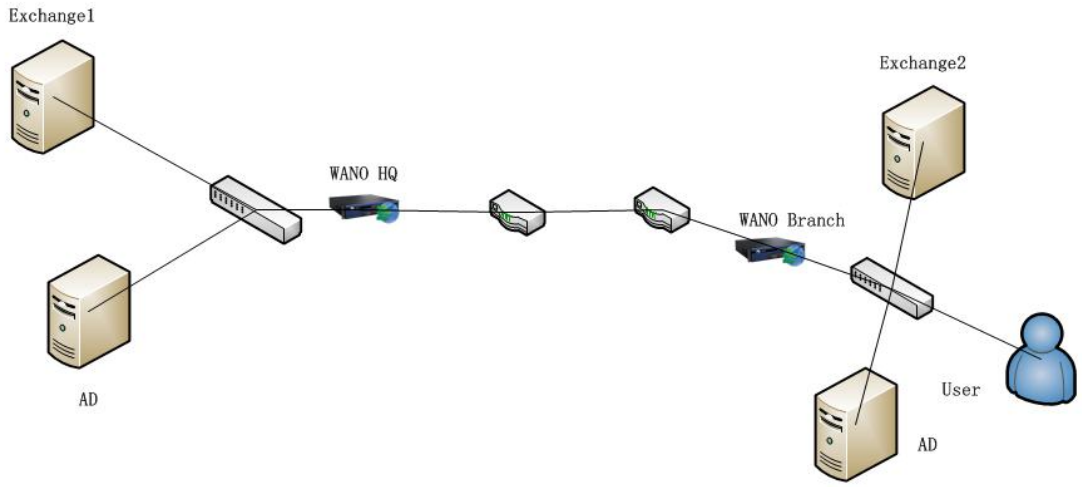
Scenario 5 : Single Domain/ Centralized AD server/ Distributed Exchange server / Exchange server cluster



Scenarios	Multi site/ Single Domain/ Single AD/ Multi Exchange
Version requested	9.1R1/9.3 or above

Item	**Email protocol enabled**	**WANO configuration**
1	SMTP/POP3	Enable SMTP/POP3 proxy
2	SMTP/POP3 over SSL	1. Import Exchange1/3 certificate to WANO HQ, configure certificate IP as Cluster IP, configure port as 0 2.Import Exchange2 certificate to WANO Branch, Certificate IP set Exchange2 IP, port set 0 3. Enable SMTP/POP3 proxy
3	MAPI	N/A
4	WebMail	N/A

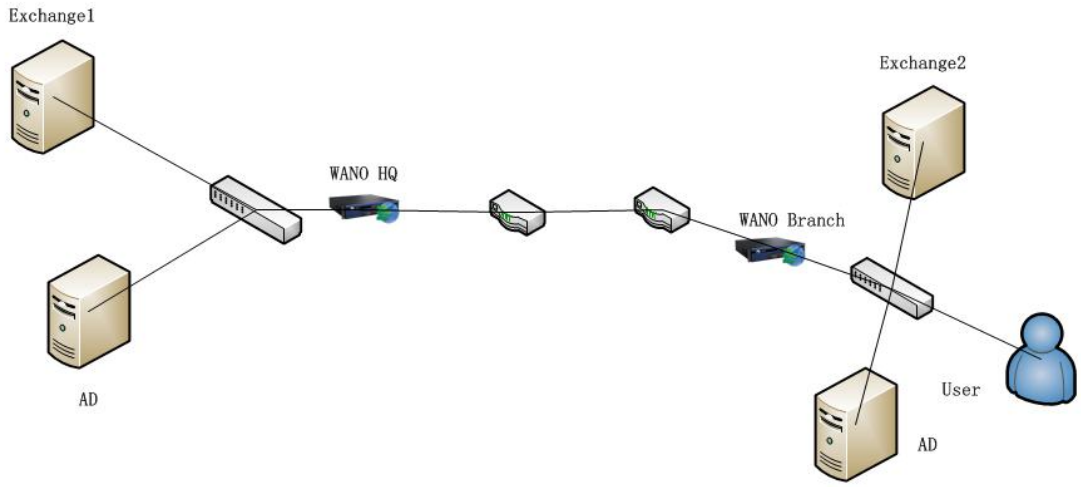
Scenario 6 : Single Domain/ Distributed AD server/ Distributed Exchange server/ Single Exchange



Scenarios	Multi site/ Single Domain/ Multi AD/ Multi Exchange
Version requested	9.1R1 or above

Item	**Email protocol enabled**	**WANO configuration**
1	SMTP/POP3	Enable SMTP/POP3 proxy
2	SMTP/POP3 over SSL	1. Import Exchange1 certificate to WANO HQ, configure certificate IP as Excahnge1 IP, configure port as 0 2. Import Exchange2 certificate to WANO Branch, configure certificate IP as Exchange2 IP, configure port as 0 3. Enable SMTP/POP3 proxy
3	MAPI	N/A
4	WebMail	N/A

Scenario 7 : Multi Domain/ Centralized AD server/ Distributed Exchange server/Exchange server cluster



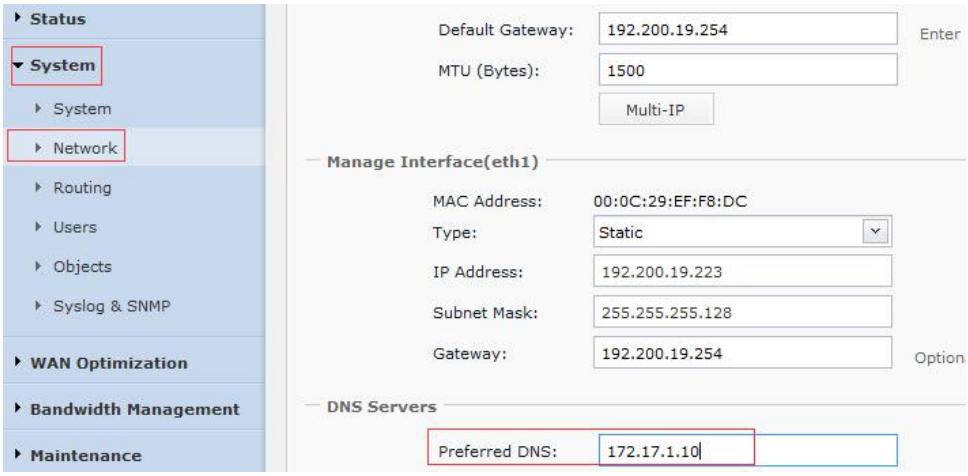
Scenarios	Multi site/ Multi Domain/ Single AD/ Multi Exchange
Version requested	9.1R1 or above

Item	**Email protocol enabled**	**WANO configuration**
1	SMTP/POP3	Enable SMTP/POP3 proxy
2	SMTP/POP3 over SSL	1. Import Exchange1 certificate to WANO HQ, configure certificate IP as Excahnge1 IP, configure port as 0 2. Import Exchange2 certificate to WANO Branch, configure certificate IP as Exchange2 IP, configure port as 0 2. Enable SMTP/POP3 proxy
3	MAPI	N/A
4	WebMail	N/A

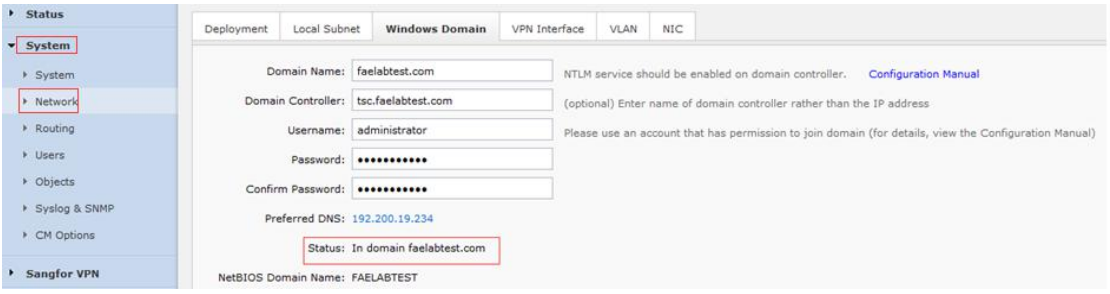
3. WANO exchange configuration

3.1 How to join domain

1. WANO Preferred DNS configure intranet DNS/AD IP.



2. Better use administrator account join domain



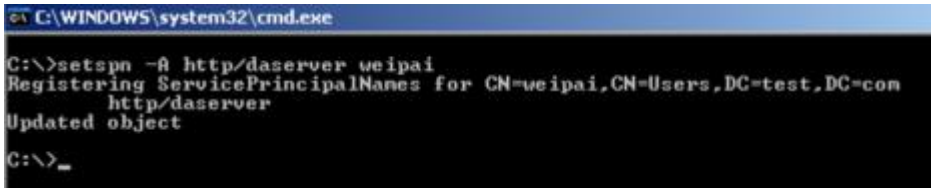
3.2 How to use domain user delegate ExchangeMDB service

Configuration refer to:
https://WANO_IP/html/wanacc/help/us_es/Windows_Domain_Authenticatin_Configuration_Guide.htm

A. Add a user in domain

B. Install setspn on Windows. Insert the Windows 2003 installation CD into the computer. Open the -SUPPORT—TOOLS and execute SUPTOOLS.MSI. To check whether setspn is installed successfully, open cmd and execute setspn. This step is not needed for Windows 2008, for setspn is already installed.

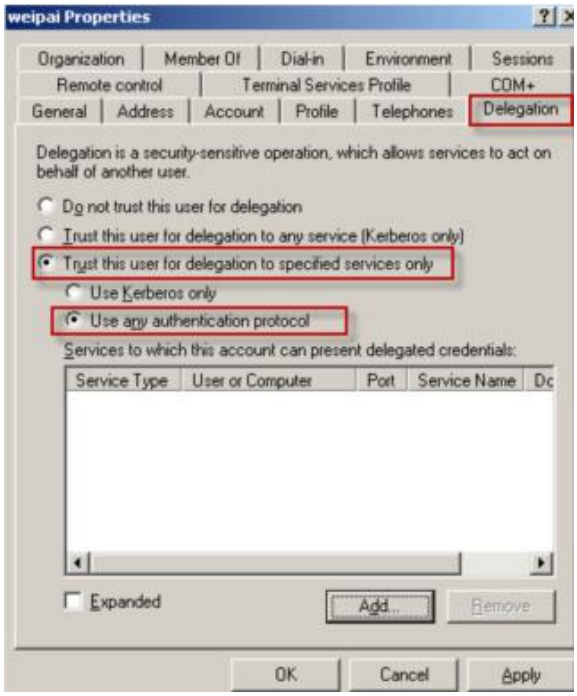
C. Create SPN (Service Principal Name). Open cmd and type the command: setspn -A http/daserver weipai, among which, weipai is the user account created on the above step.



D. Grant user rights to delegate on domain controller.

1. In Windows, choose Start > Administrative Tools > Active Directory Users and computers to open Active Directory Users and Computers.

2. Right-click on the user account weipai and select Properties > Delegation > Trust this user for delegation to specified services only > User any authentication protocol, as shown in the screenshot below. If the option Use Kerberos only is selected, decryption will fail.

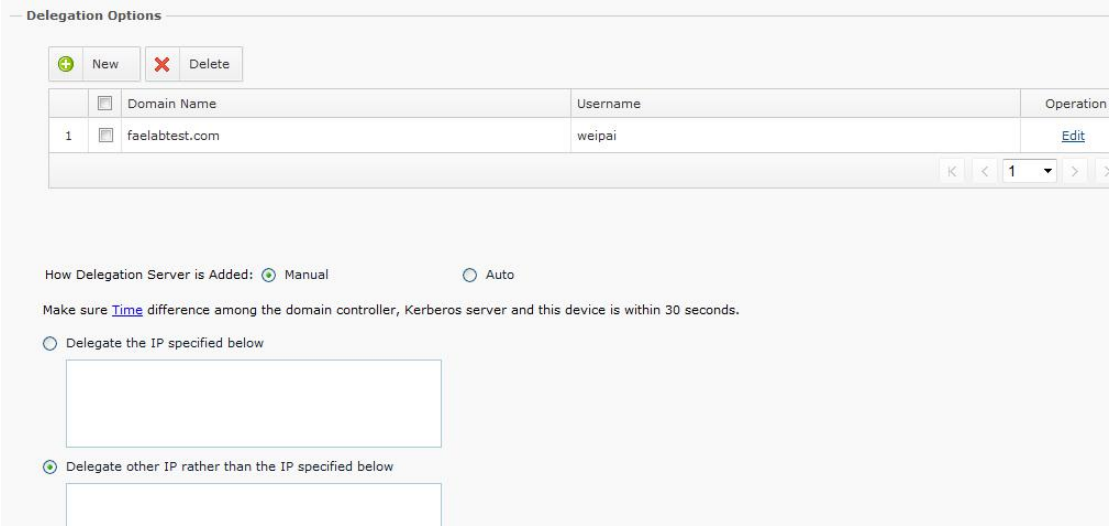


3. Click Add > Users or Computers, and enter the computer name of Exchange or CIFS server.

4. Select CIFS/ExchangeMDB.

E. Configuring Delegation Options on WOC,Navigate to System > Network > Deployment >

Windows Domain. Under the Delegation Options section, click the New button and configure the following contents:



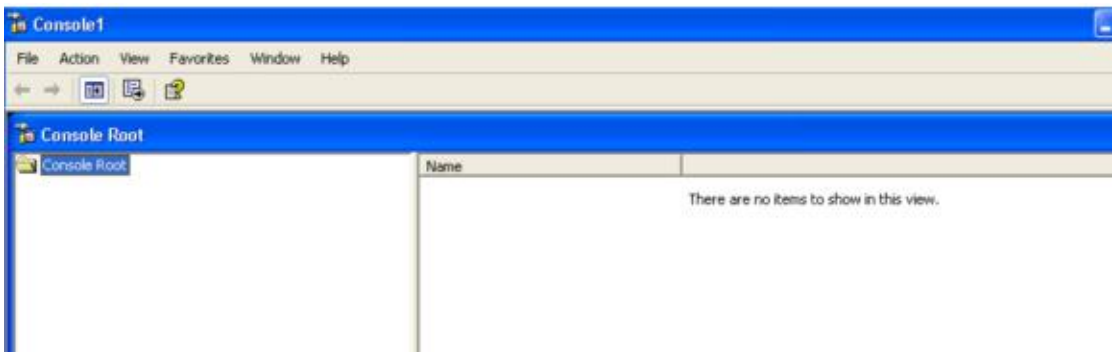
*In this part, WANO system date, time zone must the same with AD, time can't differ above 30s

3.3 How to export certificate from server and import it to WANO

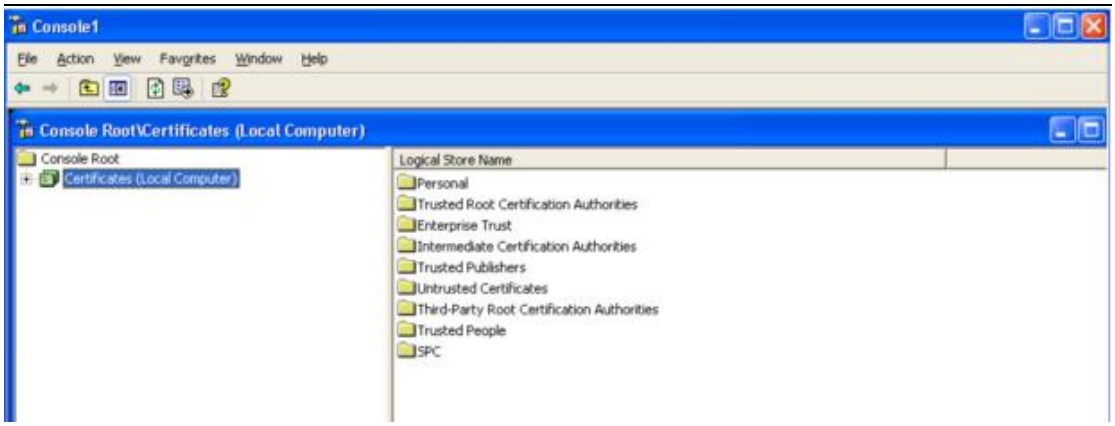
Before accessing Exchange server by using Outlook that is configured Outlook Anywhere (RPC over HTTPS), import the IIS SSL certificate onto the server-end WOC. For how to export certificate from Exchange server, refer to the document IIS SSL Certificate Export Guide.
IIS SSL Certificate Export Guide refer to:
https://WANO_IP/html/wanacc/help/us_es/IIS_SSL_Certificate_Export_Guide.html

IIS SSL Certificate Expor

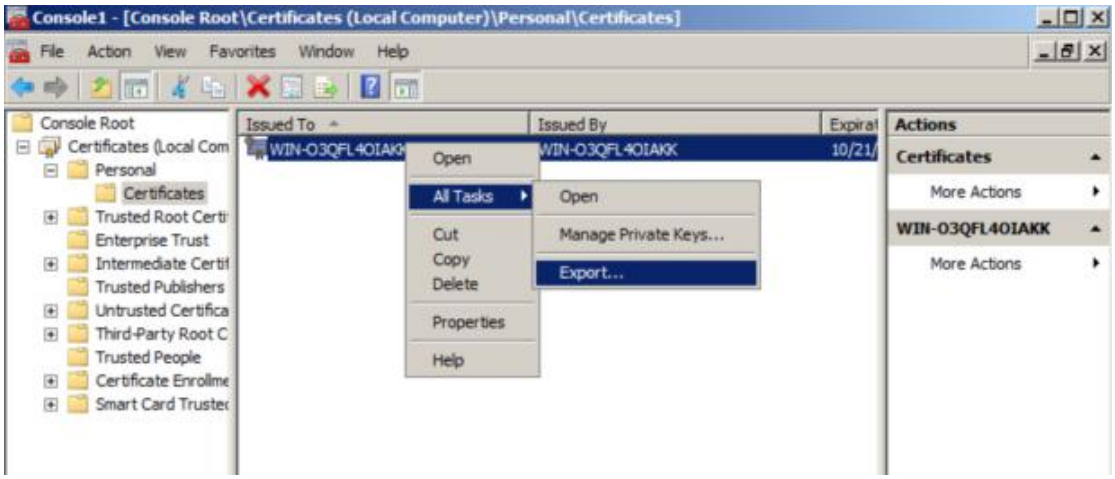
A. On Exchange server, click Start > Run and enter mmc.exe into the Open field to open a MMC window, as shown in the following figure:



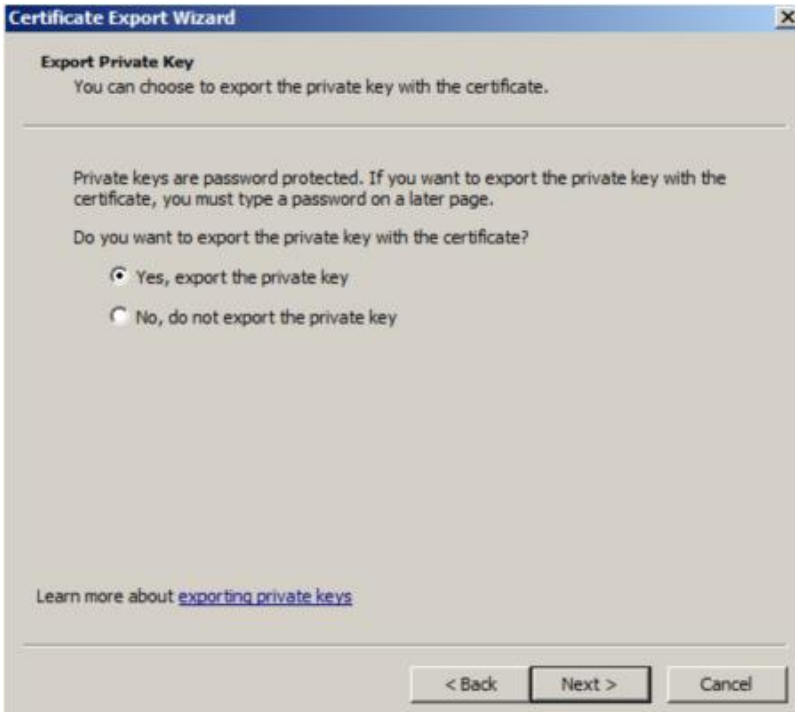
B. Click File > Add/Remove Snap-In > Add and select the certificate and click Add; select a user account and click Next; select Local Computer and click Finish and Close.



C. Click Console Root/Certificates (Local Computer) > Personal > Certificate to unfold the server certificate. Please note that the Issued By column shows the full machine name of the Exchange server and Certificate Template column shows Web server. Right-click on the certificate and select All Tasks and Export… to start the Certificate Export Wizard.



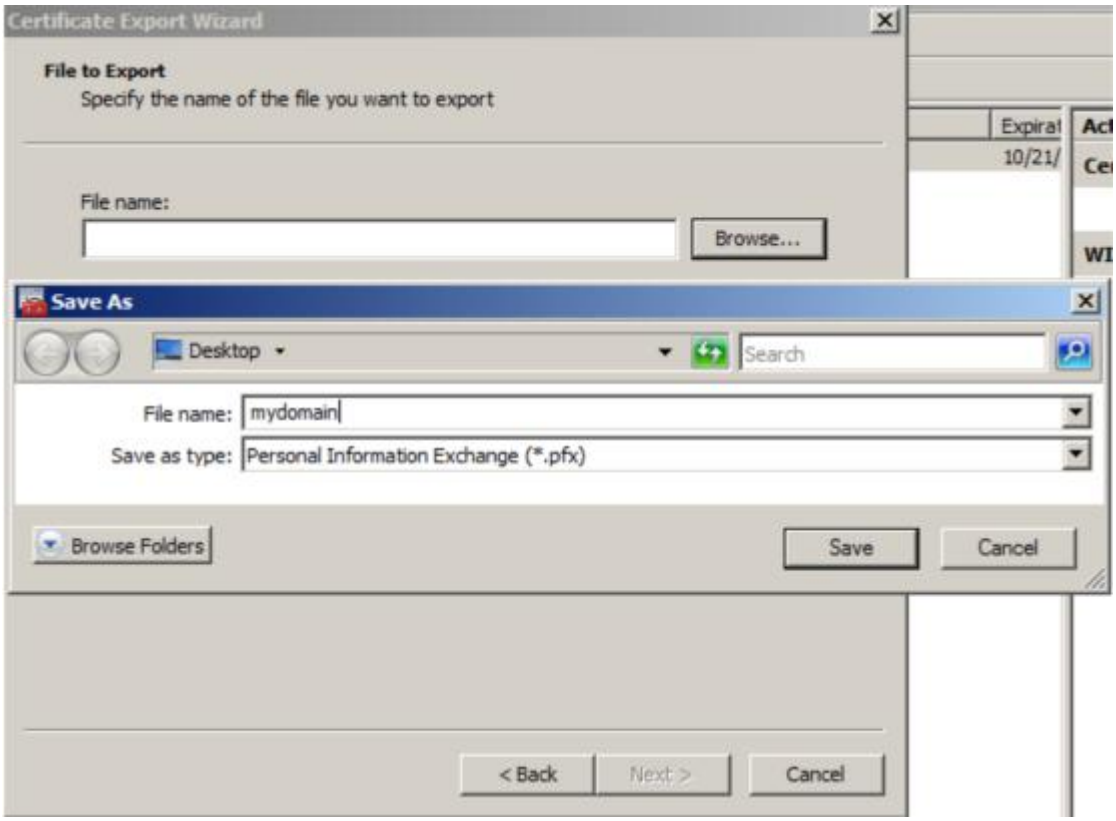
D. Select the option Yes, export the private key and Click Next.



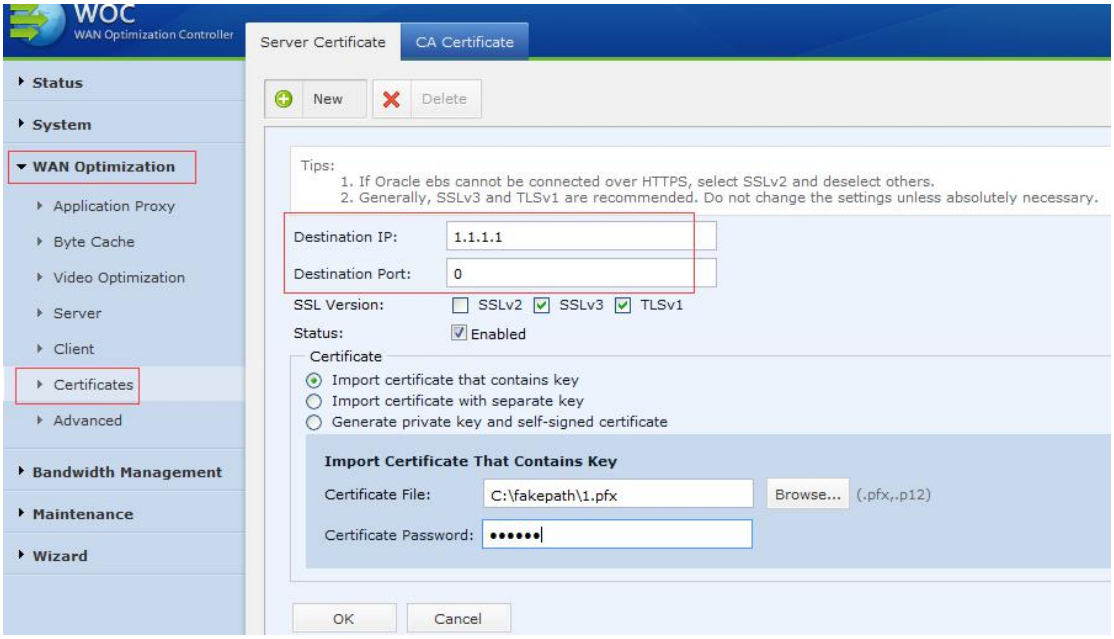
E. Select Personal Information Exchange –PKCS #12(.PFX) and Include all certificate in the certification path if possible, and select Next.

F. Set password and click Next. Please remember the password, for it is required when this certificate is imported to server-end WOC.

G. Select a path to save the PFX file and click Next and Finish.



H. Log in to Web administrator console of the server-end WOC and navigate to WAN Optimization > Certificates > Server Certificate. Enter the IP address and HTTPS port of the Exchange server, select the option Importcertificate that contains key and import the pfx certificate file saved in the above step. Enter the password and click OK.

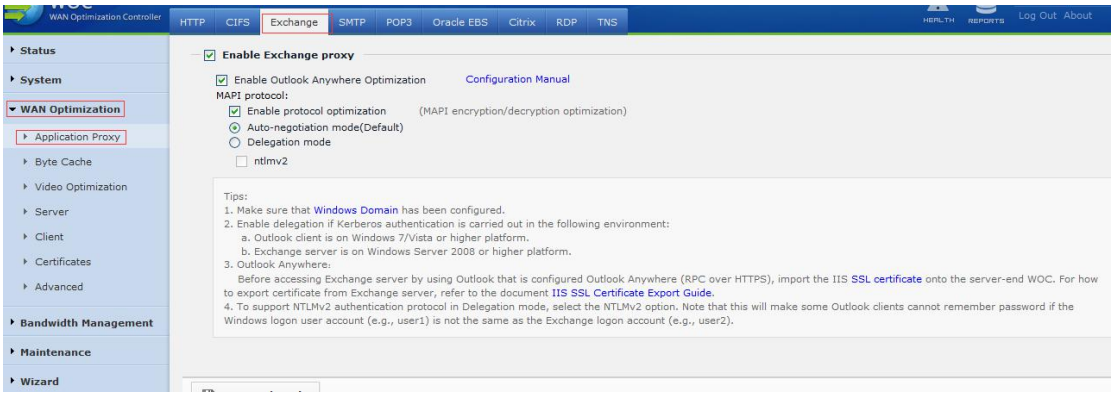


* Port 0 mean all port, if you can confirm the port ,you can specify.

3.4 How to configure Exchange proxy

Exchange proxy use accelerate from outlook to exchange server.

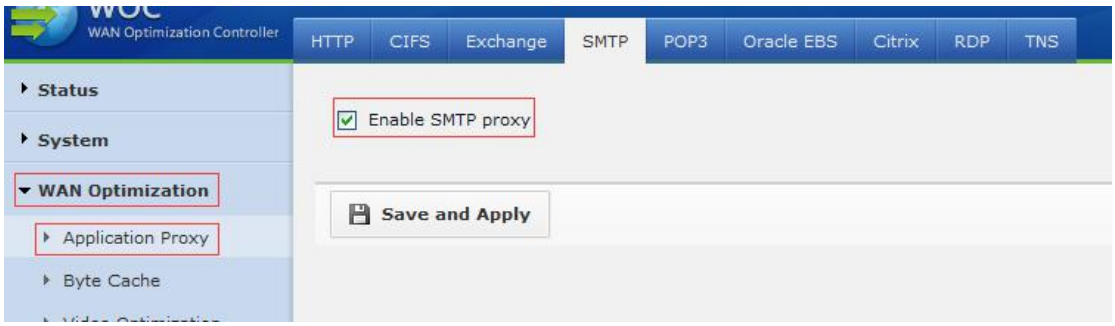
This Proxy used in Scenario 1/2, configuration refer to 3.1.1/3.1.2 4.1/4.2/4.3



* Only Win XP and 2003 server can use auto-negotiation mode, other all use Delegation mode.
Win7 and above WIN7 client default authentication is NTLMv2

3.5 How to configure SMTP/POP3 Proxy

This Proxy may used in all scenarios

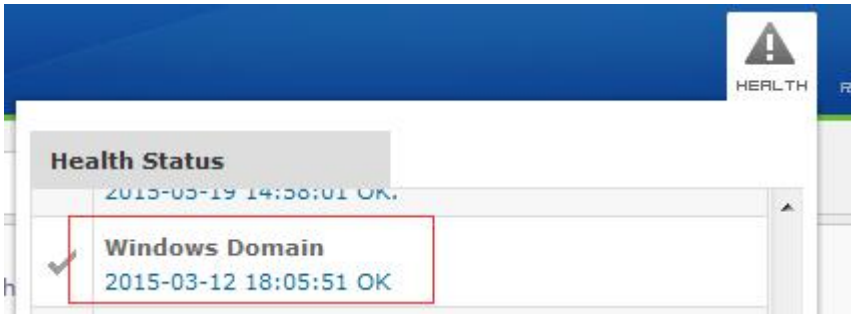

WAN Optimization Controller
HTTP
CIFS
Exchange
SMTP
POP3
Oracle EBS
Citrix
RDP
TNS
Status
System
WAN Optimization
Application Proxy
Byte Cache
Enable SMTP proxy
Save and Apply


WAN Optimization Controller
HTTP
CIFS
Exchange
SMTP
POP3
Oracle EBS
Citrix
RDP
TNS
Status
System
WAN Optimization
Application Proxy
Enable POP3 proxy
Save and Apply

4. Troubleshooting

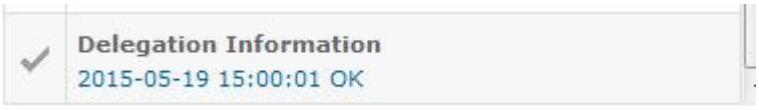
4.1. Join domain failed.

1. Make sure preferred DNS is domain server IP, and ping domain controller in the webconsole or pshell, whether it can resolve the correct IP and ping success.
2. You can check health status, WANO will remind you.

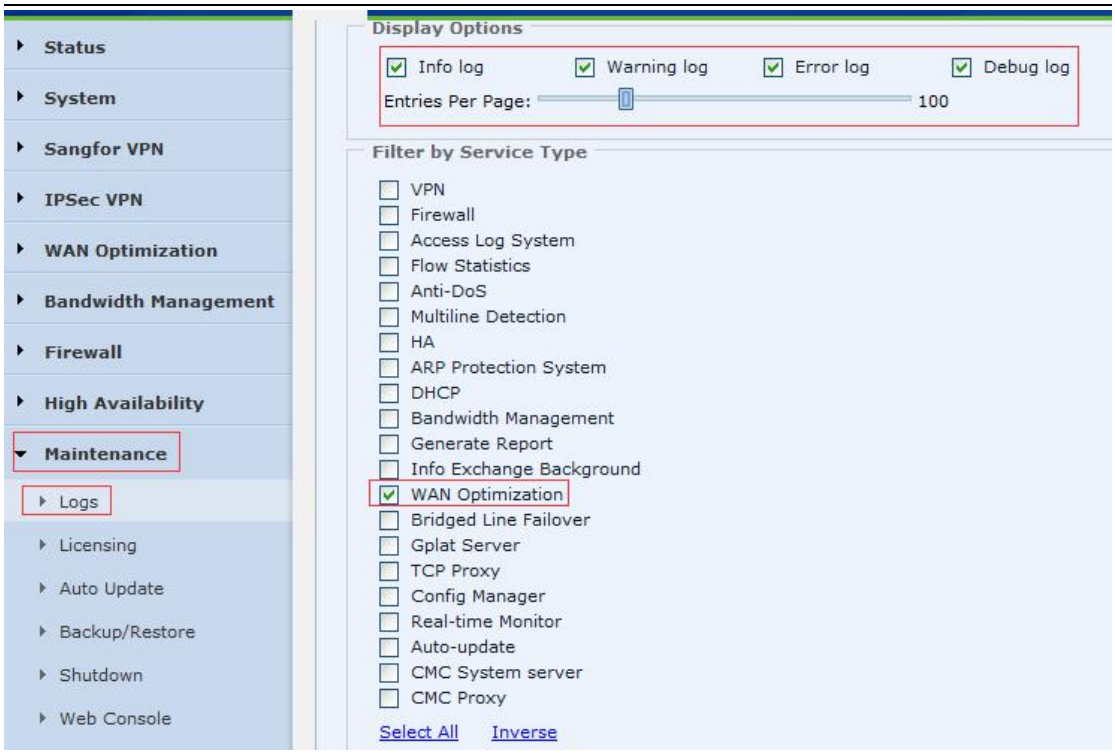


4.2. Delegation failed.

1. server 2003 need install setspan,
We need to run command in cmd " setspn -A http/daserver delegation_user" and then we can see delegation tab in user property.
2. WANO need ExchangeMDB service
3. Check health status



4.3. Check WAN Optimization logs

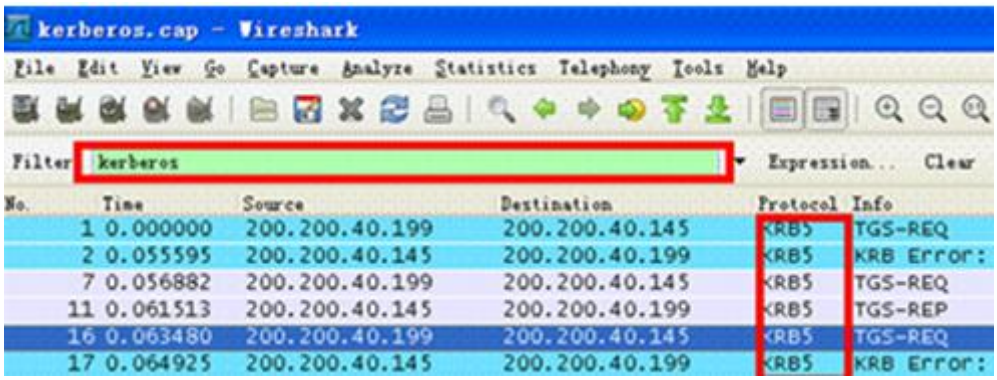


Related Logs

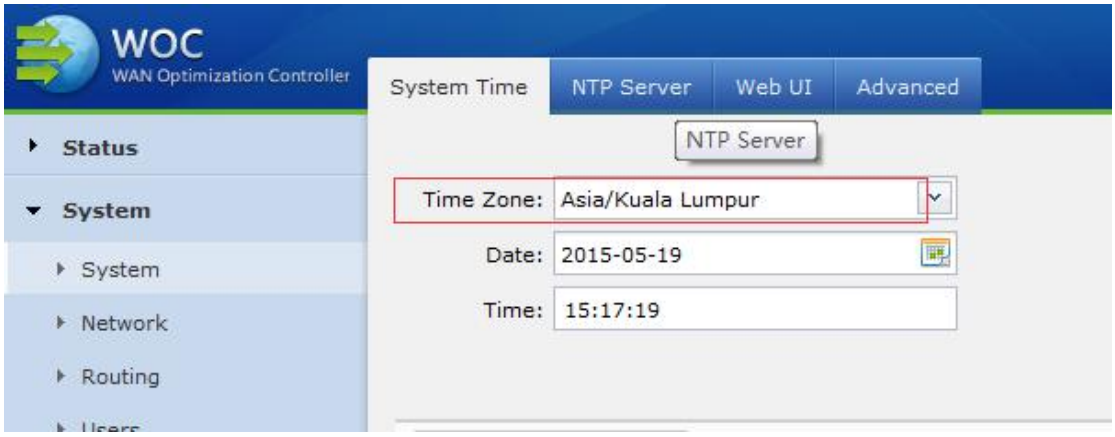
Logs	Description
Please enable NTLMv2 delegation	NTLMv2 needs to be enabled on server-side WOC
Please enable client's ntlm authentication	NTLM is not enabled on client PC
Please configure delegation user	Delegation user needs to be configured (see the section Adding Delegation User Account on WOC)
Please check delegation config	Configuration is incorrect (see the sections **Creating Delegation User Account on DC** or Configuring Delegation Options on WOC)
Please check time between WOC and KDC	Time sync between WOC and DC is required (see the section **Configuring System Time on WOC and Domain Controller**)
Please join WOC to the domain	WOC needs to be joined to the domain
Use local user or other domain user, check domain config	User is using local user account or not using acceleration account access the Exchange or CIFS server.
Please check delegation user's account and password	Username or password is incorrect (see the section Adding Delegation User Account on WOC)

4.4. Capture packets from client to Exchange server, confirm the authentication.

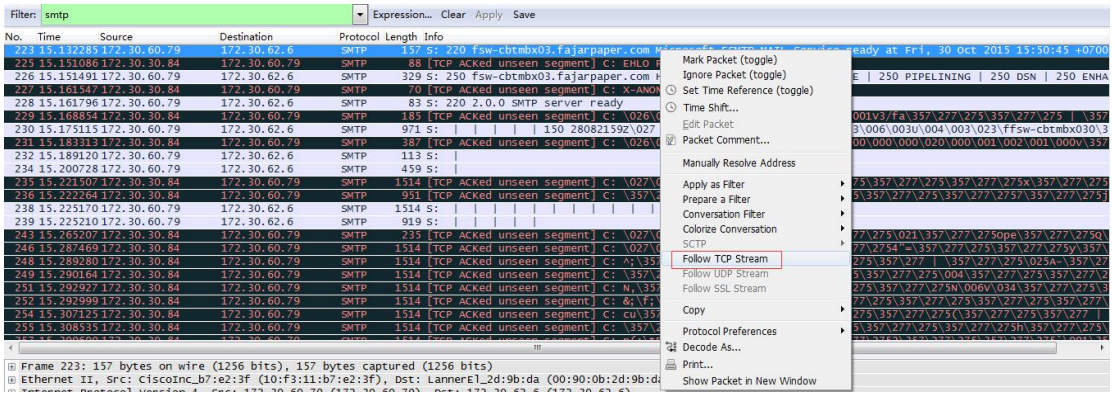
Such as following packet, it use the kerberos authentication, so we need to use delegation mode and not chose NTLMv2

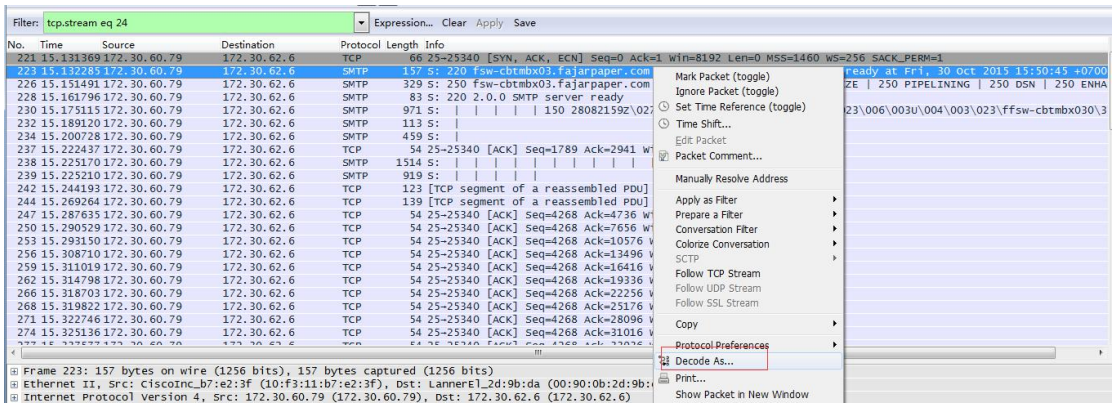


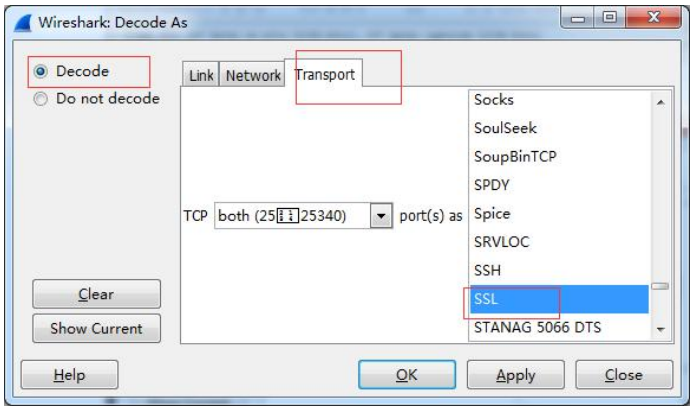
4.5. Keep WANO time zone and time the same with Domain server, or use NTP server to sync time.

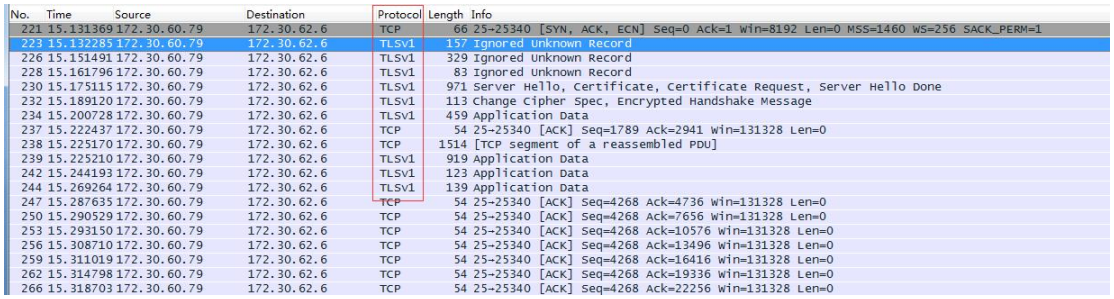


4.6. Capture between Exchange ,confirm the SMTP/POP3 traffic whether over SSL




Filter: tcp.stream eq 24
Expression... Clear Apply Save
No. Time Source Destination Protocol Length Info
221 15.131369 172.30.60.79 172.30.62.6 TCP 66 25→25340 [SYN, ACK, ECN] Seq=0 Ack=1 Win=8192 Len=0 MSS=1460 WS=256 SACK_PERM=1
223 15.132285 172.30.60.79 172.30.62.6 SMTP 157 S: 220 fsw-cbtmbx03.fajarpaper.com
226 15.151491 172.30.60.79 172.30.62.6 SMTP 329 S: 250 fsw-cbtmbx03.fajarpaper.com
228 15.161796 172.30.60.79 172.30.62.6 SMTP 83 S: 220 2.0.0 SMTP server ready
230 15.175115 172.30.60.79 172.30.62.6 SMTP 971 S:
232 15.189120 172.30.60.79 172.30.62.6 SMTP 113 S:
234 15.200728 172.30.60.79 172.30.62.6 SMTP 459 S:
237 15.222437 172.30.60.79 172.30.62.6 TCP 54 25→25340 [ACK] Seq=1789 Ack=2941
238 15.225170 172.30.60.79 172.30.62.6 SMTP 1514 S:
239 15.225210 172.30.60.79 172.30.62.6 SMTP 919 S:
242 15.244193 172.30.60.79 172.30.62.6 TCP 123 [TCP segment of a reassembled PDU]
244 15.269264 172.30.60.79 172.30.62.6 TCP 139 [TCP segment of a reassembled PDU]
247 15.287635 172.30.60.79 172.30.62.6 TCP 54 25→25340 [ACK] Seq=4268 Ack=4736
250 15.290529 172.30.60.79 172.30.62.6 TCP 54 25→25340 [ACK] Seq=4268 Ack=7656
253 15.293150 172.30.60.79 172.30.62.6 TCP 54 25→25340 [ACK] Seq=4268 Ack=10576
256 15.308710 172.30.60.79 172.30.62.6 TCP 54 25→25340 [ACK] Seq=4268 Ack=13496
259 15.311019 172.30.60.79 172.30.62.6 TCP 54 25→25340 [ACK] Seq=4268 Ack=16416
262 15.314798 172.30.60.79 172.30.62.6 TCP 54 25→25340 [ACK] Seq=4268 Ack=19336
266 15.318703 172.30.60.79 172.30.62.6 TCP 54 25→25340 [ACK] Seq=4268 Ack=22256
268 15.319822 172.30.60.79 172.30.62.6 TCP 54 25→25340 [ACK] Seq=4268 Ack=25176
271 15.322746 172.30.60.79 172.30.62.6 TCP 54 25→25340 [ACK] Seq=4268 Ack=28096
274 15.325136 172.30.60.79 172.30.62.6 TCP 54 25→25340 [ACK] Seq=4268 Ack=31016
Frame 223: 157 bytes on wire (1256 bits), 157 bytes captured (1256 bits)
Ethernet II, Src: CiscoInc_b7:e2:3f (10:f3:11:b7:e2:3f), Dst: LannerEl_2d:9b:da (00:90:0b:2d:9b:
Internet Protocol Version 4, Src: 172.30.60.79 (172.30.60.79), Dst: 172.30.62.6 (172.30.62.6)
Mark Packet (toggle)
Ignore Packet (toggle)
Set Time Reference (toggle)
Time Shift...
Edit Packet
Packet Comment...
Manually Resolve Address
Apply as Filter
Prepare a Filter
Conversation Filter
Colorize Conversation
SCTP
Follow TCP Stream
Follow UDP Stream
Follow SSL Stream
Copy
Protocol Preferences
Decode As...
Print...
Show Packet in New Window
ready at Fri, 30 Oct 2015 15:50:45 +0700
ZE | 250 PIPELINING | 250 DSN | 250 ENHA
23\006\003U\004\003\023\ffsw-cbtmbx030\3

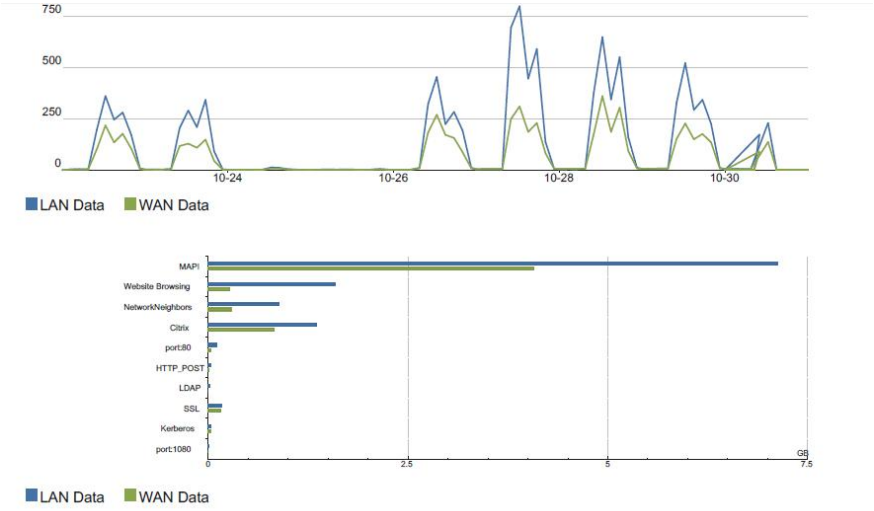

Wireshark: Decode As
Decode
Do not decode
Link
Network
Transport
TCP
both (25 25340)
port(s) as
Socks
SoulSeek
SoupBinTCP
SPDY
Spice
SRVLOC
SSH
SSL
STANAG 5066 DTS
Clear
Show Current
Help
OK
Apply
Close


No. Time Source Destination Protocol Length Info
221 15.131369 172.30.60.79 172.30.62.6 TCP 66 25→25340 [SYN, ACK, ECN] Seq=0 Ack=1 Win=8192 Len=0 MSS=1460 WS=256 SACK_PERM=1
223 15.132285 172.30.60.79 172.30.62.6 TLSv1 157 Ignored Unknown Record
226 15.151491 172.30.60.79 172.30.62.6 TLSv1 329 Ignored Unknown Record
228 15.161796 172.30.60.79 172.30.62.6 TLSv1 83 Ignored Unknown Record
230 15.175115 172.30.60.79 172.30.62.6 TLSv1 971 Server Hello, Certificate, Certificate Request, Server Hello Done
232 15.189120 172.30.60.79 172.30.62.6 TLSv1 113 Change Cipher Spec, Encrypted Handshake Message
234 15.200728 172.30.60.79 172.30.62.6 TLSv1 459 Application Data
237 15.222437 172.30.60.79 172.30.62.6 TCP 54 25→25340 [ACK] Seq=1789 Ack=2941 Win=131328 Len=0
238 15.225170 172.30.60.79 172.30.62.6 TCP 1514 [TCP segment of a reassembled PDU]
239 15.225210 172.30.60.79 172.30.62.6 TLSv1 919 Application Data
242 15.244193 172.30.60.79 172.30.62.6 TLSv1 123 Application Data
244 15.269264 172.30.60.79 172.30.62.6 TLSv1 139 Application Data
247 15.287635 172.30.60.79 172.30.62.6 TCP 54 25→25340 [ACK] Seq=4268 Ack=4736 Win=131328 Len=0
250 15.290529 172.30.60.79 172.30.62.6 TCP 54 25→25340 [ACK] Seq=4268 Ack=7656 Win=131328 Len=0
253 15.293150 172.30.60.79 172.30.62.6 TCP 54 25→25340 [ACK] Seq=4268 Ack=10576 Win=131328 Len=0
256 15.308710 172.30.60.79 172.30.62.6 TCP 54 25→25340 [ACK] Seq=4268 Ack=13496 Win=131328 Len=0
259 15.311019 172.30.60.79 172.30.62.6 TCP 54 25→25340 [ACK] Seq=4268 Ack=16416 Win=131328 Len=0
262 15.314798 172.30.60.79 172.30.62.6 TCP 54 25→25340 [ACK] Seq=4268 Ack=19336 Win=131328 Len=0
266 15.318703 172.30.60.79 172.30.62.6 TCP 54 25→25340 [ACK] Seq=4268 Ack=22256 Win=131328 Len=0

5. Real cases' Report

5.1 MAPI

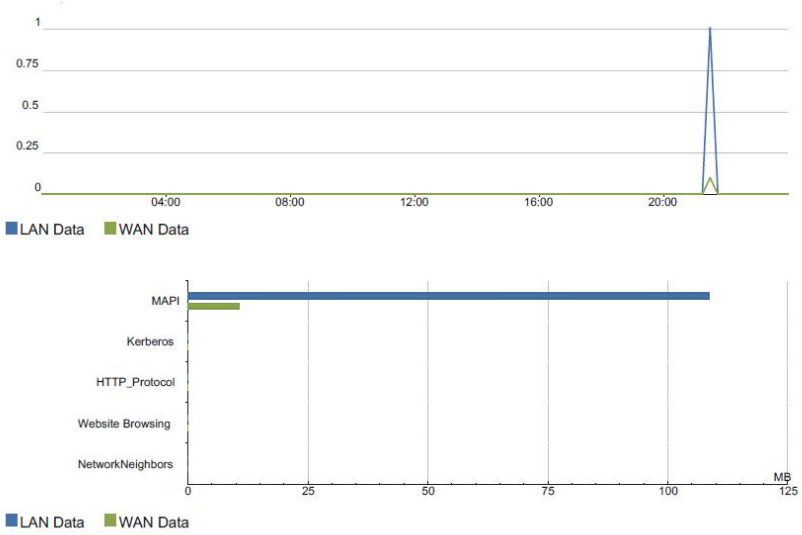
Customer: ZICO LAW use scenario 2, KEMP load balance, MAPI+SSL



	Name	LAN Data	WAN Data	Reduced	Reduction Ratio
1	MAPI	7,291.26 MB	4,177.01 MB	3,114.25 MB	42.71%
2	Website Browsing	1,623.30 MB	279,328 KB	1,350.52 MB	83.20%
3	NetworkNeighbors	938,225 KB	301,434 KB	636,792 KB	67.87%
4	Citrix	1,389.17 MB	871,614 KB	550,892 KB	38.73%

Customer: Sangfor Malaysia support center use scenario 1

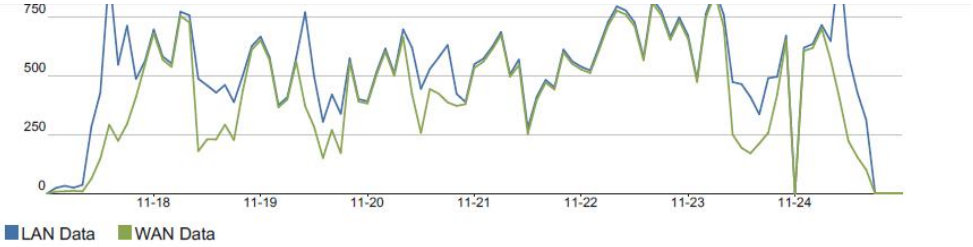
Test Repeat send same mail to different branch user

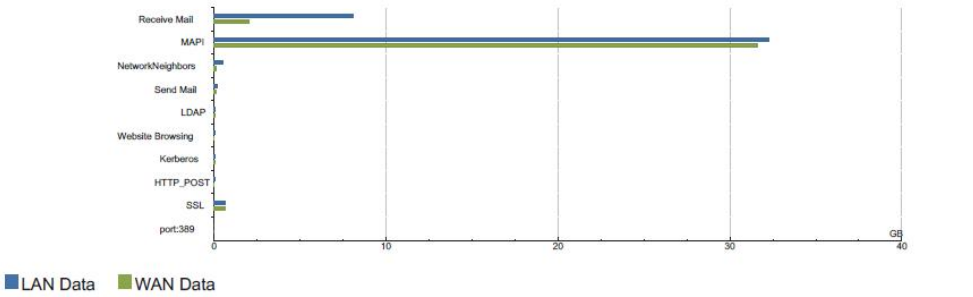


	Name	LAN Data	WAN Data	Reduced	Reduction Ratio
1	MAPI	111,230 KB	11,001 KB	100,229 KB	90.11%
2	Kerberos	73 KB	16 KB	56 KB	77.61%
3	HTTP_Protocol	34 KB	14 KB	20 KB	59.18%

5.2 SMTP/POP3

Customer: EP Polymer use scenario 1





	Name	LAN Data	WAN Data	Reduced	Reduction Ratio
1	Receive Mail	8,270.41 MB	2,088.89 MB	6,181.52 MB	74.74%
2	MAPI	33,050.48 MB	32,361.62 MB	705,396 KB	2.08%
3	NetworkNeighbors	528,941 KB	158,186 KB	370,755 KB	70.09%
4	Send Mail	230,446 KB	100,809 KB	129,637 KB	56.25%