## How to configure WFS (Windows File Sharing) Acceleration on SonicWALL WAN Acceleration Appliances

Consider the following typical deployment scenario where Head Quarters and Remote Office are connected via Site-Site VPN Tunnel.

SonicWALL WAN Acceleration devices are directly connected to the managing UTM appliances as shown at each location. At head quarters there is a Domain Controller, DNS Server and 2 file servers. Remote Office has no local domain controller, DNS server, File Servers. Users at remote office access the resources at the head quarters via Site-Site VPN.
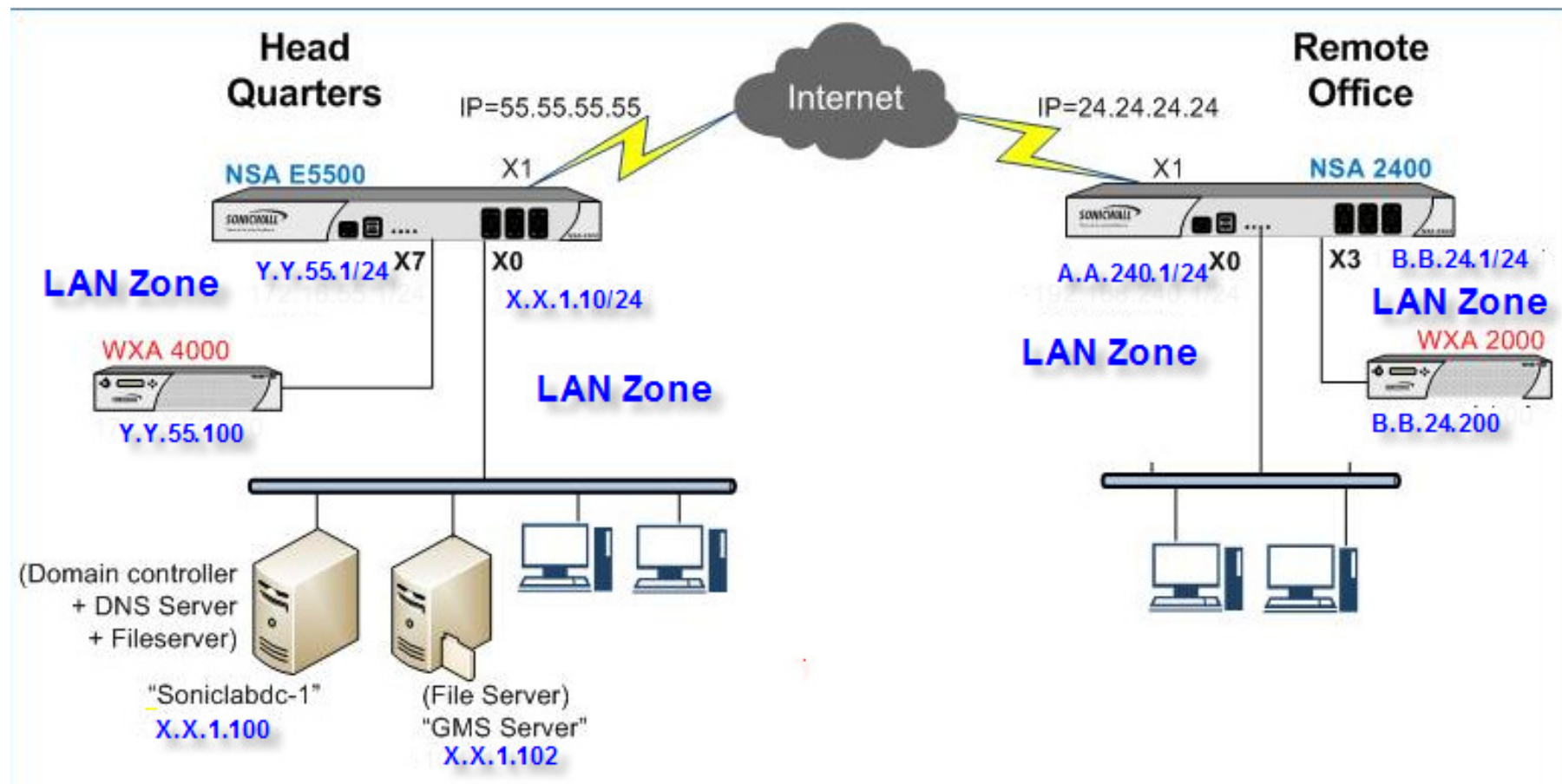
Assumptions:

There is a Site-Site VPN configured between Head Quarters and Remote Office using IPsec or Route based VPN. Please refer to the WAN Acceleration deployment modes articles/feature module for details of deployment modes.

Recommendations:

1. Create Static DHCP scope for WXA Appliance on the managing SonicWALL UTM Appliance
2. If the remote offices also have Domain Controllers and DNS servers, it is recommended to use the local DNS server addresses and domain DNS name in the DHCP scope. Configure Domain Name and Domain DNS servers' addresses in the configured DHCP scope. WXA Appliance auto-discovers Kerberos, LDAP, NTP servers based on this information to assist in joining the Appliance to the domain.
3. Review the LDAP, Kerberos and NTP services. In a multi-site domain where Sites and Services are not explicitly configured, the WXA might choose servers that are at another remote site instead of at head office.
4. Though not essential, it is recommended to create Reverse Lookup Zone for the networks on DNS servers for the necessary local and remote networks for WFS to update PTR records. Remote Lookup Zones configuration depends on whether WXA Appliance is using NAT'ed IP (of the Managing UTM Appliance's one of Interface IP address or other IP address) or using its own IP address (no NAT)
5. It is recommended that WXA Appliance gets NTP updates from local Domain Controller
6. It is recommended that the DNS server accepts secure updates

7. SonicWALL Recommends configuring the Zone properties of Interface to which SonicWALL WAN Acceleration WXA Appliance is connected as LAN Zone so that the default access rules allow traffic between WXA Appliances at both locations. This simplifies the process of configuration and deployments.

   - In the above deployment, access rules are necessary for the traffic coming from VPN->LAN and LAN->VPN to be open for WXA associated traffic and the default Zone properties of LAN takes care of handling traffic without manually adding or modifying any access rules. Both WXA Appliances deployed at each location should be able to communicate with each other without being blocked by access rules or firewall policies.

For example consider Head Quarters, if SonicWALL WXA Appliance is deployed in DMZ, then access rules must be configured/updated to allow traffic from VPN->DMZ, LAN->DMZ so that traffic to WXA Appliance from VPN (includes traffic from remote LAN Zone as well as from WXA Appliance) and from LAN zone (Traffic from Domain Controllers, DNS Servers, File Servers) is allowed to WXA Appliance. Similarly traffic must be allowed from DMZ headquarters to VPN remote must be allowed. If additional domain controllers and file servers are located in any other Zone

or custom zone, necessary access rules must be configured to allow traffic from/to WXA Appliance to those Zones as well. Similar configuration must be followed at the remote location. Custom Access rules depend on specifics of deployment scenarios.

The following services are being used by WAN Acceleration and Client PCs for Domain Controller, DNS Server, NTP server, File Server Services.

Client PCs require AD Server Services (TCP 135, 137, 139, 445) for file services and require AD Directory Services for Domain Services. WXA Appliances also require these services for Domain Services and file shares proxy.

☐ ▼ 32	AD Directory Services					✎ ⊘		💬
	LDAP	TCP	389	389		✎ ⊘		💬
	LDAPS	TCP	636	636		✎ ⊘		💬
	NTP	UDP	123	123		✎ ⊘		💬
	DNS (Name Service)					✎ ⊘		💬
	Kerberos					✎ ⊘		💬
	DCE EndPoint	TCP	135	135		✎ ⊘		💬
	LDAP (UDP)	UDP	389	389		✎ ⊘		💬
	Host Name Server					✎ ⊘		💬
	AD NetBios Services					✎ ⊘		💬
	RPC Services	TCP	1025	5000		✎ ⊘		💬
	RPC Services (IANA)	TCP	49152	65535		✎ ⊘		💬
☐ ▼ 33	AD Server					✎ ⊘		💬
	DCE EndPoint	TCP	135	135		✎ ⊘		💬
	AD NetBios Services					✎ ⊘		💬
☐ ▼ 34	Host Name Server					✎ ⊘		💬
	Host Name Server TCP	TCP	42	42		✎ ⊘		💬
	Host Name Server UDP	UDP	42	42		✎ ⊘		💬
☐ ▼ 35	AD NetBios Services					✎ ⊘		💬
	SMB	TCP	445	445		✎ ⊘		💬
	NetBios TCP	TCP	137	139		✎ ⊘		💬
	NetBios UDP	UDP	137	139		✎ ⊘		💬

Steps involved:

1. Pre-requisites
2. Enabling WFS acceleration and using correct IP address for WXA to use in NAT translation.
3. Joining WXA devices to the domain
4. Setting up shares
5. Testing shares

Pre-requisites:

1. Site-Site VPN policy is already configured between Head Quarters and remote site to allow traffic between the networks. It is not required to include WXA Subnets in the VPN Policy/Networks.
2. WXA Appliance at both locations are connected to their respective Interfaces/Zones and provisioned with IP address, Domain Name and Domain DNS Servers and NTP server. It is essential that WXA Appliances are configured to automatically get Domain DNS server and Domain Name information from the DHCP scope created for WXA Appliance. If the remote offices also have Domain Controllers and DNS servers, it is recommended to use the local DNS server addresses in the DHCP scope.

Enabling WFS acceleration and using correct IP address for WXA to use in NAT translation:
As mentioned in pre-requisite # 1, it is not required to include WXA Subnets in the VPN Policy/Networks. By default WXA Appliances uses NAT'ed IP of X0 interface IP address of Managing UTM Appliance for communications and it is essential that the NAT'ed IP be a part of VPN networks. For example, WXA 4000 that is deployed at headquarters gets NAT'ed to X.X.1.10 and WXA 2000 at remote gets NAT'ed to A.A.240.1. WXA Appliances at both the locations use these NAT'ed IP addresses for communication and hence eliminate the necessity to include WXA subnets as a part of VPN Networks. For NAT'ed IP address, it can be Managing UTM appliance's interface IP address or any IP address that is not used by any other device. But the IP address being has to be a part of the VPN networks in either case. But for simplicity, you can choose to use Managing UTM appliance's Interface IP address so that another IP is not needed.
NAT policies that are essential are automatically created based on the NAT'ed IP address being used as shown below.

On the managing SonicWALL UTM appliance, navigate to WAN Acceleration->WFS Acceleration and enable WFS Acceleration.

WAN Acceleration /

WFS Acceleration

| Configuration | Domain Details | Shares | Statistics | Tools |

☑ **Enable WFS Acceleration**

'Public' WFS Acceleration Address: X0 IP

Auto-created NAT Policies on Head Quarters UTM Appliance.

☐	#	Source		Destination		Service		Interface		Priority	Comment	Enable	Configure
		Original	Translated	Original	Translated	Original ▲	Translated	Inbound	Outbound				
☐	75	Any	Original	X0 IP	WXA Appliance	AD Server	Original	Any	Any	39	💬	✓	📊 ✏ ⊘
☐	76	WXA Appliance	X0 IP	Any	Original	AD Directory Services	Original	X7	Any	40	💬	✓	📊 ✏ ⊘

Auto-created NAT Policies on remote Site UTM Appliance.

☐	#	Source		Destination		Service		Interface		Priority	Comment	Enable	Configure
		Original	Translated	Original	Translated	Original ▲	Translated	Inbound	Outbound				
☐	18	Any	Original	X0 IP	WXA Appliance	AD Server	Original	Any	Any	18	💬	✓	📊 ✏ ⊘
☐	19	WXA Appliance	X0 IP	Any	Original	AD Directory Services	Original	X3	Any	19	💬	✓	📊 ✏ ⊘

Joining WXA Appliances to the domain:

Once WXA Appliances are configured properly with DHCP scope, based on the Domain Name and configured DNS servers, WXA Appliances automatically discovers FQDN of the domain, NetBIOS name, Kerberos, LDAP, Time Server. If any of them are not discovered properly, then that entry can be manually edited. For example, in this case, NetBIOS name is not correctly identified and is discovered as UTM and needs manual editing.

Host name can be edited or changed as per requirement.

Below screenshots are taken on head Quarters WXA 4000 Appliance and the steps to add remote site WXA to the domain are the same.

WFS Acceleration

⚠️ • The appliance has not yet joined the specified domain. You must either create an account for the appliance on the domain or have it join the domain using Administrator

| Configuration | **Domain Details** | Shares | Statistics | Tools |

The information shown in the table has been discovered from the network. Certain fields can be overridden by being configured manually.

Fully Qualified Domain Name:	utm.soniclab.us	[Discovered]	✎
NETBIOS Domain:	UTM	[Discovered]	✎
Hostname:	WXA4000-57F518E		✎
Kerberos Server:	soniclabdc-1.utm.soniclab.us:88	[Discovered]	✎
LDAP Server:	soniclabdc-1.utm.soniclab.us:389	[Discovered]	
Joined Domain:	☐		
Machine Account Exists:	☐		
Trusted for Delegation:	☐		

Auto-Discovery of Domain related information

If auto-discovery fails to correctly identify any value, entries can be manually updated

Other System Settings

Other system settings that also affect the functioning of the WFS Acceleration module are shown below.

Time Synchronization Source:	soniclabdc-1.utm.soniclab.us:88	[Domain Controller] ✎
Primary DNS Server:	X.X.1.100	[DHCP]
Secondary DNS Server:		

| Advanced Options | Join Domain | Test Configuration | Flush Cache | Restart WFS |

In this case, Hostname and NetBIOS are edited

Configure Hostname

Default hostname: WXA4000-57F518E
Leave the input field blank in order to use the default.

Hostname: WXA-4000

[Apply]   [Cancel]

Configure Domain

Discovered domain: utm.soniclab.us
Discovered NETBIOS: UTM

Fully Qualified Domain Name: utm.soniclab.us

☐ Use Discovered value for NETBIOS Domain

NETBIOS Domain: soniclabus

[Apply]   [Cancel]

Once all the necessary edits are done, click on "Join Domain" to add WXA Appliance to the domain using the domain account that has permissions to join to the domain.

Join Domain

Enter the username and password of an account that can join the SonicWALL WXA series appliance to the domain. Please refer to the documentation for more details.

Using an Administrator's credentials will ensure that the appliance is "trusted for delegation". Otherwise, you will need to configure that option on the Domain Controller.

Username: administrator

Password: ●●●●●●●●|

[Join Domain]   [Cancel]

WXA at Head Quarters added to the domain.

WFS Acceleration

⚠️ • You must configure the servers and shares to which acceleration will be applied on the Shares page.

| Configuration | **Domain Details** | Shares | Statistics | Tools |

Configured Domain

Fully Qualified Domain Name:	utm.soniclab.us	[Configured]
NETBIOS Domain:	soniclabus	[Configured]
Hostname:	WXA4000	[Configured]
Kerberos Server:	soniclabdc-1.utm.soniclab.us:88	[Discovered]
LDAP Server:	soniclabdc-1.utm.soniclab.us:389	[Discovered]
Joined Domain:	☑	
Machine Account Exists:	☑	
Trusted for Delegation:	☑	

Other System Settings

Other system settings that also affect the functioning of the WFS Acceleration module are shown below.

Time Synchronization Source:	soniclabdc-1.utm.soniclab.us:88	[Domain Controller]
Primary DNS Server:	10.2.1. X.X.1.100	[DHCP]
Secondary DNS Server:		

| Advanced Options | Rejoin Domain | Unjoin Domain | Test Configuration | Flush Cache | Restart WFS |
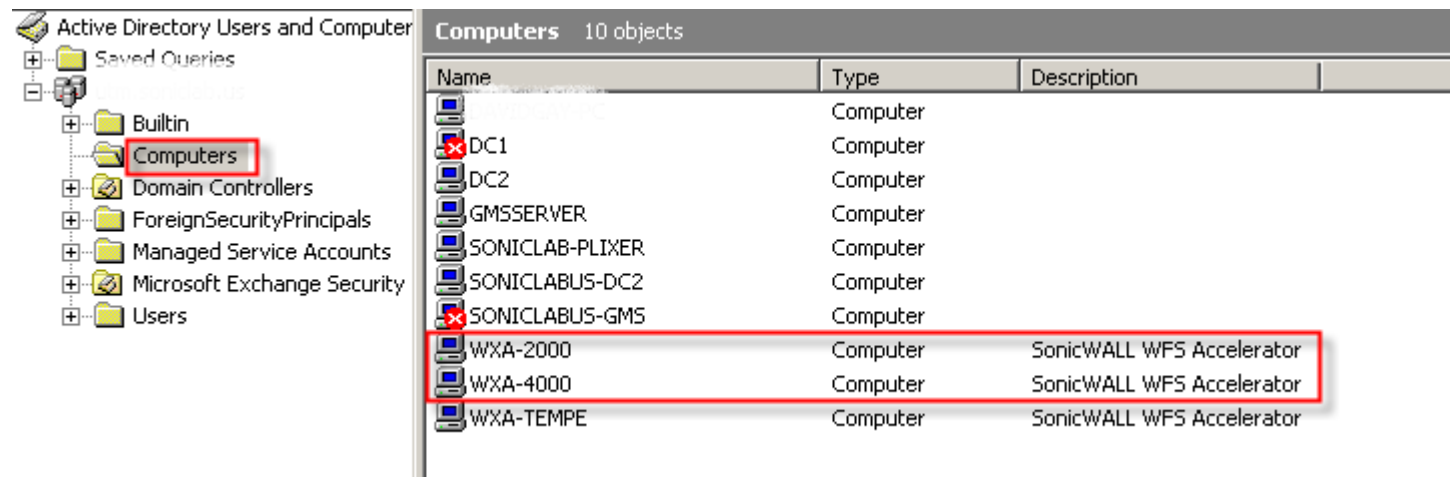
Follow the same steps to add WXA2000 at remote office to the domain.

Once both WXA Appliances are added to the domain, corresponding Computer Accounts for WXA Appliances, DNS Host name and PTR records are automatically created on Domain Controller and DNS servers as shown. For PRT records to get updated, relevant Reverse Lookup Zones could be configured on the DNS servers. Networks used for reverse lookup Zones depend on whether WFS acceleration is using NAT or no NAT. In this deployment, WXA uses NAT'ed IP for WFS Services and only the X0 Subnets are used as Networks in Reverse Lookup Zones. If WXA Appliances are not using NAT, then reverse Look up Zone networks could also be configured for WXA Subnets at both locations.

Top screenshot:

DNS
- SONICLABDC-1
  - Forward Lookup Zones
    - _msdcs.utm.soniclab.us
    - [highlighted]
  - Reverse Lookup Zones
    - 1.x Subnet
    - .20.x Subnet
    - .240.x Subnet
    - 40.x Subnet
  - Event Viewer

utm.soniclab.us   17 record(s)

Name	Type	Data
_msdcs		
_sites		
_tcp		
_udp		
DomainDnsZones		
ForestDnsZones		
TAPI3Directory		
(same as parent folder)	Start of Authority (SOA)	[1983], soniclabdc-1.utm.so...
(same as parent folder)	Name Server (NS)	soniclabdc-1.utm.soniclab.us.
(same as parent folder)	Host (A)	
(same as parent folder)	Host (A)	
DC2	Host (A)	
GMSServer	Host (A)	
soniclabdc-1	Host (A)	
soniclabus-dc2	Host (A)	
wxa-2000	Host (A)	A.A.240.1
wxa-4000	Host (A)	X.X.1.10

Bottom screenshot:

DNS
- SONICLABDC-1
  - Forward Lookup Zones
    - _msdcs.utm.soniclab.us
    - utm.soniclab.us
  - Reverse Lookup Zones
    - X.X.1.x Subnet [highlighted]
    - Subnet
    - 192.168..0.x Subnet
    - 10..0.x Subnet
  - Event Viewer

Subnet   7 record(s)

Name	Type	Data
(same as parent folder)	Start of Authority (SOA)	[50], soniclabdc-1.utm.sonic...
(same as parent folder)	Name Server (NS)	soniclabdc-1.utm.soniclab.us.
(same as parent folder)	Name Server (NS)	dc1.utm.soniclab.us.
X.X.1.10	Pointer (PTR)	wxa-4000.utm.soniclab.us.
	Pointer (PTR)	soniclabdc-1.utm.soniclab.us.
	Pointer (PTR)	soniclabus-dc2.utm.soniclab...
	Pointer (PTR)	gmsserver.utm.soniclab.us.
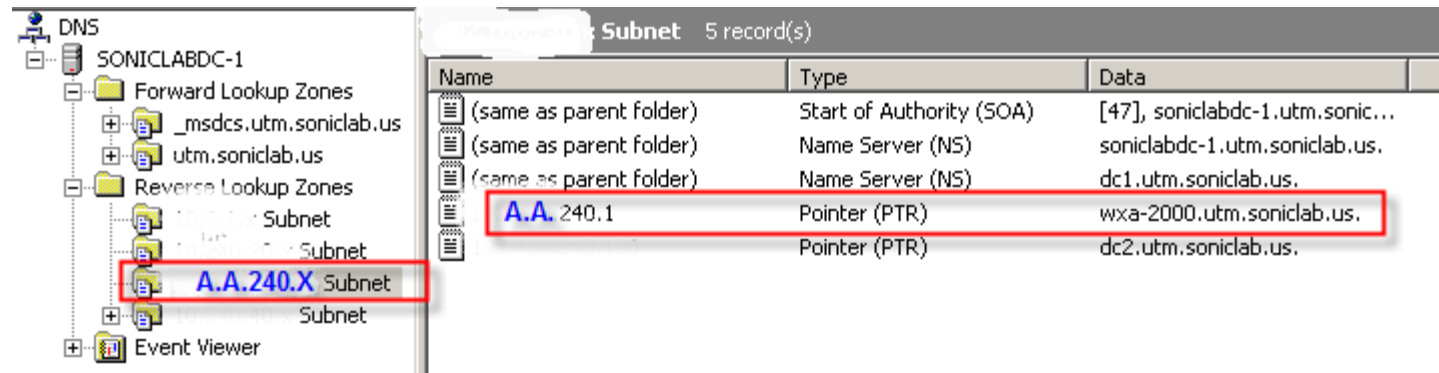
Adding File Shares:

Adding Shares that are hosted on 2 file servers at head quarters.

- Adding /Configuring Shares that are hosted on 1st File Server
  - Configuration on HQ WXA Appliance
  - Configuration on Remote WXA Appliance
- Adding/Configuring Shares that are hosted on 2nd File Server
  - Creating Service Principle Names (SPNs) for mapping shares. More on SPNs creation is discussed below.
  - Configuration on HQ WXA Appliance
  - Configuration on Remote WXA Appliance

1. **Adding Shares that are hosted on 1st File Server:**

   To add shares, you can choose to add all available shares or choose specific shares. For adding shares on the first file server, you can use WXA-4000 as Hostname for Head Quarters WXA Appliance and WXA-2000 as hostname for remote WXA Appliance.

   Adding 2nd and subsequent shares that are hosted on different file servers requires creation of Service Principle Names (SPN) on Active Directory.

Configuring 1st File Server shares on Head Quarters WXA-4000

Configuring 1st File Server shares on Head Quarters WXA-4000

Navigate to WAN Acceleration-> WFS Acceleration->Shares and add shares. In this deployment, as the File Servers are located at Head Quarters, WXA Appliance at Head Quarters directly access these file servers. So on head Quarters WXA Appliance, Remote Server name points to the actual File Server and the Local Server name is the WXA Appliance at head quarters.

Configuring 1st File Server shares on Remote WXA-2000

Navigate to WAN Acceleration-> WFS Acceleration->Shares and add shares. In this deployment, as the file servers are located at Head Quarters, remote WXA Appliance accesses these shares via WXA Appliance at Head Quarters. So on remote office WXA Appliance, Remote Server name points to the Head Quarters WXA-4000 and the Local Server name is the WXA Appliance at remote office.

2. **Adding Shares that are hosted on 2nd File Server:**

Adding 2nd and subsequent shares that are hosted on different file servers requires creation of Service Principle Names (SPN) on Active Directory. These SPNs are used as CIFS service names when mapping and accessing File Server shares. For more information on how to create additional SPNs, please refer to the following Microsoft Knowledgebase article.

http://technet.microsoft.com/en-us/library/cc737007%28WS.10%29.aspx

http://social.technet.microsoft.com/wiki/contents/articles/service-principal-names-spns.aspx

Creation of SPNs shown below is used for demonstration purposes only and additional references and knowledge of customer is required while creating/modifying/deleting SPN entries on Domain Controllers.

Create Service Principle Names for head Quarters and Remote Office WXA Appliances for CIFS/SMB Traffic

For setting up file shares that are hosted on 2nd File Server, WXA-4000-GMS is used as Hostname for Head Quarters WXA and WXA-2000-GMS is used as Hostname for remote Office WXA

For Head Quarters WXA Appliance

```
Command Prompt

Microsoft Windows [Version 5.2.3790]
(C) Copyright 1985-2003 Microsoft Corp.

C:\Documents and Settings\Administrator.SONICLABDC-1>setspn
Usage: setspn [switches data] computername
  Where "computername" can be the name or domain\name

  Switches:
   -R = reset HOST ServicePrincipalName
    Usage:   setspn -R computername
   -A = add arbitrary SPN
    Usage:   setspn -A SPN computername
   -D = delete arbitrary SPN
    Usage:   setspn -D SPN computername
   -L = list registered SPNs
    Usage:   setspn [-L] computername
Examples:
setspn -R daserver1
   It will register SPN "HOST/daserver1" and "HOST/{DNS of daserver1}"
setspn -A http/daserver daserver1
   It will register SPN "http/daserver" for computer "daserver1"
setspn -D http/daserver daserver1
   It will delete SPN "http/daserver" for computer "daserver1"

C:\Documents and Settings\Administrator.SONICLABDC-1>setspn -L WXA-4000
Registered ServicePrincipalNames for CN=WXA-4000,CN=Computers,DC=utm,DC=soniclab,DC=us:
    host/wxa-4000
    host/wxa-4000.utm.soniclab.us

C:\Documents and Settings\Administrator.SONICLABDC-1>setspn -A CIFS/WXA-4000-GMS WXA-4000
Registering ServicePrincipalNames for CN=WXA-4000,CN=Computers,DC=utm,DC=soniclab,DC=us
        CIFS/WXA-4000-GMS
Updated object

C:\Documents and Settings\Administrator.SONICLABDC-1>setspn -A CIFS/WXA-4000-GMS.utm.soniclab.us WXA-4000
Registering ServicePrincipalNames for CN=WXA-4000,CN=Computers,DC=utm,DC=soniclab,DC=us
        CIFS/WXA-4000-GMS.utm.soniclab.us
Updated object

C:\Documents and Settings\Administrator.SONICLABDC-1>
C:\Documents and Settings\Administrator.SONICLABDC-1>setspn -L WXA-4000
Registered ServicePrincipalNames for CN=WXA-4000,CN=Computers,DC=utm,DC=soniclab,DC=us:
    CIFS/WXA-4000-GMS.utm.soniclab.us
    CIFS/WXA-4000-GMS
    host/wxa-4000
    host/wxa-4000.utm.soniclab.us
```

Current listing of SPN for WXA-4000

Adding WXA-4000-GMS hostname as SPN for host WXA-4000

Adding WXA-4000-GMS.utm.soniclab.us hostname as SPN for host WXA-4000

For Remote Office WXA Appliance

C:\Documents and Settings\Administrator.SONICLABDC-1>setspn -L WXA-2000   *Current listing of SPN for WXA-2000*

Registered ServicePrincipalNames for CN=WXA-2000,CN=Computers,DC=utm,DC=soniclab,DC=us:
    host/wxa-2000
    host/wxa-2000.utm.soniclab.us

C:\Documents and Settings\Administrator.SONICLABDC-1>   *Adding WXA-2000-GMS hostname as SPN for WXA-2000*
C:\Documents and Settings\Administrator.SONICLABDC-1>setspn -A CIFS/WXA-2000-GMS WXA-2000
Registering ServicePrincipalNames for CN=WXA-2000,CN=Computers,DC=utm,DC=soniclab,DC=us
        CIFS/WXA-2000-GMS
Updated object

C:\Documents and Settings\Administrator.SONICLABDC-1>setspn -A CIFS/WXA-2000-GMS.utm.soniclab.us WXA-2000
Registering ServicePrincipalNames for CN=WXA-2000,CN=Computers,DC=utm,DC=soniclab,DC=us
        CIFS/WXA-2000-GMS.utm.soniclab.us
Updated object   *Adding WXA-2000-GMS.utm.soniclab.us hostname as SPN for WXA 2000*

C:\Documents and Settings\Administrator.SONICLABDC-1>
C:\Documents and Settings\Administrator.SONICLABDC-1>setspn -L WXA-2000
Registered ServicePrincipalNames for CN=WXA-2000,CN=Computers,DC=utm,DC=soniclab,DC=us:
    CIFS/WXA-2000-GMS.utm.soniclab.us
    CIFS/WXA-2000-GMS
    host/wxa-2000
    host/wxa-2000.utm.soniclab.us

C:\Documents and Settings\Administrator.SONICLABDC-1>

Configuring 2nd File Server shares on Head Quarters WXA-4000

Navigate to WAN Acceleration-> WFS Acceleration->Shares and add shares. In this deployment, as the File Servers are located at Head Quarters, WXA Appliance at Head Quarters directly access these file servers. So on head Quarters WXA Appliance, Remote Server name points to the actual File Server and the Local Server name is the WXA Appliance at head quarters.

On head Quarters WXA Appliance, Remote Server name points to the actual File Server (2nd File Server) and the Local Server name is the SPN name created for WXA Appliance at head quarters – (WXA-4000-GMS)

Configuring 2nd File Server shares on WXA-2000

Navigate to WAN Acceleration-> WFS Acceleration->Shares and add shares. In this deployment, as the file servers are located at Head Quarters, remote WXA Appliance accesses these shares via WXA Appliance at Head Quarters. So on remote office WXA Appliance, Remote Server name points to the Head Quarters WXA-4000 and the Local Server name is the WXA Appliance at remote office.

On remote office WXA Appliance, Remote Server name points to the Head Quarters WXA-4000-GMS (newly created SPN) and the Local Server name is the WXA Appliance newly created SPN at remote office – (WXA-2000-GMS)

Once the shares are configured for 2nd File Server, WXA Appliances updates A record and the associated PTR record for newly created SPNs (depending on Reverse Lookup Zone) on DNS server using the NAT'ed IP. If for some reason the creation on A record and PTR doesn't succeed, domain Admin can manually add them as shown below.

Manually adding SPN hostnames in DNS

Create new Host (A) records in DNS for the newly created SPNs as shown below and appropriately choose the option to update corresponding PTR record as well.

The newly created Hostname for Head Quarters WXA should be updated with the NAT'ed IP of X0 Interface of head Quarters UTM Appliance and newly created Hostname for remote office WXA should be updated with the NAT'ed IP of X0 Interface of remote office UTM Appliance as shown below

Once these A record and PTR record are created for Head Quarters and Remote Office WXA Appliances, you can ping them using these hostnames which resolves to NAT'ed IPs of Xo interfaces at Head Quarters and Remote Offices UTM Appliances.

Now WXA-4000 and WXA-4000-GMS should resolve to X.X.1.100 and WXA-2000 and WXA-2000-GMS should resolve to A.A.240.1

Final Shares on Head Quarters WXA Appliance:

WAN Acceleration /

WFS Acceleration

| Configuration | Domain Details | **Shares** | Statistics | Tools |

Add New Server...

Remote Server Name	Local Device Name	Default Cache Enabled	Default Cache Read Ahead	Configure		
SONICLABDC-1	wxa-4000	☑	32000	🖉 ✕	⊟ Shares	

Add New Share...

Name	Cache Enabled	Cache Read Ahead	Configure
-ALL SHARES-	☑	32000	🖉 ✕

Remote Server Name	Local Device Name	Default Cache Enabled	Default Cache Read Ahead	Configure		
GMSSERVER	WXA-4000-GMS	☑	32000	🖉 ✕	⊟ Shares	

Add New Share...

Name	Cache Enabled	Cache Read Ahead	Configure
-ALL SHARES-	☑	32000	🖉 ✕

Final Shares on Remote Office WXA Appliance:

WAN Acceleration /

WFS Acceleration

| Configuration | Domain Details | **Shares** | Statistics | Tools |

Add New Server...

Remote Server Name	Local Device Name	Default Cache Enabled	Default Cache Read Ahead	Configure		
WXA-4000	wxa-2000	☑	32000	✎ ✕	⊟ **Shares** Add New Share...	

	Name	Cache Enabled	Cache Read Ahead	Configure
	-ALL SHARES-	☑	32000	✎ ✕

Remote Server Name	Local Device Name	Default Cache Enabled	Default Cache Read Ahead	Configure		
wxa-4000-gms	WXA-2000-GMS	☑	32000	✎ ✕	⊟ **Shares** Add New Share...	

	Name	Cache Enabled	Cache Read Ahead	Configure
	-ALL SHARES-	☑	32000	✎ ✕

Testing:

All shares should be identical whether accessed using shares using real File Sever, or shares using Head Quarters WXA Share name or Remote Office Share Name.

In this case, Remote Office users should use \\WXA-2000 and \\WXA-2000-GMS as share names to access resources on the Head Quarters that are actually hosted on File Server 1 and File Server 2. Head office users must access the shares using the Real Server as the actual servers are local in this case.

Network administrators must also map the real shares mapped to the real server for redundancy in case of WXA appliance at remote office goes down.

\\soniclabdc-1

File Edit View Favorites Tools Help

Back | Search | Folders

Address \\soniclabdc-1 → Go

Name ▲	Comments
DC-FileShare	
NETLOGON	Logon server share
SONICLABDC-1.LOG	Exchange message tracking logs
SYSVOL	Logon server share
Printers and Faxes	Shows installed printers and fax …
Scheduled Tasks	Schedule computer tasks to run …

\\wxa-4000

File Edit View Favorites Tools Help

Back | Search | Folders

Address \\wxa-4000 → Go

Name ▲	Comments
DC-FileShare	
NETLOGON	Logon server share
SONICLABDC-1.LOG	Exchange message tracking logs
SYSVOL	Logon server share
Printers and Faxes	Shows installed printers and fax …

\\wxa-2000

File Edit View Favorites Tools Help

Back | Search | Folders

Address \\wxa-2000

Name ▲	Comments
DC-FileShare	
NETLOGON	Logon server share
SONICLABDC-1.LOG	Exchange message tracking logs
SYSVOL	Logon server share
Printers and Faxes	Shows installed printers and fax …

Security

mcxml6_msi

\\gmsserver

File Edit View Favorites Tools Help

Back | Search | Folders

Address \\gmsserver → Go

Name ▲	Comments
GMSVP	
Scheduled Tasks	Schedule computer tasks to run …

\\wxa-4000-gms

File Edit View Favorites Tools Help

Back | Search | Folders

Address \\wxa-4000-gms → Go

Name ▲	Comments
GMSVP	

\\wxa-2000-gms

File Edit View Favorites Tools Help

Back | Search | Folders

Address \\wxa-2000-gms

Name ▲	Comments
GMSVP	

Tools available for testing and troubleshooting:

WAN Acceleration /

WFS Acceleration

| Configuration | Domain Details | Shares | Statistics | **Tools** |

Diagnostic Tool: DNS Name Lookup ▼

DNS Name Lookup
Available Shares
Test WFS Configuration
List Kerberos Servers

DNS Nam

Primary DNS:	10.2.1.100
Secondary DNS:	
Lookup Name or IP:		Go