SonicWALL WAN Acceleration FAQ Document

Technology, Models, Licensing

1. What is SonicWALL's WAN Acceleration solution and how is it deployed?
    - The SonicWALL WXA series available as live CD, Hardware and Virtual Appliances are deployed in one-arm mode with SonicWALL NSA/TZ series appliances that allow network administrators to accelerate WAN traffic using TCP and Windows File Sharing (WFS) acceleration between data center and remote site there by reduces application latency, conserves bandwidth and significantly improves user-experience. It uses de-duplication, data caching, and metadata caching and data-in-flight compression techniques.

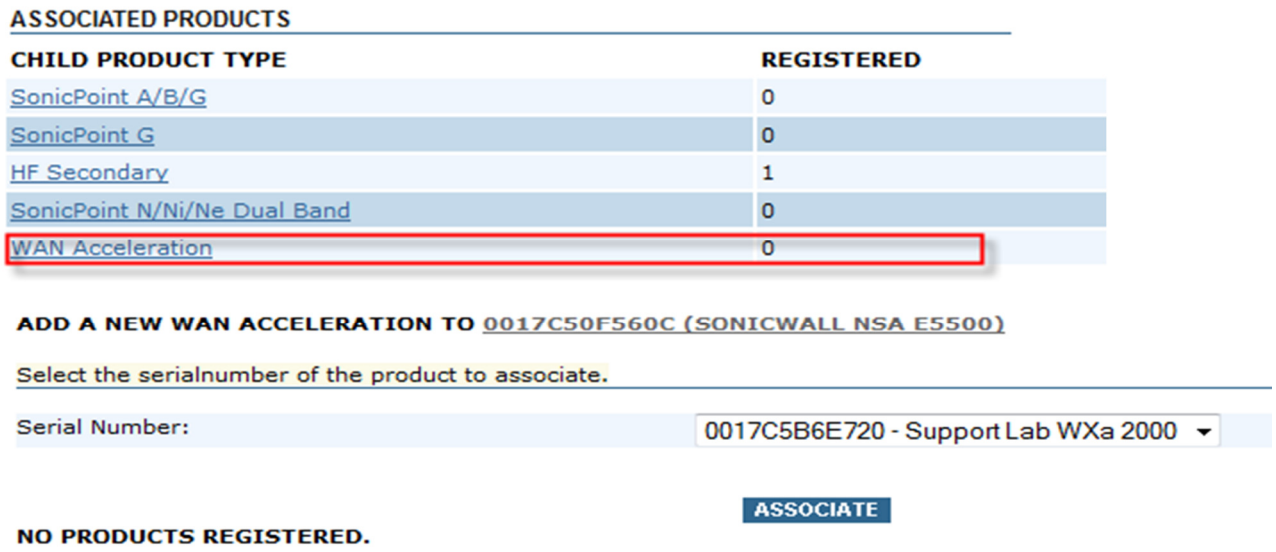
2. What are the benefits of using SonicWALL's WAN Acceleration Solution?
    - WAN optimization solution can delay or postpone the expenditure and provide an increase in application performance response time without tweaks or changes to applications; without changes to Network; Using existing WAN Infrastructure; benefits are seen immediately; improves Effective Bandwidth of the link

3. What are different available models of SonicWALL WAN Acceleration Series
    - WXA 500 Live CD
    - WXA 2000/4000 hardware appliances
    - WXA 5000 Virtual Appliance

4. What SonicWALL UTM Appliances and SonicOS firmware version support SonicWALL WXA Series devices
    - SonicWALL TZ/NSA UTM appliances (Except NSA 2400MX)
    - SonicOS 5.8.1.0 -30o and above

5. How does licensing work for SonicWALL WXA Series
    - WXA 500 Live CD – Initially licensed for 1 year and needs to be renewed after that. Just like any Subscription service screen on managing UTM appliance UI, once the subscription expires, Customer will not be able to manage the device/service.
    - WXA 2000/4000 hardware appliances – Appliances come with 1 year Hardware and Software Support. Customer has to buy Support after 1 year. However after 1st year, if the customer chooses not to buy support then like any other SonicWALL Appliance, there will be no software/firmware upgrades available. Appliance has to have valid Support in order to qualify for RMA
    - WXA 5000 Virtual Appliance - Initially licensed for 1 year and needs to be renewed after that. Just like any Subscription service screen on managing UTM appliance UI, once the subscription expires, Customer will not be able to manage the device/service.

6. How to register SonicWALL WXA Series devices
    - All SonicWALL WXA Series models must be registered as associated child products under managing SonicWALL UTM Appliances



7. What happens when the licensing for WXA 500 live CD and WXA 5000 Virtual Appliance expires?
    - Just like any Subscription service screen on managing UTM appliance UI, once the subscription expires, Customer will not be able to manage the device/service.

8. What the maximum number of users and flows supported per device?
    - Assuming total 5 flows per user (4 TCP flows and 1 CIFS/SMB session)

Model	Max Users	Max Flows
WXA 500 Live CD	20	100
WXA 2000 Appliance	120	600
WXA 5000 Appliance	240	1200
WXA 5000 Virtual Appliance	240+	1200+

9. What are different specifications for each model type?

	WXA 500 Live CD	WXA 2000	WXA 4000	WXA 5000 Virtual Appliance
Platform	Software/CD	Hardware Appliance	Hardware Appliance	Virtual Appliance (VMWare)
Maximum Users[1]	20	120	240	(See footnote 3 below)
Maximum Flows	100	600	1,200	(See footnote 3 below)
Byte Caching	Yes			
TCP/File Compression	Yes			
Management	Requires SonicOS 5.8.1 or later			
TCP Visualization	Yes			
WFS Acceleration	Yes[2]	Yes		
SNMP	Yes			
Syslog	Yes			
Operating System	Hardened SonicWALL Linux OS			
Rack-mount Chassis	—	1 RU		—
CPU	—	Intel 2.0GHz	Intel Dual Core 2.0GHz	—
RAM	—	2 GB	4 GB	—
Hard Drive	—	250 GB	2x250 GB	—
Redundant Disk Array (RAID)	—	—	RAID 1	—
Dimensions	—	17.0 x 16.4 x 1.7 in/43.18 x 41.59 x 4.44 cm		
Weight	—	16 lbs/7.26 kg		—
WEEE Weight	—	16 lbs/7.37 kg		
Power Consumption (Watts)	—	86	101	—
BTUs	—	293	344	—
MTBF (Years)	14.27			

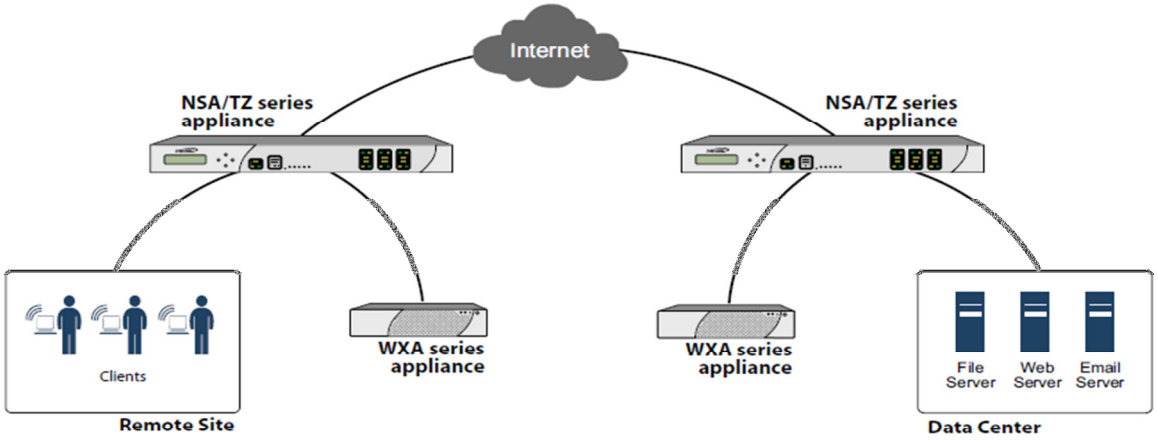
	WXA 5000 Virtual Appliance Only
Hypervisor	ESX and ESXi (version 4.0 and newer)
Operating System Installed	Hardened SonicLinux
Minimum CPU	2 x 1.6 GHz
Allocated Memory	4 GB
Applied Disk Size	250 GB
VMware Hardware Compatibility Guide	http://vmware.com/resources/compatibility/search.php

[1] Maximum users may vary depending on the number of flows being generated per user.
[2] WFS Acceleration is available only when the Live CD image is installed on the provided hardware.
[3] The virtual appliance hardware outlined above supports approximately 120 users with 600 flows. Max users and flows for the Virtual Appliance may vary depending on the provided hardware configuration.

Deployment Modes, Device Management - Firmware and Settings Management

10. What are typical SonicWALL WXA Series Deployment modes
    - Site-Site VPN (IPsec/Route based VPN)
    - Routed Mode
    - Layer 2 Bridge Mode

11. How many appliances are required between 2 locations
    - Requires 2 Appliances between Headquarters and remote offices to accelerate traffic



12. How to physically connect WXA devices?
    - Connect WXA Appliance directly to one of the unused Physical Ports on TZ/NSA running SonicOS 5.8.1.0
    - Connect WXA Virtual Appliance directly to one of the unused Physical Ports on TZ/NSA running SonicOS 5.8.1.0
    - Connect Server/PC running WXA Live CD directly to one of the unused Physical Ports on TZ/NSA running SonicOS 5.8.1.0

13. What Zone must be used to configure WXA Appliances?
    - 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 from/to WXA Appliances at both locations. This simplifies the process of configuration and deployments. Please note that traffic coming from Remote WXA Appliance and remote networks is considered as Source VPN
    - 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.

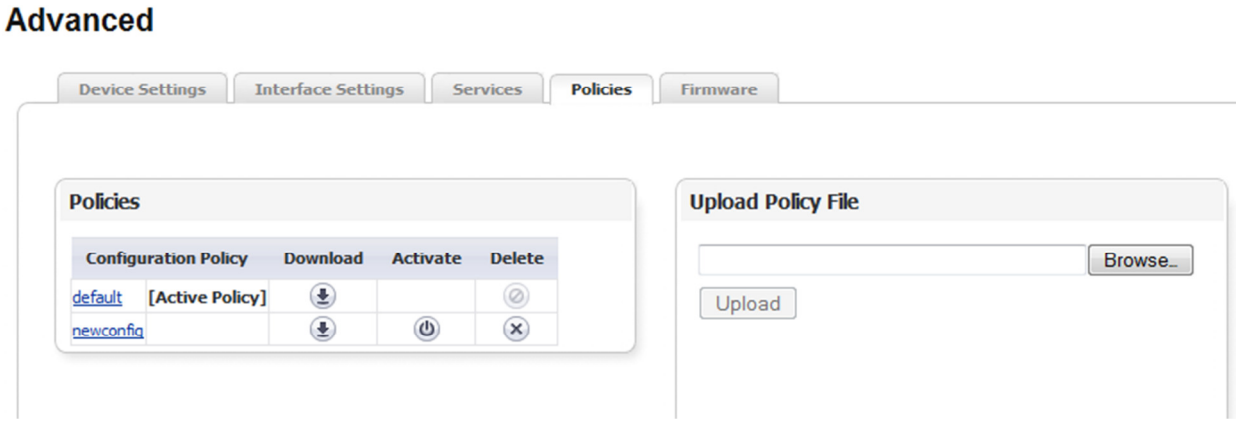
The following services are being used by WAN Acceleration and Client PCs for Domain Controller, DNS Server, NTP server, File Server Services.

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	

14. Is the firmware version on SonicWALL WXA devices tied to the firmware version of the managing UTM appliance?
    - No, firmware version on SonicWALL WXA Devices is independent of firmware version on SonicWALL UTM appliances

15. Can you have multiple copies of SonicWALL WXA settings files saved on the devices?
    - Yes, multiple copies of settings files can be saved on WXA Devices.



16. Can you have multiple versions of Firmware saved on SonicWALL WXA series devices?
    - No

17. Is it possible to downgrade firmware on SonicWALL WXA Devices or a roll back?
    - No. At this point WXA Appliance doesn't accept any firmware downgrades

18. How SonicWALL UTM appliance does know whether WXA device is still connected and operational?
    - SonicWALL UTM Appliance probes connected WXA device for its operational status – every 30 seconds. The probe is a HTTPS request for the "Status update" message to the WXA device and the WXA responds back (XML response) with data relating to : Model, SN#, Firmware Version, Uptime, load, TCP and WFS acceleration parameters and statistics
    - If the probe fails to get a response, the UTM will stop forwarding traffic via WXA device. When the probe succeeds again UTM will begin forwarding new connections to the WXA

19. What are current assumptions and limitations?

    - Assumptions:
        - A SonicWALL NSA/TZ series appliance is required to deploy the SonicWALL WXA series device
        - The Remote sites use services in the datacenter, for example a central file or SharePoint repository.
        - Traffic passing through the SonicWALL WXA series appliance is IPv4
    - Deployment Limitations
        - WAN Acceleration will not accelerate IPSEC or SSL traffic.
        - WAN Acceleration is compatible with IPv4 only.
        - WAN Acceleration currently supports Windows-based file services only.
            - support for NetApp, FreeNAS, OpenFiler and EMC might come at a later stage
        - If a VPN is not configured on the SonicWALL NSA/TZ series appliance, then the user will have to configure the destination subnets to be accelerated manually.
        - WFS Acceleration currently supports deployments using Active Directory/Kerberos for authentication and authorization.
        - WFS Acceleration currently does not support NTLM or other authentication mechanisms.

20. Does SonicWALL WXA Appliances provide any option like Safe Mode?
    - No. There is no option like Safe mode in SonicOS UTM Appliances

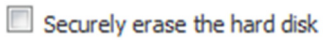
21. Can external DHCP servers be used to provide DHCP lease to SonicWALL WXA devices?
    - No. Only SonicWALL DHCP Server on UTM Appliance should be used to provide DHCP lease. SonicOS identifies WXA Appliance by using Client ID

22. What is firmware version type that runs on SonicWALL WXA Appliances
    - SonicWALL WXA Appliances runs SonicWALL Linux OS

23. What are the requirements to run SonicWALL WXA 500 Live CD
    - Any Server OS with at least Pentium 4 CPU, 2G RAM, 80G hard disk

24. What are the modes in which you can run SonicWALL WXA 500 Live CD
    - Live CD supports 2 modes : Live Mode and Install Mode
        - Live Mode - Live mode is run from RAM and doesn't touch the Server. All the dictionaries are built and saved in RAM and lost on a reboot. Once configured, user can download the configuration file and save it for the next time run. Windows File Sharing (WFS) is not available in Live Mode. WFS require Install Mode.
        - Install Mode – In Install Mode, the Application gets installed on the Server. All dictionaries and configuration files are saved on the hard disk

25. What are the minimum requirements to install SonicWALL WXA Virtual Appliance
    - VMWare ESX, ESXi 4.0 and newer
    - CPU – 2 Virtual CPUs each at least 1.6 GHz
    - Memory – 4 GB
    - Hard Disk – 80 GB

26. What does  mean and how long does it take to securely erase hard disk on SonicWALL WXA Appliances
    - Secure Erase writes Zeros to the whole disk and it might take about 2 hrs to complete. The OS partition is then re-written back to the disk and the appliance rebooted.
    - If customers wish to do a secure erase but preserve their configuration data, then they can check the “restore current configuration” which will make a backup of the settings file (xml) AS WELL AS the WFS domain information – so the device doesn’t need to join the domain again.

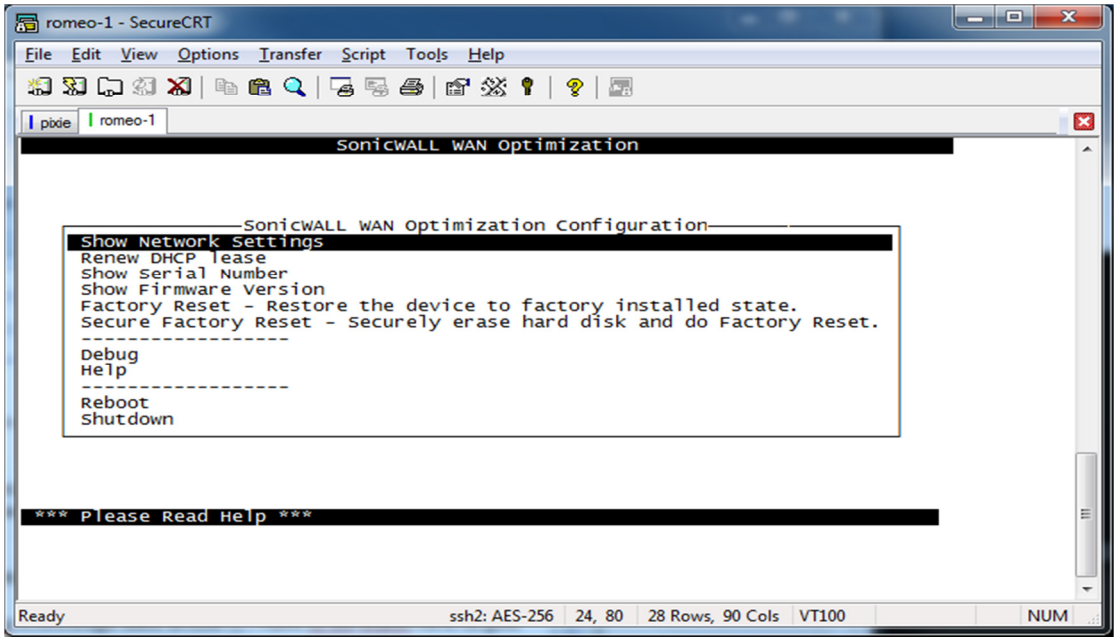
27. How many passes does “Secure Erase” go through on the hard drive?
    - 1

28. How does Secure Erase Work?
    - Secure erase will do the following:
        - Make a backup image of the current OS
        - Restart the appliance
        - Boot a different kernel
        - Copy the back-up made in step 1 to memory
        - Write zeroes to the entire disk – this process takes about 2 hours and should NOT be interrupted
        - Write the back-up images back to disk
        - Reboot to normal kernel

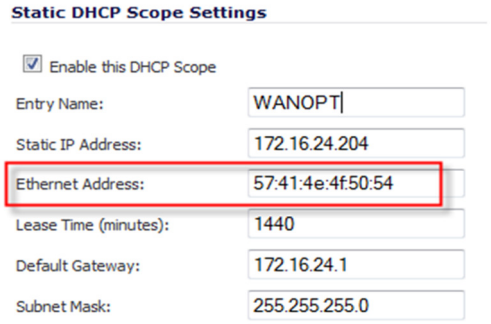
The back-up images only contain the OS. Logs and cached data are not part of these back-ups. (they are different partitions)
If customers wish to do a secure erase but preserve their configuration data, then they can check the “restore current configuration” which will make a backup of the settings file (xml) AS WELL AS the WFS domain information – so the device doesn’t need to join the domain again.
This process is similar to the above one except that it takes slightly longer.

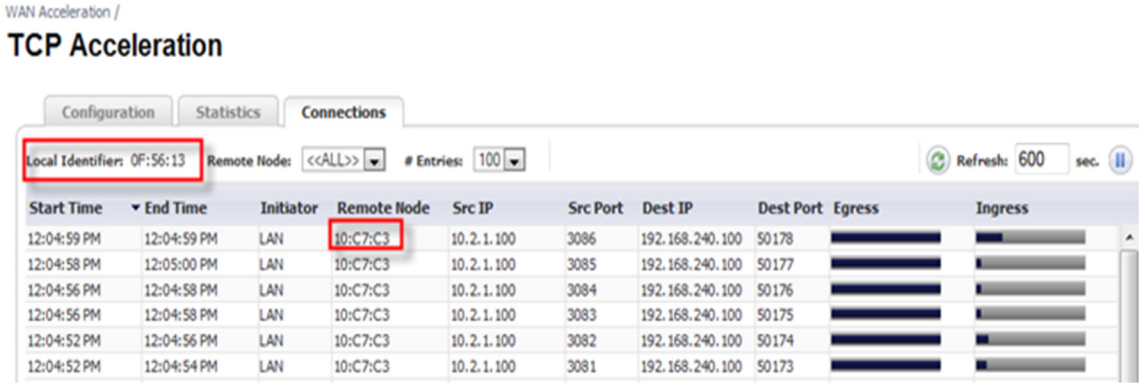
29. What is recommended practice when unit is RMA’ed?
    - If the unit is still in some functional state and accessible via UTM Appliance, then it is recommended to perform “Secure Erase” from the UI of the Firewall. If the NIC is dead and unit is not accessible via UTM, secure erase can still be done from the console.
    - The factory reset has the option of doing a secure erase which will wipe everything from the disk first. This is especially useful for customers who need to do an RMA and they are a bit concerned to send their appliance with all of their data on the disk! Companies in the healthcare, financial and legal fields will most likely see this as a requirement.

    - The menu can be accessed by plugging in to the appliance with a console cable with the following settings: 9600-8N1. Username: wxauser; password: password



30. There are 2 different local ID's that the WXA device uses. One is on the DHCP Server Lease scope which shows itself as Ethernet Address that is auto added when you push the button to create Static DHCP Scope - 57:41:4e:4f:50:54. The other is found on TCP Acceleration page on the connections tab. Why are they different? How are they generated?





- 57:41:4e:4f:50:54 is used for the firewall to identify that it is a WXA device and based on this ID, it knows which IP to serve, if reserved.
- The ID's in TCP Acceleration are the last 6 hex characters of the MAC addresses of the interface of the UTM where the WXA is connected to. This ID is used to build a unique cache database on the WXA for each peer.

31. How many WXA Appliances can be configured per each UTM appliance?
    - One. Currently you cannot configure more than 1 unit for Failover or redundancy purposes.

TCP and WFS Acceleration

32. What types of Acceleration is supported by SonicWALL WXA Devices
    1. TCP Acceleration
    2. Windows File Sharing Acceleration – WFS

33. Is TCP and WFS Acceleration supported when managing UTM Appliances are deployed in High Availability mode?
    - Yes. We do Support WXA Appliances to handle TCP and WFS Acceleration in Stateful and Active/Active DPI deployments and require a switch connected to both UTM Appliances and WXA Appliance
    - We do not yet Support WXA Appliances in Active-Active Clustering Deployments

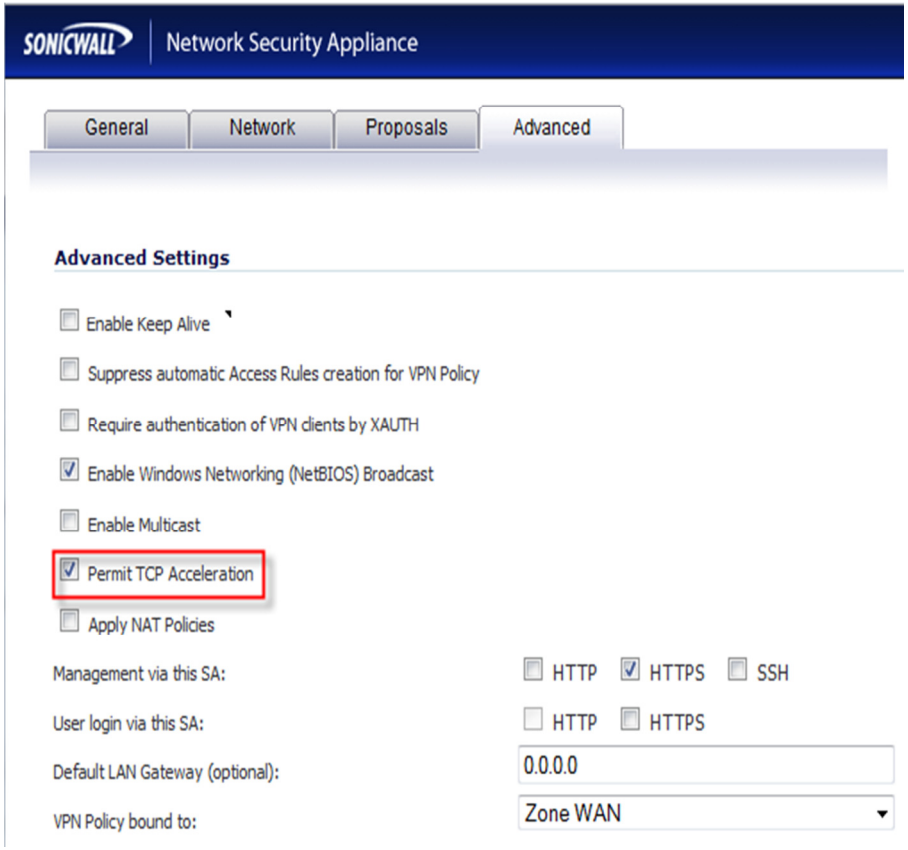
34. Does traffic between WXA Appliances going through DPI engine?
    - No, the traffic between WXA Appliances doesn't go through the DPI engine, but the traffic from the source and destination networks goes through DPI engine for inspection

TCP Acceleration

35. How does TCP acceleration work?
    - TCP Acceleration uses transparent TCP Proxy. What it means is that user has to tell the UTM device what Network traffic needs to be sent to WXA for TCP acceleration – remember that Source/Destination traffic HITS the UTM device first and firewall should know whether to send the traffic directly to Destination networks or send it to WXA Appliance for Acceleration
    - If using Site-Site IPSec VPN, by default if you enable TCP Acceleration on a Policy, UTM chooses the local and destination networks defined for TCP acceleration
    - If using Site-Site Tunnel Interface VPN, when defining route statements, you can specify if the traffic should be subjected to TCP Acceleration
    - If using regular Layer 2 bridge or route mode, when defining route statements, you can specify if the traffic should be subjected to TCP Acceleration

36. Where and how to enable TCP acceleration?
    - TCP acceleration must be enabled Globally and
        - If using Site-Site VPN, TCP acceleration must be enabled on the VPN policy. If using a route based VPN, TCP acceleration must be enabled on the route Statement
        - If using Layer2 Bridge or routed mode, TCP acceleration must be enabled on the route statements.

Site-Site VPN



Route based VPN, L2Bridge Mode, Routed Mode

37. What TCP traffic is accelerated by WXA Appliance?
    - WXA accelerates all TCP traffic except
        - TCP traffic that is encrypted and RPC based
        - TCP traffic that is excluded by default
          44,88,135,137,136,138,139,7,23,37,107,179,513,514,1494,1718,1719,1720,2000,2001,2002,2003,2427,2598,2727,3389,
          5060,5631,5900,5901,5902,5903,6000,22,49,261,443,445,448,465,563,585,614,636,684,695,989,990,992,993,994,995,1

701,1723,2252,2478,2479,2482,2484,2492,2679,2762,2998,3077,3078,3183,3191,3220,3269,3410,3424,3471,3496,3509,3529,3539,3660,3661,3713,3747,3864,3885,3896,3897,3995,4031,5007,5061,7674,9802,11751,12109,8443

38. For TCP acceleration do the WXA devices sync up their dictionaries upon a request for Data or automatically on a scheduled interval?
    - Data is added to the database upon request.

39. How does the TCP compression compare with the compression used by the CDP appliance?
    - The major difference is that CDP is file aware while TCP acceleration isn't.

40. Is it necessary that WXA Appliance to be added to the domain if only TCP acceleration is used?
    - No, TCP acceleration doesn't require the device to be added to the domain, but WFS needs the device to be added to the domain.

41. Why should source and destination networks need to be included for TCP acceleration in VPN policies and route statements?
    - TCP is a transparent proxy and UTM should know what traffic needs to be accelerated, where as WFS is an EXPLICIT proxy and in that share is accessed using share mapped to WXA.

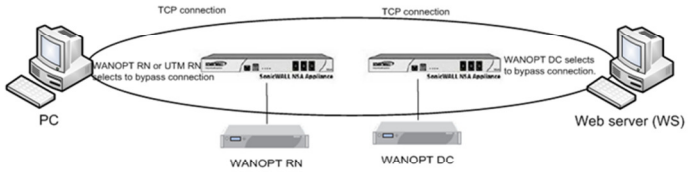
42. For TCP acceleration, what happens when one side of WXA device goes down?
    - UTM would sense that WXA is down and would bypass acceleration. Connections need to be re-established as it is transparent proxy

43. Do SonicWALL WXA devices accelerate TCP traffic that has associated control channel – for example, FTP, Oracle, SQL?
    - No, only Data channel traffic is optimized for efficiency

44. Is TCP acceleration supported when NAT over VPN is used?
    - We currently do not support NAT over VPN for TCP acceleration

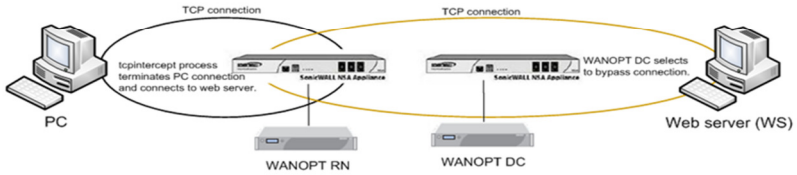
45. What happens when one end of WXA Appliance is down or when one side of UTM Appliance chooses not to optimize traffic for TCP acceleration

TCP Acceleration (Connection hand off)



When both Remote and Data Center WXA Devices or UTM devices choose not to optimize a Specific traffic type

TCP Acceleration (Connection hand off)



When Data Center WXA Devices or UTM devices choose not to optimize a Specific traffic type or the Data Center WXA Appliance is down

46. How come Windows file shares connections are not accelerated by TCP acceleration and not seen in TCP Acceleration->Connections page
    - TCP 445, TCP 135-139 traffic is excluded from TCP acceleration and handled by WFS Acceleration

47. Does TCP acceleration update/modify any Domain or DNS related entries?
    - No, TCP acceleration doesn't involve in any domain or DNS related updates or modifications.

WFS Acceleration

48. What is WFS Acceleration
    - WFS is an Explicit Layer 7 Proxy and users access the shares using shares mapped to WXA appliance

49. What are the recommendations for configuring WFS?
    - Create Static DHCP scope for WXA Appliance on the managing SonicWALL UTM Appliance
    - 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.

- 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.
- 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)
- It is recommended that WXA Appliance gets NTP updates from local Domain Controller
- It is recommended that the DNS server accepts secure updates

- 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.

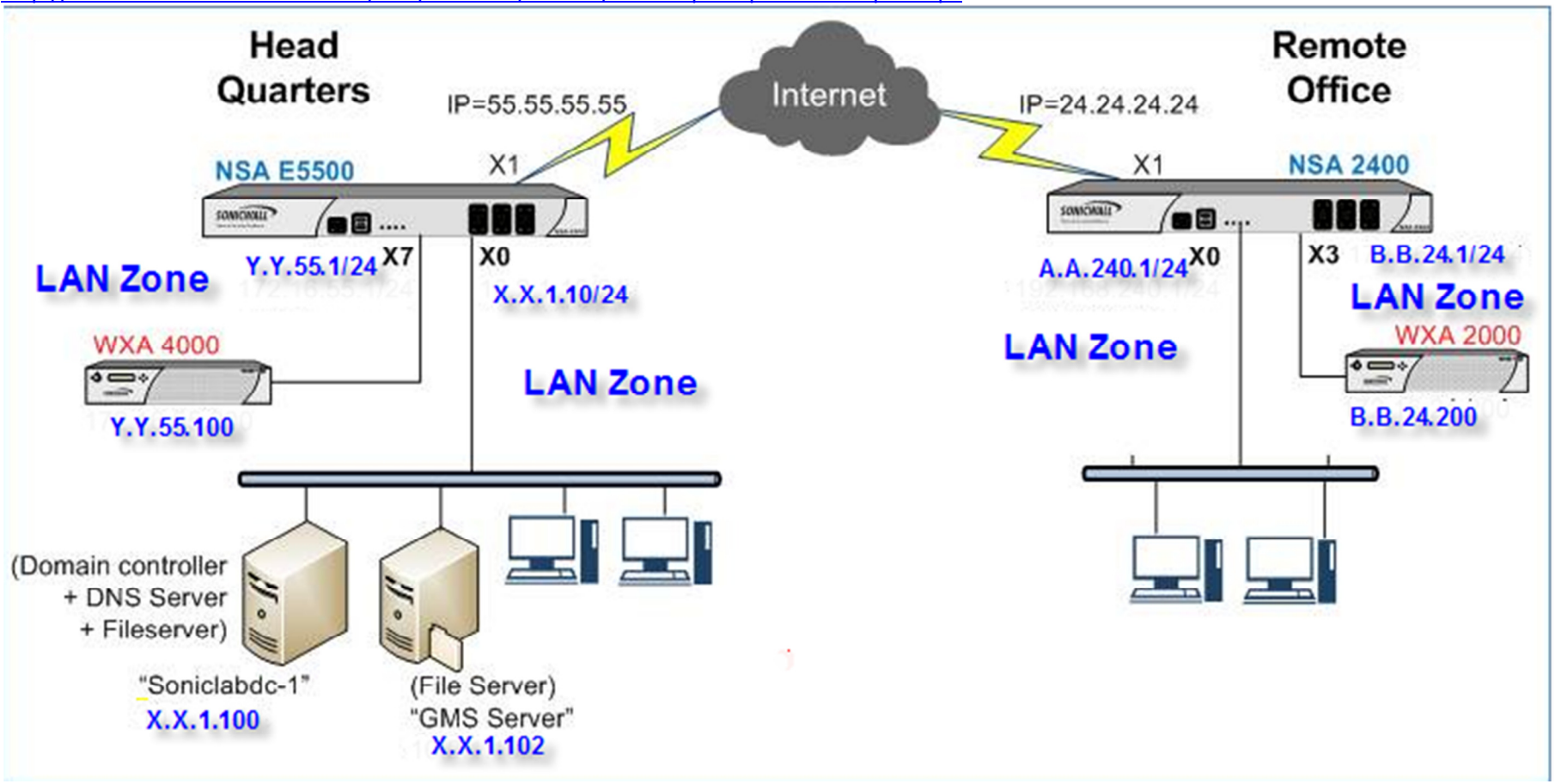
50. Is it required to add WXA Appliance to the domain for WFS Acceleration?
    - Yes, WXA Appliance must be added to the domain

51. Can a remote WXA Appliance be added to a domain that is different from the domain that is used by Head Quarters WXA Appliances?
    - Yes, you can add remote WXA Appliance to a different domain as long as both domains have inter-domain and forest trusts between themselves and able to communicate with each other with out permissions issues.

52. What is the order of steps to configure WFS Acceleration
    - Configure DHCP scope properly for WXA Appliance to get Domain Name and Domain DNS server information from the scope
    - Enable WFS Acceleration and choose proper NAT'ed IP to be used for communication purposes (in NAT mode) or choose WXA Appliance IP for communication (no NAT)
    - Add WXA Appliance to the domain, make sure that Computer account, A record and PTR records are updated on DNS server
    - Configure Shares on local and remote WXA Appliances

53. When configuring WFS shares what are local and remote server names and how to map the shares?
    - Consider a deployment where 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.

WXA-4000 is the host name of WXA at Head Quarters and WXA-2000 is the host name of WXA at remote office. Separate Service Principles Names (SPNs) are created for WXA-4000 and WXA-2000 for CIFS services that will be used to map File 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



Head Quarter Name Mapping:

Hostname WXA-4000 is used for FileServer1 Mapping
Hostname WXA-4000-GMS is used for FileServer 2 Mapping

Remote Office Name Mapping

Hostname WXA-2000 used for file server1 mapping
Hostname WXA-4000-GMS is used for FileServer 2 Mapping

In this example, Clients at remote use \\wxa-2000 to access shares on FileServer1 and \\wxa-2000-gms to access shares on FileServer2

Final Shares on Head Quarters WXA Appliance:

Final Shares on Remote Office WXA Appliance:

54. Does WFS acceleration update/modify any Domain or DNS related entries?
    - Yes, once WXA Appliance is added to the Domain, Computer Account for WXA Appliance is auto-created on Domain Controller.
    - On DNS servers, A record and PTR records are auto-added for the WXA Appliance and it uses the NAT'ed IP address (in NAT mode) for A record and PTR record and uses original WXA Appliance IP address for A record and PTR record for non NAT Mode.

55. Is it required to enable NetBIOS on VPN policies for WFS Acceleration?

    - It is not necessary to enable NetBIOS on VPN policies and NetBIOS broadcast is not necessary. Client PCs mostly use TCP 445 for file shares and if the PCs use TCP 137 WXA handles WFS acceleration effectively in both cases.

56. How does Managing UTM Appliance automatically determine what traffic to send to WXA Appliance for WFS acceleration?

    - UTM Appliances doesn't determine what traffic to send to WXA Appliance for WFS acceleration. WFS is explicit Layer 7 proxy and the clients explicitly access shares that are mapped to WXA appliance unlike TCP acceleration which is an implicit TCP proxy

57. Can SonicWALL WXA device auto-detect domain name, Kerberos, LDAP and NTP server information automatically for WFS?

- Yes, provided that WXA device is using Internal Domain DNS servers (initial Firmware 1.0 also require reverse DNS look-up zone on DNS server). If auto-discovery fails, you can manually configure domain name, Kerberos Server, LDAP server and time synchronization server which are critical for Windows File Sharing Configuration

58. For WFS acceleration when checking to see if a file needs to be synched up and it is determined that it does need to sync is the whole file overwritten or is it only the delta changes?
    - Just the deltas

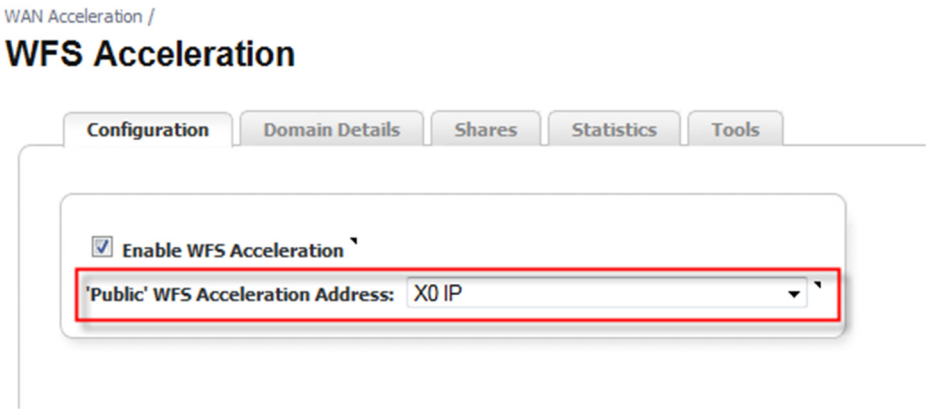
59. What services are being used by WFS Acceleration?
    - The following services are being used by WAN Acceleration and Client PCs for Domain Controller, DNS Server, NTP server, File Server Services.

    - 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	

60. Can WXA be used for WFS Acceleration without using NAT policies?

- WFS can be configured to work using NAT or no NAT.
- If NAT is being used (default mode), automatic NAT policies are created by Firewall depending on the NAT IP being used by WXA Appliance. In the below screenshot, WXA Appliance IP is NAT'ed to X0 interface IP of the managing UTM Appliance. 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. When NAT is used, WXA Subnets on both side of the tunnel are not needed to be included in source and destination VPN networks.



#	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			

- WXA can also be used without using NAT, implying that WXA Appliance IP is not translated to any other IP address, but rather use its own IP address. In this case WXA subnets also need to be included in the VPN Local and Destination networks for WFS.