

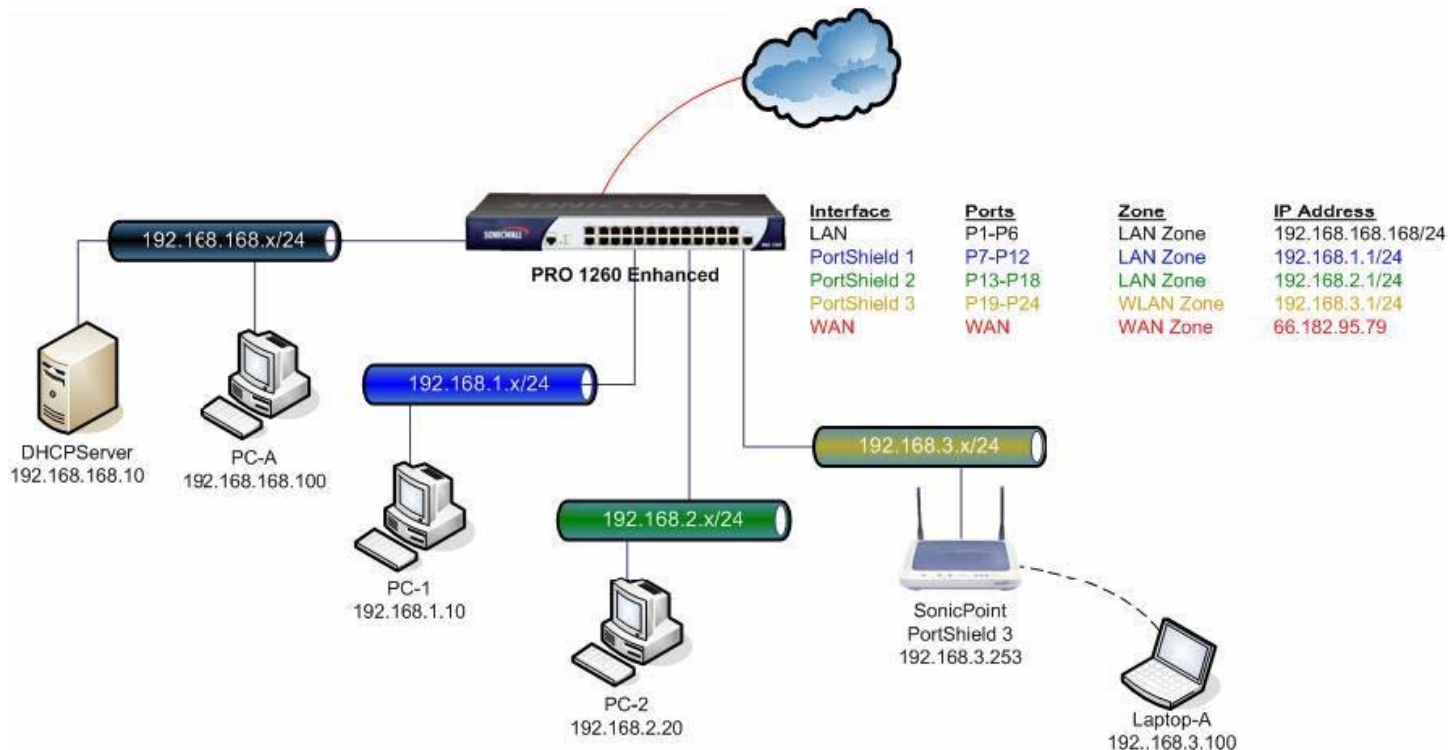
TechNote

IP Helper

Network Browsing with IP Helper NetBIOS Relay

IP Helper

The IP Helper NetBIOS relay translates NetBIOS subnet broadcasts from one or more selected source subnets to NetBIOS broadcasts bearing addresses that will be interesting to one or more selected destination subnets. The IP Helper NetBIOS relay acts specifically on UDP 137 (NetBIOS Name Service) and UDP 138 (NetBIOS Datagram) broadcast traffic to enable broadcast node (b-node) style name resolution (e.g. Network Neighborhood) across subnet boundaries.



In the scenario above, if PC-2 (NetBIOS name 'PC-2') attempts to browse a share on PC-A, it will send a NetBIOS Name Service (NBNS) query to the layer 2 destination broadcast address (FF:FF:FF:FF:FF:FF) and to its subnet broadcast address (192.168.2.255) on UDP port 137.

```
Ethernet II, Src: 08:00:46:a2:eb:4d, Dst: ff:ff:ff:ff:ff:ff
Internet Protocol, Src Addr: 192.168.2.20 (192.168.2.20), Dst Addr: 192.168.2.255 (192.168.2.255)
User Datagram Protocol, Src Port: 137 (137), Dst Port: 137 (137)
  Source port: 137 (137)
  Destination port: 137 (137)
  Length: 58
  Checksum: 0x976b (correct)
NetBIOS Name Service
  Transaction ID: 0x9a2b
  Flags: 0x0110 (Name query)
  Questions: 1
  Answer RRs: 0
  Authority RRs: 0
  Additional RRs: 0
  Queries
    PC-A<20>: type NB, class inet
```



Tech Note

Without IP Helper, the SonicWALL would drop this broadcast traffic. But with IP Helper, it is possible to define where the broadcast traffic should go, and to translate it accordingly.

When the IP Helper NetBIOS relay receives a NetBIOS broadcast packet, it translates the subnet broadcast address to match the subnet (or subnets) of its policies' configured destinations.

Some considerations about the NetBIOS relay and its policies:

- When IP Helper forwards a packet, it decrements the TTL (time to live) specified in the source IP header by a value of 12. Microsoft operating systems generally specify a default TTL value of 128.
- NetBIOS policy source and destination must be a Network Address Object, or a Group of Network Address Objects.
- NetBIOS policy source and destination cannot overlap. In other words, you cannot specify a policy from Network Address Object 'PortShield Interface 1 Subnet' to 'PortShield Interface 1 Subnet', or from Network Address Object 'LAN Primary Subnet' to Group 'mySubnetGroup' if 'mySubnetGroup' contains 'LAN Primary Subnet' as a member.
- The same source cannot be specified in multiple policies. In other words, if you want NetBIOS broadcasts from 'LAN Primary Subnet' to be relayed to 3 different destination subnets, rather than creating 3 policies, you would create a Group comprising the 3 destination Network Address Objects.
- Configurations requiring the relaying of NetBIOS broadcasts to both local and VPN subnets require special consideration. See the 'IP Helper NetBIOS Relay with VPNs' section.

Defining Destination Groups

With these considerations in mind, the goal should be to design the destination Groups for each of our four source subnets from which we will be relaying NetBIOS broadcasts to all other subnets. The four Groups to create would look like:

<input type="checkbox"/>	<input type="checkbox"/>	25	NBNS from Primary LAN	Group				
			▶ PortShield Interface 1 Subnet	192.168.1.0/255.255.255.0	Network	LAN		
			▶ PortShield Interface 2 Subnet	192.168.2.0/255.255.255.0	Network	LAN		
			▶ PortShield Interface 3 Subnet	192.168.3.0/255.255.255.0	Network	WLAN		
<input type="checkbox"/>	<input type="checkbox"/>	26	NBNS from PortShield1	Group				
			▶ LAN Primary Subnet	192.168.168.0/255.255.255.0	Network	LAN		
			▶ PortShield Interface 2 Subnet	192.168.2.0/255.255.255.0	Network	LAN		
			▶ PortShield Interface 3 Subnet	192.168.3.0/255.255.255.0	Network	WLAN		
<input type="checkbox"/>	<input type="checkbox"/>	27	NBNS from PortShield2	Group				
			▶ LAN Primary Subnet	192.168.168.0/255.255.255.0	Network	LAN		
			▶ PortShield Interface 1 Subnet	192.168.1.0/255.255.255.0	Network	LAN		
			▶ PortShield Interface 3 Subnet	192.168.3.0/255.255.255.0	Network	WLAN		
<input type="checkbox"/>	<input type="checkbox"/>	28	NBNS from PortShield3	Group				
			▶ LAN Primary Subnet	192.168.168.0/255.255.255.0	Network	LAN		
			▶ PortShield Interface 1 Subnet	192.168.1.0/255.255.255.0	Network	LAN		
			▶ PortShield Interface 2 Subnet	192.168.2.0/255.255.255.0	Network	LAN		

Now these groups can be selected as the destinations in the four IP Helper NetBIOS policies you will create for each of our four source subnets.

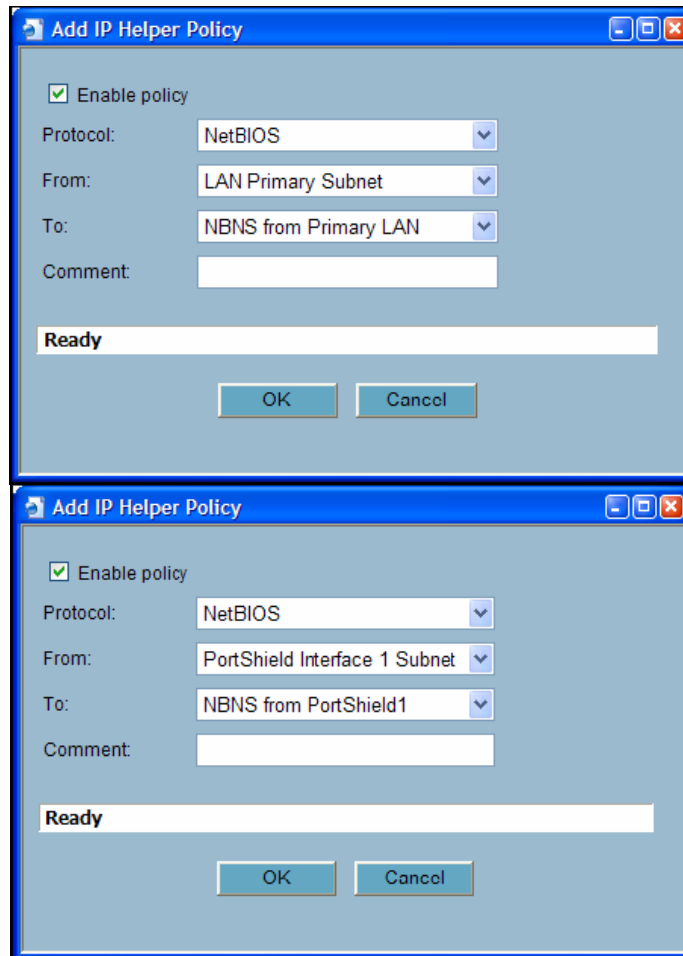


Tech Note

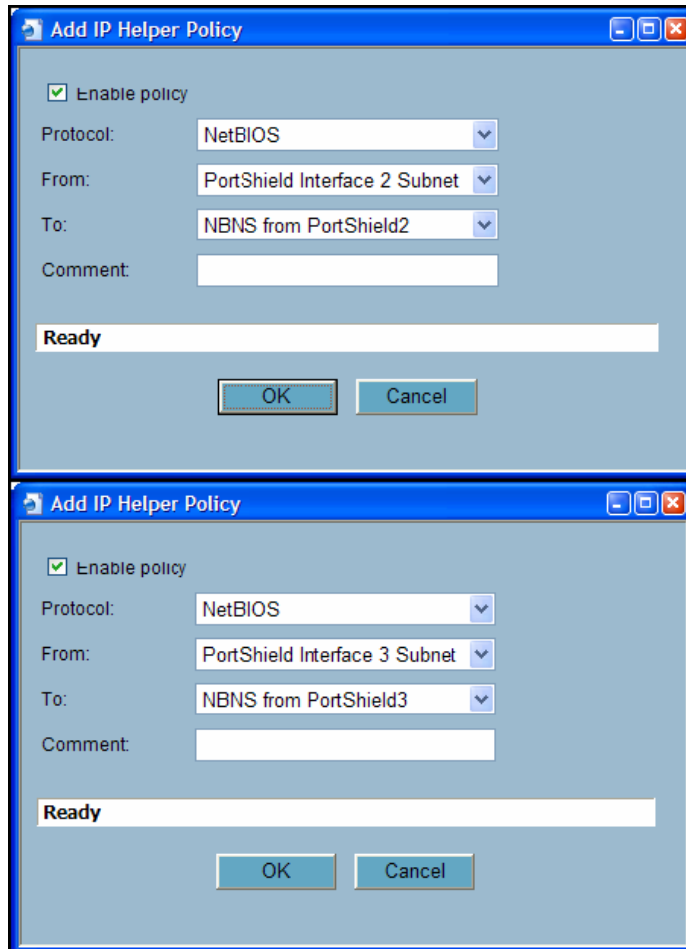
Configuring IP Helper for NetBIOS

To configure the IP Helper, perform the following steps:

- 1) Navigate to the **Network > IP Helper**.
- 2) Select the **Enable IP Helper** checkbox and click **Apply**.
- 3) Select the **Enable NetBIOS Support** checkbox and click **Apply**.
- 4) Click the **Add** button below the IP Helper Policies table, and add the following four policies:

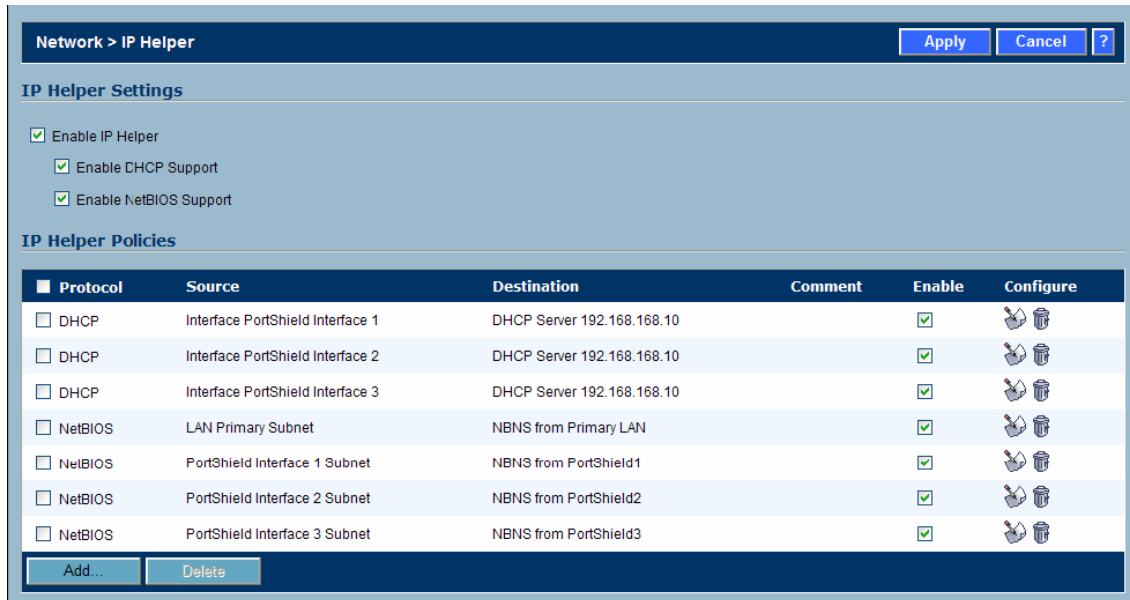


Tech Note



The resulting table will look as follows (DHCP policies from previous section included):

Tech Note



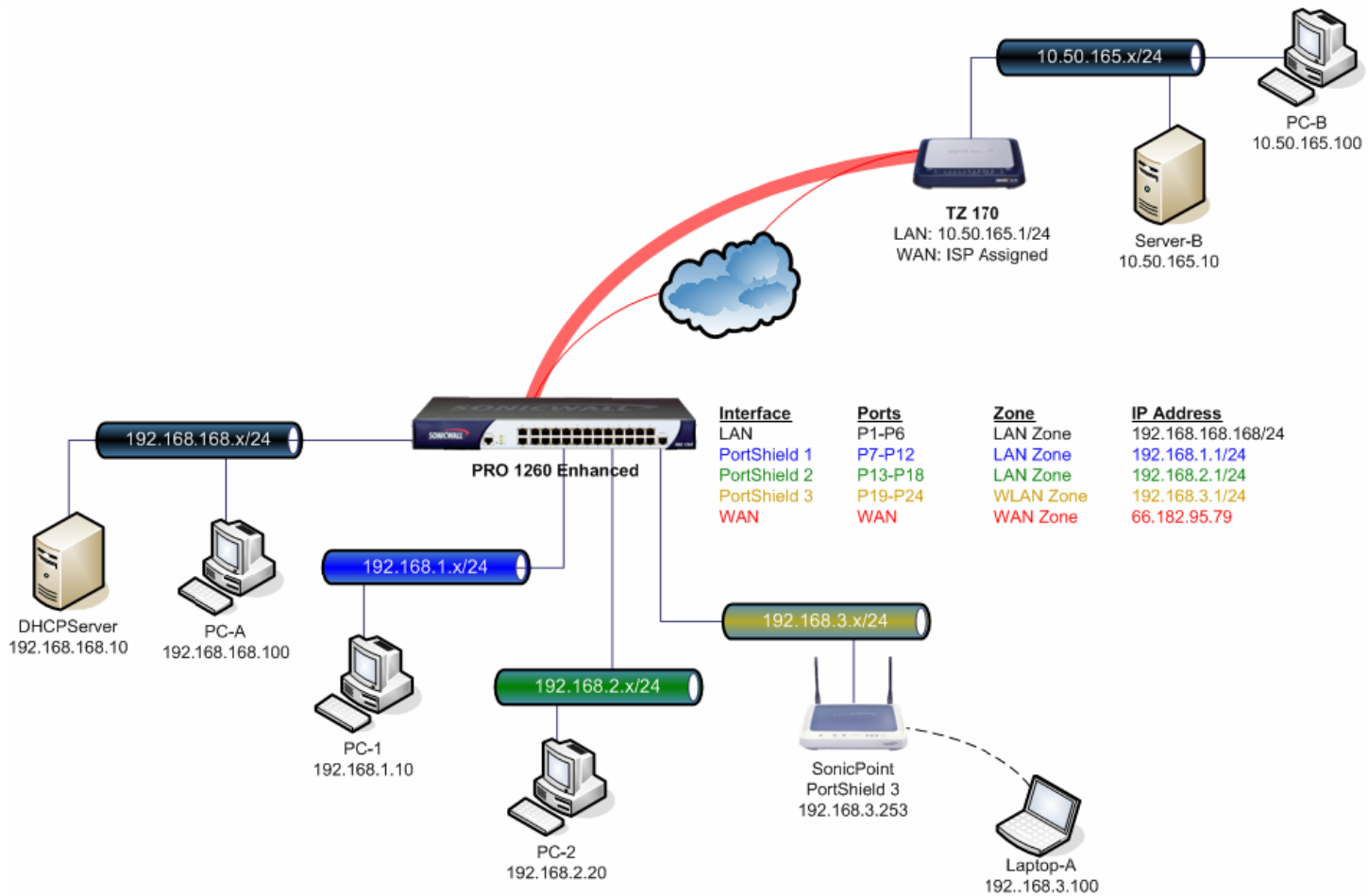
With these policies in place, all NetBIOS broadcast traffic received on any one of the four segments will be relayed to the other 3 segments. For example, NetBIOS broadcast traffic sourced from 'PortShield Interface 1 Subnet' (192.168.1.255) will be translated to:

- 192.168.168.255, and sent out the LAN interface
- 192.168.2.255, and sent out the PortShield2 interface
- 192.168.3.255, and sent out the PortShield3 interface

IP Helper NetBIOS Relay with VPN

VPN Policies will auto-create IP Helper NetBIOS relay policies if the 'Enable Windows Networking (NetBIOS) Broadcast' checkbox is selected on the 'Advanced' tab of the VPN Policy. The source of the IP Helper policy will be the local network selected on the 'Network' tab of the VPN Policy. If your network requires that you forward NetBIOS broadcasts both to VPN destination subnets, as well as to local destination subnets, the 'Enable Windows Networking (NetBIOS) Broadcast' should not be used on the VPN policy. An alternative configuration will be described in this section. Consider the following network:

Tech Note



Here we have the same sample network as was reviewed in the 'IP Helper NetBIOS Relay' section above, but we've added a site-to-site VPN connection. There is a requirement to forward NetBIOS broadcasts among all subnets—both local and remote.

Assume the PRO 1260 Enhanced has a VPN Policy with the local network defined as the Group 'Firewalled Subnets' (which comprises 192.168.168.x, 192.168.1.x, 192.168.2.x, and 192.168.3.x) and a destination network on the '10.50.165.0 Subnet'. The remote TZ 170 has a complementary VPN policy configured.

If the VPN policy on the PRO 1260 Enhanced had the 'Enable Windows Networking (NetBIOS) Broadcast' option selected, that would auto-create the IP Helper NetBIOS policy from 'Firewalled Subnets' to the '10.50.165.0 Subnet' destination Network Address Object. This would preclude any of the 'Firewalled Subnets' from being used in another IP Helper policy for the relaying of NetBIOS traffic among themselves.

Important: If your network requires the relaying of NetBIOS to both local destination subnets and VPN destination subnets, do not select the 'Windows Networking (NetBIOS) Broadcast' option on your VPN policy. If this option is enabled, attempts to create the IP Helper policies for your local networks will fail because of the source overlap. Conversely, attempts to enable this option after the definition of the IP Helper policies for your local networks will result in failure to auto-create the VPN related IP Helper policies. Instead you must manually craft the appropriate destination groups for NetBIOS relaying.

Instead of using the 'Enable Windows Networking (NetBIOS) Broadcast' option on the PRO 1260 Enhanced, the '10.50.165.0 Subnet' Network Address Object should be added to each of the four destination Groups defined in the previous section, resulting in the following:



Tech Note

<input type="checkbox"/>	<input type="checkbox"/>	25 NBNS from Primary LAN	Group				
	▶	10.50.165.0 Subnet	10.50.165.0/255.255.255.224	Network	VPN		
	▶	PortShield Interface 1 Subnet	192.168.1.0/255.255.255.0	Network	LAN		
	▶	PortShield Interface 2 Subnet	192.168.2.0/255.255.255.0	Network	LAN		
	▶	PortShield Interface 3 Subnet	192.168.3.0/255.255.255.0	Network	WLAN		
<input type="checkbox"/>	<input type="checkbox"/>	26 NBNS from PortShield1	Group				
	▶	LAN Primary Subnet	192.168.168.0/255.255.255.0	Network	LAN		
	▶	10.50.165.0 Subnet	10.50.165.0/255.255.255.224	Network	VPN		
	▶	PortShield Interface 2 Subnet	192.168.2.0/255.255.255.0	Network	LAN		
	▶	PortShield Interface 3 Subnet	192.168.3.0/255.255.255.0	Network	WLAN		
<input type="checkbox"/>	<input type="checkbox"/>	27 NBNS from PortShield2	Group				
	▶	LAN Primary Subnet	192.168.168.0/255.255.255.0	Network	LAN		
	▶	10.50.165.0 Subnet	10.50.165.0/255.255.255.224	Network	VPN		
	▶	PortShield Interface 1 Subnet	192.168.1.0/255.255.255.0	Network	LAN		
	▶	PortShield Interface 3 Subnet	192.168.3.0/255.255.255.0	Network	WLAN		
<input type="checkbox"/>	<input type="checkbox"/>	28 NBNS from PortShield3	Group				
	▶	LAN Primary Subnet	192.168.168.0/255.255.255.0	Network	LAN		
	▶	10.50.165.0 Subnet	10.50.165.0/255.255.255.224	Network	VPN		
	▶	PortShield Interface 1 Subnet	192.168.1.0/255.255.255.0	Network	LAN		
	▶	PortShield Interface 2 Subnet	192.168.2.0/255.255.255.0	Network	LAN		

As long as the TZ 170 only requires the forwarding of NetBIOS broadcasts across the VPN (and not to another local subnet, such as the OPT subnet), the 'Enable Windows Networking (NetBIOS) Broadcast' should be used on its VPN policy for the auto-creation of the IP Helper NetBIOS policy.

Related Documents

For more information, refer to the following SonicWALL TechNotes on www.sonicwall.com/support/documentation:

- SonicOS Enhanced: Configuring the SonicWALL DHCP for GVC
- SonicOS Standard: Configuring the SonicWALL DHCP for GVC
- Common Issues with GVC
- SonicOS Enhanced: Using a Secondary Public IP Range for NAT
- Configuring Port Forwarding with the SonicWALL
- Terminating the WAN GroupVPN and Using VPN Access in SonicOS Enhanced
- Terminating the WAN GroupVPN to the LAN/DMZ using SonicOS Standard
- Typical DMZ Setups with FTP, SMTP, and DNS Servers
- Using the SonicOS Enhanced Wizard To Configure a Public Server
- Creating One-to-One NAT Policies in SonicOS Enhanced
- SonicOS Enhanced: Three Types of Network Modes

Document Created: 9/27/06

Document Last Updated: 10/10/06



