

Tech Note

Deploying SonicOS Enhanced L2 Bridge Mode and Transparent Mode

Note: This SonicOS Enhanced feature is currently in development. This document and the features described are subject to change.

Overview of L2 Bridge Mode and Transparent Mode

SonicOS Enhanced introduces **L2 (Layer 2) Bridge Mode**, a new method of unobtrusively integrating a SonicWALL security appliance into any Ethernet network. L2 Bridge Mode is ostensibly similar to SonicOS Enhanced's **Transparent Mode** in that it enables a SonicWALL security appliance to share a common subnet across two interfaces, and to perform stateful and deep-packet inspection on all traversing IP traffic, but it is functionally more versatile.

In particular, L2 Bridge Mode employs a secure learning bridge architecture, enabling it to pass and inspect traffic types that cannot be handled by many other methods of transparent security appliance integration. Using L2 Bridge Mode, a SonicWALL security appliance can be non-disruptively added to any Ethernet network to provide in-line deep-packet inspection for all traversing IPv4 TCP and UDP traffic. Unlike other transparent solutions, L2 Bridge Mode can pass all traffic types, including IEEE 802.1Q VLANs, Spanning Tree Protocol, multicast, broadcast, and IPv6, ensuring that all network communications will continue uninterrupted.

L2 Bridge Mode provides an ideal solution for networks that already have an existing firewall, and do not have immediate plans to replace their existing firewall but wish to add the security of SonicWALL Unified Threat Management (UTM) deep-packet inspection, such as Intrusion Prevention Services, Gateway Anti Virus, and Gateway Anti Spyware. If you do not have SonicWALL UTM security services subscriptions, you may sign up for free trials from the **Security Service > Summary** page of your SonicWALL, and you can obtain more information at: http://www.sonicwall.com/products/gav_ips_spyware.html and <http://www.sonicwall.com/products/cfs.html>

Key Features of SonicOS Enhanced L2 Bridge Mode

Feature	Benefit
L2 Bridging with Deep Packet Inspection	This method of transparent operation means that a SonicWALL security appliance can be added to any network without the need for readdressing or reconfiguration, enabling the addition of deep-packet inspection security services with no disruption to existing network designs. Developed with connectivity in mind as much as security, L2 Bridge Mode can pass all Ethernet frame types, ensuring seamless integration.
Secure Learning Bridge Architecture	True L2 behavior means that all allowed traffic flows natively through the L2 Bridge. Whereas other methods of transparent operation rely on ARP and route manipulation to achieve transparency, which frequently proves problematic, L2 Bridge Mode dynamically learns the topology of the network to determine optimal traffic paths.
Universal Ethernet Frame-Type Support	All Ethernet traffic can be passed across an L2 Bridge, meaning that all network communications will continue uninterrupted. While many other methods of transparent operation will only support IPv4 traffic, L2 Bridge Mode will inspect all IPv4 traffic, and will pass (or block, if desired) all other traffic, including LLC, all Ethertypes, and even proprietary frame formats.
Mixed-Mode Operation	L2 Bridge Mode can concurrently provide L2 Bridging and conventional security appliance services, such as routing, NAT, VPN, and wireless operations. This means it can be used as an L2 Bridge for one segment of the network, while providing a complete set of security services to the remainder of the network. This also allows for the introduction of the SonicWALL security appliance as a pure L2 bridge, with a smooth migration path to full security services operation.

Key Concepts to Configuring L2 Bridge Mode and Transparent Mode

The following terms will be used when referring to the operation and configuration of L2 Bridge Mode:

- **L2 Bridge Mode** – A method of configuring a SonicWALL PRO security appliance (with the exception of the PRO 1260), which enables the SonicWALL to be inserted inline into an existing network with absolute transparency, beyond even that provided by Transparent Mode. Layer 2 Bridge Mode also refers to the *IP Assignment* configuration that is selected for *Secondary Bridge Interfaces* that are placed into a *Bridge-Pair*.
- **Transparent Mode** – A method of configuring a SonicWALL security appliance, introduced in SonicOS Enhanced 2.5, which allows the SonicWALL to be inserted into an existing network without the need for IP reconfiguration by spanning a single IP subnet across two or more interfaces through the use of automatically applied ARP and routing logic.
- **IP Assignment** – When configuring a Trusted (LAN) or Public (DMZ) interface, the IP Assignment for the interface can either be:
 - **Static** – The IP address for the interface is manually entered.
 - **Transparent Mode** – The IP address (es) for the interface is assigned using an Address Object (Host, Range, or Group) that falls within the WAN Primary IP subnet, effectively spanning the subnet from the WAN interface to the assigned interface.
 - **Layer 2 Bridge Mode** – An interface placed in this mode becomes the *Secondary Bridge Interface* to the *Primary Bridge Interface* to which it is paired. The resulting Bridge-Pair will then behave like a two-port learning bridge with full L2 transparency, and all IP traffic that passes through will be subjected to full stateful and deep-packet inspection.
- **Bridge-Pair** – The logical interface set composed of a *Primary Bridge Interface* and a *Secondary Bridge Interface*. The terms primary and secondary do not imply any inherent level of operational dominance or subordination; both interfaces continue to be treated according to their Zone type, and to pass IP traffic according to their configured Access Rules. Non-IPv4 traffic across the Bridge-Pair is controlled by the *Block all non-IPv4 traffic* setting on the *Secondary Bridge Interface*. A system may support as many Bridge Pairs as it has interface pairs available. In other words, the maximum number of Bridge-Pairs is equal to ½ the number of physical interfaces on the platform. Membership in a Bridge-Pair does not preclude an interface from conventional behavior; for example, if X1 is configured as a *Primary Bridge Interface* paired to X3 as a *Secondary Bridge Interface*, X1 can simultaneously operate in its traditional role as the Primary WAN, performing NAT for Internet-bound traffic through the *Auto-added X1 Default NAT Policy*.
- **Primary Bridge Interface** – A designation that is assigned to an interface once a *Secondary Bridge Interface* has been paired to it. A Primary Bridge Interface can belong to an Untrusted (WAN), Trusted (LAN), or Public (DMZ) Zone.
- **Secondary Bridge Interface** – A designation that is assigned to an interface whose *IP Assignment* has been configured for *Layer 2 Bridge Mode*. A Secondary Bridge Interface can belong to a Trusted (LAN), or Public (DMZ) Zone.
- **Bridge Management Address** – The address of the Primary Bridge Interface is shared by both interfaces of the *Bridge-Pair*. If the Primary Bridge Interface also happens to be the Primary WAN interface, it is this address that is used for outbound communications by the SonicWALL, such as NTP, and License Manager updates. Hosts that are connected to either segment of the Bridge-Pair may also use the Bridge Management Address as their gateway, as will be common in *Mixed-Mode* deployments.
- **Bridge-Partner** – The term used to refer to the 'other' member of a *Bridge-Pair*.
- **Non-IPv4 Traffic** - SonicOS Enhanced supports the following IP protocol types: ICMP (1), IGMP (2), TCP (6), UDP (17), GRE (47), ESP (50), AH (51), EIGRP (88), OSPF (89), PIM-SM (103), L2TP (115). More esoteric IP types, such as Combat Radio Transport Protocol (126), are not natively handled by the SonicWALL, nor are non-IPv4 traffic types such as IPX or (currently) IPv6. L2 Bridge Mode can be configured to either pass or drop Non-IPv4 traffic.
- **Captive-Bridge Mode** – This optional mode of L2 Bridge operation prevents traffic that has entered an L2 bridge from being forwarded to a non-Bridge-Pair interface. By default, L2 Bridge logic will forward traffic that has entered the L2 Bridge to its destination along the most optimal path as determined by ARP and routing tables. In some cases, the most optimal path might involve routing or NATing to a non-Bridge-Pair interface. Activating Captive-Bridge mode ensures that traffic which enters an L2 Bridge exits the L2 Bridge rather than taking its most logically optimal path. In general, this mode of operation is only required in complex networks with redundant paths, where strict path adherence is required.
- **Pure L2 Bridge Topology** – Refers to deployments where the SonicWALL will be used strictly in *L2 Bridge Mode* for the purposes of providing in-line security to a network. This means that all traffic entering one side of the *Bridge-Pair* will be bound for the other side, and will not be routed/NATed through a different interface. This will be common in cases where there is an existing perimeter security appliance, or where in-line security is desired along some path (for example, inter-departmentally, or on a trunked link between two switches) of an existing network. Pure L2 Bridge Topology is not a functional limitation, but rather a topological description of a common deployment in heterogeneous environments.
- **Mixed-Mode Topology** – Refers to deployments where the *Bridge-Pair* will not be the only point of ingress/egress through the SonicWALL. This means that traffic entering one side of the *Bridge-Pair*

Tech Note

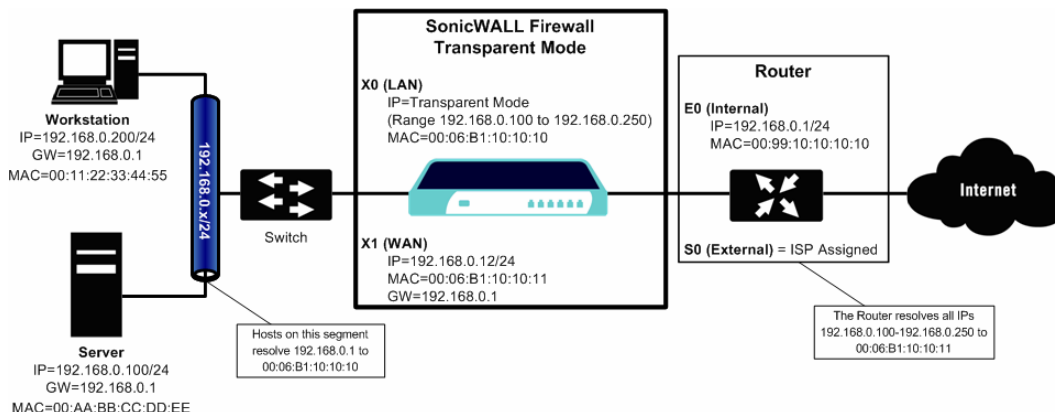
Pair may be destined to be routed/NATed through a different interface. This will be common when the SonicWALL is simultaneously used to provide security to one or more Bridge-Pair while also providing:

- o Perimeter security, such as WAN connectivity, to hosts on the Bridge-Pair or on other interfaces.
- o Firewall and Security services to additional segments, such as Trusted (LAN) or Public (DMZ) interface, where communications will occur between hosts on those segments and hosts on the Bridge-Pair.
- o Wireless services with SonicPoints, where communications will occur between wireless clients and hosts on the Bridge-Pair.

Comparing L2 Bridge Mode to Transparent Mode

While Transparent Mode allows a security appliance running SonicOS Enhanced to be introduced into an existing network without the need for re-addressing, it presents a certain level of disruptiveness, particularly with regard to ARP, VLAN support, multiple subnets, and non-IPv4 traffic types. Consider the diagram below, in a scenario where a Transparent Mode SonicWALL appliance has just been added to the network with a goal of minimally disruptive integration, particularly:

- Negligible or no unscheduled downtime
- No need to re-address any portion of the network
- No need reconfigure or otherwise modify the gateway router (as is common when the router is owned by the ISP)



ARP in Transparent Mode

ARP – Address Resolution Protocol (the mechanism by which unique hardware addresses on network interface cards are associated to IP addresses) is *proxied* in Transparent Mode. If the Workstation on Server on the left had previously resolved the Router (192.168.0.1) to its MAC address 00:99:10:10:10:10, this cached ARP entry would have to be cleared before these hosts could communicate through the SonicWALL. This is because the SonicWALL proxies (or answers on behalf of) the gateway's IP (192.168.0.1) for hosts connected to interfaces operating in Transparent Mode. So when the Workstation at the left attempts to resolve 192.168.0.1, the ARP request it sends is responded to by the SonicWALL with its own X0 MAC address (00:06:B1:10:10:10).

The SonicWALL also proxy ARPs the IP addresses specified in the Transparent Range (192.168.0.100 to 192.168.0.250) assigned to an interface in Transparent Mode for ARP requests received on the X1 (Primary WAN) interface. If the Router had previously resolved the Server (192.168.0.100) to its MAC address 00:AA:BB:CC:DD:EE, this cached ARP entry would have to be cleared before the router could communicate with the host through the SonicWALL. This typically requires a flushing of the router's ARP cache either from its management interface or through a reboot. Once the router's ARP cache is cleared, it can then send a new ARP request for 192.168.0.100, to which the SonicWALL will respond with its X1 MAC 00:06:B1:10:10:11.

VLAN Support in Transparent Mode

While the network depicted in the above diagram is simple, it is not uncommon for larger networks to use VLANs for segmentation of traffic. If this were such a network, where the link between the switch and the router was a VLAN trunk, a Transparent Mode SonicWALL would have been able to terminate the VLANs to sub-interfaces on either side of the link, but it would have required unique addressing; that is, non-Transparent Mode operation requiring re-addressing on at least one side. This is because only the Primary WAN interface can be used as the *source* for Transparent Mode address space.

Multiple Subnets in Transparent Mode

It is also common for larger networks to employ multiple subnets, be they on a single wire, on separate VLANs, multiple wires, or some combination. While Transparent Mode is capable of supporting multiple subnets through



Tech Note

the use of Static ARP and Route entries, as the Technote

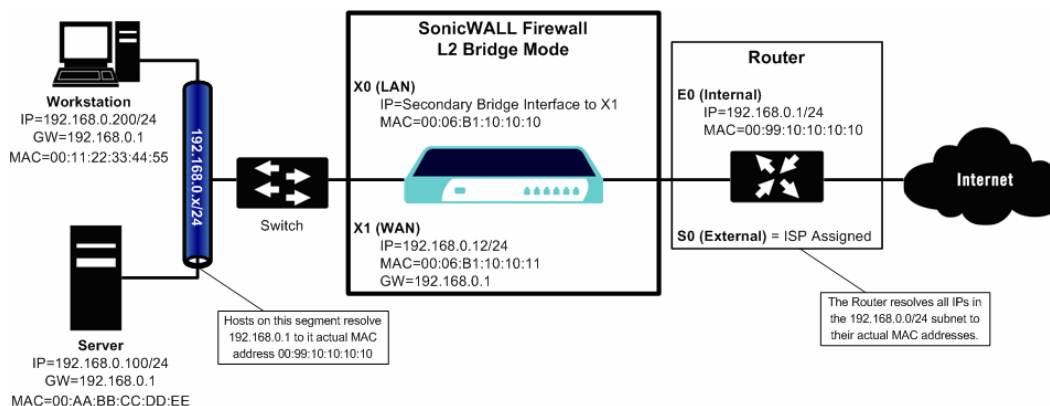
http://www.sonicwall.com/support/pdfs/technotes/supporting_multiple_firewalled_subnets_on_sonicos_enhanced.pdf describes, it is not an effortless process.

Non-IPv4 Traffic in Transparent Mode

Transparent Mode will drop (and generally log) all non-IPv4 traffic, precluding it from passing other traffic types, such as IPX, or unhandled IP types.

L2 Bridge Mode addresses these common Transparent Mode deployment issues and is described in the following section.

Simple L2 Bridge Topology



ARP in L2 Bridge Mode

L2 Bridge Mode employs a learning bridge design where it will dynamically determine which hosts are on which interface of an L2 Bridge (referred to as a Bridge-Pair). ARP is passed through natively, meaning that a host communicating across an L2 Bridge will see the actual host MAC addresses of their peers. For example, the Workstation communicating with the Router (192.168.0.1) will see the router as 00:99:10:10:10:10, and the Router will see the Workstation (192.168.0.100) as 00:AA:BB:CC:DD:EE.

This behavior allows for a SonicWALL operating in L2 Bridge Mode to be introduced into an existing network with no disruption to most network communications other than that caused by the momentary discontinuity of the physical insertion.

It should be noted that stream-based TCP protocols communications (for example, an FTP session between a client and a server) will need to be re-established upon the insertion of an L2 Bridge Mode SonicWALL. This is by design so as to maintain the security afforded by stateful packet inspection (SPI); since the SPI engine can not have knowledge of the TCP connections which pre-existed it, it will drop these *established* packets with a log event such as *TCP packet received on non-existent/closed connection; TCP packet dropped*.

VLAN Support in L2 Bridge Mode

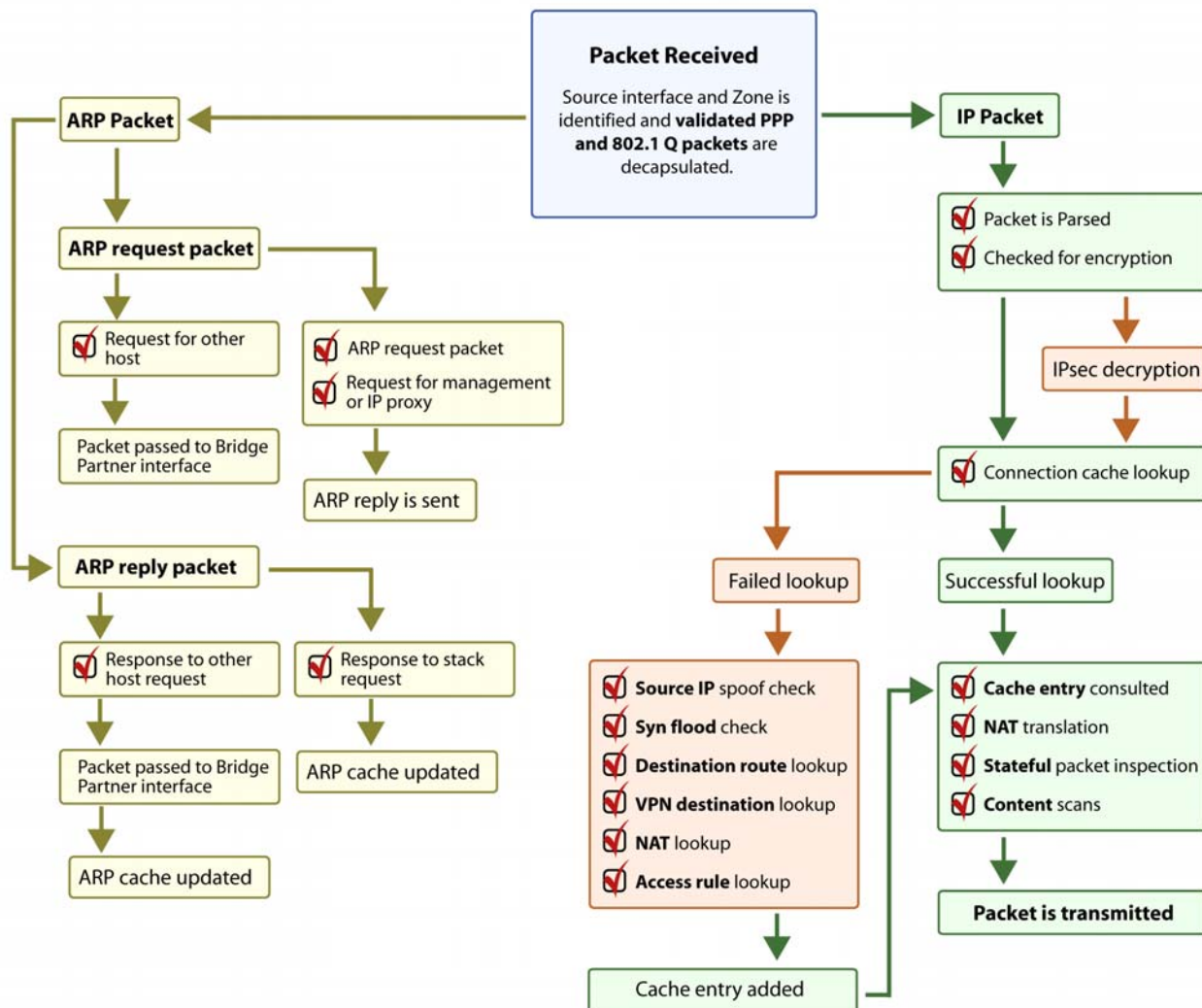
L2 Bridge Mode provides fine control over 802.1Q VLAN traffic traversing an L2 Bridge. The default handling of VLANs is to allow and preserve all 802.1Q VLAN tags as they pass through an L2 Bridge, while still applying all firewall rules, and stateful and deep-packet inspection to the encapsulated traffic. It is further possible to specify white/black lists for allowed/disallowed VLAN IDs through the L2 Bridge.

This allows a SonicWALL operating in L2 Bridge Mode to be inserted, for example, inline into a VLAN trunk carrying any number of VLANs, and to provide full security services to all IPv4 traffic traversing the VLAN without the need for explicit configuration of any of the VLAN IDs or subnets. Firewall Access Rules can also, optionally, be applied to all VLAN traffic passing through the L2 Bridge Mode because of the method of handling VLAN traffic.

Tech Note

L2 Bridge IP Packet Path

The following is an overview of the L2 Bridge packet path:



- 802.1Q encapsulated frame enters an L2 Bridge interface (this first step, the next step, and the final step apply only to 802.1Q VLAN traffic)
- The 802.1Q VLAN ID is checked against the VLAN ID white/black list:
 - If the VLAN ID is disallowed, the packet is dropped and logged.
 - If the VLAN ID is allowed, the packet is de-capsulated, the VLAN ID is stored, and the inner packet (including the IP header) is passed through the full packet handler.
- Since any number of subnets is supported by L2 Bridging, no source IP spoof checking is performed on the source IP of the packet. It is possible to configure L2 Bridges to only support a certain subnet or subnets using Firewall Access Rules.
- SYN Flood checking is performed.
- A destination route lookup is performed to the destination Zone, so that the appropriate Firewall Access rule can be applied. Any Zone is a valid destination, including the same Zone as the source Zone (e.g. LAN to LAN), the Untrusted Zone (WAN), the Encrypted (VPN), Wireless (WLAN), Multicast, or custom Zones of any type.

Tech Note

- A NAT lookup is performed and applied, as needed.
 - In general, the destination for packets entering an L2 Bridge will be the *Bridge-Partner* interface (that is, the other side of the bridge). In these cases, no translation will be performed.
 - If Captive-Bridge mode (Never route traffic on this bridge-pair) is enabled, the traffic will always be forwarded through to the Bridge-Partner.
 - In cases where the L2 Bridge Management Address is the gateway, as will sometimes be the case in *Mixed-Mode topologies*, then NAT will be applied as need (see the **L2 Bridge Path Determination** section for more details).
- Firewall Access Rules are applied to the packet. For example, the following packet decode shows an ICMP packet bearing VLAN ID 10, source IP address 110.110.110.110 destined for IP address 4.2.2.1.

```
⊞ Frame 219 (102 bytes on wire, 102 bytes captured)
⊞ Ethernet II, Src: 08:00:46:a2:eb:4d (08:00:46:a2:eb:4d), Dst: 99:88:77:66:55:44 (99:88:77:66:55:44)
⊞ 802.1Q Virtual LAN
    000. .... = Priority: 0
    ...0 .... = CFI: 0
    .... 0000 0000 1010 = ID: 10
    Type: IP (0x0800)
⊞ Internet Protocol, Src: 110.110.110.110 (110.110.110.110), Dst: 4.2.2.1 (4.2.2.1)
⊞ Internet Control Message Protocol
```

It is possible to construct a Firewall Access Rule to control any IP packet, independent of its VLAN membership, by any of its IP elements, such as source IP, destination IP, or service type. If the packet is disallowed, it will be dropped and logged. If the packet is allowed, it will continue.

- A connection cache entry is made for the packet, and required NAT translations (if any) are performed.
- Stateful packet inspection and transformations are performed for TCP, VoIP, FTP, MSN, Oracle, RTSP and other media streams, PPTP and L2TP. If the packet is disallowed, it will be dropped and logged. If the packet is allowed, it will continue.
- Deep packet inspection, including GAV, IPS, Anti-Spyware, CFS and email-filtering is performed. If the packet is disallowed, it will be dropped and logged. If the packet is allowed, it will continue. Client notification will be performed as configured.
- If the packet is destined for the Encrypted Zone (VPN), the Untrusted Zone (WAN), or some other connected interface (the last two of which might be the case in Mixed-Mode Topologies) the packet will be sent via the appropriate path.
- If the packet is not destined for the VPN/WAN/Connected interface, the stored VLAN tag will be restored, and the packet (again bearing the original VLAN tag) will be sent out the *Bridge-Partner* interface.

Multiple Subnets in L2 Bridge Mode

L2 Bridge Mode is capable of handling any number of subnets across the bridge, as described above. The default behavior is to allow all subnets, but Access Rules can be applied to control traffic as needed.

Non-IPv4 Traffic in L2 Bridge Mode

Unsupported traffic will, by default, be passed from one L2 Bridge interface to the Bridge-Partner interface. This allows the SonicWALL to pass other traffic types, including LLC packets such as Spanning Tree, other EtherTypes, such as MPLS label switched packets (EtherType 0x8847), Appletalk (EtherType 0x809b), and the ever-popular Banyan Vines (EtherType 0xbad). These non-IPv4 packets will only be passed across the Bridge, they will not be inspected or controlled by the packet handler. If these traffic types are not needed or desired, the bridging behavior can be changed by enabling the **Block all non-IPv4 traffic** option on the *Secondary Bridge Interface* configuration page.

Tech Note

Comparison of L2 Bridge Mode to Transparent Mode

	L2 Bridge Mode	Transparent Mode
Layer of Operation	Layer 2 (MAC)	Layer 3 (IP)
ARP behavior	ARP (Address Resolution Protocol) information is unaltered. MAC addresses natively traverse the L2 bridge. Packets that are destined for SonicWALL's MAC addresses will be processed, others will be passed, and the source and destinations will be learned and cached.	ARP is proxied by the interfaces operating in Transparent Mode.
Path determination	Hosts on either side of a Bridge-Pair are dynamically learned. There is no need to declare interface affinities.	The Primary WAN interface is always the master ingress/egress point for Transparent mode traffic, and for subnet space determination. Hosts transparently sharing this subnet space must be explicitly declared through the use of Address Object assignments.
Maximum interfaces	Two interfaces, a Primary Bridge Interface and a Secondary Bridge Interface.	Two or more interfaces. The master interface is always the Primary WAN. There can be as many transparent subordinate interfaces as there are interfaces available.
Maximum pairings	The maximum number of Bridge-Pairs allowed is limited only by available physical interfaces. For example, a PRO 2040 could have two Bridge-Pairs (X1+X0, X2+X3), and a PRO 4100 could have five Bridge-Pairs, etc. This can be described as "many one-to-one pairings".	Transparent Mode only allows the Primary WAN subnet to be spanned to other interfaces, although it allows for multiple interfaces to simultaneously operate as transparent partners to the Primary WAN. This can be described as "a single one-to-one" or "a single one-to-many pairing".
Zone restrictions	The Primary Bridge Interface can be Untrusted, Trusted, or Public. The Secondary Bridge Interface can be Trusted or Public.	Interfaces in a Transparent Mode pair must consist of one Untrusted interface (the Primary WAN, as the master of the pair's subnet) and one or more Trusted/Public interface (e.g. LAN or DMZ).
Subnets supported	Any number of subnets is supported. Firewall Access Rules can be written to control traffic to/from any of the subnets as needed.	In its default configuration, Transparent Mode only supports a single subnet (that which is assigned to, and spanned from the Primary WAN). It is possible to manually add support for additional subnets through the use of ARP entries and routes.
Non-IPv4 Traffic	All non-IPv4 traffic, by default, is bridged from one Bridge-Pair interface to the Bridge-Partner interface, unless disabled on the Secondary Bridge Interface configuration page. This includes IPv6 traffic, STP (Spanning Tree Protocol), and unrecognized IP types.	Non IPv4 traffic is not handled by Transparent Mode, and is dropped and logged.
VLAN traffic	VLAN traffic is passed through the L2 Bridge, and is fully inspected by the Stateful and Deep Packet Inspection engines.	VLAN sub-interfaces can be created and can be given Transparent Mode Address Object assignments, but the VLANs will be terminated by the SonicWALL rather than passed.
VLAN sub-interfaces	VLAN sub-interfaces can be configured on Bridge-Pair interfaces, but they will be passed through the bridge to the Bridge-Partner unless the destination IP address in the VLAN frame matches the IP address of the VLAN sub-interface on the SonicWALL, in which case it will be processed (e.g. as management traffic).	VLAN sub-interfaces can be assigned to physical interfaces operating in Transparent Mode, but their mode of operation will be independent of their parent. These VLAN sub-interfaces can also be given Transparent Mode Address Object assignments, but in any event VLAN sub-interfaces will be terminated rather than passed.
PortShield interfaces	PortShield interfaces cannot be assigned to either interface of an L2 Bridge Pair.	PortShield interfaces may be assigned a Transparent Mode range.
Dynamic addressing	Although a Primary Bridge Interface may be assigned to the WAN Zone, only static addressing is allowable for Primary Bridge Interfaces.	Although Transparent Mode employs the Primary WAN as a master interface, only static addressing is allowable for Transparent Mode.
VPN support	VPN operation is supported with no special configuration requirements.	VPN operation is supported with no special configuration requirements.

Tech Note

	L2 Bridge Mode	Transparent Mode
DHCP support	DHCP can be passed through a Bridge-Pair.	Interfaces operating in Transparent Mode can provide DHCP services, or they can pass DHCP using IP Helper.
Routing and NAT	Traffic will be intelligently routed in/out of the L2 Bridge-Pair from/to other paths. By default, traffic will not be NATed from one Bridge-Pair interface to the Bridge-Partner, but it can be NATed to other paths, as needed. Custom routes and NAT policies can be added as needed.	Traffic will be intelligently routed from/to other paths. By default, traffic will not be NATed from/to the WAN to/from Transparent Mode interface, but it can be NATed to other paths, as needed. Custom routes and NAT policies can be added as needed.
Stateful Packet Inspection	Full stateful packet inspection will be applied to all IPv4 traffic traversing the L2 Bridge, for all subnets, including VLAN traffic.	Full stateful packet inspection will be applied to traffic from/to the subnets defined by Transparent Mode Address Object assignment.
Security services	All security services (GAV, IPS, Anti-Spy, CFS) are fully supported. All regular IP traffic, as well as all 802.1Q encapsulated VLAN traffic.	All security services (GAV, IPS, Anti-Spy, CFS) are fully supported from/to the subnets defined by Transparent Mode Address Object assignment.
Broadcast traffic	Broadcast traffic is passed from the receiving Bridge-Pair interface to the Bridge-Partner interface.	Broadcast traffic is dropped and logged, with the possible exception of NetBIOS which can be handled by IP Helper.
Multicast traffic	Multicast traffic is inspected and passed across L2 Bridge-Pairs providing Multicast has been activated on the Firewall > Multicast page. It is not dependent upon IGMP messaging, nor is it necessary to enable multicast support on the individual interfaces.	Multicast traffic, with IGMP dependency, is inspected and passed by Transparent Mode providing Multicast has been activated on the Firewall > Multicast page, and multicast support has been enabled on the relevant interfaces.

Benefits of Transparent Mode over L2 Bridge Mode

The following are circumstances in which *Transparent Mode* might be preferable over *L2 Bridge Mode*:

- Two interfaces are the maximum allowed in an L2 Bridge Pair. If more than two interfaces are required to operate on the same subnet, Transparent Mode should be considered.
- PortShield interface may not operate within an L2 Bridge Pair. If PortShield interfaces are required to operate on the same subnet, Transparent Mode should be considered.
- VLAN sub-interfaces may not operate within an L2 Bridge Pair. If VLAN sub-interfaces are required to operate on the same subnet, Transparent Mode should be considered. It is, however, possible to configure a VLAN sub-interface on an interface that is part of a Bridge-Pair; the sub-interface will simply operate independently on the Bridge-Pair in every respect.

Comparing L2 Bridge Mode to the CSM Appliance

L2 Bridge Mode is more similar in function to the CSM than it is to Transparent Mode, but it differs from the current (SonicOS CF 2.x Software) CSM behavior in that it handles VLANs and non-IPv4 traffic types, which the CSM does not. Future versions of the SonicOS CF Software for the CSM will likely adopt the more versatile traffic handling capabilities of L2 Bridge Mode.

L2 Bridge Path Determination

Packets received by the SonicWALL on **non-Captive-Bridge mode Bridge-Pair interfaces will be forwarded along the appropriate and optimal path** toward their destination, whether that path is the Bridge-Partner, some other physical or sub interface, or a VPN tunnel. Similarly, packets arriving from other paths (physical, virtual or VPN) bound for a host on a Bridge-Pair must be sent out over the correct Bridge-Pair interface. The following summary describes, in order, the logic that is applied to path determinations for these cases:

1. If present, the most specific *non-default* route to the destination is chosen. This would cover, for example:
 - a. A packet arriving on X3 (non-L2 Bridge LAN) destined for host 15.1.1.100 subnet, where a route to the 15.1.1.0/24 subnet exists through 192.168.0.254 via the X0 (Secondary Bridge Interface, LAN) interface. The packet would be forwarded via X0 to the destination MAC address of 192.168.0.254, with the destination IP address 15.1.1.100.
 - b. A packet arriving on X4 (Primary Bridge Interface, LAN) destined for host 10.0.1.100, where a route to the 10.0.1.0/24 exists through 192.168.10.50 via the X5 (DMZ) interface. The packet would be forwarded via X5 to the destination MAC address of 192.168.10.50, with the destination IP address 10.0.1.100.
2. If no specific route to the destination exists, an ARP cache lookup is performed for the destination IP address. A match will indicate the appropriate destination interface. This would cover, for example:
 - a. A packet arriving on X3 (non-L2 Bridge LAN) destined for host 192.168.0.100 (residing on L2 Primary Bridge Interface X2). The packet would be forwarded via X2 to the known destination MAC and IP address of 192.168.0.100, as derived from the ARP cache.
 - b. A packet arriving on X4 (Primary Bridge Interface, LAN) destined for host 10.0.1.10 (residing on X5 – DMZ). The packet would be forwarded via X5 to the known destination MAC and IP address of 10.0.1.10, as derived from the ARP cache.
3. If no ARP entry is found:
 - a. If the packet arrived on a Bridge-Pair interface, it will be sent to the Bridge-Partner interface.
 - b. If the packet arrived from some other path, the SonicWALL will send an ARP request out both interfaces of the Bridge-Pair to determine on which segment the destination IP resides.

In this last case, since the destination is unknown until after an ARP response is received, the destination Zone also remains unknown until that time. This precludes the SonicWALL from being able to apply the appropriate Access Rule until after path determination is completed. Upon completion, the correct Access Rule will be applied to subsequent related traffic.

With regard to address translation (NAT) of traffic arriving on an L2 Bridge-Pair interface:

- If it is determined to be bound for the Bridge-Partner interface, no IP translation (NAT) will be performed.
- If it is determined to be bound for a different path, appropriate NAT policies will apply:
 - If the path is another connected (local) interface, there will likely be no translation. That is, it will effectively be routed as a result of hitting the *last-resort* Any->Original NAT Policy.
 - If the path is determined to be via the WAN (which will be common in the case of Mixed-Mode topologies, such as that depicted in the **Internal Security** example on page 13) then the default Auto-added *[interface] outbound NAT Policy for X1 WAN* will apply, and the packet's source will be translated for delivery to the Internet.

Captive-Bridge Mode

Enabling Captive-Bridge Mode ((Never route traffic on this bridge-pair) on a Bridge-Pair forces all traffic entering an L2 Bridge interface to exit through the Bridge-Partner interface, even if there is a more logically optimal path. This mode of operation is designed to accommodate certain complex network environments, characterized by redundant paths.

For example, assume a Bridge-Pair of X0 and X1, and interface X3 (DMZ) configured as 10.1.1.1. When operating in Captive-Bridge mode, a packet arriving on X0 (Secondary Bridge Interface, LAN) destined for host 10.1.1.100 (directly connected to X3) will be forwarded out X1 (Bridge-Partner) despite X3 being the more optimal path. Delivery of that packet to the destination (10.1.1.100) will then depend on some device (e.g. a router) connected to the X1 segment of the L2 Bridge.

In general, Captive-Bridge mode should not be enabled on a Bridge-Pair unless there is an explicit need to override L2 Bridge Mode's path selection logic, and to force all traffic that enters an L2 Bridge to remain strictly on the bridge's physical segments.

L2 Bridge Interface Zone Selection

Bridge-Pair interface Zone assignment should be done according to your network's traffic flow requirements. Unlike Transparent Mode, which imposes a system of "more trusted to less trusted" by requiring that the source interface be the Primary WAN, and the transparent interface be Trusted or Public, L2 Bridge mode allows for greater control of operational levels of trust. Specifically, L2 Bridge Mode allows for the *Primary* and *Secondary Bridge Interfaces* to be assigned to the same or different Zones (e.g. LAN+LAN, LAN+DMZ, WAN+CustomLAN, etc.) This will affect not only the default Access Rules that are applied to the traffic, but also the manner in which Deep Packet Inspection security services are applied to the traffic traversing the bridge. Important areas to consider when choosing and configuring interfaces to use for in a Bridge-Pair are Security Services, Access Rules, and WAN connectivity:

Security Services Directionality

As it will be one of the primary employments of L2 Bridge mode, understanding the application of security services is important to the proper Zone selection for Bridge-Pair interfaces. Security services applicability is based on the following criteria:

1. **The direction of the service:**
 - o GAV is primarily an Inbound service, inspecting inbound HTTP, FTP, IMAP, SMTP, POP3, and TCP Streams. It also has an additional Outbound element for SMTP.
 - o Anti Spyware is also primarily Inbound, inspecting inbound HTTP, FTP, IMAP, SMTP, POP3 for the delivery (i.e. retrieval) of Spyware components as generally recognized by their class IDs.
 - o It also has an additional Outbound component, where Outbound is used relative to the directionality (namely, Outgoing) ascribed to it by the IPS signatures that trigger the recognition of these Spyware components. The Outgoing classifier (described in the table below) is used because these components are generally retrieved by the client (e.g. LAN host) via HTTP from a web-server on the internet (WAN host). Referring to the table below, that would be an *Outgoing* connection, and requires a signature with an Outgoing directional classification.
 - o IPS has three directions: Incoming, Outgoing, and Bidirectional. Incoming and Outgoing are described in the table below, and Bidirectional refers to all points of intersection on the table.
 - o For additional accuracy, other elements are also considered, such as the state of the connection (e.g. SYN or Established), and the source of the packet relative to the flow (i.e. initiator or responder).
2. **The direction of the traffic.** The direction of the traffic as it pertains to IPS is primarily determined by the Source and Destination Zone of the traffic flow. When a packet is received by the SonicWALL, its source Zone is generally immediately known, and its destination Zone is quickly determined by doing a route (or VPN) lookup. Based on the source and destination, the packet's directionality is categorized as either *Incoming* or *Outgoing*, (not to be confused with Inbound and Outbound) where the following criteria is used to make the determination:

Dest Src	Untrusted	Public	Wireless	Encrypted	Trusted	Multicast
Untrusted	Incoming	Incoming	Incoming	Incoming	Incoming	Incoming
Public	Outgoing	Outgoing	Outgoing	Incoming	Incoming	Incoming
Wireless	Outgoing	Outgoing	Trust	Trust	Trust	Incoming
Encrypted	Outgoing	Outgoing	Trust	Trust	Trust	Outgoing
Trusted	Outgoing	Outgoing	Trust	Trust	Trust	Outgoing

Table data is subject to change.

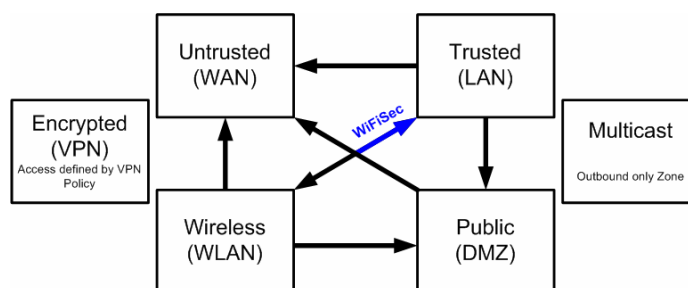
In addition to this categorization, packets traveling to/from Zones with levels of additional trust, which are inherently afforded heightened levels of security (LAN|Wireless|Encrypted<-->LAN|Wireless|Encrypted) are given the special *Trust* classification. Traffic with the Trust classification has all signatures applied (Incoming, Outgoing, and Bidirectional).

Tech Note

3. **The direction of the signature.** This pertains primarily to IPS, where each signature is assigned a direction by SonicWALL's signature development team. This is done as an optimization to minimize false positives. Signature directions are:
 - o Incoming – Applies to *Incoming* and *Trust*. The majority of signatures are Incoming, and they include all forms of application exploits and all enumeration and footprinting attempts. Approximately 85% of signatures are Incoming.
 - o Outgoing – Applies to *Outgoing* and *Trust*. Examples of Outgoing signatures would include IM and P2P login attempts, and responses to successfully launched exploits (e.g. Attack Responses). Approximately 10% of signatures are Outgoing.
 - o Bidirectional – Applies to all. Examples of Bidirectional signatures would include IM file transfers, various NetBIOS attacks (e.g. Sasser communications) and a variety of DoS attacks (e.g. UDP/TCP traffic destined to port 0). Approximately 5% of signatures are Bidirectional.
4. **Zone application.** For a signature to be triggered, the desired security service *must be active on at least one of the Zones it traverses*. For example, a host on the internet (X1, WAN) accessing a Microsoft Terminal Server (on X3, Secondary Bridge Interface, LAN) will trigger the *Incoming* signature "IPS Detection Alert: MISC MS Terminal server request, SID: 436, Priority: Low" if IPS is active on the *WAN*, the *LAN*, or both.

Access Rule Defaults

Default, zone-to-zone Access Rules. The default Access Rules should be considered, although they can be modified as needed. The defaults are as follows:



WAN Connectivity

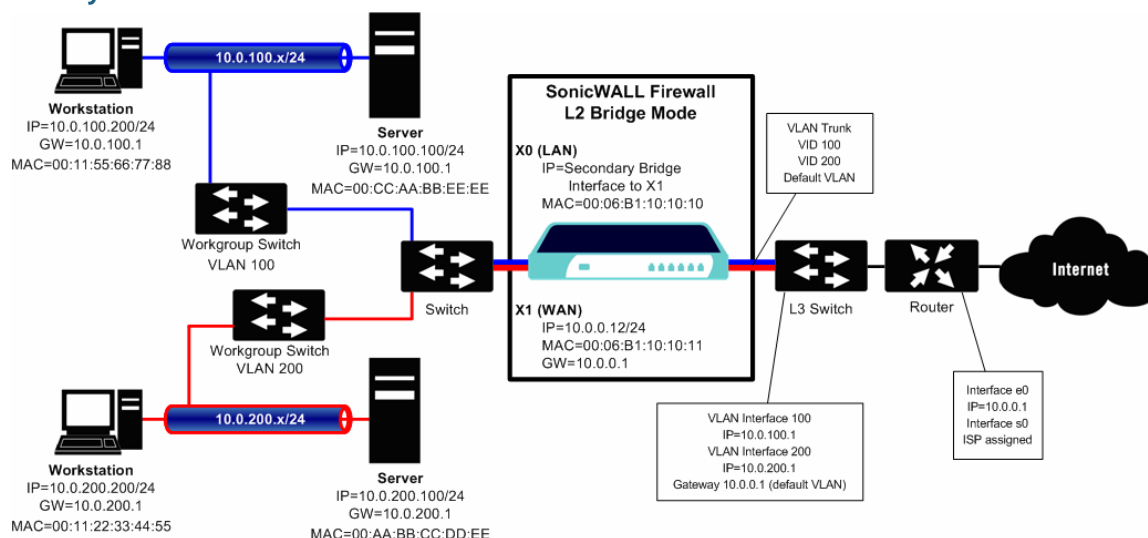
Internet (WAN) connectivity is required¹ for *stack* communications, such as licensing, security services signature downloads, NTP (time synchronization), and CFS (Content Filtering Services). At present, these communications can only occur through the Primary WAN interface. If you require these types of communication, the Primary WAN should have a path to the Internet. Whether or not the Primary WAN is employed as part of a Bridge-Pair will not affect its ability to provide these stack communications (for example on a PRO 4100, X0+X2 and X3+X4 could be used to create two Bridge-Pairs separate of X1).

¹ If Internet connectivity is not available, licensing can be performed manually (http://www.sonicwall.com/support/pdfs/technotes/Manual_Upgrade_Closed_Environments_Technote.pdf) and signature updates can also be performed manually (http://www.sonicwall.com/support/pdfs/Configuring_Manual_Signature_Updates.pdf).

Sample Topologies

The following are sample topologies depicting common deployments. **Perimeter Security** represents the addition of a SonicWALL security appliance in *pure L2 bridge-mode* to an existing network, where the SonicWALL is placed near the perimeter of the network. **Internal Security**, illustrated on page 13, represents the full integration of a SonicWALL security appliance in *mixed-mode*, where it provides simultaneous L2 bridging, WLAN services, and NATed WAN access.

Perimeter Security



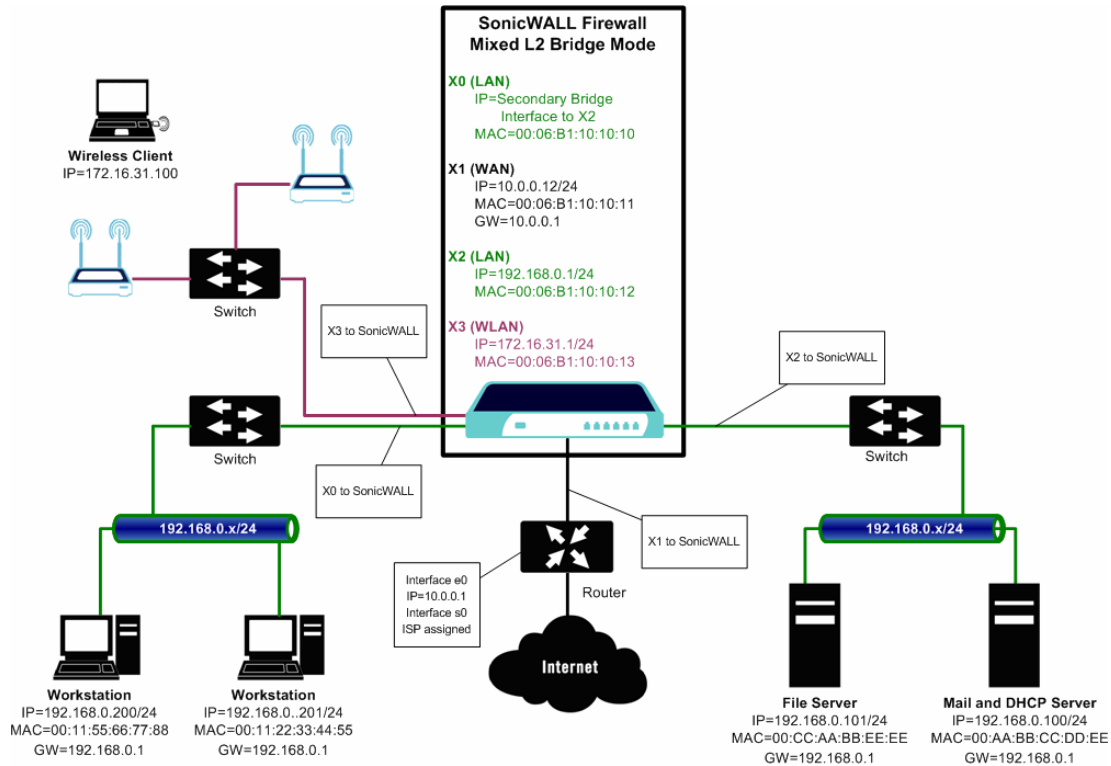
The above diagram depicts a network where the SonicWALL is added to the perimeter for the purpose of providing security services (the network may or may not have an existing firewall between the SonicWALL and the router). In this scenario, everything to the right of the SonicWALL (the *Primary Bridge Interface* segment) will generally be considered as having a lower level of trust than everything to the left of the SonicWALL (the *Secondary Bridge Interface* segment). For that reason, it would be appropriate to use X1 (Primary WAN) as the *Primary Bridge Interface*.

Traffic from hosts connected to the *Secondary Bridge Interface* (LAN) would be permitted outbound through the SonicWALL to their gateways (VLAN interfaces on the L3 switch and then through the router), while traffic from the *Primary Bridge Interface* (WAN) would, by default, not be permitted inbound.

If there were public servers, for example, a mail and web server, on the *Secondary Bridge Interface* (LAN) segment, an Access Rule allowing WAN->LAN traffic for the appropriate IP addresses and services could be added to allow inbound traffic to those servers.

Tech Note

Internal Security



This diagram depicts a network where the SonicWALL will act as the perimeter security device and secure wireless platform. Simultaneously, it will provide L2 Bridge security between the workstation and server segments of the network *without having to readdress any of the workstation or servers*.

This typical inter-departmental Mixed Mode topology deployment demonstrates how the SonicWALL can simultaneously Bridge and route/NAT. Traffic to/from the *Primary Bridge Interface* (Server) segment from/to the *Secondary Bridge Interface* (Workstation) segment will pass through the L2 Bridge.

Tech Note

Since both interfaces of the Bridge-Pair are assigned to a Trusted (LAN) Zone, the following will apply:

- All traffic will be allowed by default, but Access Rules could be constructed as needed.

Consider, for the point of contrast, what would occur if the X2 (Primary Bridge Interface) was instead assigned to a Public (DMZ) Zone: All the Workstations would be able to reach the Servers, but the Servers would not be able to initiate communications to the Workstations. While this would probably support the traffic flow requirements (i.e. Workstations initiating sessions to Servers), it would have two undesirable effects:

1. The DHCP server would be in the DMZ. DHCP requests from the Workstations would pass through the L2 Bridge to the DHCP server (192.168.0.100), but the DHCP offers from the server would be dropped by the default DMZ->LAN Deny Access Rule. An Access Rule would have to be added, or the default modified, to allow this traffic from the DMZ to the LAN.
 2. Security services directionality would be classified as *Outgoing* for traffic from the Workstations to the Server since the traffic would have a Trusted source Zone and a Public destination Zone. This might be sub-optimal since it would provide less scrutiny than the *Incoming* or (ideally) *Trust* classifications.
- Security services directionality would be classified as *Trust*, and all signatures (*Incoming*, *Outgoing*, and *Bidirectional*) will be applied, providing the highest level of security to/from both segments.

Configuration Tasklist


- Choose a topology that suits your network
- Select the Primary Bridge Interface
 - Select the Zone for the Primary Bridge Interface
 - Activate management
 - Activate security services
- Select the Secondary Bridge Interface
 - Select the Zone for the Primary Bridge Interface
 - Activate management
 - Activate security services
- Apply security services to the appropriate Zones

Procedure

Refer to the **L2 Bridge Interface Zone Selection** section for choosing a topology that best suits your network. In this example, we will be using a topology that most closely resembles the **Simple L2 Bridge Topology** presented on page 4.

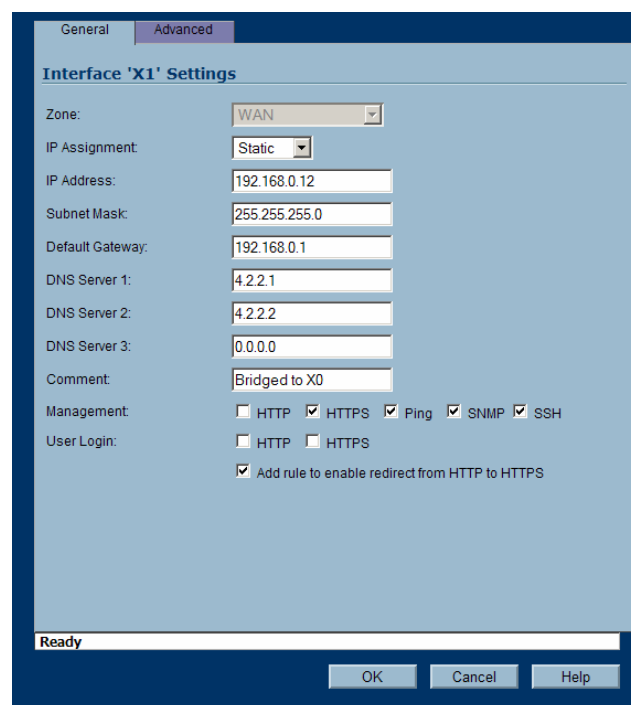
Choose an interface to act as the Primary Bridge Interface. Refer to the **L2 Bridge Interface Zone Selection** section for information in making this selection. In this example, we will use X1 (automatically assigned to the Primary WAN):

Configuring the Primary Bridge Interface

1. Select the **Network** tab, **Interfaces** folder from the navigation panel.
2. Click the Configure  icon in the right column of the X1 (WAN) interface.
3. Configure the interface with a Static IP Address (e.g. 192.168.0.12).

Note: The Primary Bridge Interface must have a Static IP assignment.

4. Configure the default gateway. This is required for the security appliance itself to reach the Internet. *Applies only to WAN interfaces.*
5. Configure the DNS server. *Applies only to WAN interfaces.*
6. Configure management (HTTP, HTTPS, Ping, SNMP, SSH, User Logins, HTTP Redirects).
7. Click **OK**.



General Advanced

Interface 'X1' Settings

Zone: WAN

IP Assignment: Static

IP Address: 192.168.0.12

Subnet Mask: 255.255.255.0

Default Gateway: 192.168.0.1

DNS Server 1: 4.2.2.1

DNS Server 2: 4.2.2.2

DNS Server 3: 0.0.0.0

Comment: Bridged to X0

Management: ☐ HTTP ☒ HTTPS ☒ Ping ☒ SNMP ☒ SSH

User Login: ☐ HTTP ☐ HTTPS

☒ Add rule to enable redirect from HTTP to HTTPS


Ready

OK Cancel Help

Tech Note

Choose an interface to act as the Secondary Bridge Interface. Refer to the **L2 Bridge Interface Zone Selection** for information in making this selection. In this example, we will use X0 (automatically assigned to the LAN):

Configuring the Secondary Bridge Interface

8. Select the **Network** tab, **Interfaces** folder from the navigation panel.
9. Click the Configure  icon in the right column of the X0 (LAN) interface.
10. In the **IP Assignment** drop-down, select **Layer 2 Bridged Mode**.
11. In the **Bridged to** drop-down, select the **X1** interface.
12. Configure management (HTTP, HTTPS, Ping, SNMP, SSH, User Logins, HTTP Redirects).

Do not enable *Never route traffic on the bridge-pair* unless your network topology requires that all packets entering the L2 Bridge remain on the L2 Bridge segments. See the **Captive-Bridge Mode** section for more details.

You may optionally enable the *Block all non-IPv4 traffic* setting to prevent the L2 bridge from passing non-IPv4 traffic.



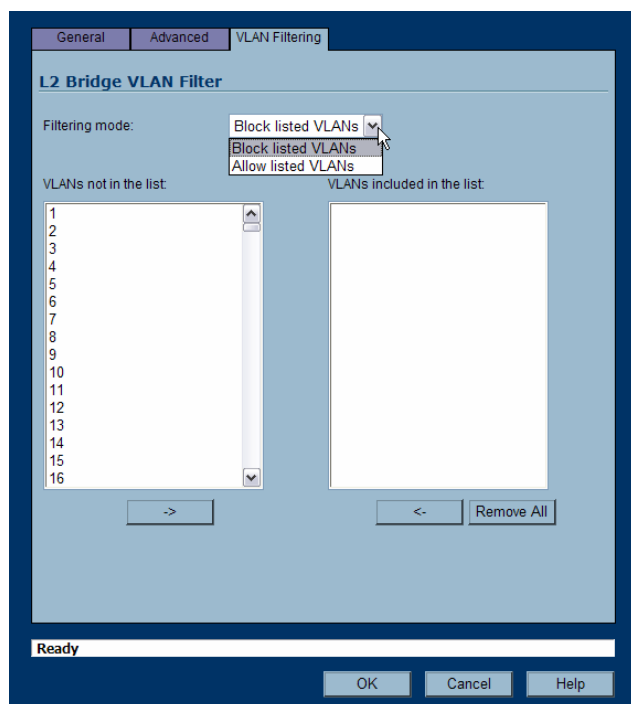
VLAN Filtering

You may also optionally navigate to the **VLAN Filtering** tab to control VLAN traffic through the L2 bridge. By default, all VLANs are allowed:

Select *Block listed VLANs* (blacklist) from the drop-down and add the VLANs you wish to block from the left-pane to the right pane. All VLANs added to the right-pane will be blocked, and all VLANs remaining in the left-pane will be allowed.



Select *Allow listed VLANs* (whitelist) from the drop-down and add the VLANs you wish to explicitly allow from the left-pane to the right pane. All VLANs added to the right-pane will be allowed, and all VLANs remaining in the left-pane will be blocked.

13. Click **OK**.



Tech Note

The **Network > Interfaces** page displays the updated configuration:

Network > Interfaces							
Interface Settings							
Name	Zone	IP Address	Subnet Mask	IP Assignment	Status	Comment	Configure
X0	LAN	192.168.0.12	255.255.255.0	Secondary Bridged I/F	10 Mbps half-duplex	Bridged to X1	
X1	WAN	192.168.0.12	255.255.255.0	Primary Bridged I/F	100 Mbps full-duplex	Bridged to X0	

You may now apply security services to the appropriate Zones, as desired. In this example, they should be applied to the LAN, WAN, or both zones.

For more information on this SonicOS Enhanced feature or other enhancements, contact your SonicWALL Sales Representative.