NEXT-GENERATION FIREWALL

SonicWALL SuperMassive E10000 Series Deployment Guide

"Knowing that defense against escalating threats requires extremely resource-intensive content inspection, how can I adequately secure my increasingly utilized, mission-critical, multi-gigabit networks without impeding performance?"

Introduction

As global dependency on information systems continues to grow, so do network capacities and our utilization thereof. Simultaneously, the increasing sophistication of network-borne threats has triggered a race to adopt and deploy the most efficient next-generation threat prevention technologies. The cornerstone of such technologies, the Next-Generation Firewall (NGFW), transcends earlier firewall designs through core integrations of Deep Packet Inspection (DPI), SSL decryption and unified policy engines. These combined engines perform intensive transformations and analyses of network traffic to detect and defend against present and emerging malware and to provide precise controls over the explosive diversity of applications running on today's networks. The coincidence of these two trends (increasing network speeds and the need for progressively rigorous content analysis) has created a dilemma for today's security professionals.

In response to these complex yet critical requirements, SonicWALL® created the SuperMassive™ E10000 Series, an NGFW platform fusing highly scalable 64-bit multi core architecture with the patented SonicWALL Reassembly-Free Deep Packet Inspection™ (RFDPI)* technology, affording heretofore-unparalleled levels of inspection, application control, visibility and performance. Further, the real-time SonicOS operating system is replete with high-availability (HA) and flexible deployment options to ensure minimal downtime and seamless insertion into most any network environment.

Adding to the broad collection of traditional modes of SonicOS interface operation, including all LAN modes (Static, NAT, Transparent Mode, L2 Bridge Mode, PortShield Switch Mode) and all WAN modes (Static, DHCP, PPPoE, PPTP and L2TP), SonicOS 6.0 introduces Wire-Mode, which provides four new methods for non-disruptive, incremental insertion into networks:

*U.S. Patents 7,310,815; 7,600,257; 7,738,380; 7,835,361

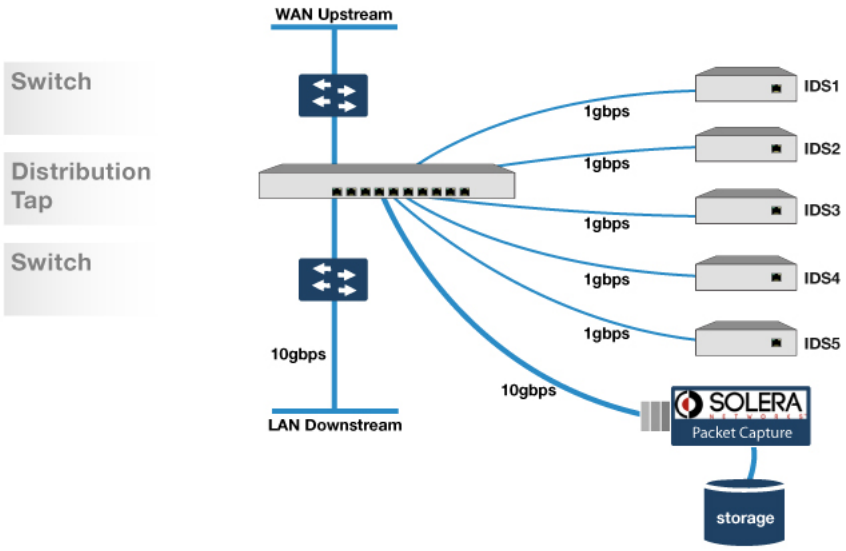
Wire-Mode Setting	Description
Bypass Mode	Bypass Mode allows for the quick and relatively non-interruptive introduction of the SuperMassive E10000 Series hardware into a network. Upon selecting a point of insertion into a network (e.g., between a core switch and a perimeter firewall, in front of a VM server farm or at a transition point between data classification domains), the E10000 is inserted into the physical data path, requiring a very short maintenance window. One or more pairs of switch ports on the E10000 are used to forward all packets across segments at full line rates, with all the packets remaining on the E10000's 240 Gbps switch fabric, rather than getting passed up to the multi-core inspection and enforcement path. While Bypass Mode does not offer any inspection or firewalling, this mode allows the administrator to introduce the E10000 physically into the network with a minimum of downtime and risk and obtain a level of comfort with the newly inserted component of the networking and security infrastructure. The administrator can then transition from Bypass Mode to Inspect or Secure Mode instantaneously through a simple user-interface-driven reconfiguration.

Wire-Mode Setting	Description
Inspect Mode	Inspect Mode extends Bypass Mode without functionally altering the low-risk, zero-latency packet path. Packets continue to pass through the E10000's switch fabric, but they are also mirrored to the multi-core RFDPI engine for the purposes of passive inspection, classification and flow reporting. This reveals the SuperMassive E10000 Series's application intelligence and threat detection capabilities without any actual intermediated processing.
Secure Mode	Secure Mode is the progression of Inspect Mode, actively interposing the E10000's multi-core processors into the packet-processing path. This unleashes the inspection and policy engines' full-set of capabilities, including SonicWALL Application Intelligence and Control, Intrusion Prevention Service, Gateway and Cloud-based Anti-Virus, Anti-Spyware and Content Filtering. Secure Mode affords the same level of visibility and enforcement as conventional NAT or L2 Bridge mode deployments, but without any L3/L4 transformations, and with no alterations of ARP or routing behavior. Secure Mode thus provides an incrementally attainable NGFW deployment requiring no logical, and only minimally physical, changes to existing network designs.
Tap Mode	Tap Mode is designed for use in environments employing network taps, smart taps, port mirrors or SPAN ports to deliver packets to external devices for inspection or collection. Tap Mode provides the same visibility as Inspect Mode, but differs from the latter in that it ingests a mirrored packet stream via a single switch port on the E10000, eliminating the need for physically intermediated insertion. Like all other forms of Wire-Mode, Tap Mode can operate on multiple concurrent port instances, supporting discrete streams from multiple taps.

Network Insertion: A More Efficient Network Tap Model

Network taps and port mirrors are designed to deliver packets from select network segments to third-party devices for the purpose of inspection, analysis or collection. Given this out-of-path packet vectoring model, and also that taps generally operate in a fail-safe (open) mode, they provide what is essentially a risk free means of performing traffic inspection and collection.

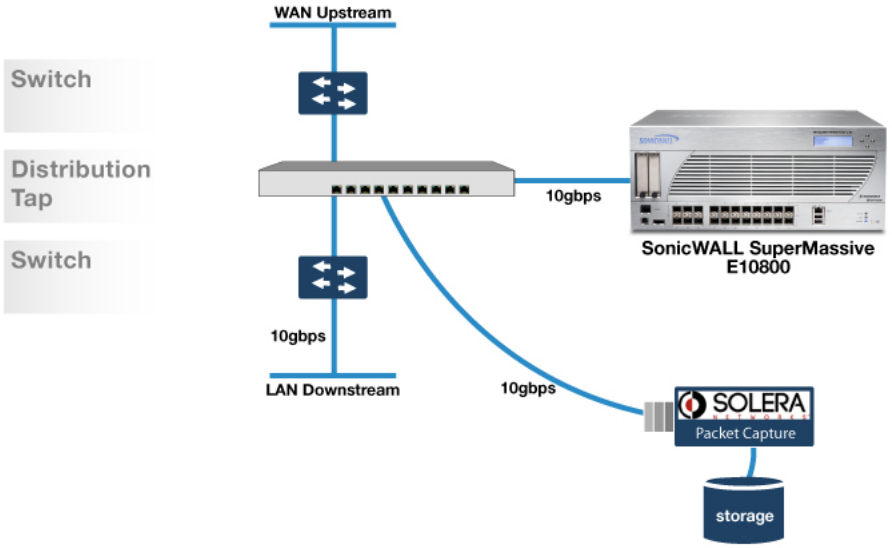
As it has historically been difficult to inspect traffic at rates exceeding 1 Gbps, it has been common industry practice to employ distribution taps to split 10 Gbps links into multiple 1 Gbps links and feed these into stacks of inspection devices:



Distribution Tap with IPS Stack

While this provides a functional workaround to performance limitations, it has the distinct disadvantage of power, space and cooling inefficiency. Moreover, because this method distributes traffic by flow n-tuples, it often disintegrates and mishandles compound flows composed of discrete control and data streams, such as FTP, VoIP, RTSP, IM file transfers and BitTorrent.

To resolve the deficiencies of such configurations, Tap Mode offers one of the industry's first single-appliance full-10-Gbps-capable detection and application classification platforms. This provides an ideal starting point for the circumspect security administrator looking to introduce a DPI solution or a path to greatly optimize existing distributed tap solutions:

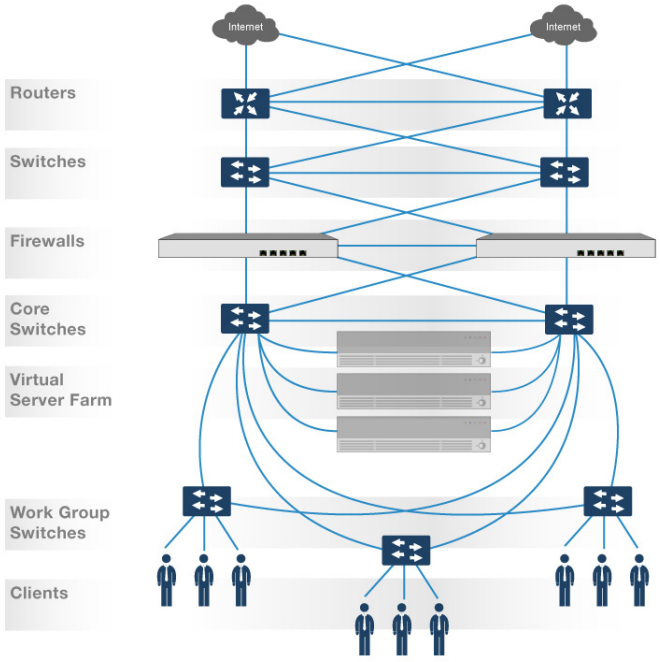


Tap with single 10 Gbps SonicWALL SuperMassvie E10800

Network Insertion: Augmenting Existing Firewalls

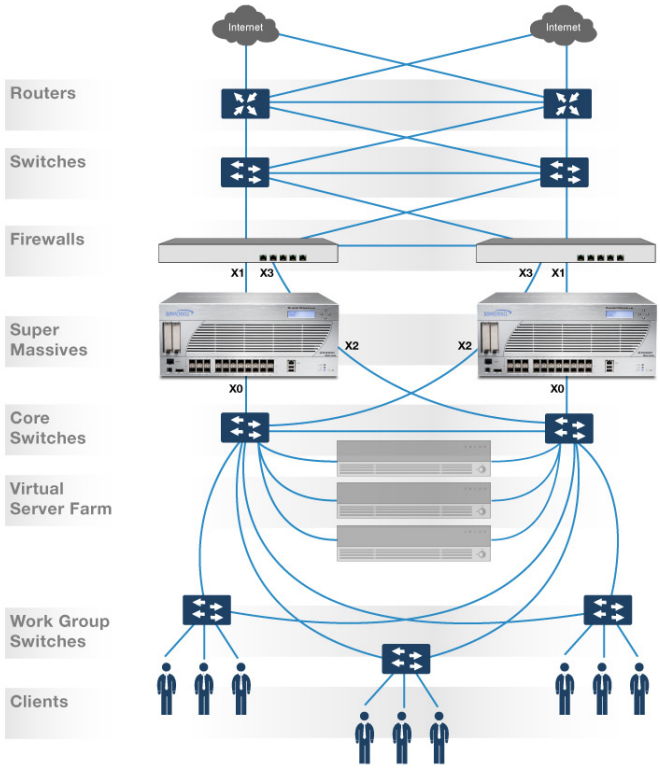
While Wire-Mode does not support the set of High Availability (HA) options of other interface operation modes described below, Wire-Mode deployments need not introduce a single point of failure into the network.

Tap Mode, as described above, never introduces a point of failure, and Bypass, Inspect and Secure mode deployments can be as redundant as the topology into which they are being introduced. For example, consider the following environment:



Redundant Network / Data Center

Assume that the current firewalls in use are older models, incapable of providing essential NGFW protection, but still providing other services and deemed not quite ready for retirement. Assume further that traffic rates on the network at this point average around 1 Gbps with occasional spikes up to 3 Gbps. A reasonable point of insertion for the appropriately sized E10400 would be between the core-switches and the existing firewalls:



Wire-Mode E10400 Insertion

The redundant paths between the switches and the firewalls are fully preserved across the two Secure Mode interface pairs through each SonicWALL SuperMassive E10400 and, although the addition of another component technically increases the system's calculated hazard rate, the system is still spared a single point of failure. In the event of a failure of any of the elements in the diagram (e.g., a switch, a fiber path, an SPF+ transceiver, a firewall, etc.) the traffic would proceed through the redundant counterpart.

The Link-State Propagation feature of Wire-Mode supports this kind of resiliency in redundant path networks. Consider a fiber cable failure on the primary link between the E10400's X1 interface and the upstream firewall. Without Link-State Propagation, the switch below, connected to the E10400's X0, would not know of the path failure (since its link to the E10400 would still be in an up state) and it would not fail over to its redundant path to the upstream firewall on the right (connected through the E10400's X2 and X3 Wire Mode interfaces). With Link-State Propagation, when the X1 link state changes to down, its paired interface X0 is switched to an administratively down state, allowing path failover to occur. When link state is restored on X1, X0 is brought back up and the path again becomes available.

Because Wire-Mode also disables TCP handshake enforcement, previously established connections are allowed to continue unimpeded. So in the example above, when the path transitions from the X0:X1 Wire Mode pair to the X2:X3 pair, all of the connections (as supported by the underlying applications and protocols) will resume without needing to be re-established. This would be true for path failures from one E10400 to the other, as well (e.g., in the event of total switch failure).

With the newly inserted application intelligence layer, the security administrator is finally able to see precisely the sort of traffic that is passing through the access rule access-list SIEVE permit tcp any object-group LOCALNETS eq http on the existing firewalls and define real access controls.

High Availability and Cluster Deployments

SonicWALL's SonicOS supports modes of interface configuration designed to provide full basic and advanced L2, L3 and L4 services and functionality such as ARP, static and dynamic routing, NAT, DHCP services, SSL and IPSec VPN services, WLAN services, multicast support, VLAN sub-interfaces, Active/Active Clustering and Virtual Groups. Whereas Wire Mode (and to a lesser extent, L2 Bridge Mode) is designed for unobtrusive insertion into operational networks, NAT and routing configurations are intended to serve as primary or exclusive security gateways within networks, providing all requisite services. For maximum flexibility, it is possible to configure multiple different simultaneous modes of interface operation on a single SonicWALL security appliance, such as X0:X1 in Secure Wire-Mode, X5 in Tap Wire-Mode, X2 and X3 in load-balanced static WAN NAT mode and X6 through X21 in LAN/DMZ/WLAN modes.

To best accommodate the requirements of today's most demanding networks, particularly the concurrent needs for high-speed/low-latency throughput, robust NGFW services and high-availability, SonicOS supports a variety of configurations designed to eliminate single-points of failure and to provide the aggregate performance of multiple appliances. These configurations, described below, rely on certain core networking functions that are currently available only on interfaces configured with static L3 addressing (i.e., operating in NAT or routing Modes) unless otherwise noted:

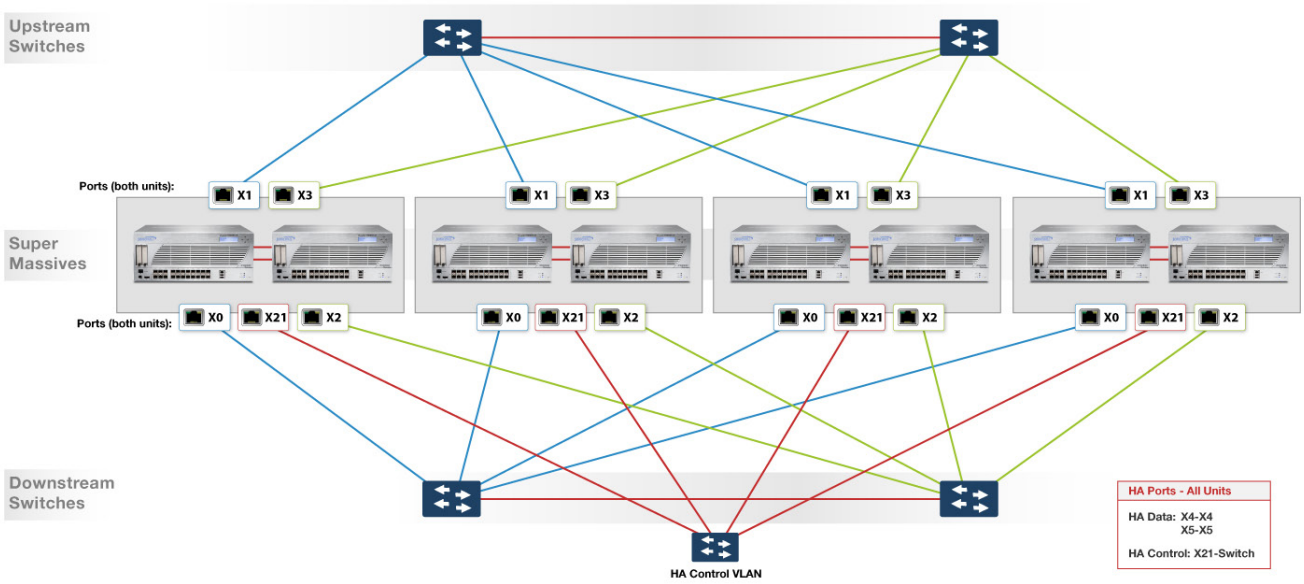
HA Mode	Description
Active/Passive HA	The most basic mode of HA, an Active/Passive HA pair contains a Primary and a Backup unit. In the event of failure of the Primary unit, the Backup unit will transition from an Idle to Active role, assuming the IP addresses of all configured network interfaces and issuing gratuitous ARPs to update switches, routers and hosts on the network. Active/Passive HA does not synchronize connection-cache or other sub-system state across the pair, so all connections must be re-established following a failover event. While this mode does offer a level of fault tolerance, it is less frequently used than other modes because of its disruptiveness. (Not available on E10100) This reveals the SuperMassive E10000 Series's application intelligence and threat detection capabilities without any actual intermediated processing.
Stateful HA	Stateful HA adds state synchronization to Active/Passive HA, ensuring that on a failover event all connections resume through the Backup unit without interruption. This continuity extends to all local IP protocol connections, as well as all VPN connections. Stateful HA is available on the SuperMassive E10200, E10400 and E10800. Although Stateful HA is not available on the E10100, alternative method of achieving state-synchronized high availability is offered using a single an synchronized Virtual Group.
Active/Active DPI	Active/Active DPI, introduced in SonicOS 5.5, is a method of distributing the RFDPI workload across both units in a stateful HA pair for increasing performance. The E10100 model employs Active/Active DPI internally to distribute the RFDPI workload between its 12 primary cores and its 12 offload cores. The E10200, E10400 and E10800 models support Active/Active DPI when configured as a stateful HA pair, both within and without clustering (see below). When operating in Active/Active DPI mode, traffic traverses only the active unit in the HA pair. DPI services traffic (Application Intelligence, IPS, GAV, and Anti-Spyware) is sent exclusively via the dedicated HA data link to the idle unit for RFDPI processing. Since Active/Active DPI is a method of load sharing rather than symmetric traffic distribution, it does not provide a full doubling of performance, but rather a variable gain of up to 90 percent, depending on the properties of the traffic.

HA Mode	Description
Active/Active Clustering	Essential to the selection and implementation of any element of a mission-critical network is an assurance of that component's high-availability, uninterrupted service and scalability. Active/Active Clustering allows for the assembly of stateful HA pairs, non-stateful HA pairs or singleton units into "Nodes" within a Cluster. A Cluster can comprise up to four Nodes (each containing one or two units) for directed distribution of flows across all Nodes with linear performance scaling. To achieve traffic distribution, up to four Virtual Groups can be created within each Cluster, where each Virtual Group presents a unique IP address that serves as gateway for some set of hosts on the network. Distribution of traffic across the gateways can be accomplished through such methods as multiple DHCP scopes, a load-balancer or Equal Cost Multi-Path (ECMP) capable routers. Additionally, when a Node consists of a stateful HA pair, that pair may operate in Active/Active DPI mode for further performance enhancements. Communication between Cluster Nodes uses the SonicWALL Virtual Router Redundancy Protocol (SVRRP), but state is not synchronized across Nodes in Clusters containing more than a single Virtual Group. It is for this reason that stateful HA pairs are recommended as the building blocks for the most highly available Cluster configuration. (Single Virtual Group with state-synch is available on E10100)
Virtual Groups	Virtual Groups are collections of one or more virtual IP addresses associated with all configured interfaces from Nodes participating in Active/Active Clusters. Up to four Virtual Groups can be configured, related to the maximum of four Nodes in a Cluster. For example, assume a 2 Node HA Cluster (total of 4 units) with active X0 (LAN) and X1 (WAN) interfaces. To balance traffic equally across these two HA Nodes, two Virtual Groups would be created: VG1 could contain the virtual X0 and X1 IP addresses 10.10.10.10 and 208.122.35.38, and VG2 could contain the virtual X0 and X1 IP addresses 10.10.10.11 and 208.122.35.39. The Node-1 pair would own VG1 and be standby for VG2, and the Node-2 pair would own VG2 and be standby for VG1. In the event of failure of a single HA member in a Node, the standby HA unit can take over (with state) and VG ownership will not transfer across Nodes. But in the unlikely event of failure of both HA units in a Node, VG ownership will transfer (without state) to the other Node. While there is no strict correlation between the number of Virtual Groups and the number of Nodes, it is generally a one to one mapping for equally distributing traffic across all available Nodes. One common exception to this would be the E10100 Active/Active Cluster configuration employing a single synchronized Virtual Group for continuous operation in the event of a failover.
Redundant Port Mesh	Designed for use in highly available networks (i.e., redundant switches and routers), full or partial mesh topologies take advantage of the SonicOS Port Redundancy feature to minimize or eliminate single points or single paths of failure in Active/Active Cluster configurations.

Network Insertion: Augmenting Existing Firewalls

While Wire-Mode does not support the set of High Availability (HA) options of other interface operation modes described below, Wire-Mode deployments need not introduce a single point of failure into the network.

Tap Mode, as described above, never introduces a point of failure, and Bypass, Inspect and Secure mode deployments can be as redundant as the topology into which they are being introduced. For example, consider the following environment:



60 Gbps Full Mesh Active/Active DPI Cluster

SonicWALL, Inc.
2001 Logic Drive, San Jose, CA 95124
T +1 408.745.9600 F +1 408.745.9300
www.sonicwall.com

SONICWALL®
DYNAMIC SECURITY FOR THE GLOBAL NETWORK™