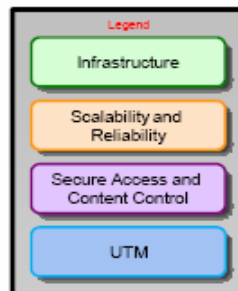


SISTESEG EDUCATION SERVICES

Certified Soniwall Security Administrator (CSSA)



SISTESEG



Elaborado por: SISTESEG

Revisado por: Rodrigo Ferrer

Plan de entrenamiento CSSA

Aprobado por:

DOCUMENTO PLAN DE ENTRENAMIENTO SONICWALL

Fecha revisión: 20/09/2008

CONFIDENCIAL

Versión:1.0

Página 2 de 17

INDICE

1	INTRODUCCIÓN	5
2	OBJETIVO	5
3	COMPONENTES DE LAS EMPRESAS HOY DÍA	6
4	ALCANCE DEL CURSO	7
5	TÉRMINOS Y DEFINICIONES ÚTILES PARA ESTE DOCUMENTO	7
6	DURACIÓN DEL CURSO	9
7	METODOLOGÍA DEL CURSO	9
7.1	Presentación del concepto	10
7.2	Escenario del laboratorio	10
7.3	Laboratorio	10
7.4	Sesión de preguntas y respuestas	11
8	AUDIENCIA Y PRERREQUISITOS	11
9	INFRAESTRUCTURA Y MEDIOS	11
10	DESCRIPCIÓN Y CONTENIDO DEL CURSO	13
10.1	Infraestructura	13
10.2	Escalabilidad y disponibilidad	14
10.3	Acceso seguro y control de contenido	14
10.4	Unified Threat Management (UTM)	15



Elaborado por: SISTESEG

Revisado por: Rodrigo Ferrer

Plan de entrenamiento CSSA

Aprobado por:

DOCUMENTO PLAN DE ENTRENAMIENTO SONICWALL

Fecha revisión: 20/09/2008

CONFIDENCIAL

Versión:1.0

Página 3 de 17

SECCIÓN DE CONTROL DEL DOCUMENTO

Todos los derechos están estrictamente reservados. Ninguna parte de este documento puede ser reproducida de ninguna forma o por ningún medio sin la previa autorización escrita de SONICWALL O SISTESEG.

Nombre del Archivo: 01 SONICWALL_Plan de Entrenamiento.doc

Historia del Documento

Autor/Actualizador del documento	Versión	Fecha de realización	Estado	Comentarios
Rodrigo Ferrer	V1.00	15-Sept-08	Para Revisión	
Rodrigo Ferrer	V2.00	20-Sept-08	Para Aprobación	

Nombre del manejador del documento	Deisy Correa.
------------------------------------	---------------

Lista de Distribución

Nombre	Cargo	Acción [aprobar, revisar, información]
SONICWALL		

SISTESEG		
Rodrigo Ferrer	Consultor de Redes de Datos - Experto en Seguridad	Revisar, Aprobar



Elaborado por: SISTESEG

Revisado por: Rodrigo Ferrer

Plan de entrenamiento CSSA

Aprobado por:

DOCUMENTO PLAN DE ENTRENAMIENTO SONICWALL

Fecha revisión: 20/09/2008

CONFIDENCIAL

Versión:1.0

Página 4 de 17

Derechos de Autor 2008 de Sisteseg. Todos los derechos reservados. Esta publicación no puede ser reproducida total ni parcialmente, ni ser registrada o transmitida por un sistema de recuperación de información, en ninguna forma ni por ningún medio, sea mecánico, fotoquímico, electrónico, magnético, electro-óptico, fotostático o por cualquier otro, sin el permiso previo escrito de los propietarios de copyright, Sisteseg. La información contenida en este documento no puede ser cambiada sin la autorización expresa de Sisteseg y Sonicwall.

© **SISTESEG Colombia. Derechos reservados.**
Impreso en Colombia.



1 Introducción

Las organizaciones hoy en día, no podrían garantizar la confidencialidad, disponibilidad e integridad de la información sin la participación activa de tecnología con características de desempeño y funcionalidad adecuada a las necesidades cambiantes en materia de seguridad de la información y específicamente en el control y mitigación de amenazas potenciales sobre las redes de datos, tales como virus, gusanos y troyanos entre otros.

Por otro lado, la seguridad de la información es un componente crítico de la estrategia de negocio de cualquier organización. Este curso de seguridad avanzado enfocado a la tecnología Sonicwall le permitirá por medio del estudio de los diferentes conceptos que conforman una arquitectura de seguridad, ayudar a diseñar, planear, instalar, y mantener un sistema de seguridad. La metodología que utilizaremos a lo largo del curso, le facilitará conocer las tecnologías, protocolos, características de hardware y software, que conforman los elementos de una red segura, profundizando en el detalle de su funcionamiento, para así poder llegar a tener la capacidad de tomar las mejores decisiones para el diseño de una arquitectura de red segura, no dejando de lado el hecho que también se está en un proceso de formación integral y formal, que ayude en la preparación para el procesos de certificación a nivel internacional en la tecnología Sonicwall.

El curso cubre aspectos como: disponibilidad, desempeño, confidencialidad, integridad, control de acceso lógico, enrutamiento, balanceo de cargas, redes virtuales privadas de tal manera que se está proponiendo un enfoque integral de acercamiento a la seguridad de la información: tratando de esta manera de combinar efectivamente controles de tipo lógico, físico y administrativos, hasta llegar a una verdadera arquitectura de seguridad en las redes de información.

2 Objetivo

El curso sobre tecnologías Sonicwall tiene como objetivo principal, realizar un recorrido de las diferentes tecnologías implementadas en los equipos Sonicwall con el fin de poder aplicarlas para en casos concretos para así mejorar la seguridad de la información.

Entonces, resumiendo el curso busca realizar un análisis crítico de las tecnologías de seguridad en las redes, junto con una comprensión global de los elementos que conforman la arquitectura de los sistemas de información seguros preparando de esta manera al estudiante para el diseño, implementación y solución de problemas de tecnologías Sonicwall.

Por ultimo, esto facilitará a los asistentes al curso, cuando se enfrenten a situaciones reales, tener un criterio no sólo tecnológico, sino más bien un enfoque de tipo sistémico, con el fin de avanzar hacia la mejor solución que apoye al negocio y a la operación de la organización, con que se puedan ver enfrentados en algún momento de su vida profesional cuando se trata del diseño de una arquitectura de seguridad. Se busca con este conocimiento adquirido, reunir la

teoría con la práctica y una orientación hacia el diseño de una seguridad integral y no simplemente el esquema del tradicional filtro de paquetes o elementos no integrados.

3 Componentes de las empresas hoy día

Las organizaciones modernas necesitan una definición adecuada de los procesos que respaldan sus funciones con el fin de poder diseñar una arquitectura de seguridad orientada a sus necesidades. Una forma de aproximarse a la integración de dichos procesos es partiendo de una clasificación global de sus componentes, los cuales son:

- ✚ Procesos de soporte de los servicios
- ✚ Participantes (personas)
- ✚ Tecnología(firewalls, UTM, Mail security, Gateway antivirus y otros)
- ✚ Infraestructura física

Estos elementos tienen una interacción secuencial de forma que cada uno de ellos se apoya en los otros para lograr el funcionamiento total del sistema. En la figura 1, se visualiza la relación secuencial entre los mismos:

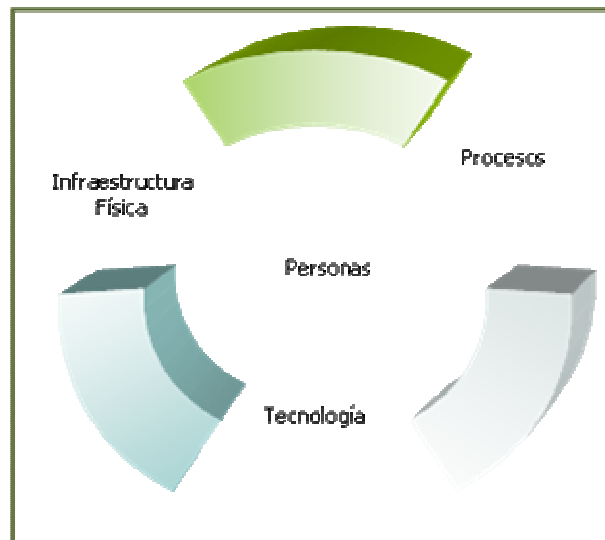


Figura 1. Componentes de una entidad apoyados en la tecnología.

A continuación se definirá la interacción de cada uno de los componentes, como elementos fundamentales.



PERSONAS: es uno de los elementos más vitales e importantes en el funcionamiento de las operaciones de las empresas. Es parte fundamental para el soporte de los procesos críticos del servicio. Adicionalmente, es el elemento que crea y desarrolla la planeación, implementación y mantenimiento de sistema de gestión de seguridad, tales como políticas, procedimientos y estándares de configuración.

PROCESOS: los procesos son los elementos más dinámicos en una entidad. Un proceso es una serie de actividades correlacionadas entre sí que permiten lograr las metas y objetivos propuestos por una entidad. Los procesos reciben elementos de entradas y producen otros elementos en la salida. Estos procesos pueden ser clasificados según su nivel de criticidad para priorizar las estrategias de seguridad de la empresa.

INFRAESTRUCTURA FÍSICA: este elemento físico es uno de los apoyos necesarios que poseen las personas y los procesos para poder realizar sus funciones de manera normal, adecuada y organizada. Está normalmente conformado por edificios, sedes, y oficinas.

TECNOLOGÍA: La tecnología cumple la función de soporte a los procesos de servicio. Comprende factores tanto instrumentales (redes informáticas, UTM, Mail Security, etc.) como cognitivos (métodos, procedimientos, etc.) que constituyen y fortalecen el componente tecnológico.

4 Alcance del curso

El curso de entrenamiento en tecnología Sonicwall tiene como objetivo principal lograr conocer en profundidad los siguientes temas:

- ✚ Infraestructura
- ✚ Escalabilidad y confiabilidad
- ✚ Acceso seguro y control de contenido
- ✚ UTM (Unified Thread Management)

5 Términos y Definiciones útiles para este documento.

Activos de información: Es todo activo que contenga información, la cual posee un valor y es necesaria para realizar los procesos del negocio y de soporte. Se pueden clasificar de la siguiente manera:

- ✚ **Personas:** Incluyendo sus calificaciones, competencias y experiencia.
- ✚ **Intangibles:** Ideas, conocimiento, conversaciones.
- ✚ **Electrónicos:** Bases de datos, archivos, registros de auditoría, aplicaciones, herramientas de desarrollo y utilidades.
- ✚ **Físicos:** Documentos impresos, manuscritos y hardware.
- ✚ **Servicios:** Servicios computacionales y de comunicaciones.



SGSI: Sistema de Gestión de la Seguridad de la Información. Es recomendable que las empresas que estén en proceso de adquirir una arquitectura de seguridad hayan adoptado este sistema.

Política de Seguridad: Una política de seguridad, es una declaración formal de las reglas, directivas y prácticas que rigen la forma de gestión de los activos de tecnología e información dentro de una organización. La arquitectura de seguridad debe apoyarse en las políticas de seguridad.

Procedimientos: Los procedimientos constituyen la descripción detallada de la manera como se implanta una política.

Estándares: Un estándar es definido como un producto o mecanismo específico el cual es seleccionado desde un punto de vista universal, para su uso a lo largo de toda la organización, con el objetivo fundamental de soportar una política ya aceptada y aprobada por las directivas de la compañía. Es recomendable que la configuración de los firewalls sigan los lineamientos establecidos por estos estándares de configuración.

Área IT: Es el área encargada de soportar, diseñar y mantener los activos electrónicos y el hardware, tales como firewalls, sistemas de gestión de seguridad y redes. Se requiere obtener un 75% para aprobar el examen.

CSSA: Certified Sonicwall Security Administrador. Esta es la certificación que se pretende alcanzar al tomar el curso de tecnologías Sonicwall.

Información: Entendemos por INFORMACIÓN cualquier manifestación (ya sea visual, auditiva, escrita, electrónica, óptica, magnética, táctil...) de un conjunto de conocimientos. Por ejemplo:

- ✚ Una noticia que escuchamos por la radio.
- ✚ Una señal de tráfico que advierte un peligro.
- ✚ Una fórmula que usamos en un problema.

La información se representa mediante conjuntos de símbolos, que pueden ser de diferente naturaleza:

- ✚ Textuales o numéricos, como las letras y números que usamos al escribir.
- ✚ Sonoros, como los fonemas, las notas musicales...
- ✚ Cromáticos, como los colores de los semáforos.
- ✚ Gestuales, como los que usamos para hacer mímica.

Propietario: Es el responsable y dueño del activo de información. Define también sus niveles de clasificación.

Usuario: Es el que utiliza los activos de información para llevar a cabo las funciones de su trabajo.



Elaborado por: SISTESEG

Revisado por: Rodrigo Ferrer

Plan de entrenamiento CSSA

Aprobado por:

DOCUMENTO PLAN DE ENTRENAMIENTO SONICWALL

Fecha revisión: 20/09/2008

CONFIDENCIAL

Versión:1.0

Página 9 de 17

Incidente de Seguridad: Un evento o una serie de eventos de seguridad de la información no deseados o inesperados que tienen una posibilidad significativa de comprometer las operaciones del negocio y amenazar la seguridad de la información.

Red privada virtual – VPN: Método de conexión a través de una red pública o privada, que permite a los usuarios establecer conexiones seguras. La utilización más frecuente corresponde a la conexión por Internet y los protocolos utilizados más frecuentemente son el IPSEC y el SSL.

Oficial de Seguridad: Persona responsable por velar, mantener y gestionar la seguridad de los activos de información. Es la persona responsable de gestionar los firewalls y UTM de la red.

UTM: Unified Threat Management (gestión unificada del riesgo).

6 Duración del curso

El curso sobre tecnologías Sonicwall comprende sesiones teóricas y prácticas con una duración de 20 horas y es de asistencia obligatoria dentro del proceso de certificación. En la última sesión se realizará el examen¹ de certificación Certified Sonicwall Security Administrator CSSA el cual tendrá una duración de dos horas y se permitirá a los asistentes consultar información tales como manuales y *white papers* durante el examen. El curso se realizará de la siguiente manera:

- ✚ Jueves: 8 horas (9:00 AM a 1:00PM y de 2:00PM a 6:00PM).
- ✚ Viernes: 8 horas (9:00 AM a 1:00PM y de 2:00PM a 6:00PM).
- ✚ Sábado: 4 horas (9:00 AM a 1:00PM)

7 Metodología del curso

A continuación haremos una descripción de las fases que componen la metodología del entrenamiento en tecnologías Sonicwall, tal como se muestra en la figura 2.

¹ El examen consta de 50 preguntas tanto teóricas como de la aprendido en las prácticas.



Figura 2. Metodología del Plan de Entrenamiento Sonicwall.

7.1 Presentación del concepto

Durante esta fase el instructor realizará una descripción de los conceptos necesarios con el fin de comprender la tecnología que subyace a la implementación de los equipos Sonicwall. La importancia de esta fase radica en el hecho que al comprender de manera clara y concisa los fundamentos de una tecnología determinada, facilitará a futuro el poder resolver los problemas técnicos que se presente en el campo bajo una situación específica y también ayudará a realizar la práctica relacionada a estos conceptos de una manera más efectiva.

7.2 Escenario del laboratorio

El instructor en esta fase explicara claramente el objetivo de la práctica o laboratorio a realizar con el fin de explicar sus posibles aplicaciones en el campo y también sus posibles limitaciones.

7.3 Laboratorio

En esta fase de la metodología los estudiantes guiados por el material de trabajo, realizarán lo expuesto en la fase anterior de escenario del laboratorio. Se espera que después de un tiempo razonable la práctica se haya realizado a satisfacción con ayuda y soporte de instructor y su monitor. En esta fase el estudiante contará con el material del curso el cual lo guiará en el desarrollo de los ejercicios y contará con la ayuda y el soporte del instructor y/o monitor.



7.4 Sesión de preguntas y respuestas

Esta sesión está orientada a familiarizar a los asistentes al curso sobre el tipo de preguntas que encontrarán durante la presentación del examen CSSA.

8 Audiencia y prerequisites

El curso de entrenamiento en tecnologías de Sonicwall está orientado a profesionales del área de tecnologías de información y comunicaciones y requiere algún manejo previo y adiestramiento en los siguientes conceptos y tecnologías:

- + Direccionamiento IP.
 - o DNS
 - o ARP
 - o Subnet
- + Conceptos básicos de enrutamiento (estático y dinámico).
- + Conceptos básicos de seguridad de la información.
 - o Confidencialidad
 - o Integridad
 - o Disponibilidad
- + Protocolos TCP, UDP, SMTP, Netbios, FTP, HTTPS y HTTP.
- + Herramientas de análisis de protocolos de red.
 - o Pings
 - o NMAP
 - o Wireshark
- + Conceptos básicos de criptografía simétrica y asimétrica.
 - o PKI
 - o Diffie-Hellman
 - o DES, 3DES y AES.
- + Tomar los cursos de *elearning* básicos de seguridad en www.mysonicwall.com.

9 Infraestructura y medios

Con el fin de poder desarrollar el curso de forma eficiente, se muestra en la figura 3, la distribución que tendrá el salón donde se desarrollará el curso orientado a obtener la certificación CSSA.

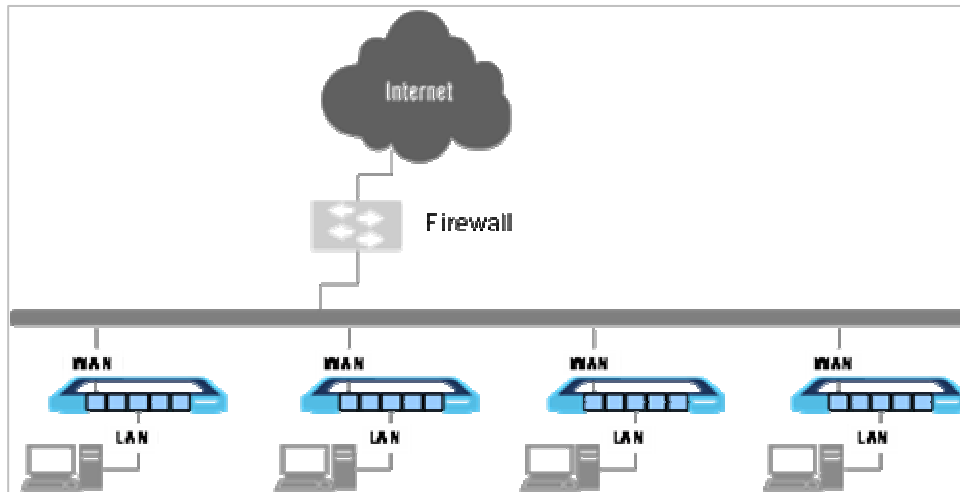


Figura 4. Diagrama de conectividad para el desarrollo del curso.

Por otro lado, en la figura 4, se muestran los componentes desde un punto de vista tecnológico donde se observa que los UTM Sonicwall con software enhanced se conectan por un lado al estudiante que tendrá bajo su responsabilidad realizar el Laboratorio y sus respectivas configuraciones y por otro, la conectividad de todos los UTM hacia la Internet, lo que permitirá probar reglas del firewalls y el control de contenido, además de permitir su registro a mysonicwall².

Cada estudiante tendrá a su vez una estación de trabajo con Windows XP Professional (Service pack 2 o mayor), software de monitoreo de red (Wireshark), Microsoft Active Directory³, Web server, FTP server, software de máquina virtual⁴ y otras herramientas de pruebas y diagnósticos (pings, dnslookup, tracert) útiles para el desarrollo del curso.

10 Descripción y contenido del curso

El curso de tecnologías Sonicwall comprende los temas de infraestructura, escalabilidad y disponibilidad, acceso seguro, control de contenido y por último las tecnologías asociadas al concepto de UTM tales como Gateway Antivirus, IPS y Antispyware. A continuación una descripción más detallada de cada uno de estos temas principales.

10.1 Infraestructura

² Se debe conectar al sitio www.mysonicwall.com para crear su respectiva cuenta de registro.

³ Con el objetivo de probar base de datos externas usando LDAP.

⁴ La herramienta recomendada es fabricada por VMware.



- ✚ Tipos de firewall
 - Packet filtering
 - Stateful
 - Proxy
- ✚ Firmware Upgrade a SonicOS Enhanced.
- ✚ Registro del Sonicwall (cuenta mysonicwall)
- ✚ Configuración Inicial
 - Interfaces
 - DHCP server
- ✚ Administración del Sonicwall
 - Administradores
 - Administradores de sólo lectura
 - Administradores limitados
- ✚ Grupos, usuarios y objetos.
- ✚ Reglas del firewall
 - LAN > WAN
 - WAN > LAN
- ✚ Acceso a Internet.
- ✚ Acceso a Web Server y FTP Server.
 - Configuración NAT.

10.2 Escalabilidad y disponibilidad

- ✚ La Importancia de redes de alta disponibilidad (High Availability).
- ✚ WAN ISP Failover y Load Balancing (alta disponibilidad).
 - Failover.
 - Round Robin.
 - Spillover.
 - Percentage Based.
- ✚ Policy Based Routing (Enrutamiento basado en políticas).
 - HTTP Routing
 - FTP Routing

10.3 Acceso seguro y control de contenido

- ✚ Conceptos de IPSEC y SSL.
 - ESP
 - AH
 - Modo túnel y modo transporte
 - Encriptación
 - DES
 - 3DES
 - AES

- IKE
 - Modo "Main"
 - Modo agresivo.
- ✚ Site to Site VPN
 - Configuración
 - Verificar conectividad
 - Acceder a archivos
 - Modificar parámetros
 - Fin
- ✚ GVC con bases de datos local
- ✚ GVC con LDAP
 - Concepto de LDAP
 - Importar grupos LDAP
- ✚ CFS con LDAP
 - Políticas más permisivas
 - Políticas más restrictivas.
- ✚ Concepto de Single Sign On (SSO).

10.4 Unified Threat Management (UTM)

- ✚ Concepto de detección y prevención de intrusos.
- ✚ Configuración IPS.
 - Prevención
 - Detección
 - Configuración de firmas
- ✚ Concepto de Gateway Antivirus.
- ✚ Configuración Gateway Antivirus.
 - HTTP
 - FTP
 - IMAP
 - POP3
 - CIFS
 - TCP STREAMS
- ✚ Concepto de antispymware.
- ✚ Configuración Antispymware.
 - HTTP
 - FTP
 - IMAP
 - SMTP
 - POP3



Elaborado por: SISTESEG

Revisado por: Rodrigo Ferrer

Plan de entrenamiento CSSA

Aprobado por:

DOCUMENTO PLAN DE ENTRENAMIENTO SONICWALL

Fecha revisión: 20/09/2008

CONFIDENCIAL

Versión:1.0

Página 16 de 17

ANEXOS

SOLUCIONES DE SEGURIDAD SONICWALL



Elaborado por: SISTESEG

Revisado por: Rodrigo Ferrer

Plan de entrenamiento CSSA

Aprobado por:

DOCUMENTO PLAN DE ENTRENAMIENTO SONICWALL

Fecha revisión: 20/09/2008

CONFIDENCIAL

Versión:1.0

Página 17 de 17



TZ Series

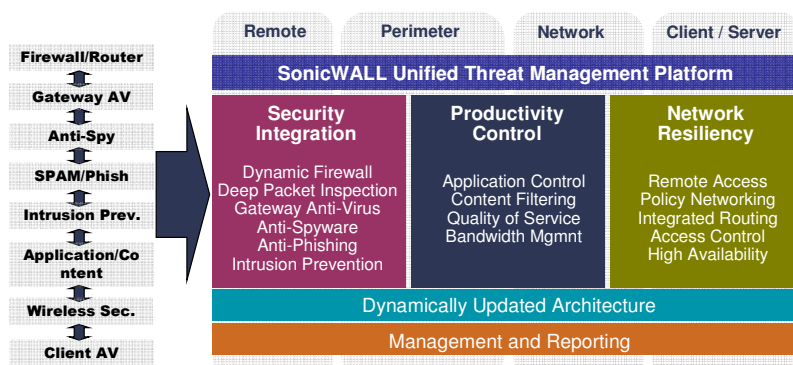
SonicWALL Security Solutions



Product	TZ 150/150 Wireless	TZ 170	TZ 170 SP	TZ 170 Wireless	TZ 170 SP Wireless	TZ 190
Part Numbers	01-SSC-5811 (10) 01-SSC-5816 (10)	01-SSC-5556 (10) 01-SSC-5559 (25) 01-SSC-5562 (Unrestricted) 01-SSC-5568 (SonicOS Enhanced)	01-SSC-5732 (10) 01-SSC-5568 (SonicOS Enhanced)	01-SSC-5716 (10) 01-SSC-5718 (25) 01-SSC-5720 (Unrestricted) 01-SSC-5568 (SonicOS Enhanced)	01-SSC-5742 (10)	01-SSC-6850 (Unrestricted)
Market Positioning and Specific Features	Delivers layered protection to small and home offices through an integrated deep packet inspection firewall in an easy-to-use, low cost platform. Includes: • SonicOS Standard • 4-port Auto-MDIX Switch • Compact Form Factor • Comprehensive Logging Additional TZ 150 Wireless Features: • 802.11n/g Support • Wireless Guest Services • Wireless Intrusion Detection and Prevention	A total security platform that delivers rock-solid network security, flexibility and scalability in a low TCO solution for home, small, remote and branch office networks. Includes: • SonicOS Standard • 1 VPN Client License (25- and Unrestricted-node versions) • Object-based Policy Mgmt * • WAN ISP Failover * • Load Balancing* • Optional Port • 5-port Auto-MDIX Switch	A total security platform designed for Retail/POS and telecommuter applications that ensures continuous network uptime through integrated and automated broadband and analog failover and fallback technologies. Includes: • SonicOS Standard • Network Failover/Failback • Integrated Analog Modem • Object-based Policy Mgmt * • WAN ISP Failover * • Load Balancing* • Optional Port* • 5-port Auto-MDIX Switch	A total security platform delivering enterprise-class wireless security to small, remote and branch office networks, integrating secure 802.11n/g wireless, firewall and VPN technologies in a cost-effective, easy-to-use solution. Includes: • SonicOS Standard • 1 VPN Client License (25- and Unrestricted-node versions) • Object-based Policy Mgmt * • WAN ISP Failover * • Load Balancing* • Optional Port* • 5-port Auto-MDIX Switch	A total wired and wireless security platform designed for Retail/POS and telecommuter applications ensuring continuous network uptime through integrated and automated failover and fallback technologies. Includes: • SonicOS Enhanced • 802.11n/g Support • Network Failover/Failback • Integrated Analog Modem • Object-based Policy Mgmt • WAN ISP Failover • Load Balancing • Optional Port • 5-port Auto-MDIX Switch	A network security solution with deep packet protection that instantly provides secure 3G wireless broadband access anywhere when other broadband options are impractical. Includes: • SonicOS Enhanced • GSM/CDMA PC Card Support • Network Failover/Failback • Object-based Policy Mgmt • WAN ISP Failover • PortShield Architecture • Optional Port • 8-port Auto-MDIX Switch
Bundled Services Across all TZ Appliances	• 30 Days GAV, Anti-Spyware and IPS	• 30 Days CFS Premium Edition	• 30 Days 10-user Network Anti-Virus	• 30 Days ViewPoint		• 90 Days 8x5 Support (30 Days on TZ 150 Series)
General Features Across all TZ Appliances	• Deep Packet Inspection Firewall • Clean VPN	• Dynamic DNS • IPSec 3DES/AES Encryption	• Voice and Video over IP • Hub and Spoke VPN Support	• DHCP Server • Policy-based User Authentication	• PPTP/DHCP/PPPoE/L2TP Client • Bandwidth Management	
Specifications	10 Nodes 5 10/100 Base-T (w/Switch) 30+ Mbps 10+ Mbps (3DES/AES) 2 Site-to-Site VPN Policies 2 VPN Client Licenses 2,000 Concurrent Connections 1-Yr hardware/30 day support, firmware updates	10, 25 or Unrestricted (7) 10/100 Base-T (w/Switch) 90 Mbps 30+ Mbps (3DES/AES) 2/10/10 Optional Upgrade/1/1 (5/50/50 max) 6,000 1-Yr hardware/90 day support, firmware updates	10 (7) 10/100 Base-T (w/Switch); Modem 90 Mbps 30+ Mbps (3DES/AES) 2 Optional Upgrade (5 max) 6,000 1-Yr hardware/90 day support, firmware updates	10, 25 or Unrestricted (7) 10/100 Base-T (w/Switch) 90 Mbps 30+ Mbps (3DES/AES) 2/10/10 Optional Upgrade/1/1 (5/50/50 max) 6,000 1-Yr hardware/90 day support, firmware updates	10 (7) 10/100 Base-T (w/Switch); Modem 90 Mbps 30+ Mbps (3DES/AES) 2 Optional Upgrade (5 max) 6,000 1-Yr hardware/90 day support, firmware updates	Unrestricted (10) 10/100 Base-T (w/Switch) 90 Mbps 30+ Mbps (3DES/AES) 15 2 (25 max) 6,000 1-Yr hardware/90 day support, firmware updates
General Upgrade Options Across all TZ Appliances	• Comprehensive Gateway Security Suite • Gateway AV, Anti-Spyware and IPS	• Content Filtering Service • Complete Anti-Virus	• Global Management System • ViewPoint Reporting Software	• Global Security Client • 8x5 and 24x7 Support		
Product-specific Upgrade Options	• N/A	• SonicOS Enhanced Upgrade • Node/Bundle Upgrades		• Node/Bundle Upgrades		
Key Selling Points	• Secure Wireless LAN capabilities (with SonicPoints – not available on TZ 150 Series) • Price-Performance leadership • Comprehensive layered security • Deep packet inspection firewall			• Easy to deploy and manage • Powerful firewall throughput and VPN concentration • Simple VPN Client provisioning through automatic, user-authenticated VPN policy download and synchronization		

*With SonicOS Enhanced

SONICWALL MANEJO UNIFICADO DEL RIESGO



One platform solution for more reliable business communications and lower total cost of ownership