

nX SecurityAppliance



nX Security Appliance es la línea de productos de Network Experts en el área de soluciones de networking que proporciona a las empresas los necesarios niveles de seguridad para proteger sus oficinas, sucursales y la red perimetral. El alto rendimiento de nuestros productos proporciona una solución integrada completa que hace innecesario disponer de distintos equipamientos para solventar necesidades paralelas. Son posibles diversas configuraciones para incluir, además de un firewall de alto rendimiento, VPNs, gestión de ancho de banda, priorización de tráfico, routing avanzado y balanceo de carga. Cada uno de estos módulos puede desarrollarse en forma de capas para proporcionar los necesarios niveles de control y gestión de la red. Los nX Security Appliance soportan múltiples servicios sin compromiso con una única plataforma maximizando la rentabilidad y minimizando los costes operacionales y de capital. Este portafolio de servicios continúa creciendo con cada versión de cada módulo obteniéndose una flexibilidad y un rendimiento muy elevados. Cada módulo se implementa por separado con la mínima carga administrativa de acuerdo con los requerimientos del cliente.

Se presenta con un elegante diseño all-in-one en dos modelos SA3 y SA4 orientados a un amplio espectro de empresas pequeñas, medianas y grandes. Tanto el SA3 como el SA4 incluyen un firewall integrado, VPNs así como funciones de priorización de tráfico y gestión de ancho de banda que los convierte en una potente herramienta de red. El SA3 incorpora tres interfaces Ethernet y el SA4 cuatro ampliables a otras cuatro

permitiendo incorporar los puertos que se desee como por ejemplo Gigabit Ethernet, RDSI, Frame Relay...etc.

Puede usarse solamente como firewall o puede desplegarse como una solución completa de protección y gestión de redes. Los nX Security Appliance soportan zonas de seguridad independientes y políticas personalizadas para redes virtuales de área local VLAN permitiendo configuraciones granulares únicas para cada grupo o departamento.

Soportan operaciones de alta disponibilidad activo-pasivo para aplicaciones críticas. Un sistema de monitorización en tiempo real proporciona una visión del estado de la red y las sesiones concurrentes.

¿Por qué nX Security Appliance?

nX Security Appliance es mucho más un firewall, es una solución integrada altamente escalable, sin límite de usuarios, que integra todos los aspectos de control y gestión de la red protegiendo contra ataques y accesos no autorizados, permitiendo además una gestión adecuada del ancho de banda y los recursos disponibles de forma que los servicios críticos de la empresa siempre tengan prioridad sobre las aplicaciones no críticas y estén disponibles con total seguridad y confidencialidad en las comunicaciones para usuarios locales y remotos.

nX Security Appliance se compone de un módulo firewall integrado y de cuatro módulos de software opcionales:

Módulo VPN, Módulo Priorización de Tráfico, Módulo Gestión Ancho de Banda y Módulo de Alta Disponibilidad.

Módulo Firewall

Todo lo que se refiere a seguridad es una preocupación importante cuando se conecta una red local al exterior. Si no se cifran y se filtran los paquetes de datos, su información -Contraseñas e Información Confidencial almacenada en sus servidores y estaciones de trabajo- puede ser leída, alterada o eliminada por personas que cuenten con los medios y conocimientos precisos. La función de este módulo base es la de disponer de un acceso controlado a la red y a Internet realizando un control de acceso basado en la identificación, filtrado y eliminación de paquetes de datos, detectando e impidiendo el acceso de posibles intrusos mediante una administración de seguridad centralizada.

Las políticas de seguridad de tráfico pueden definirse por tipo de servicio, dirección de origen, dirección de destino, puerto de origen, puerto de destino, protocolo de comunicación, etc. El Módulo de Firewall es Statefull Inspection, el Standard de la industria para firewalls, el cual extrae la información requerida para decisiones de seguridad y mantiene esta información en tablas de estado dinámicas para evaluar subsiguientes intentos de conexión. Esto proporciona una solución que es altamente segura y ofrece máximo rendimiento, escalabilidad y extensibilidad.

Mucho más que un Firewall

nX
NetworkExperts

Módulo VPN

Se denomina VPN -Red Privada Virtual o Virtual Private Network- a un mecanismo mediante el cual se puede atravesar de modo seguro y privado una red pública y a la cual se pueden conectar redes de ordenadores, usuarios móviles, proveedores y clientes y que es accesible a través de Internet estableciendo un túnel de información cifrada.

Si usted está ampliando su red para incluir trabajadores móviles y remotos está dando a los intrusos acceso sin precedentes a datos sensibles de la corporación. Para proporcionar a los usuarios finales libertad y movilidad a la vez que se protegen datos y aplicaciones debe establecerse una VPN.

Mediante la utilización de túneles cifrados, puede entubarse el tráfico crítico enrutando directamente los paquetes IP desde los clientes a los servidores utilizados y viceversa. Los túneles permiten también que dos o más redes internas en localidades remotas puedan verse y trabajar como si fueran la misma red, utilizando Internet como asiento del túnel, lo que representa un ahorro muy importante de costes, pudiendo llegar a sustituir líneas tipo punto a punto, frame relay o similares.

Módulo Gestión Ancho de Banda

Permite establecer un ancho de banda mínimo y máximo para un tipo concreto de tráfico. El ancho de banda de la red puede garantizarse para los servicios esenciales durante los períodos de alta congestión. Por lo tanto,

en caso de congestión, ese tipo de tráfico disfruta del ancho de banda asignado y no nota esa congestión. Moldee el ancho de banda de las redes de su organización. Asegúrese que las aplicaciones y recursos críticos reciben una cantidad garantizada del ancho de banda disponible.

En las redes en las que no se aplica ningún tipo de mecanismo para la gestión del ancho de banda el acceso a aplicaciones críticas puede ser menoscabado, o inclusive inhabilitado, por aplicaciones no críticas; personal bajando o subiendo grandes archivos vía http o ftp u observando aplicaciones multimedia vía Internet. Ciertos servicios de uso regular, pero de menos prioridad, como correos con pesados anexos, larguísimas colas de impresión, tráfico para efectuar respaldos y la copia o transferencia de archivos, sustraen el ancho de banda disponible y causan congestión en las redes provocando el colapso de aplicaciones críticas. Para evitarlo basta con aplicar políticas de gestión del ancho de banda.

Módulo Priorización de Tráfico

Asigna prioridad a uno o varios tipos de tráfico respecto a otros sin establecer un ancho de banda específico. Los tipos de tráfico con prioridad baja en momentos de congestión la notarán, sin embargo los tipos de tráfico con prioridad alta no la notarán.

Utilizando esquemas de priorización de tráfico que se modifiquen en función del tiempo se logra una mejor administración y uso de los recursos de ancho de banda limitados. En momentos en los que hay excesivo tráfico

y congestión se priorizan los servicios esenciales y se les entrega la mayor disponibilidad del ancho de banda; luego al disminuir la carga o cuando los servicios considerados esenciales no están en uso, el ancho de banda se retorna automáticamente al resto de los solicitadores de recursos. La diferencia respecto al Módulo de Gestión de Ancho de banda, radica en que con el Módulo de Priorización de Tráfico no se asignan anchos de banda mínimos ni máximos para un tipo de tráfico sino que lo que se asigna son prioridades.

Módulo de Alta Disponibilidad

Cuando disponemos de un nX Security Appliance, que controla la seguridad perimetral mediante el módulo de Firewall, que da acceso a usuarios remotos mediante VPN y que además gestiona el uso del ancho de banda disponible, mediante los módulos de gestión del ancho de banda y de Priorización de Tráfico, se convierte en un equipo crítico dentro de nuestra red que no puede fallar nunca. Para garantizar unos niveles de fiabilidad superiores al 99,99%, se dispone del Módulo de Alta Disponibilidad.

Mediante este módulo se tiene la posibilidad de trabajar con dos nX Security Appliance en cluster activo-pasivo con todas las características de los módulos que se hayan adquirido. De este modo se consigue, en caso de fallo en uno de los dos dispositivos, continuar disponiendo de todos los servicios sin que los usuarios noten que, al producirse el fallo, se han interrumpido las funcionalidades que disfrutaban.



Características técnicas

- Basado en Linux.
- Statefull Inspection.
- Alta Disponibilidad (cluster de Security Appliances).
- Gestión de Ancho de Banda.
- Priorización de Tráfico.
- Balanceo de Carga.
- VPNs mediante protocolos IPSEC 3DES, AES, PPTP tanto site-to-site como site-to-roadwarrior.
- Routing Avanzado que permite utilizar varios operadores de Internet de forma simultánea.
- Gestión Segura mediante SSL (entorno Web) o SSH (entorno texto).
- Protección contra ataques DoS como TCP SYN flood, ICMP flood, UDP flood, Smurf, Trinoo y IP spoofing.
- Posibilidad de recepción de notificaciones y actualizaciones automáticas.
- Comodidad en la definición de reglas de filtrado y NAT por puerto/protocolo.
- Solución escalable mediante módulos de ampliación para WIFI (802.11b/g), ADSL y RDSI, etc.

Modelos		SA3	SA4
Interfases Ethernet		3	4 ampliable a 8
Throughput VPN		67 Mbps	67 Mbps
Dimensiones (mm)		50x270x174	75x300x173
Peso		2,0 kg	2,4 kg
Potencia y consumo		AC 100-240 V (50/60 Hz) 60 W	
Temperatura		0° hasta +50° C	
Humedad		10 hasta 95%	
Sesiones concurrentes		256.000	512.000
Gestión		HTTPS, SSH	
Standards funcionales		IEEE 802.3, IPsec, IKE, PPPoE, L2TP/IPsec, 168-bit 3DES, TCP/IP v4 y v6, UDP, HTTP, HTTPS, SSLv1&2, SNMP v1, FTP, DHCP	
POLÍTICAS	Firewall	Ilimitadas	
	VPN	Remotas y concurrentes ilimitadas. Cliente IPsec	
	Ancho de Banda	Ilimitadas y anidables	
	Priorización de Tráfico	Ilimitadas y anidables	

nX Network Experts proporciona estas páginas y su contenido de buena fe sólo como información general y para guiarle en sus propósitos pero no da garantía o representación de que su contenido sea exacto, completo o actualizado. Aunque se ha hecho el máximo esfuerzo para asegurar que la información proporcionada es correcta en el momento de la impresión nX Network Experts no acepta responsabilidad alguna sobre errores u omisiones que pueda contener. Especificaciones sujetas a cambios sin preaviso. El throughput actual puede variar en función del tamaño del paquete y las características permitidas.

Linux es una marca registrada de Linus Torvalds. Los logotipos NX Network Experts y NX Security Appliance son marcas registradas o comerciales de Network Experts S.L. Los otros nombres de sociedades, productos o servicios pueden ser marcas registradas o marcas de servicios de terceros.

©2004 by Network Experts S.L. Impreso en Barcelona. Reservados todos los derechos. Se prohíbe la reproducción de esta publicación, ya sea mediante fotocopias, almacenamiento en un sistema de recuperación u otros métodos de transmisión sin el consentimiento previo de Network Experts S.L.