



UNIVERSIDAD MILITAR NUEVA GRANADA
ANEXO TÉCNICO 06
BALANCEADORES DE CARGA



Contenido

REQUERIMIENTOS TÉCNICOS

Ítem 1. Solución de Balanceo de Carga Calle 100

Ítem 2. Solución de Balanceo de Carga Campus Nueva Granada

Ítem 3. Administración de tráfico, Calle 100 y en el Campus Nueva Granada.

Ítem 4. Funciones de seguridad, Calle 100 y en el Campus Nueva Granada.

Ítem 5. Funciones de aceleración de tráfico, Calle 100 y en el Campus Nueva Granada.

Ítem 6. Funciones de Anti-DDOS, Calle 100 y en el Campus Nueva Granada.

Ítem 7. Web application firewall (WAF), Calle 100 y en el Campus Nueva Granada.

Ítem 8. Funciones de acceso, Calle 100 y en el Campus Nueva Granada.

Ítem 9. Estándares de red, Calle 100 y en el Campus Nueva Granada.

Ítem 10. Administración del sistema, Calle 100 y en el Campus Nueva Granada.

Ítem 11. Otros requerimientos

Ítem 12. Mejora Tecnología

Elemento solicitado



UNIVERSIDAD MILITAR NUEVA GRANADA
ANEXO TÉCNICO 06
BALANCEADORES DE CARGA



[por la Universidad](#)

[Características del elemento solicitado por la Universidad:](#)

1. REQUERIMIENTOS TÉCNICOS

La Universidad Militar Nueva Granada desea adquirir una solución capaz de administrar y proteger el conjunto de aplicaciones de misión crítica, brindando adicionalmente la capacidad de realizar aceleración de las mismas y balanceo de carga dentro del data center principal ubicado en las sedes de Calle 100 y en el Campus Nueva Granada.

Ítem 1. Solución de Balanceo de Carga Calle 100	Capacidad o Cantidad ofertada	Folio	Observaciones
Los equipos ofertados deben ser basados en una plataforma de hardware de propósito específico.			
El sistema operativo del equipo ofertado debe ser de propósito específico y no uno de uso genérico, es decir un SO desarrollado por el fabricante específicamente para propósitos de Balanceo de Carga de Servicios y Aplicaciones basadas en IP (TCP/UDP) y servicios web.			
Deben ser dos (2) equipos en Alta disponibilidad funcionando en par activo es decir que se vea un único balanceador, no una solución de clúster virtual entre múltiples equipos pues se busca eficiencia en energía, espacios en rack, administración y facilidad de configuración, escalable.			



UNIVERSIDAD MILITAR NUEVA GRANADA
ANEXO TÉCNICO 06
BALANCEADORES DE CARGA



<p>Cada equipo debe contar con las siguientes Interfaces de red: Puertos Ópticos a 10 Gbps. Con transceiver sfp+ Por cada Blade o appliance. Permitir crecimiento en puertos de Fibra Óptica a 10 Gbps</p>			
<p>Cada equipo debe contar con fuentes de poder redundantes AC intercambiables en caliente, entradas de voltaje de 110 a 220 VAC al igual que el fan tray.</p>			
<p>Los equipos deberán ser instalados en rack.</p>			
<p>Los equipos deben tener la característica de soportar alta disponibilidad y verse como un único balanceador, adicional tener la capacidad de conectarse a una unidad similar y operar en modo activo y la otra unidad en modo pasivo (fail-over) y deberá contar con la capacidad de direccionamiento virtual. El esquema debe tener la capacidad para recuperación de las sesiones del sistema en forma inmediata y automática en caso de fallo de un adaptador, cable de red, canal de controladora o alimentación de fluido eléctrico.</p>			
<p>Cada equipo deberá contar con interfaces de administración dedicada tipo lightout o fuera de banda garantizando administración continua.</p>			
<p>Debe soportar clúster Activo/Activo entre dos o más plataformas, no necesariamente del mismo modelo</p>			
<p>Para mejorar el rendimiento de la sincronización de configuración deberá poder sincronizar la configuración de manera incremental.</p>			
<p>Ante la necesidad de conmutar el tráfico a otros dispositivos del grupo, el sistema deberá poder realizar cálculos para determinar el mejor dispositivo basado en: recursos, capacidad, carga de tráfico en cada</p>			



UNIVERSIDAD MILITAR NUEVA GRANADA
ANEXO TÉCNICO 06
BALANCEADORES DE CARGA



dispositivo. Identificando la mejor opción cuando el ambiente sea heterogéneo en cuanto se refiere a plataformas			
La configuración será sincronizada entre todos los dispositivos del grupo pudiendo optar si la sincronización se realiza de manera automática o manual.			
La plataforma deberá garantizar la creación de mínimo instancias independientes para el perímetro con las funcionalidades de protección de DDoS y para la zona interna con balanceo local y web application firewall, estas dos instancias deben estar incluidas en 2 ambientes independientes Producción y Pruebas.			

Ítem 2. Solución de Balanceo de Carga Campus Nueva Granada	Capacidad o Cantidad ofertada	Folio	Observaciones
Los equipos ofertados deben ser basados en una plataforma de hardware de propósito específico.			
El sistema operativo del equipo ofertado debe ser de propósito específico y no uno de uso genérico, es decir un SO desarrollado por el fabricante específicamente para propósitos de Balanceo de Carga de Servicios y Aplicaciones basadas en IP (TCP/UDP) y servicios web.			
Deben ser un (1) equipo con redundancia interna a nivel de conectividad, fuentes de poder, sistema de ventilación y unidades de procesamiento, no una solución de clúster virtual entre múltiples equipos pues se busca eficiencia en energía, espacios en rack, administración y facilidad de configuración, la plataforma debe ser la misma marca que la ofrecida en calle 100.			



UNIVERSIDAD MILITAR NUEVA GRANADA
ANEXO TÉCNICO 06
BALANCEADORES DE CARGA



La plataforma debe contar con las siguientes Interfaces de red: Puertos Ópticos a 10 Gbps. Con mínimo 4 transceiver sfp+ por cada Blade o appliance. Permitir crecimiento de puertos de Fibra Óptica a 10 Gbps			
Cada equipo debe contar con fuentes de poder redundantes AC intercambiables en caliente, entradas de voltaje de 110 a 220 VAC al igual que el fan tray.			
Los equipos deberán ser instalados en rack.			
Los equipos deben tener la característica de soportar alta disponibilidad, es decir, tener la capacidad de conectarse a una unidad similar y operar en modo activo y la otra unidad en modo pasivo (fail-over) y deberá contar con la capacidad de direccionamiento virtual. El esquema debe tener la capacidad para recuperación de las sesiones del sistema en forma inmediata y automática en caso de fallo de un adaptador, cable de red, canal de controladora o alimentación de fluido eléctrico.			
Debe soportar clúster Activo/Activo entre dos o más plataformas, no necesariamente del mismo modelo			
Para mejorar el rendimiento de la sincronización de configuración deberá poder sincronizar la configuración de manera incremental.			
Ante la necesidad de conmutar el tráfico a otros dispositivos del grupo, el sistema deberá poder realizar cálculos para determinar el mejor dispositivo basado en: recursos, capacidad, carga de tráfico en cada dispositivo. Identificando la mejor opción cuando el ambiente sea heterogéneo en cuanto se refiere a plataformas			
La configuración será sincronizada entre todos los dispositivos del grupo pudiendo optar si la sincronización se realiza de manera automática o manual.			



UNIVERSIDAD MILITAR NUEVA GRANADA
ANEXO TÉCNICO 06
BALANCEADORES DE CARGA



<p>La plataforma deberá garantizar la creación de mínimo instancias independientes para el perímetro con las funcionalidades de protección de DDoS y para la zona interna con balanceo local y web application firewall, estas dos instancias deben estar incluidas en 2 ambientes independientes Producción y Pruebas.</p>			
-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------	--	--	--

Ítem 3. Administración de tráfico, Calle 100 y en el Campus Nueva Granada.	Capacidad o Cantidad ofertada	Folio	Observaciones
<p>La solución debe realizar funciones de balanceo de tráfico a aplicaciones basadas en TCP/UDP, incluidos servicios web.</p>			
<p>La solución debe permitir la definición de dirección IP y puerto virtual para la prestación de un servicio, que permita atenderlo mediante una granja de servidores identificados mediante una dirección IP y un puerto del servicio igual o diferente del presentado al público.</p>			
<p>La solución debe tener arquitectura Full-Proxy, control de entrada y salida de conexiones distinguiendo conexiones del lado del cliente y del lado del servidor o los recursos</p>			
<p>Deberá permitir hacer persistencia de conexiones hacia la aplicación con base en cualquier información contenida en cualquier parte del paquete completo, esto para poder adaptar la solución a las necesidades de las diferentes aplicaciones</p>			
<p>La solución debe permitir hacer control de balanceo de tráfico según se defina entre uno o varios tipos de algoritmos especializados de balanceo: Round Robin Proporcional dinámico Respuesta rápida Conexiones mínimas Análisis de carga Menor número de sesiones</p>			



UNIVERSIDAD MILITAR NUEVA GRANADA
ANEXO TÉCNICO 06
BALANCEADORES DE CARGA



El sistema debe ser capaz de identificar fallos en servicios para redundancia de las aplicaciones.			
La solución debe tener reglas que permitan el control de ancho de banda de manera dinámica			
Control de persistencia de las conexiones: Dirección IP origen Dirección IP destino Cookies Hash SIP: Debe permitir definir el campo SIP sobre el cual hacer persistencia Sesiones SSL Microsoft Remote Desktop Debe Permitir crear persistencia por cualquier valor del paquete por medio de reglas. Debe garantizar afinidad del servidor, de tal forma que una solicitud de un cliente y cada solicitud posterior se dirijan al mismo servidor de la granja.			
Soporte de API para construir aplicaciones de administración o monitoreo personalizadas: Soporte de SOAP/XML, que sea base del Sistema Operativo. Que permita la integración con aplicaciones como VMWare vCenter, Microsoft System Center Virtual Machine Manager (SCVMM), Soporte de Java, .NET, PERL, PHP, PowerShell o cualquier otra plataforma de virtualización. Las interfaces de control deben ser accesibles por conexiones SSL con requerimientos de autenticación vía http básica, para evitar accesos no autorizados. Soporte de API REST			
Deberá ser posible modificar el contenido HTML utilizando objetos de configuración y sin necesidad de generar scripts.			
El sistema deberá soportar scripts de programación basados en un lenguaje estructurado (TCL) que permita crear funcionalidades que por defecto no se encuentren en el menú de configuración u opciones y debe soportar la creación de Procedimientos o funciones que pueden ser utilizadas desde cualquier otro script			
El equipo debe ser compatible con tráfico IPSEC.			



UNIVERSIDAD MILITAR NUEVA GRANADA
ANEXO TÉCNICO 06
BALANCEADORES DE CARGA



Ítem 4. Funciones de seguridad, Calle 100 y en el Campus Nueva Granada.	Capacidad o Cantidad ofertada	Folio	Observaciones
Cada equipo debe soporte de seguridad SSL.			
La solución debe manejar AES, AES-GCM, SHA1/MD5 y soporte a algoritmos de llave pública: RSA, Diffie-Hellman, Digital SignatureAlgorithm (DSA) y Elliptic curve cryptography (ECC)			
Debe soportar e incluir Geolocalización de direcciones IP			
Cada equipo debe contar con Protección de la cookie de SYN contra ataques de SYNflood.			
Firmado criptográfico de cookies para verificar su integridad.			
Capacidad de integración con dispositivos HSM externos. Deberá soportar al menos ThalesnShield Y SafeNet Luna S			
La solución debe permitir la funcionalidad Proxy SSL. esta funcionalidad permite que sesión SSL se establezca directamente entre el usuario y el servidor final, pero el equipo balanceador debe ser capaz de des-encryptar, optimizar y re encryptar el tráfico SSL sin que el balanceador termine la sesión SSL			
Se requiere que soporte la extensión STARTTLS para el protocolo SMTP de manera de poder cambiar una conexión en texto plano a una conexión encriptada sin necesidad de cambiar el puerto.			



UNIVERSIDAD MILITAR NUEVA GRANADA
ANEXO TÉCNICO 06
BALANCEADORES DE CARGA



Ítem 5. Funciones de aceleración de tráfico, Calle 100 y en el Campus Nueva Granada.	Capacidad o Cantidad ofertada	Folio	Observaciones
La implementación de la solución debe incluir la capacidad de hacer aceleración de aplicación a nivel de: Memoria cache. Compresión tráfico HTTP.Optimización de conexiones a la aplicación a nivel TCP Multiplexación de conexiones hacia los servidores			
Debe soportar el protocolo SPDY y funcionar como Gateway SPDY aun cuando los servidores Web no soporten esta característica.			
Permitir la modificación de los tags de cache para cada objeto del sitio web de manera independiente, pudiendo respetar los tags generados por el Web server o modificarlos			
Permitir la definición de múltiples subdominios para un sitio web con el fin de incrementar el número de conexiones simultáneas que puedan darse desde un browser hacia este sitio.			
Permitir reordenamiento de contenido para objetos CSS y Javascript.			
Permitir especificar subdominios adicionales para permitir un mayor número de conexiones TCP mayor.			
Incorporar aceleración para contenidos PDF en el sitio Web			
El acelerador Web debe permitir optimización de imágenes en el sitio web cambiando el formato de la imagen, cambiando el tamaño de la imagen, eliminando encabezados EXIF, cambiando el número de colores.			
Permitir definir múltiples políticas de aceleración y políticas generadas por el usuario			



**UNIVERSIDAD MILITAR NUEVA GRANADA
ANEXO TÉCNICO 06
BALANCEADORES DE CARGA**



Debe contar con un editor de políticas de aceleración web integrado a la solución			
Permitir la configuración de reglas de aceleración basado en los encabezados del request o en los encabezados de la respuesta			
Permitir aceleración simétrica y asimétrica			
Soporte al protocolo SPDY, debe permitir funcionar como Gateway SPDY una cuando los servidores Web no soporten el protocolo			
Debe soportar optimización de video HTTP Live Streaming (HLS)			
Debe soportar Adaptive Forward Error Correction a nivel TCP y UDP			
Debe permitir optimización realizando "Content Inlining", permitiendo poner en línea Javascripts, CSS e imágenes directamente en el HTML (codificados)			
Debe soportar Minificación de contenido removiendo espacios y comentarios del código fuente de Javascripts y CSS reduciendo el tamaño de los archivos.			
La solución debe soportar la optimización de enlaces WAN entre dos equipos utilizando De duplicación, Compresión y optimizaciones TCP de ser necesario.			

Ítem 6. Funciones de Anti-DDOS, Calle 100 y en el Campus Nueva Granada.	Capacidad o Cantidad ofertada	Folio	Observaciones
--------------------------------------------------------------------------------	--------------------------------------	--------------	----------------------



UNIVERSIDAD MILITAR NUEVA GRANADA
ANEXO TÉCNICO 06
BALANCEADORES DE CARGA



Debe incluir protección contra ataques de DDoS en capas 2-4 utilizando vectores de ataque personalizables			
Debe bloquear ataques a nivel de red como flood, sweep, teardrop, smurfattacks			
Debe mitigar ataques basados en protocolos, incluyendo SYN, ICMP, ACK, UDP, TCP, IP, DNS, ICMP, ARP			
Opcionalmente debe soportar un sistema de suscripción de reputación IP para prevenir conexiones bidireccionales (entrantes y salientes) a direcciones IP no confiables y agrupadas en categorías.			
Debe permitir la creación de reglas basadas en aplicación, independientes para cada una de ellas.			
Debe permitir la creación de reglas globales.			
Debe permitir la definición de horarios que apliquen a las reglas configuradas, permitiendo activar reglas entre intervalos de tiempo hasta una fecha específica.			
Debe soportar e incluir Geolocalización de direcciones IP			
Debe permitir la creación de listas blancas de direcciones IP			
Debe permitir la configuración de túnel IPSECSite-to-Site			
Debe incluir funcionalidad de application delivery controller o integrarse con dispositivos de ApplicationDelivery			
Debe brindar protección contra Ataques de Denegación de Servicio para el protocolo DNS, poder controlar el tráfico DNS de acuerdo al tipo de registro solicitado y detectar anomalías a nivel del protocolo			
Debe brindar protección contra Ataques de Denegación de Servicio para el protocolo SIP y poder controlar el tráfico SIP de acuerdo al Método SIP recibido y detectar anomalías a nivel del protocolo			



**UNIVERSIDAD MILITAR NUEVA GRANADA
ANEXO TÉCNICO 06
BALANCEADORES DE CARGA**



Debe permitir personalizar los Logs, y ser exportados a un repositorio Syslog externo que conste de uno o varios servidores.			
------------------------------------------------------------------------------------------------------------------------------	--	--	--

Ítem 7. Web application firewall (WAF), Calle 100 y en el Campus Nueva Granada.	Folio	Observaciones
Debe trabajar en un esquema proxy TCP reverso y/o transparente		
Debe soportar la creación automática de políticas		
La creación automática de políticas deberá unificar múltiples Urls explícitas utilizando wildcards de manera de reducir la cantidad de objetos en la configuración.		
Debe trabajar en modo de bloqueo o en modo informativo		
Debe permitir diferentes políticas de seguridad para diferentes aplicaciones		
Debe permitir la creación de firmas personalizadas		
Debe trabajar con modelos de seguridad positiva y negativa		
Debe poder aprender el comportamiento de la aplicación automáticamente sin intervención humana		
Debe permitir personalizar las páginas de bloqueo incluyendo la capacidad de responder a webservices mediante un código HTTP 500.		
Debe prevenir exponer el "OS fingerprinting"		



UNIVERSIDAD MILITAR NUEVA GRANADA
ANEXO TÉCNICO 06
BALANCEADORES DE CARGA



Debe permitir la integración con Herramientas de verificación de vulnerabilidades.		
<p>El WAF debe soportar:</p> <ul style="list-style-type: none"> • Restringir protocolo y versión utilizada multi-byte language encoding • Validar URL-encoded characters • Restringir la longitud del método de request • Restringir la longitud del URI solicitado • Restringir el número de Encabezados (headers) • Restringir la longitud del nombre de los encabezados • Restringir la longitud del valor de los encabezados • Restringir la longitud del cuerpo (body) de la solicitud • Restringir la longitud del nombre y el valor de las cookies • Restringir el número de cookies • Restringir la longitud del nombre y valor de los parámetros • Restringir el número de parámetros 		
El WAF Debe incluir protección a Web Services XML y restringir el acceso a métodos definidos vía Web Services Description Language (WSDL)		
El WAF debe incluir protección contra el Top 10 de ataques definidos en OWASP		
El WAF debe incluir protección contra Web Scraping		
Debe ser Session-aware es decir identificar y forzar que el usuario tenga una sesión e identificar los ataques por usuario		
Permitir la definición y detección de las condiciones a cumplir para que una aplicación externa que vía Java realiza un requerimiento crossdomain, permitiendo evitar un CORS (Cross-OriginResourceSharing).		



UNIVERSIDAD MILITAR NUEVA GRANADA
ANEXO TÉCNICO 06
BALANCEADORES DE CARGA



Debe permitir verificar las firmas de ataque en las respuestas del servidor al usuario		
Debe permitir el enmascaramiento de información sensible filtrada por el servidor		
Debe poder bloquear basado en la ubicación geográfica e incluir la base de datos de geolocalización.		
Debe permitir la integración con servidores Antivirus por medio del protocolo ICAP		
Debe brindar reportes respecto a la normativa PCIDSS 2.0		
Debe proteger contra ataque DoS /DDoS de Capa 7		
Una vez detectado un ataque deberá ser posible descartar todos los paquetes que provengan de una dirección IP sospechosa		
En caso de detectarse un ataque se requiere tener la posibilidad de iniciar una captura de tráfico (tipo tcpdump) para poseer información forense.		
Debe soportar tecnologías AJAX y JSON		
Debe proteger como mínimo: Ataques de Fuerza Bruta Cross-site scripting (XSS)Cross Site Request Forgery SQL injection Parameter and HPP tampering Sensitive information leakage Session highjacking Buffer overflows Cookie manipulation Various encoding attacks Broken access control Forceful browsing Hidden fields manipulation Request smuggling XML bombs/DoS Open Redirect		
Debe poder identificar y configurar Urls que generen un gran consumo de recursos en los servidores como método de protección de ataques de denegación de servicios.		



UNIVERSIDAD MILITAR NUEVA GRANADA
ANEXO TÉCNICO 06
BALANCEADORES DE CARGA



Debe permitir verificaciones de seguridad y validación a protocolos FTP y SMTP		
Debe permitir comparar dos políticas de seguridad y mostrar las diferencias entre ambas		
El equipo debe soportar bases de datos de reputación de IP que permita bloquear tráfico desde y hacia direcciones IP en categorías como: Scanners Exploits Windows Denial of Service Proxies de Phishing Botnets Proxies anónimos		

Ítem 8. Funciones de acceso, Calle 100 y en el Campus Nueva Granada.	Folio	Observaciones
El equipo debe soportar la implementación de VPN SSL		
Entre los métodos soportados deben incluir un modo "Portal" donde la máquina se comporte como un proxy reverso, buscando los contenidos de portales web internos y presentarlos como vínculos seguros en el portal del usuario		
Entre los métodos soportados deben incluir un modo de "Network", donde un usuario se conecta a la red interna obteniendo una dirección IP enrutable dentro de la red interna		
Proporcionar un acceso remoto seguro a toda la red para cualquier aplicación basada en IP (TCP o UDP)		
Soporte de Split Tunnel, solo el tráfico especificado debe ir por VPN		
Soportar túneles de aplicación, donde únicamente una aplicación en particular tenga acceso a los recursos de red		



UNIVERSIDAD MILITAR NUEVA GRANADA
ANEXO TÉCNICO 06
BALANCEADORES DE CARGA



Soporte de compresión HTTP.		
Permitir establecimiento de una conexión segura para el acceso remoto sin la necesidad de instalar software de cliente en la máquina del usuario		
Permitir un transporte seguro utilizando encapsulamiento DTLS (Datagramas TLS)		
Posibilidad de personalizar la página de acceso de usuario, portal, y mensajes de pre-inicio de sesión presentados al usuario		
De requerirse se deben incluir licencias para usuarios simultáneos VPN SSL mínimo 500 conexiones.		
El equipo suministrado debe soportar un crecimiento de 1000 usuarios concurrentes VPN SSL, que se pueden habilitar por medio de licencias adquiridas a futuro		
El equipo debe tener soporte para Single-Sign-On (SSO)		
El equipo deberá ser capaz de solicitar las credenciales de usuario sólo una vez, y autenticar al usuario en todos los portales que requieran autenticación		
El equipo debe ser capaz de almacenar en caché todas las credenciales del usuario y utilizar las credenciales adecuadas en cada portal (por ejemplo, algunos portales requieren correo electrónico como nombre de usuario, otros requieren el usuario de Dominio/ AD).		
La solución es incluir soporte para la validación de la estación del usuario. Debe validar por lo menos: Presencia de anti-virus y que este actualizado Presencia de Firewall personal Presencia de los procesos ejecutándose en el equipo Presencia de los certificados digitales instalados en la máquina Presencia de		



UNIVERSIDAD MILITAR NUEVA GRANADA
ANEXO TÉCNICO 06
BALANCEADORES DE CARGA



archivos en el equipo Búsqueda de entradas de registro en clientes Windows Verificación de Sistema Operativo Identificación de hardware del equipo CPU Motherboard Número Serial BIOS MAC Address		
Para cada elemento de la validación de la estación del usuario, debe ser posible configurar una acción a tomar si la prueba es satisfactoria o no.		
La configuración de estas acciones debe ser a través de una interfaz gráfica y fácil de entender		
El sistema debe ser capaz de verificar la ubicación geográfica de las direcciones IP, lo que permite la creación de reglas de acceso en función del país o del estado		
La base de datos de direcciones IP debe estar presente en la caja, y debe ser periódicamente suministrada por el fabricante de la solución sin coste adicional		
La solución debe ser capaz de autenticar a los usuarios contra sistemas LDAP, LDAPS, RADIUS, TACACS+, Directorio Activo, HTTP, RSA, OCSP, CRLDP		
La solución debe soportar limpieza de cache del lado del cliente final		
La solución debe permitir la creación de un Entorno Protegido para los usuarios donde no se permita la creación de archivos fuera del entorno.		
La solución debe ser compatible con múltiples factores de autenticación que utiliza tokens de hardware		
La solución debe soportar el uso de un cliente stand-alone incluido con la solución		



UNIVERSIDAD MILITAR NUEVA GRANADA
ANEXO TÉCNICO 06
BALANCEADORES DE CARGA



El cliente stand-alone debe ser capaz de hacer Roaming inteligente, donde el cambio de dirección IP no implica re-autenticación manual del usuario sin importar el tipo de enlace utilizado. (Punto de Acceso WiFi, 3G, etc.)		
-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------	--	--

Item 9. Estándares de red, Calle 100 y en el Campus Nueva Granada.	Folio	Observaciones
Soporte VLAN 802.1q, Vlan tagging		
Soporte de 802.3ad para definición de múltiples troncales		
Soporte de NAT, SNAT		
Soporte de IPv6: El equipo debe funcionar como Gateway entre redes IPv6 e IPv4 permitiendo tener ambos tipos de redes simultáneamente.		
Soporte de Rate Shapping.		
Soporte de dominios de enrutamiento, donde cada uno pueda tener su propio Default Gateway y estar conectados a redes IP con el mismo direccionamiento.		
Debe soportar VXLAN, VXLAN Gateway, NVGRE y Transparent Ethernet Bridging para entornos de redes virtualizadas.		
El cliente stand-alone debe soportar Windows, Linux, MAC OS, iOS, Android		



UNIVERSIDAD MILITAR NUEVA GRANADA
ANEXO TÉCNICO 06
BALANCEADORES DE CARGA



Debe soportar Single-Sign-On utilizando Security AssertionMarkupLanguage (SAML) 2.0 funcionando como identityprovider (IdP) y/o serviceprovider (SP).		
-------------------------------------------------------------------------------------------------------------------------------------------------------	--	--

Ítem 10. Administración del sistema, Calle 100 y en el Campus Nueva Granada.	Folio	Observaciones
La solución debe permitir el acceso para la administración del equipo appliance vía CLI (Interfaz de línea de comandos) por SSH, interfaz de administración gráfica basada en Web seguro (HTTPS)		
La solución de integrarse con Directorio Activo Windows 2003 o superior, LDAP, RADIUS.		
La solución debe incluir comunicación cifrada y permitir la autenticación del equipo y de los usuarios administradores/supervisores con Certificados Digitales.		
La solución debe soportar el envío de alertas y eventos a un Sistema Centralizado mediante: Protocolo SysLog Notificación vía SMTPSNMP versión 2.0 o superior.		
El sistema de administración debe ser totalmente independiente del sistema de procesamiento de tráfico.		
El equipo debe contar con un módulo de administración tipo lightsout que permita encender/apagar el sistema de manera remota y visualizar el proceso de arranque.		
La interfaz gráfica debe contar con un Dashboard personalizable que permita monitorear el estado del equipo en tiempo real		
Debe contar con un módulo de reportes que permita visualizar gráficamente el comportamiento de las aplicaciones HTTP como latencias hacia los servidores, latencias en los URL, Direcciones IPs que acceden		



**UNIVERSIDAD MILITAR NUEVA GRANADA
ANEXO TÉCNICO 06
BALANCEADORES DE CARGA**



las aplicaciones, Urls más visitados en las aplicaciones, Throughput hacia los servidores y estadísticas acerca de los servicios creados y los servidores físicos.		
Debe Contar con plantillas para la implementación rápida de aplicaciones de mercado conocidas (ej., Oracle, Microsoft, SAP, IBM) y permitir crear plantillas personalizadas que puedan ser actualizadas/exportadas entre equipos.		

Ítem 11. Otros requerimientos	Folio	Observaciones
La solución debe permitir configurar clúster entre chasis o equipos de rack con el fin de contar con un sistema altamente escalable y en demanda que permita hacer failover de uno o más servicios hacia cualquier equipo miembro del clúster.		
1 Año de Garantía de fábrica (mínimo requerido)		
1 Año en modalidad 7x24x4 de Tiempo de Servicios de reposición de partes y piezas (Hardware) (mínimo requerido)		
Tiempo máximo de respuesta a llamadas de servicio técnico para reposición de Hardware de 4 horas en modalidad 7x24x4 Proactivo, una vez confirmado el daño de la parte y la necesidad de reposición		
Tiempo de Servicios de actualización del sistema operativo (Software) y Sistema de gestión 1 año en modalidad 7x24x4) (mínimo requerido)		
El oferente deberá adjuntar en su propuesta una hoja de vida de un ingeniero especialista en networking para que lidere las actividades de instalación e integración con la red actual, con certificación técnica a nivel de especialización (Cisco CCIE, HP MASE, Juniper JNCIE-ENT).		



**UNIVERSIDAD MILITAR NUEVA GRANADA
ANEXO TÉCNICO 06
BALANCEADORES DE CARGA**



Esto con el fin de garantizar la calidad en la integración de los productos ofrecidos.		
El oferente debe ser partner, además de estar autorizado en Colombia por el fabricante de los equipos ofertados y estar en capacidad técnica de configurar mantener y dar soporte técnico de los equipos. En consecuencia el oferente deberá presentar documentación que lo acredite como partner de la marca, documento que debe ser expedido por el fabricante de los equipos ofertados.		
El contratista deberá realizar capacitaciones oficiales (impartidas por fabricante) del producto ofrecido para los módulos de Administración, DDoS, Balanceo de Datacenter y Protección de aplicaciones en capa 7, cada capacitación deberá ser independiente y el plan de estudio deberá ser aprobado por la entidad		

Ítem 12. Mejora Tecnología				
Elemento solicitado por la Universidad	Características del elemento solicitado por la Universidad:	Elemento propuesto	Comparativo de mejora	Justificación

Se solicita a los proponentes diligenciar en su integridad el presente anexo, con el fin de facilitar la verificación de su ofrecimiento.