La intarface de Web Interface ha sufrido, probablemente cientos de evaluaciones en entornos de clientes, así como auditorías periodicas de seguridad de Citrix, todo ello cmo parte del proceso de desarrollo seguro que Citrix dispone.
Web Interface, se ha diseñado con todas las funcionalidades y control de las amenazas conocidas de aplicaciones Web, y en el proceso de “webappsec” que permite el control y la defensa contra nuevos ataques a medida que estos van surgiendo.

La protección y endurecimiento del propio servidor Web es el primero o la primera de las mejores prácticas recomendadas para todo el mundo.

Existen aún algunos clientes que desean emplear medidas adicionales, como un Firewall y otros sistemas de seguridad para la detección de ataques. NetScaler puede ser fácilmente configurado para proporcionar seguridad adicional en una aplicación Web mediante SSL.

Para Citrix los aspectos específicos de la seguridad y la administración debe comenzar por comprender la razón del negocio, enfocado a la publicación de los recursos (aplicaciones, escritorios, documentos, etc) a través de la web, y las políticas adecuadas sobre los derechos de acceso y restricciones.

Estos requisitos de diseño son necesarios para el sistema que presta el servicio, incluyendo la configuración de la interfaz web. El objetivo aquí es, sobre todo garantizar que a los usuarios autorizados se les permita el acceso, mientras que los usuarios no autorizados se les niega el acceso, y que las políticas no se eludan en dicho control.

Web Interface tiene un papel de intermediación en el sistema de prestación de servicio, por lo que es una solución eficaz para aplicar determinadas políticas, por ejemplo, garantizar la autenticación fuerte, en este caso ello ocurre antes de concederse el acceso, mediante el uso de dispositivos adicionales integradas con Active Directory y un sistema de digitos de autenticación adicional sumadas al sistema de validación tradicional.

Todo este sistema puede ser ampliada considerablemente con Citrix Access Gateway, en este

caso integrando la interfaz Web permitiendo desempeñar un papel de soporte en la defensa mediante el uso de políticas. También permite llevar a cabo una serie de características sensibles, como cambio de contraseñas y de restablecimiento de la contraseñas.

Las precauciones de seguridad prescritas para WI, pueden ser variables.

Hay unas cuantas precauciones estándar se recomienda seguir :

- Requerir SSL en el servidor Web Interface, lo que protege las credenciales de usuario en el tránsito y ayuda a prevenir ataques de "spoofing" (como las que podrían derivarse de las recientes vulnerabilidades DNS).
- Usar SSL o IPSec para las solicitudes a los servicios XML en XenApp o XenDesktop; de nuevo este protege las credenciales.
- Desactivar el puerto HTTP, o que tengan que reorientar a HTTPS. Luego, para prevenir posibles ataques de "phishing" (MITM en contra de la conexión HTTP a que redireccione un sitio replicado WI) la opción de configuración desede Internet debe de estar desactivado.
- Siempre que sea posible, se recomienda utilizar Kerberos o una tarjeta inteligente en apoyo en el proceso de validación con XenApp que evita la necesidad de enviar las contraseñas a todos.

Evidentemente la seguridad es un hecho que no deja de ser importante en cualquier plataforma, pero siempre hay que tener en cuenta que una seguridad excesiva puede producir un sistema totalmente inoperativo e inaccesible, en este sentido es siempre aconsejable buscar el punto intermedio que se adapte mejor a las necesidades reales de nuestro negocio o clientes.