

**Los Firewalls VPN de NETGEAR ayudan a
pequeñas y medianas empresas a alcanzar la
compatibilidad con los estándares PCI en 2009**

Introducción

La comunicación empresarial depende cada vez más de Internet. Los robos y fraudes de identidades online también se han vuelto más comunes. Los hackers y cibercriminales utilizan diferentes métodos para entrar en los sistemas y robar información personal a cambio de dinero. Los objetivos online más atacados son las empresas de venta y de procesos de pago online. Como resultado, millones de números de tarjetas de crédito han caído en manos de hackers y criminales durante los últimos años. En Enero del 2007, unos hackers entraron en los sistemas informáticos de una cadena de tiendas de descuento, T.J. Maxx, y robaron la información de casi 45 millones de tarjetas de crédito y débito¹. La información robada incluía números de tarjeta, información de la transacción y datos personales del usuario. En Enero del 2009, la empresa de proceso de pagos Heartland Payment Systems publicó una nota de prensa informando de que un keylogger se había infiltrado en su sistema en el año 2008². Heartland Payment Systems procesa tarjetas de crédito/débito y otras transacciones de pagos de unos 250.000 usuarios de todo el país con casi 100 millones de transacciones al mes. Todavía se desconoce la magnitud del daño causado. Casos como los mencionados en este apartado han causado a muchas empresas daños insuperables y han puesto en peligro la información privada financiera de muchas personas.

Compatibilidad con PCI

Dado que las amenazas con cada vez más sofisticadas, ya no es suficiente con nombres de usuarios, claves encriptadas y la presencia de un firewall para proteger las redes. Las empresas de informática y seguridad han reconocido la necesidad de ir más allá de los procesos de seguridad tradicionales. Por eso la Industria de tarjetas de Pago creó un estándar para la información de seguridad en los procesos de pago (PCI DSS - Payment Card Industry Data Security Standard). PCI DSS define 12 requisitos base de cómo la información de acceso de un usuario de tarjeta de crédito es monitorizada, cargada, controlada y auditada.

Desde su introducción, el Consejo de Estándares de Seguridad PCI (PCI Security Standards Council) ha solicitado a todas las empresas, comerciantes y proveedores de servicios que operan o transmiten información de cuentas de pago, tener dos modos de autenticación para accesos remotos a la red por parte de los empleados, administradores y terceros. NETGEAR ha reconocido y respondido a este nuevo requisito añadiendo un sistema más robusto de autenticación conocido como 2FA o T-FA (Two Factor Authentication) a la tecnología SSL e IPsec de su línea de productos Firewall VPN para ayudar a las empresas a cumplir la compatibilidad con los nuevos estándares PCI.

Requisitos PCI para ser compatible con los dos modos de autenticación (Two-Factor Authentication)

8.3 Implementar dos modos de autenticación para accesos remotos a la red por parte de los empleados, administradores y terceros. Utilizar tecnologías tales como autenticación remota y servicio dial-in (RADIUS) o sistema de control de accesos por terminal controlador de accesos (TACACS - Terminal Access Controller Access Control System) con señales; o VPN (basado en SSL/TLS o IPsec) con certificados individuales

Dos factores de Autenticación

La autenticación mediante dos factores es una solución de seguridad nueva que mejora y refuerza la seguridad implementando múltiples factores en el proceso de autenticación que cuestiona y confirma las identidades de los usuarios antes de que ellos puedan acceder a la red. Hay varios factores que se utilizan para validar usuarios y asegurarse de que ellos son los que dicen ser. Estos factores son:

- 1.- Algo que tú sabes - por ejemplo, tu clave o tu PIN
- 2.- Algo que tú tienes - por ejemplo un objeto o un teléfono compatible con JAVA que genera un código de acceso de entre 6 u 8 dígitos de largo.
- 3.- Quién eres - por ejemplo, nombre de usuario o biometría como huella digital o de retina.

Para los propósitos de este documento vamos a centrarnos y discutir los dos primeros: algo que tú sabes y algo que tú tienes. Este nuevo método de seguridad puede verse como dos formas de autenticación porque simplemente confía en lo que sabes y lo que tienes. Un ejemplo común de una autenticación de dos factores es una tarjeta de banco (ATM) que lo emite una institución bancaria:

- 1.- El PIN para acceder a tu cuenta es “algo que sabes”
- 2.- La tarjeta para el cajero automático es “algo que tienes”

Una persona debe tener ambas para tener acceso a su cuenta bancaria. Del mismo modo, el acceso a redes y datos corporativos también pueden reforzarse utilizando una combinación de factores como un PIN y un objeto (hardware o software) para validar al usuario y reducir los robos de identidades online.

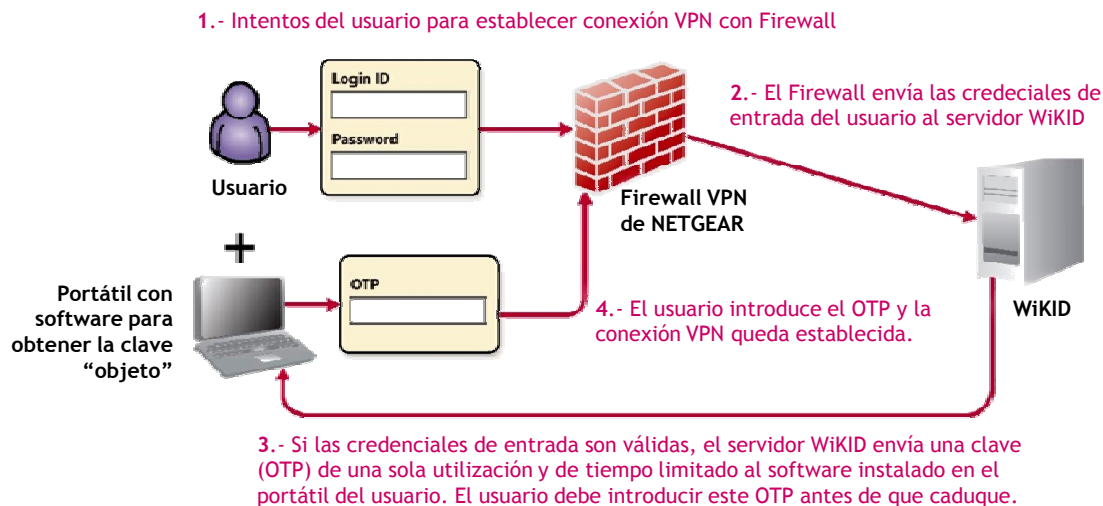
La implementación de autenticación de dos factores de NETGEAR

NETGEAR ha implementado una solución de autenticación de dos factores desde WiKID (www.wikidsystems.com). WiKID es una solución en la que se solicita un objeto basado en software. En vez de utilizar el Windows Active Directory o LDAP como servidor de autenticación, los administradores ahora tienen la opción de utilizar el servidor de autenticación WiKID para ofrecer una autenticación robusta en los productos de firewall con tecnología SSL, VPN y UTM de NETGEAR.

La solución WiKID está basada en una arquitectura de pregunta-respuesta donde se genera una clave de un sólo uso (OTP - One Time Passcode), que se sincroniza con el servidor de autenticación y se envía al usuario una vez el servidor confirma la validez del usuario. Los usuarios finales pueden fácilmente poner en funcionamiento esta arquitectura de pregunta-respuesta, reduciendo de forma considerable los costes de implementación y mantenimiento.

Tradicionalmente un usuario entraría a la red utilizando solamente su nombre de usuario y clave, teniendo de este modo acceso completo a la red. Con la solución WiKID, un usuario puede lanzar el software para obtener un OTP, la clave generada puede ser utilizada esa vez y por un tiempo limitado, junto con el nombre de usuario para entrar en la red. Si los usuarios no utilizan el OTP en ese momento, tienen que pedir un nuevo OTP antes de poder entrar en la red.

Explicemos como funciona. Cada usuario sabe su nombre de usuario y clave (algo que sabes). Los nombres de usuario y claves se almacenan o se asocian con el servidor de autenticación WiKID. Como segundo factor en el proceso de autenticación, los usuarios necesitarán utilizar el software (algo que tienes) para verificar quiénes son. El software se comunica con el servidor de autenticación WiKID para validar el nombre de usuario y la clave. Una vez que el nombre de usuario y la clave se validan, se generará un OTP para el usuario. Entonces el usuario puede introducir su nombre de usuario (algo que sabe) y ese OTP (algo que tiene) para acceder a la red. Combinando el nombre de usuario, la clave y el OTP dado por el servidor de autenticación WiKID, la autenticación por dos factores asegura la seguridad de la red.



La implementación de la autenticación de dos factores de NETGEAR se ha añadido sin cargo alguno a través de una actualización de firmware a los siguientes firewalls VPN:

- FV336G
- FVS338
- FVX538
- DGFV338

Conclusión

NETGEAR comprende la importancia de ser compatible con PCI. Mientras que muchas empresas siguen trabajando para ser compatibles con PCI, NETGEAR ya ha implementado una solución de autenticación de dos factores en todos sus productos firewall con tecnología SSL, VPN y UTM. La autenticación de dos factores es otro paso para mejorar la seguridad de la red y al mismo tiempo cumplir con los estándares PCI sin tener que reemplazar el hardware existente. Para obtener y probar la nueva solución de autenticación de dos factores en sus productos, visite la página de Servicio de Soporte de Producto de NETGEAR: <http://kbserver.netgear.com>

¹ <http://www.msnbc.msn.com/id/17871485/>

² http://www.usatoday.com/money/perfi/credit/2009-01-20-heartland-credit-card-security-breach_N.htm