Hanwha Vision

White Paper

Seguridad cibernética

Protección de dispositivos de vigilancia por vídeo para cerrar vulnerabilidades de red

17/11/2020

Índice

1. Introducción

Vivimos en un mundo cada vez más conectado donde cada vez más dispositivos y sistemas son conectados en red y compartidos con otros sistemas. La conveniencia es el principal impulsor de esta tendencia, ya que las personas esperan tener la capacidad de conectarse y controlar dispositivos y sistemas en cualquier lugar, en cualquier momento.

Sin embargo, existe una desventaja para el nivel de conveniencia sin precedentes suministrado por el creciente número de dispositivos en red, o sea, mayor riesgo para la seguridad. Como cada dispositivo es un punto de extremo para redes, ellos presentan el potencial de convertirse en puntos de entrada para hackers y otras personas con intenciones maliciosas. En realidad, en muchas de las más recientes violaciones de datos que ocurrieron recientemente, los hackers lograron acceder a redes corporativas por medio de POS, *AVAC y otros sistemas en red que no ofrecieron un nivel adecuado de seguridad para evitar estos tipos de violaciones.

*AVAC: calefacción, ventilación y aire condicionado

Vigilancia por vídeo con base en IP y otras soluciones crecieron en popularidad para convertirse en el estándar aceptado para nuevas implementaciones y actualizaciones y los sistemas de seguridad no son excepción. Un hacker no discrimina entre dispositivos en red, ya sea que ejecuten o no alguna función importante como seguridad. Como tal, cámaras de vigilancia por vídeo y otros dispositivos están en la extensa lista de posibles puntos de entrada en la red que están siendo continuamente probados con respecto a vulnerabilidades que pueden ser explotadas. Por tanto, es esencial que las organizaciones tomen las medidas necesarias para garantizar el más alto nivel de seguridad para sus redes y cámaras IP, codificadores, NVRs y DVRs. Hay varias prácticas recomendadas que deben ser adoptadas para fortalecer la seguridad del dispositivo a fin de impedir el acceso no autorizado y proteger los sistemas de vigilancia por vídeo de los usuarios finales y su red en general.

Hanwha Vision no solamente está consciente de estas prácticas recomendadas, sino también incorporó varias tecnologías y recursos en sus productos para facilitar la organización de esos importantes pasos para mejorar la seguridad de la red.

Estos ítems deben ser revisados por el propietario de los sistemas de seguridad, equipo de TI e integradores de sistemas que instalan sistemas para determinar el nivel de seguridad necesario, equilibrando la facilidad de uso con riesgos aceptables.

Esta guía mostrará instantáneas de cámaras de red, cuando sea aplicable. La mayoría de las configuraciones puede ser definida en lote para varias cámaras usando el software administrador de dispositivos Wisenet (Figura 1).

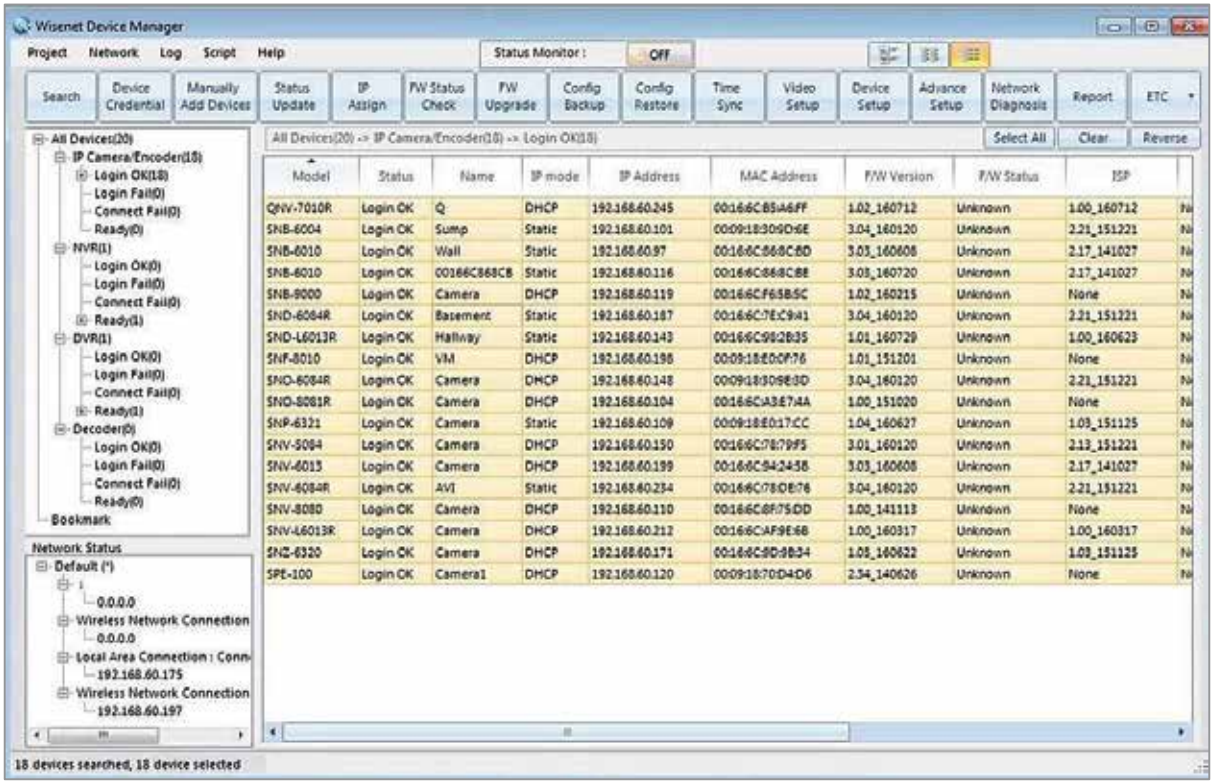

Imagen 1. Pantalla del Administrador de dispositivos Wisenet

2. Contraseña

Desde la verificación de e-mails hasta el desbloqueo de smartphones o logon en computadoras, las contraseñas son parte integrante de nuestras vidas diarias. Por eso, parece muy intuitivo que las personas reconozcan la importancia de crear contraseñas fuertes para proteger sus dispositivos y redes pero en realidad no siempre ese es el caso. Estas prácticas recomendadas ayudarán a garantizar el más alto nivel de seguridad de las contraseñas.

Si dispositivos como cámara y grabador tuvieren una contraseña inicial el usuario no deberá utilizar la contraseña inicial y definir su propia contraseña pues la contraseña inicial es ampliamente abierta por medio del manual del usuario o de Internet. Hanwha Vision no suministra una contraseña inicial y todos los dispositivos son proyectados para definir la contraseña en su uso inicial.

Sin embargo solamente la modificación de la contraseña no es suficiente. Porque muchas personas cometen dos errores con mucha frecuencia para su conveniencia al definir la contraseña.

El primero es utilizar la misma contraseña para todo. El peligro aquí es que, si alguien logra descifrar la contraseña, digamos, de su cuenta de e-mail, tendrá acceso a todo lo que fue protegido por contraseña, abriendo un potencial para robo, robo de identidad y mucho más. El segundo — y más arriesgado — error que las personas cometen para recordar más fácilmente sus contraseñas es utilizar nombres, fechas de nacimiento y/o palabras que pueden ser encontradas en el diccionario.

Hackear se convirtió en una práctica altamente organizada y sofisticada que emplea herramientas poderosas como tecnologías que circulan de manera rápida y automática por combinaciones posibles de palabras para descifrar contraseñas. Estas herramientas han sido muy exitosas con contraseñas fácilmente recordadas que son muy convenientes para los usuarios. Además de esto, con tantas informaciones personales disponibles online, contraseñas que usan nombres, cumpleaños u otras fechas importantes también pueden ser fácilmente descubiertas. Así, es imperativo usar contraseñas fuertes que sean mucho más difíciles de descubrir. Hay muchas prácticas recomendadas que deben ser seguidas para conseguir esto utilizándose una combinación de letras, números y otros símbolos.

A pesar de que no sea obligatorio también es una buena práctica utilizar contraseñas diferentes para cada dispositivo o utilizar la misma contraseña solamente para algunos — no todos — de los dispositivos, clientes y sistemas en la red. Es altamente recomendable crear un nombre de usuario exclusivo en vez de usar la cuenta de administrador del VMS (software administrador de vídeo) y de otros clientes para conectarse. Esto impide que la contraseña del administrador sea constantemente transmitida por la red, en un esfuerzo para evitar que sea interceptada.

Los productos de Hanwha Vision exigen una contraseña de 8 a 15 letras. Si la contraseña tiene de 8 a 9 letras ella debe ser una combinación de por lo menos tres tipos de letras mayúsculas/minúsculas, números y caracteres especiales. Si la contraseña tiene de 10 a 15 letras ella debe ser una combinación de por lo menos dos tipos de letras mayúsculas/minúsculas, números y caracteres especiales. Además de esto, secuencia de texto consecutiva o repetida no está disponible para contraseña.

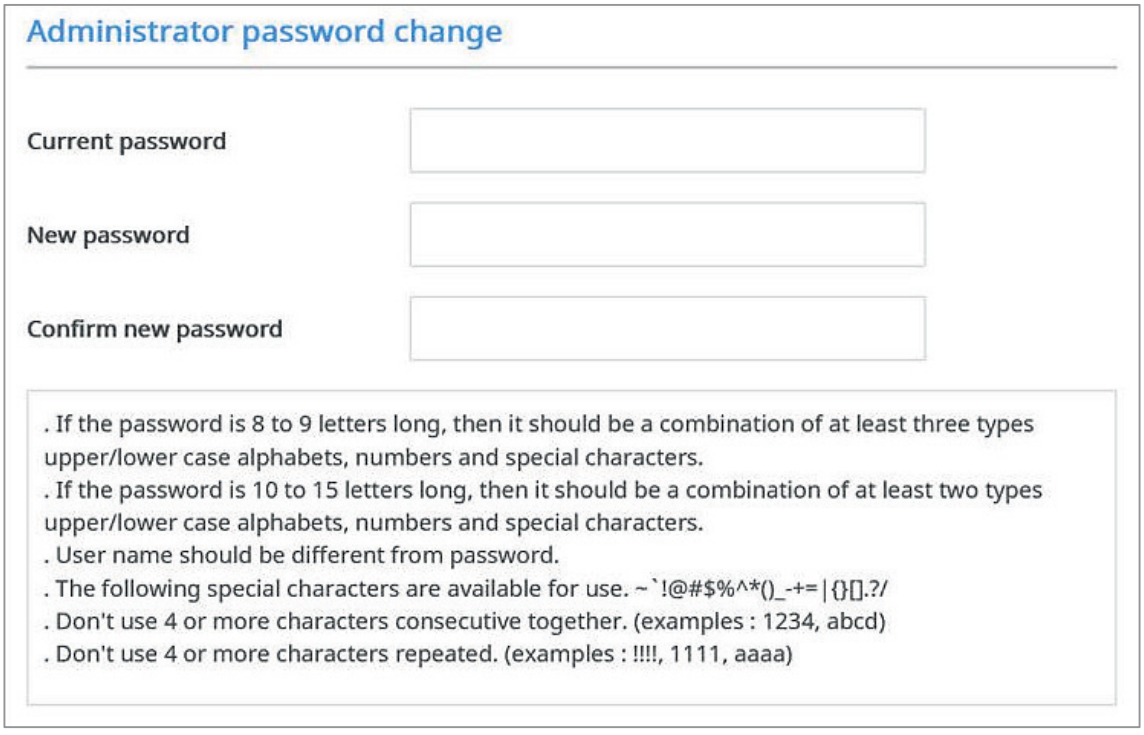

Imagen 2. Configuración de la contraseña de la cámara

3. Separación de autoridad

Limitar la autorización asociada a esta cuenta exclusiva también limita el acceso de hackers. Por tanto, si una cuenta es comprometida, el impacto no afectará a la cámara entera, incluyendo sus configuraciones. Además de esto, credenciales exclusivas tornan mucho más fácil e informativo el análisis de registros. Cámaras y grabadores de Hanwha Vision permiten que muchos usuarios/ grupos de usuarios sean creados con varios permisos y niveles de usuario.

3.1. Principio del menor privilegio

Use el principio del menor privilegio, ofreciéndole al usuario los recursos mínimos necesarios para ejecutar sus funciones requeridas. Si necesitan acceder al menú de configuración una vez por año, suministre un logon de usuario alternativo por medio de la interfaz de Internet, en vez de permitir acceso total a la cuenta del VMS o, mejor aún, un usuario de nivel más alto puede ejecutar esta tarea no rutinaria. Esto ayudará a evitar modificaciones en la configuración de "drive-by" y mantendrá las credenciales de alto nivel al máximo posible fuera de la red.

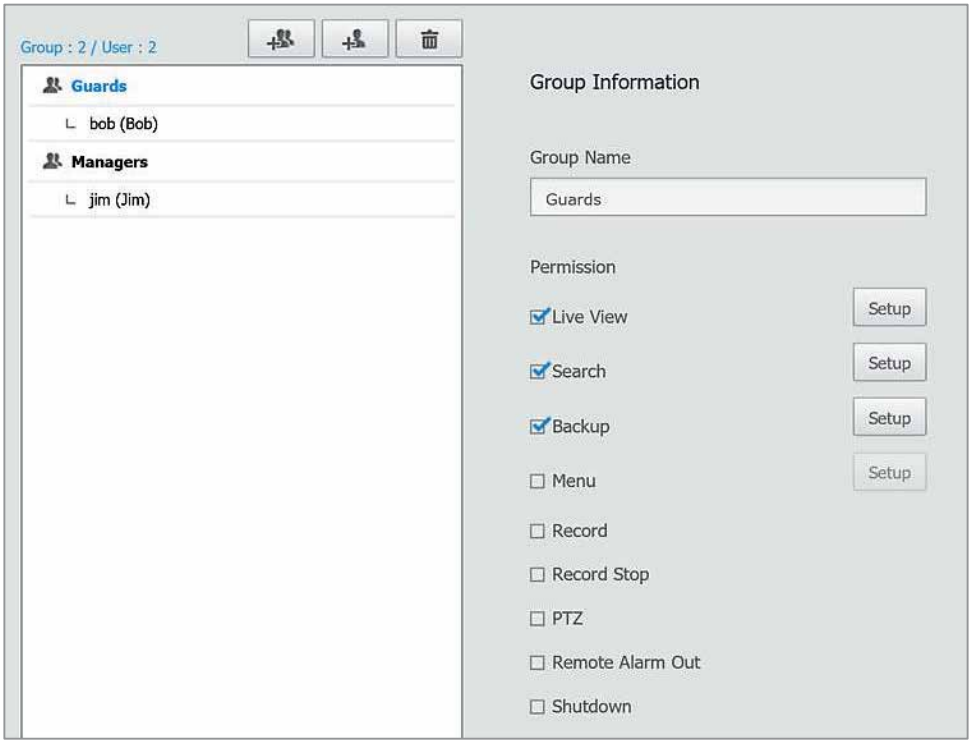

Imagen 3. Configuración de autoridad del usuario SSM

3.2. Acceso para invitados

Las cámaras de Hanwha Vision suministran un recurso de logon de invitado separado con el nombre de usuario y la contraseña “invitado”. Esta cuenta tiene privilegios limitados y está inactiva por defecto. Por tanto debe ser específicamente activada en el menú de configuración. Esto es ideal para usos de acceso limitado pero debe permanecer desactivada cuando no sea necesaria.

4. Autenticación y Criptografía

4.1. Autenticación Digest vs. Clear Text

Nombres de usuario y contraseñas son enviados por redes utilizando texto no cifrado, codificación base64 y autenticación básica de protocolos HTTP, lo que permite acceso abierto a esas credenciales para cualquier persona que esté monitoreando la red para interceptar y visualizar el tráfico, permitiendo acceso a un dispositivo.

Mientras la autenticación digest encripta los datos utilizando una función de hash que es entonces comparada con las credenciales de hash en el dispositivo. Como resultado la autenticación digest refuerza la seguridad al no enviar nombres de usuarios y contraseñas reales por la red.

Los productos de Hanwha Vision ofrecen soporte a contraseñas resumidas y no suministran autenticación básica. Sin embargo lo mismo no puede ser dicho para todos los clientes que se conectan a un dispositivo. Por tanto es importante determinar sus recursos para garantizar que todos los clientes a) funcionen y b) no reviertan para limpiar contraseñas de texto o base64.

4.2. Criptografía de SSL

SSL es un método excelente para garantizar que las credenciales del usuario y los propios datos sean enviados a los destinos pretendidos. Este método simple y barato aumenta aún más la seguridad de los dispositivos.

Certificados integrados permiten que la criptografía SSL esté activa y en ejecución en segundos. El certificado SSL también puede ser adquirido de una autoridad de certificación comercial o puede ser emitido por entidades empresariales para una seguridad aún mayor, a fin de evitar un mensaje de seguridad de certificado en el momento del acceso. A pesar de que la seguridad SSL sea una excelente manera de fortalecer su canal de comunicación en red o nube potencialmente inseguras, determine cuáles canales deben ser cifrados y son admitidos. Esto incluye cámara para NVR / VMS y VMS para el cliente. La criptografía SSL también debe ser usada al enviar notificaciones por e-mail usando el protocolo SMTP para impedir que las credenciales sean enviadas en texto no cifrado. Verifique si su servidor SMTP es compatible con SSL / TLS y cuál puerto es usado.

Las opciones de configuración permiten la selección de un certificado exclusivo (incorporado) o público e instalación y nombramiento de un certificado y archivo de clave. Cuando las opciones HTTPS fueren modificadas la cámara será reiniciada y enseguida permitirá que solamente las comunicaciones HTTPS cifradas ocurran en el puerto HTTPS (consulte la Imagen 4).

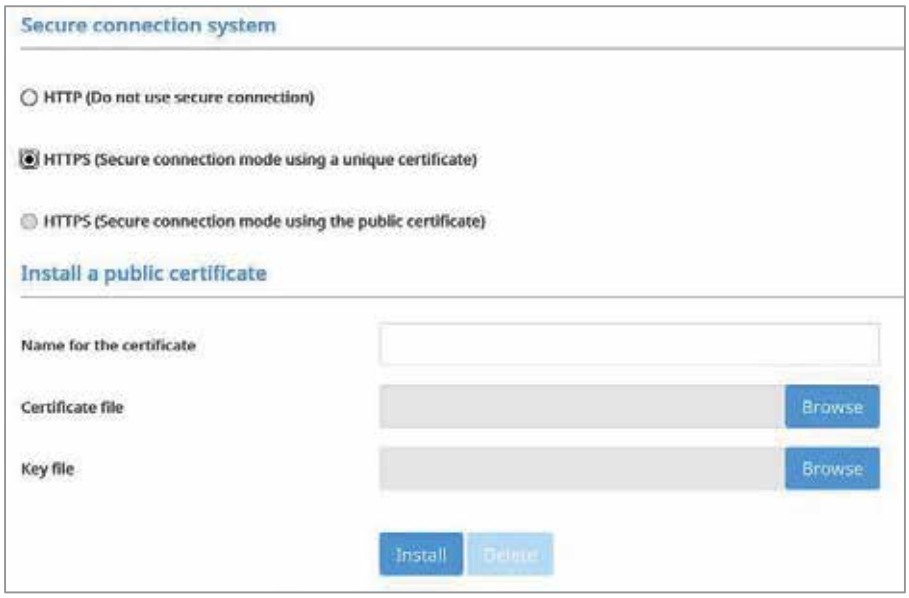

Imagen 4. Configuración de criptografía de SSL

4.3. Uso mínimo de almacenamiento en nube

Utilizar un servicio de nube para registrar o visualizar su sistema no solamente requiere grandes cantidades de ancho de banda sino también puede introducir un problema de seguridad. Cuando la nube se conecta a un dispositivo, él envía informaciones de logon. Si esta información fue capturada o es utilizado algún ataque man-in-the-middle (MITM, de interceptación de datos), las credenciales pueden ser descifradas o reproducidas, permitiendo acceso no autorizado. Además de esto, no todos los servicios en nube son compatibles con criptografía SSL o incluso autenticación digest.

5. Configuración y definición de red

5.1. Segregación de red física

Una técnica común y eficaz para aumentar la seguridad de una red de seguridad es separar físicamente las cámaras y los grabadores de la red empresarial. Esto impide que invasores tengan acceso por causa de la falta de acceso. Muchos NVRs poseen varias interfaces de red, permitiendo que graben a partir de uno y ofrezcan acceso a la estación de trabajo del otro. Esta técnica reduce el número de dispositivos expuestos externamente, que necesitan de controles de seguridad mayores.

5.2. VLAN

Se recomienda el uso de LANs virtuales (VLANs) para mantener una red de seguridad separada de la red empresarial cuando no sea utilizada una red separada. Las VLANs operan en los conmutadores de red y segregan el tráfico comúnmente basado en los puertos del conmutador. Esto permite que los firewalls protejan los dispositivos de seguridad de otros dispositivos en la red. Si es necesario acceso para dispositivos específicos, reglas de firewall pueden ser creadas o un dispositivo puede ser adicionado a la VLAN.

5.3. Filtrado de IP

Filtrado de IP es un método para especificar explícitamente quién tiene permiso para acceder a un dispositivo de red o, inversamente, quien tiene acceso negado al dispositivo. Una dirección IP o intervalo / sub-red pueden ser especificados. Esto puede garantizar que solamente las personas correctas, con base en las direcciones IP de sus computadoras, tengan acceso al dispositivo y que un intento de drive-by de la red local o de acceso negado a Internet sea negado. Los dispositivos de Hanwha Techwin permiten la entrada de direcciones IP y prefijos IPv4 e IPv6 para negar o permitir accesos. El intervalo a ser filtrado será exhibido para validar el IP y el prefijo antes de confirmar y aplicar. Verifique esto antes de inscribirse, en el caso contrario podrá tener acceso negado. Hasta 10 entradas pueden ser adicionadas para IPv4 e IPv6 (Imagen 5).

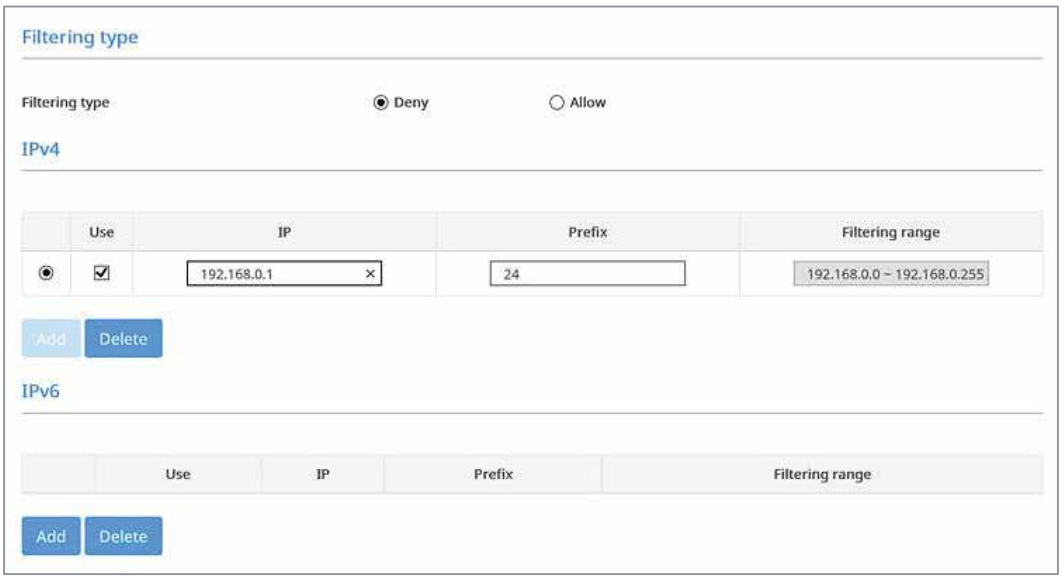

Imagen 5. Configuración de filtrado de IP

5.4. VPN

La práctica recomendada para conectar locales remotos, como varias oficinas o funcionarios remotos, es usar una solución VPN. Esto crea un canal seguro y cifrado, eliminando la posibilidad de fuga de informaciones, como nombres de usuarios y contraseñas. Una solución VPN puede involucrar hardware específico, como un ruteador VPN y/o VPN de software en ejecución en un PC cliente.

5.5. Modificar los puertos estándar

En el mundo conectado de hoy, muchos dispositivos están conectados a Internet (intencionalmente o no) y hay varios servicios empleados por hackers para realizar barreduras buscando estos dispositivos.

Una manera simple de ayudar a dificultar estos scanners, así como la creación de scripts, ataques directos y acceso inadvertido es modificar los puertos de los dispositivos en red a partir de sus estándares conocidos, rápidamente disponibles online para números de puerto más altos de su elección. Especialmente importante es el puerto HTTP, que para la mayoría de los dispositivos es estandarizado para el puerto 80 para permitir acceso por medio de un navegador de Internet. Modificar ese puerto para 8000, por ejemplo, exige una etapa extra al insertar la dirección en un navegador de Internet, generalmente protegiendo de un scanner simple o de alguien que digite manualmente una dirección en un navegador de Internet.

5.6. Deshabilitar puertos, servicios y protocolos no utilizados

Una vez que muchos dispositivos de seguridad son computadoras completas ejecutándose en sistemas operativos modernos, Hanwha Vision adoptó el enfoque de usar sistemas operativos Linux despojados y personalizados en que cualquier servicio no utilizado fue retirado o desactivado. Muchos otros fabricantes dejan estos servicios disponibles para depuración o debido a la falta de una fuerte concientización y/o postura acerca de seguridad. Varios incidentes recientes en que dispositivos de otros fabricantes fueron invadidos involucraron a invasores que entraron en un dispositivo vía protocolo de red telnet, que suministra acceso total a todos los archivos y servicios. Las plataformas de grabación basadas en Windows tienen una serie de servicios siendo ejecutados, además de exigir constantes actualizaciones de seguridad y patches, demandando tiempo, rastreo y acceso a Internet.

Los dispositivos de Hanwha Vision utilizan una variedad de protocolos que suministran funciones útiles. Sin embargo, es recomendable que todos los servicios no necesarios para las aplicaciones sean desactivados. Esto puede incluir multicast, DNS dinámico (DDNS), Calidad de servicio (QdS), Bonjour, conexión y utilización universales (UPnP), localización y encaminamiento de puerto, dirección local de link, Protocolo de transferencia de archivos (FTP), almacenamiento en red (NAS) y notificaciones por e-mail. Conforme fue mencionado anteriormente la implementación de credenciales exclusivas y la restricción de privilegios para FTP, NAS y e-mail también son excelentes maneras de aumentar aún más la seguridad. Los protocolos de configuración automática de IP quedan activados por defecto, mientras otros servicios relacionados quedan todos desactivados.

5.7. RTSP

Muchos VMS transmiten vídeo usando el protocolo RTSP. Las cámaras de Hanwha Vision suministran la opción de permitir conexiones de vídeo RTSP sin exigir autenticación. Esto puede ser útil al enviar transmisiones por Internet para exhibición pública a fin de garantizar que las credenciales no sean expuestas o para integración de terceros cuando la autenticación no sea admitida. Para las cámaras de Hanwha Vision esta función puede ser fácilmente activada en la interfaz del usuario de la cámara durante la implementación, si es necesario. Sin embargo, es recomendable exigir autenticación para todas las transmisiones de vídeo en términos de seguridad. Si es necesaria visualización pública, los servicios de terceros pueden ingerir la transmisión autenticada y suministrar acceso público por medio de otro portal, aislando la cámara de acceso público directo. Las cámaras de Hanwha Vision no abren contraseñas por el protocolo RTSP por ofrecer soporte a la autenticación resumida así como al protocolo HTTP por defecto.

6. Identificar y frustrar ataques

Tres de los métodos más comunes de ataques usados por hackers son fuerza bruta, negación de servicio (DoS) y desbordamiento de datos. Cada uno de ellos probó ser eficaz en ataques y, por tanto, debe ser tratado adecuadamente para proteger dispositivos y redes contra accesos no autorizados. Las cámaras de Hanwha Vision incluyen dos métodos que se mostraron altamente eficaces para alcanzar este objetivo.

6.1. Bloqueo de cuenta de usuario

Hackers verifican sistemáticamente todas las contraseñas y frases secretas posibles hasta que la correcta sea encontrada. Si este ataque es permitido la contraseña será desactivada en algún momento. Los dispositivos de Hanwha Vision bloquean el ataque de fuerza bruta al no permitir 5 o más intentos de logon en 30 segundos para mejorar su seguridad. Además de esto, la conexión existente de usuarios autorizados es mantenida para evitar la negación de servicio mientras la entrada de contraseña es bloqueada.

Imagen 6. Bloqueo de entrada de contraseña

6.2. Protección contra desbordamiento de datos

Otro vector de ataque común es que los hackers pasen comandos cuidadosamente creados para un dispositivo con la intención de divulgar informaciones o enviar comandos directamente para otros servicios subyacentes, como bases de datos o sistemas de archivos. Generalmente, estos comandos explotan una falla en el analizador o en la base de datos o interrumpen la interfaz, permitiendo que los comandos sean enviados directamente para el servidor de base de datos, sistema operativo o sistema de archivos. Los dispositivos de Hanwha Vision filtran comandos antes de pasarlos para un servidor de Internet o base de datos, impidiendo ataques con base en desbordamiento de datos e invasiones directas, tornando los servicios básicos subyacentes inaccesibles a hackers.

6.3. Posicionamiento del Dispositivo y Acceso Físico

Las cámaras deben ser instaladas de forma que no puedan ser fácilmente alcanzadas, mal dirigidas o desconectadas, de preferencia con un alojamiento apropiado, de modo que no pueda ser obtenido acceso físico. La red y el cableado de energía deben pasar por conductos o atrás/a través de paredes y techos, de modo que los cables no puedan ser desconectados o interceptados. Considere modelos de domo antivandalismo para obtener mejor seguridad física.

Acceso físico a cualquier seguridad del dispositivo de red es fundamental. Con el acceso físico, la mayoría de los dispositivos puede ser estandarizada, permitiendo que nuevas configuraciones sean configuradas potencialmente por personas no autorizadas. De acuerdo con el modelo de seguridad de defensa profunda, es esencial que los dispositivos de red sean instalados atrás de llave de seguridad, de preferencia con control de acceso y/o monitoreo de seguridad de vídeo. Esto suministra varias capas de seguridad, no contando con un único mecanismo.

6.4. Garantizar la grabación continua

Durante una invasión, un ladrón muchas veces roba o destruye un grabador o servidor con la intención de destruir pruebas por vídeo. Un método para combatir esto es usar tarjetas SD en cada una de sus cámaras. El período de retención de grabación será menor pero ofrecerá recursos de grabación redundantes. La grabación de la tarjeta SD también puede ser usada en el caso de falla NVR / VMS y interrupción intencional o accidental de la red, permitiendo que la cámara también tenga energía. Las opciones de configuración incluyen habilitar / deshabilitar las funciones de la tarjeta SD, grabación continua / de evento en completo / I-frame / ninguno, duración de grabación pre y post-evento, tipo de archivo de grabación (AVI / STW), sobrescribir, exclusión / duración automáticas, programación de grabación normal y sistema de archivos de la tarjeta SD. Cualesquiera perfil / códec pueden ser seleccionados para grabación. Una tarjeta SD puede ser reformateada, si es necesario. Sin embargo, una tarjeta SD vacía insertada será configurada automáticamente. Un NAS también puede ser configurado en vez de una tarjeta SD o como un dispositivo de grabación principal con una tarjeta SD como medio opcional de grabación de copia de seguridad para fallas. La grabación NAS tiene las mismas opciones de configuración con aumento de dirección IP, identificación de usuario, contraseña y carpeta estándar.

6.5. Control de acceso con base en certificado 802.1x

En muchos edificios, los conectores de red pueden estar accesibles o la cámara puede ser desconectada o un cable puede ser adulterado para que se obtenga acceso a la infraestructura de red Ethernet. El estándar 802.1x suministra control de acceso a la red con base en puerto que requiere que un certificado de identificación sea instalado en cada dispositivo conectado para obtener acceso a la red protegida. Así, si un invasor conectar un dispositivo no autorizado a la red, el acceso será negado.

El administrador de dispositivos Hanwha Vision puede ser utilizado para fácilmente activar 802.1x además de implementar certificados a partir de algún local centralizado sin la necesidad de hacer configuraciones en la interfaz de cada cámara. Opciones de configuración incluyen selección de tipo EAP, versión EAPOL, identificación de usuario y contraseña e instalación de certificado/clave.

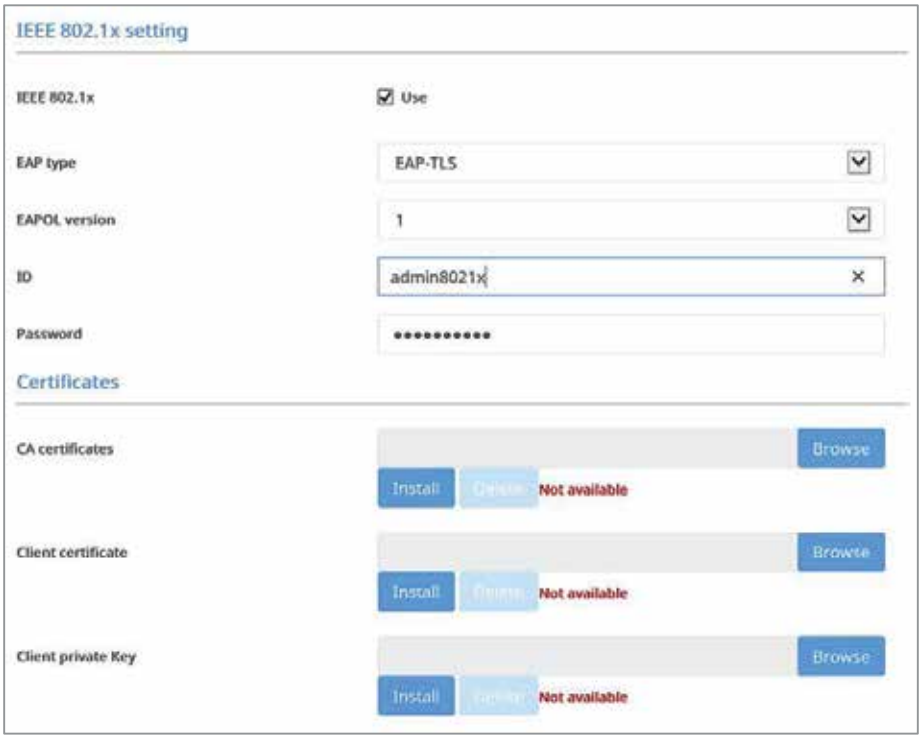

Imagen 7. Pantalla de instalación de certificados

6.6. Alimentación

Un nobreak puede garantizar que sus dispositivos de red permanezcan activos y eviten daños durante períodos de falta de energía, desconexiones administradas, caídas de energía y desconexión inadvertida o malintencionada. Si un nobreak está conectado a la red para gestión verifique si está adecuadamente protegido y si actualizaciones de seguridad están instaladas. Hubo casos en que invasores obtuvieron acceso a la red segura por medio de dispositivos auxiliares, como un nobreak conectado a una LAN o a Internet para monitoreo. Muchas cámaras IP también pueden tener dos fuentes de energía – PoE y bajo voltaje 12 vCC / 24 vCA, dependiendo del modelo, energía redundante en el caso que el presupuesto de energía PoE sea excedido. La mayoría de los conmutadores de red puede tener una prioridad especificada para indicar qué tipo de dispositivo (teléfonos, cámaras, WAP etc.) o cuáles puertos son más importantes en una falta de energía.

6.7. Administración de red

Además de la implementación, hay varias tareas que los administradores de red deben realizar continuamente para garantizar la seguridad continua de sus cámaras y otros dispositivos. Entre las más importantes están la revisión de todas las modificaciones, el desarrollo y la garantía de configuraciones constantes y aprobadas, la ejecución de actualizaciones de software y la garantía de conformidad del software con los estándares de seguridad de la empresa. Conforme es descrito aquí, Hanwha Vision reconoce el papel importante que cada una de ellas desempeña en la creación de una fuerte estrategia global para bloquear dispositivos y proteger las redes de hackers.

6.8. Verificar registros de los dispositivos

Una vez que las cámaras de Hanwha Vision registran todas las modificaciones hechas en las configuraciones del dispositivo, es importante verificar los registros para determinar cuáles modificaciones fueron hechas y quién las hizo. Para permitir una fácil reversión, la mayoría de las entradas de registro incluye configuraciones anteriores y nuevas y los registros son mantenidos durante un estándar de fábrica. Los logs retenidos pueden ser utilizados para análisis de ruta y rastreo en el caso de invasión.

El administrador de dispositivos Hanwha Vision puede ser utilizado para bajar fácilmente los registros de varios dispositivos de una sola vez.

Si las configuraciones no pueden ser verificadas, un estándar de fábrica podrá ser usado para garantizar que configuraciones válidas estén en vigor. Para las cámaras de Hanwha Vision esto puede ser hecho simplemente apretando el botón estándar de fábrica por cinco segundos mientras la cámara esté encendida. Después de estandarizar la cámara, es importante configurar la dirección IP y modificar la contraseña estándar del administrador. Un estándar de fábrica puede ser ejecutado y, al mismo tiempo, retener todas las configuraciones de menú “IP y puerto” y “Red”.

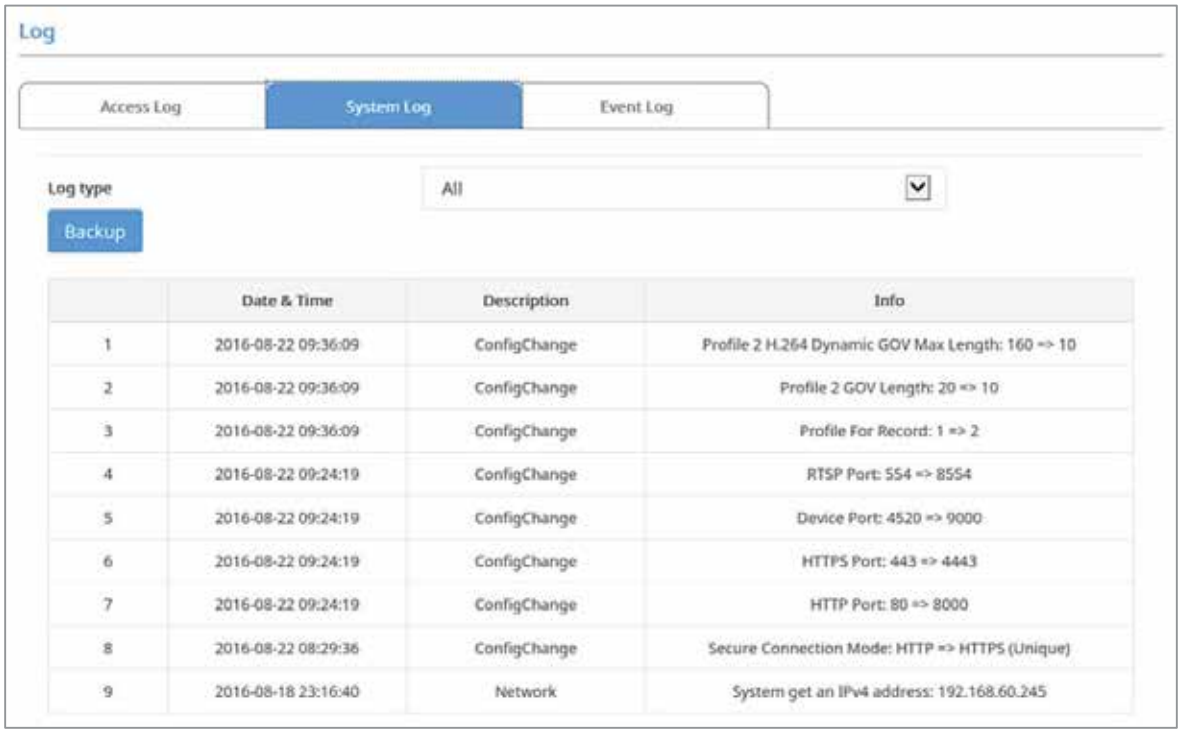

Imagen 8. Historial de modificaciones de configuración en los logs del sistema

6.9. Actualización Regular de Firmware

Hackers trabajan incansablemente para identificar y explotar vulnerabilidades en software, particularmente en versiones desactualizadas que no fueron actualizadas para mejorar la seguridad. Una vez que una vulnerabilidad es encontrada, ella generalmente es rápidamente diseminada online, abriendo el puerto para que varias personas entren fácilmente a cualquier dispositivo que ejecute versiones de firmware más antiguas y, por extensión, la propia red. Los proveedores de

software reconocen esto y lanzan continuamente actualizaciones para suministrar mejorías y/o patches que cerrarán esos puertos y protegerán a los usuarios contra acceso no autorizado.

Firmware para todos los dispositivos de Hanwha Vision incluye una lista de actualizaciones que los administradores pueden verificar para garantizar que estén ejecutando la versión más reciente. Se recomienda que el firmware esté actualizado antes de una implementación del sistema y que sea actualizado de modo regular y continuo. Muchos instaladores optan por actualizar el firmware, atribuir direcciones IP y definir contraseñas de administrador en la base antes de la implantación.

La herramienta administradora de dispositivos Hanwha Vision puede ser usada para verificar fácilmente la versión del firmware y el status actualizado de todos los dispositivos de una sola vez y el firmware puede ser bajado e instalado con solamente algunos clics.

6.10. Firmware cifrado

La mayoría de los fabricantes de dispositivos de seguridad ofrece firmware para permitir que los usuarios adicionen recursos, correcciones de bugs y actualizaciones de seguridad. El firmware suministrado para este perfeccionamiento también puede ser blanco de hackers.

El firmware contiene informaciones importantes — más de lo que pensamos. Por ejemplo, él contiene algoritmos para identificar cuentas de usuarios, algoritmos de criptografía e informaciones importantes utilizadas para cifrar informaciones confidenciales, archivos del sistema operativo o URLs importantes de servicios de Internet y, si fueren expuestos, también existe la posibilidad de exposición a puntos débiles que pueden infiltrarse en el backdoor (puerto trasero de accesos) en el firmware. Si el firmware corrompido que incluye backdoor es distribuido el hacker puede asumir el control de un dispositivo y usarlo como un puesto avanzado para otros ataques de sistema periférico.

La mayoría de los dispositivos incorporados, incluyendo dispositivos de seguridad de red, no posee protecciones especiales para seguridad de firmware. Sin embargo Hanwha Vision distribuye firmware cifrado utilizando el algoritmo de criptografía recomendado por el sector para seguridad y actualizaciones seguras. Por tanto, si un nuevo firmware es lanzado, actualice con el firmware más reciente con confianza.

6.11. Formatos de vídeo

La mayoría de los equipos de seguridad ofrece soporte a formatos de vídeo abiertos y estándar de la industria así como formatos de vídeo exclusivo. Superficialmente, un formato de vídeo abierto puede parecer ideal porque los usuarios pueden simplemente abrir el vídeo con su reproductor de música favorito. Sin embargo, las aplicaciones de seguridad exigen un formato que no pueda ser editado, modificado o adulterado. Esto es esencial, determinando que cuando el vídeo es bajado debe haber un mecanismo para autenticar el vídeo y garantizar que él no haya sido manipulado — función que simplemente no existe en formatos abiertos.

Hanwha Vision suministra una función de marca de agua que puede verificar si el vídeo fue falsificado, almacenando las informaciones de hash del vídeo para cada cuadro cuando él es almacenado en el formato SEC en NVR / VMS. Si la contraseña es definida ella será almacenada en formato SEC cifrado para que sus informaciones personales puedan ser protegidas incluso si el archivo de vídeo se filtra. El formato SEC requiere un reproductor específico para reproducción que es incluido automáticamente durante el backup. VMS, SSM de Hanwha Vision admiten no solamente la función de marca de agua pero también firma digital. Y pueden firmar y verificar adulteración de vídeo utilizando informaciones de hash de toda la imagen de vídeo. Validación de la marca de agua y de la firma digital es posible utilizándose el visualizador de backup.

Puede hacer backup en formato de archivo AVI por medio del visualizador de Internet de los dispositivos de grabación. Como el archivo de vídeo es un formato de vídeo abierto él puede ser reproducido por el reproductor de multimedia universal. Las cámaras IP de Hanwha Vision pueden almacenar vídeos en formato de archivo STW y exportarlos vía visualizador de Internet. Puede ser reproducido y convertido para el formato de archivo AVI utilizándose el reproductor de tarjeta SD independiente.

6.12. Aplicaciones de plataforma abierta

Muchas cámaras de Hanwha Vision permiten la instalación de aplicaciones de terceros para mejorar sus funciones, como el reconocimiento de matrículas de vehículos, informaciones sobre empresas minoristas, conteo de personas y mucho más. Al ejecutar aplicaciones en cámaras, es importante saber cuáles están instaladas, así como el origen del paquete de software.

Durante la instalación las cámaras de Hanwha Vision informan sobre los permisos necesarios de una aplicación. Lea estas informaciones con atención y entienda si los datos serán enviados para cualquier otro lugar. Si una aplicación no puede ser verificada o si su finalidad es desconocida, interrumpa la instalación inmediatamente, desinstale la aplicación y obténgala del colaborador confiable que la suministra. Las opciones de configuración incluyen configuración de inicio automático, nivel de prioridad, inicialización / interrupción de aplicaciones, instalación / desinstalación de aplicaciones y ejecución de una página de Internet de la aplicación.

6. Conclusión

La dura realidad en el mundo conectado de hoy es que individuos y grupos continuarán en sus intentos de identificar y explotarán vulnerabilidades para violar la seguridad de la red. Y mientras nos beneficiamos de la conveniencia de un número creciente de dispositivos accesibles por medio de estas redes la realidad es que estos dispositivos solamente aumentan la probabilidad de acceso no autorizado a la red. Por tanto es vital que todos estos dispositivos sean protegidos para evitar que se conviertan en una puerta abierta para hackers. Emplear estas prácticas recomendadas no solo puede impedir que dispositivos y sistemas de vídeo en red actúen como puntos de entrada, sino también garantiza la integridad y la continuidad de la operación de esta función esencial — garantizando la protección y la seguridad continuas de personas y activos. Además de esto, muchas de estas etapas también son aplicables a otros dispositivos y sistemas. Por tanto, estas prácticas recomendadas sirven como un requisito para las organizaciones que reconocen la importancia y toman en serio la protección de sus redes.

Por tanto, estas prácticas recomendadas sirven como iniciación de conversación para las organizaciones que reconocen la importancia y toman en serio la protección de sus redes. Diálogo abierto e informado entre el usuario final, su departamento de TI, el instalador y el integrador de sistemas es la clave para encontrar la mejor solución para satisfacer las necesidades de seguridad de organizaciones individuales.

Hanwha Vision inspecciona la seguridad del producto y diagnostica la vulnerabilidad de la etapa de desarrollo por el propio equipo de seguridad e institución especializada. Políticas rígidas, como autenticación de usuario, criptografía de base de datos y firmware, remoción de puertas traseras e identificación y regla de contraseña rígidas son aplicadas a todos los productos para garantizar una seguridad confiable.

Hanwha Vision

Hanwha Vision

13488 Centro de I+D Hanwha Vision
6 Pangyoro 319-gil, Bundang-gu, Seongnam-si, Gyeonggi-do
TEL 070.7147.8771-8
FAX 031.8018.3715
http://hanwhavisionamerica.com/

Hanwha Vision