Ejemplo de aplicación de Microwall Gigabit:

Aislamiento de una fresadora CNC

Ir a la introducción
Hoja de datos Microwall

Para la realización de prototipos y series pequeñas utilizamos en nuestra empresa una fresadora CNC. El ordenador de control, integrado en nuestra red de producción, trabaja con Windows 7 Embedded Standard, con la última versión del parche. Microsoft va a suspender el soporte avanzado de este sistema operativo en el año 2020, por lo que vamos a aislar esta fresadora de forma preventiva. Con ayuda del router cortafuegos "Microwall Gigabit" se le va a asignar un segmento de red dedicado y la comunicación con este segmento de la red va a estar muy restringido por filtros.

Elevada seguridad en la red mediante aislamiento

En el año 2017 WannaCry devoró redes de todo el mundo y al público mediático. El criptotroyano aprovechó un punto débil en la autorización para compartir archivos e impresoras de las redes de Windows. Su efecto fue tan nocivo que Microsoft no solo parcheó los sistemas operativos actuales, sino que puso a disposición actualizaciones de seguridad para los productos que ya estaban excluidos del soporte avanzado.

WannaCry mostró de un modo impresionante los potenciales riesgos que representa mantener activos servicios de red innecesarios.

Resulta obvia la simple desactivación los servicios superfluos. Pero no siempre está claro qué servicios son realmente necesarios entre los componentes de una instalación. Por otra parte, los cambios en las máquinas pueden conllevar, según los casos, una pérdida de la certificación y, a su vez, un traspaso de la responsabilidad al operador.

Por esa razón hemos desarrollado el pequeño cortafuegos Microwall Gigabit, una alternativa de fácil manejo para proteger los sistemas de producción. Se trata de un sencillo cortafuegos de 2 puertos que trabaja con el principio de listas blancas. Eso significa que es necesario autorizar explícitamente todas las conexiones permitidas.

Planteamiento

La fresadora está equipada con un ordenador de control Windows en el que trabaja un programa CNC. Este dispone de dos interfaces de red: una conecta el ordenador con la fresadora misma y la otra lo conecta con la red de producción. Contra las lagunas de seguridad para el estado actual del sistema operativo se puede contar con una pronta actualización de seguridad por Microsoft. Pero, tras finalizar el soporte avanzado en el año 2020, no se dispondrá de ninguna otra actualización de seguridad. Un atacante podría intentar comprometer al ordenador de control y, si tiene éxito, amenazar al equipo, pero también a la red envolvente.

Por esa razón es necesario aislar la fresadora empleando la estrategia de aislamiento. Con ayuda de Microwall Gigabit se externaliza la fresadora en un segmento de red propio y se restringe fuertemente la comunicación permitida con ese segmento de red mediante reglas cortafuegos.

Situación de peligro

Un breve análisis de la situación actual con el escáner de puertos nmap [Tutorial: Búsqueda de puertos abiertos en la red] resulta alarmante: el ordenador de control muestra doce puertos abiertos accesibles desde la red, entre ellos un servidor web.

Un segundo escaneado más detallado encuentra 24 puertos TCP abiertos. El servidor web es un servidor de información de Internet 7.5 sin configurar, con puntos débiles conocidos que pueden servir para la ejecución de códigos remotos. Esto significa que un atacante puede ejecutar los programas que desee a través de la red. Un premio de lotería para los ciberguerreros. Detalle mordaz: el servidor web parece no suministrar más que una página de información, o sea que, con toda probabilidad, es tan superfluo como los otros puertos abiertos. Nos alegramos de habernos tomado el tiempo de efectuar el escáner detallado y comenzamos de inmediato con el aislamiento.

Modo de proceder

Paso 1: determinar el modo de servicio y las reglas cortafuegos necesarias

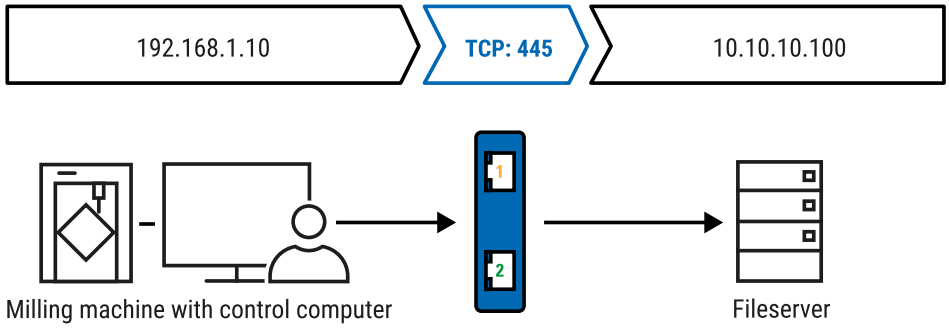
Para mantener la configuración lo más sencilla posible utilizamos Microwall en el modo NAT. Así, el ordenador de control de la fresadora ya no está visible, es decir que Microwall suplanta su lugar como actor en la red.

En realidad solo hay un caso en el que la fresadora deba comunicar a través de la red. Para acceder a los datos de producción, usted tiene que poder establecer una conexión con el servidor central de archivos de Windows. El resto de las conexiones quedan prohibidas.

Puesto que el ordenador de control mismo no pone recursos a disposición en la red, se puede bloquear por completo todas las conexiones entrantes. Además, la autorización para el servidor de archivos, al que el programa CNC debe tener acceso, es conocido y unívoco. Como la dirección IP del servidor de archivos también es conocida no se necesita ninguna resolución de nombres. También otras funciones de confort, como la búsqueda de ordenadores y autorizaciones a través de la red, son superfluas; igual que los protocolos de transporte Netbios. Por lo tanto, los puertos 137, 138 y 139 pueden ser ignorados y bloqueados. Para la actualización automática de la hora se podría autorizar el puerto UDP 123 y para la resolución de nombres por DNS el puerto UPD 53. Puesto que esas funciones no son necesarias para el funcionamiento de la fresadora, permanecen también cerradas.

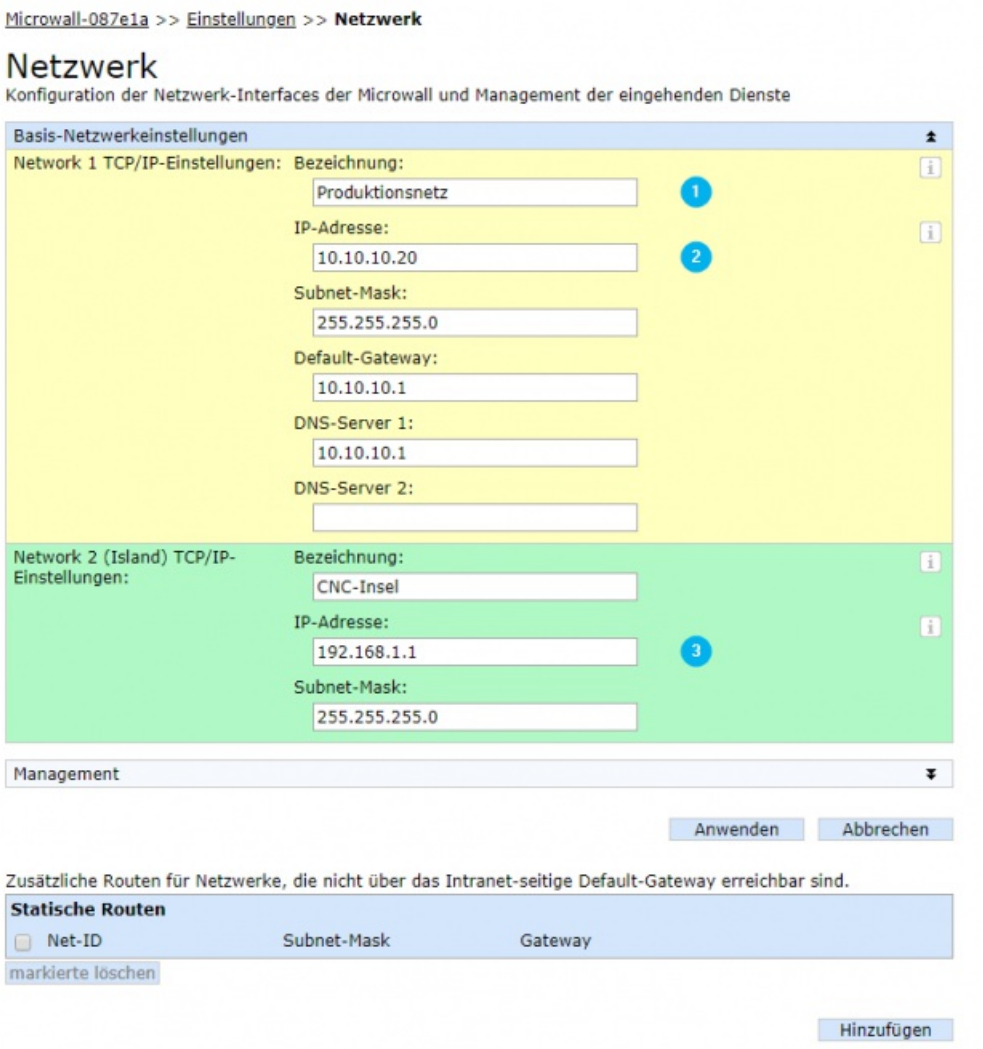
La gestión de los parches se realiza a través de nuestro departamento de TI, así pues también pueden permanecer cerrados los puertos para una actualización automática. De no ser así tendríamos que permitir aquí las conexiones TCP para el servidor WSUS.

El ordenador de control solo necesita la posibilidad de establecer una conexión SMB con el servidor de archivos con una dirección IP conocida. Esto se realiza a través del puerto de destino 445. Puesto que esa comunicación tiene lugar vía TCP, se mantiene el canal de respuesta en la conexión. **Con la introducción de tan solo una regla se asegura la fresadora de forma permanente. ¡Garantizando al mismo tiempo su funcionamiento!**



Paso 2: configurar los dispositivos

Microwall actúa de router para conectar la red envolvente con un segmento aislado. Para las interfaces en las dos redes, Microwall necesita la respectiva configuración del IP en ambas.



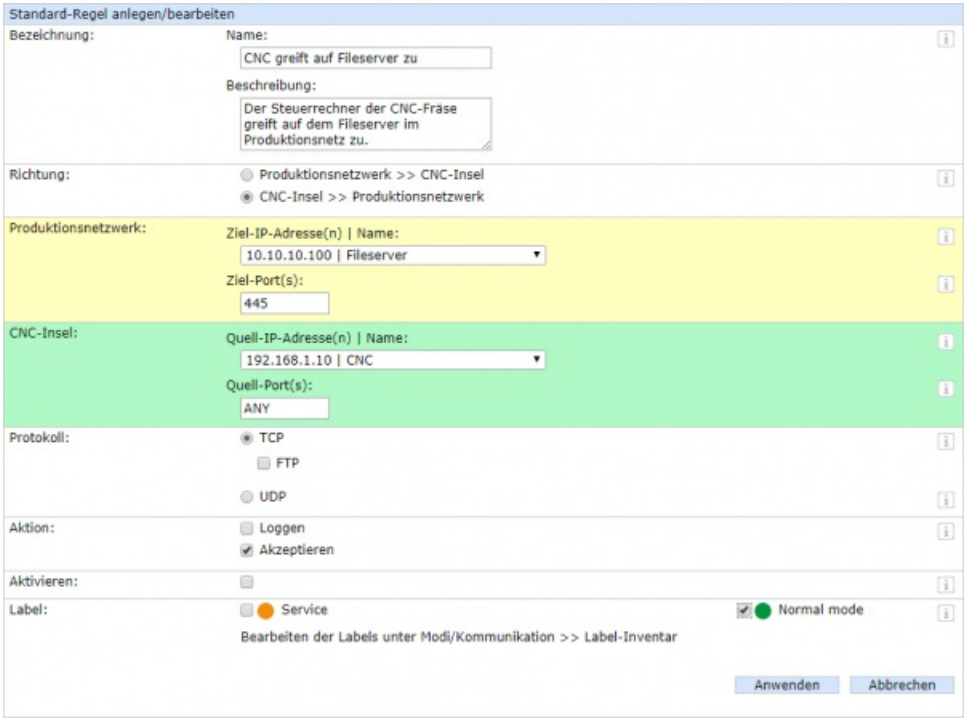
1 Introducir un nombre para la red facilita al administrador la asignación de reglas más tarde.

2 La configuración de IP original del ordenador de control (es decir: 10.10.10.20) se adopta para la interfaz pública. A parte de la dirección del hardware no cambia nada en la red envolvente.

3 En la isla seleccionamos para mayor simplicidad la clásica red 192.168.1.0/24. Microwall sirve para esa red de gateway estándar con la dirección: 192.168.1.1

Configuración de IP del ordenador de control
Al ordenador de control se le asigna la dirección IP 192.168.1.10. Como gateway estándar se le asigna Microwall Gigabit con la dirección 192.168.1.1.

Reglas cortafuegos para el acceso al servidor de archivos
El último paso es configurar las reglas cortafuegos necesarias. El ordenador de control con la dirección de IP 192.168.1.10 tiene que poder establecer una conexión TCP a través del puerto 445 con el servidor de datos de producción con la dirección de IP 10.10.10.100.



Paso 3: prueba de funcionamiento

La prueba de funcionamiento, que dura ya varias semanas, muestra que la fresadora realiza su trabajo como de costumbre.

Resumen

Con ayuda de Microwall se ha podido aislar la fresadora CNC en solo unos minutos en un segmento de red propio. Para garantizar el funcionamiento ha bastado una sola regla cortafuegos. Y, de paso, se ha bloqueado los protocolos NetBIOS para la compartir archivos e impresoras, ocultando así detalles sobre la fresadora tras Microwall.

¡Lo mejor es probarlo!

Si lo desea, ponemos a su disposición un Microwall gratuitamente durante un periodo de cuatro semanas.

Solicitar dispositivo de prueba

Thomas Clever
t.clever@wut.de

Nuestros técnicos están a su disposición en el teléfono+49 202/2680-110 (lu-vi de 8-17 horas)

W&T
www.WuT.de

Le atendemos personalmente:

Wiesemann & Theis
GmbH
Porschestr. 12
42279 Wuppertal
Tel: +49 202/2680-110 (lu-vi de 8-17 horas)
Fax: +49-202/2680-265
info@wut.de

© Wiesemann & Theis GmbH, salvo errores y modificaciones: como podemos cometer errores, no se debe utilizar nuestros enunciados sin verificarlos. Por favor, notifíquenos todas las erratas y malentendidos que detecte, para que podamos localizarlo y solucionarlo lo antes

posible.