APROVECHAMIENTO DE LOS PROGRAMAS BRING YOUR OWN DEVICE

SERVICIOS DE RED DISEÑADOS PARA PERMITIR LA ELECCIÓN, MOVILIDAD Y SEGURIDAD DEL EMPLEADO

NOTA DE APLICACIÓN

Alcatel·Lucent Enterprise

RESUMEN

En un momento en el que crece el número de empresas que estudian cómo utilizar de forma óptima los programas BYOD (Bring Your Own Device: Traiga su propio dispositivo) para mejorar la productividad de los empleados, es importante que los departamentos informáticos cuenten con la flexibilidad necesaria para desarrollar soluciones adaptadas a sus necesidades específicas. Alcatel-Lucent ofrece todos los elementos que las empresas necesitan para crear arquitecturas ágiles que aprovechen con efectividad los programas BYOD. La incorporación de servicios BYOD de Alcatel-Lucent a la solución Converged Campus Network de Alcatel-Lucent garantiza que los usuarios adecuados puedan acceder en todo momento a los recursos que necesitan mediante dispositivos autorizados. Ofrece a todos los usuarios la misma experiencia de alta calidad con cualquier aplicación en redes de cable e inalámbricas. Ofrece la libertad que los empleados esperan disfrutar con conectividad ubicua, acceso sencillo y comunicaciones siempre activas desde cualquier lugar. Además, impide que el personal no autorizado o los dispositivos que no cumplan los requisitos accedan a recursos corporativos y pongan en peligro la integridad y la seguridad de la información corporativa.

ÍNDICE

BRING YOUR OWN DEVICE Y LAS COMUNICACIONES EMPRESARIALES

Las prácticas de Bring Your Own Device de los empleados son desde hace algún tiempo motivo de preocupación para las empresas. Hace poco más de un año, un informe de Accenture señalaba que el 45 % de los empleados encuentran los dispositivos y las aplicaciones personales más útiles que los proporcionados por la empresa.[1] El 66 % no se preocupa por las políticas informáticas de la empresa y simplemente utiliza las tecnologías que necesita para realizar su trabajo. Un 23 % utiliza sus propios dispositivos para trabajar de forma regular, y un 27 % utiliza aplicaciones no corporativas para mejorar su productividad en el trabajo.

Al mismo tiempo, este y otros informes se centraban en explicar la creciente tendencia BYOD que están experimentando empresas de todos los tamaños. Un año más tarde, Gartner informa de que esta tendencia es cada vez más aceptada por departamentos informáticos de empresas de todo el mundo. De hecho, Gartner señala que los programas empresariales diseñados para aprovechar BYOD son cada vez más habituales y que, para 2016, el 38 % de las empresas espera dejar de proporcionar dispositivos de hardware a sus empleados.

La aparición de la cultura BYOD y la consumerización de las comunicaciones empresariales son resultado directo de la proliferación de dispositivos móviles fácilmente transportables, como netbooks, smartphones y tablets. Los usuarios utilizan cada vez más estos dispositivos para el trabajo y para su vida personal. Como resultado, las aplicaciones se han hecho más móviles y están “permanentemente activas”, y cada vez son más las personas en todo el mundo que están “permanentemente conectadas”. En este proceso, los empleados están cada vez más conectados a sus nubes personales de aplicaciones y servicios que a sus redes empresariales, y esperan que todas las aplicaciones resulten igual de fáciles de usar.

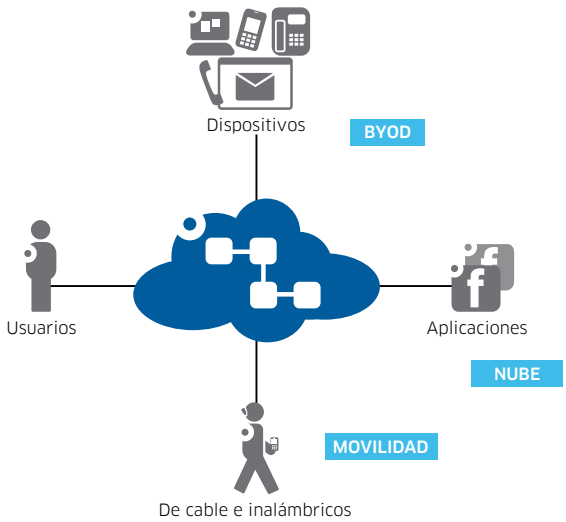
Los empleados, acostumbrados a poder acceder a sus aplicaciones de consumidor desde cualquier lugar, en cualquier momento y con cualquier dispositivo, desean disfrutar del mismo acceso armonizado y ubicuo a las aplicaciones empresariales en sus dispositivos personales, ya se encuentren dentro del entorno de trabajo o fuera de él. Desean utilizar sus dispositivos personales para continuar las comunicaciones digitales con colegas, socios y clientes en cualquier lugar, en cualquier momento y con cualquier aplicación que elijan. Además, desean conectar a través de cualquier red de cable o inalámbrica que elijan.

Sin embargo, BYOD está suponiendo un reto considerable para los departamentos informáticos de las empresas. Dado que los dispositivos móviles personales y las redes personales de los empleados no están bajo el control del departamento informático, existe el riesgo de que se produzca un acceso no autorizado a información corporativa de carácter sensible desde fuera cuando se utilizan estos dispositivos y aplicaciones. Por consiguiente, las empresas no solo deben encontrar una forma de sumarse a la tendencia BYOD para atender las necesidades de comunicación de los empleados, sino que también deben aprovechar el cambio de paradigma para mejorar la productividad de los empleados y proteger sus redes frente al acceso no deseado.

[1] “Consumer IT: The Global Infiltration into the Workforce”, Accenture BlogPodium, mayo de 2012, www.accenture-blogpodium.nl/site.
[2] “Bring Your Own Device: The Facts and the Future”, Gartner, http://www.gartner.com/newsroom/id/2466615.a

Alcatel-Lucent ofrece todos elementos que las empresas necesitan para crear arquitecturas, soluciones y servicios ágiles que atiendan las necesidades de comunicaciones cambiantes de los empleados y aprovechen los programas BYOD de forma efectiva. Con una cartera completa de productos inalámbricos y de cable, la gama de soluciones y servicios de comunicaciones de Alcatel-Lucent ofrece a las empresas diversas formas de hacer posible la movilidad y la comunicación armonizada de los empleados a través de una nube personal y una red empresarial. Asimismo, Alcatel-Lucent ofrece servicios de comunicaciones para smartphones y tablets optimizados para permitir una gestión efectiva de las comunicaciones (Figura 1)

Figura 1. Alcatel-Lucent ofrece servicios de comunicaciones optimizados para permitir una gestión efectiva de las comunicaciones



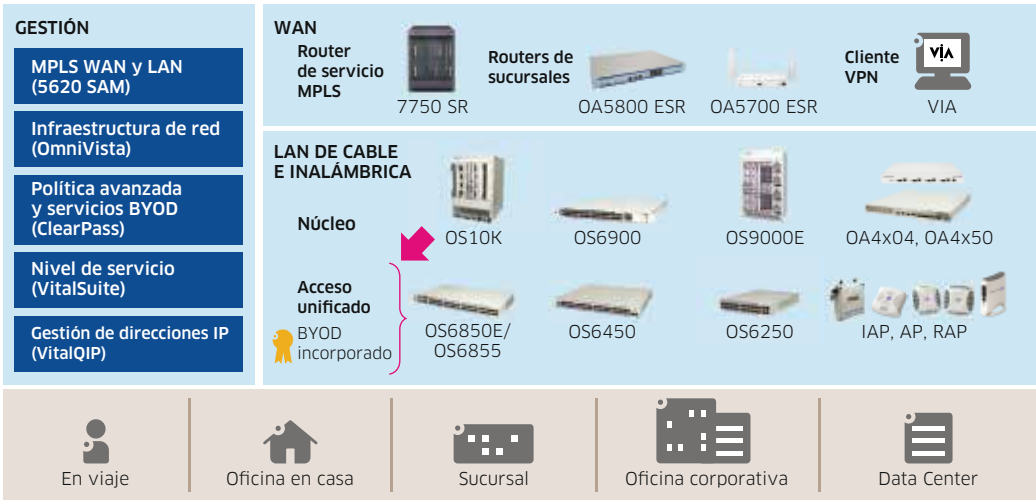
Como parte de este enfoque completo, Alcatel-Lucent ofrece un elemento habilitador de BYOD como parte de su solución Converged Campus Network. El enfoque que adopta Alcatel-Lucent para BYOD está pensado para garantizar que los usuarios adecuados, con dispositivos autorizados, puedan acceder a los recursos que necesitan en todo momento. Ofrece a todos los usuarios una experiencia de alta calidad con cualquier aplicación. Además, ofrece la libertad de la que los empleados esperan disfrutar, con conectividad ubicua, acceso sencillo y comunicaciones siempre activas desde cualquier lugar. Y lo que es más importante aún, la solución de Alcatel-Lucent para BYOD impide que el personal no autorizado o los dispositivos que no cumplan los requisitos accedan a recursos corporativos y pongan en peligro la integridad y la seguridad de la información corporativa.

LIBERTAD DE MOVIMIENTO, APLICACIONES Y DISPOSITIVOS

La solución Converged Campus Network de Alcatel-Lucent hace posible BYOD a través de una experiencia de usuario final para comunicaciones empresariales de alta calidad y con la comodidad que habitualmente disfrutan los consumidores. Ello garantiza que las comunicaciones empresariales del usuario final, tanto personales como de negocio, se mantengan en un contexto de alta calidad de servicio. Además, ofrece a los usuarios capacidad de elección y control sobre todos los soportes y dispositivos a su disposición, de manera que puedan interactuar con el número de personas que deseen en el momento que deseen y empleando el dispositivo que deseen.

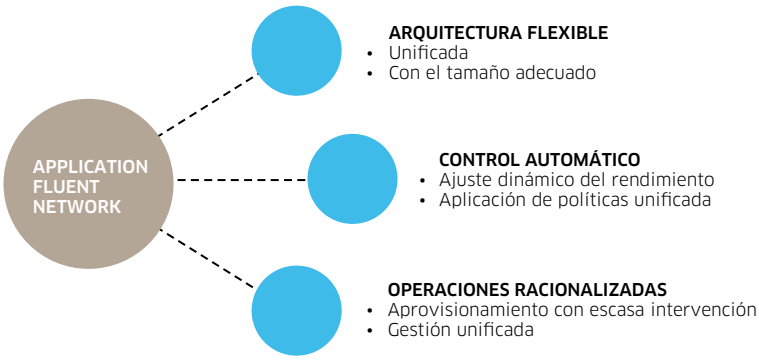
La estrategia BYOD para redes empresariales basada en la solución Converged Campus Network de Alcatel-Lucent es posible gracias a un amplio conjunto de productos y soluciones integrados que han sido diseñados para que dicha estrategia sea apta para aplicaciones (Figura 2).

Figura 2. La solución Converged Campus Network de Alcatel-Lucent permite la estrategia BYOD con productos y soluciones que hacen que sea apta para aplicaciones



Una AFN (Application Fluent Network: red apta para aplicaciones) creada con estos elementos está preparada para responder a los nuevos modelos de aplicaciones y tráfico requeridos para hacer posible la estrategia BYOD (Figura 3). La arquitectura de la red es más inteligente y dinámica. Admite la interconexión armonizada de todas las aplicaciones personales de los usuarios para que funcionen a través de la red empresarial. La red supervisa y reconoce la naturaleza del tráfico generado por cada usuario, prioriza el tráfico empresarial crítico y gestiona dicho tráfico con el nivel de calidad requerido para hacer posibles los procesos de comunicaciones empresariales. Como resultado, se optimiza la productividad de los usuarios finales en todo momento.

Figura 3: Una red AFN de Alcatel-Lucent da prioridad al tráfico empresarial sobre el tráfico personal menos importante



Cómo funciona

La implementación de BYOD de Alcatel-Lucent en la solución Converged Campus Network se basa en un seguimiento de los dispositivos y una gestión de políticas inteligentes. Estas capacidades garantizan que las personas adecuadas, empleando dispositivos aprobados, puedan obtener los recursos de comunicaciones que necesitan y que disfruten de una experiencia de alta calidad al utilizarlos (Figura 4). También impide al personal no autorizado o a los dispositivos que no cumplan los criterios exigidos el acceso a los recursos corporativos.

Figura 4. BYOD de Alcatel-Lucent en la solución Converged Campus Network se basa en el seguimiento inteligente de los dispositivos

Una vez que se conoce el dispositivo, pueden tomarse decisiones acerca de cómo gestionar el dispositivo y las aplicaciones de comunicaciones que está utilizando. Esto se consigue mediante:

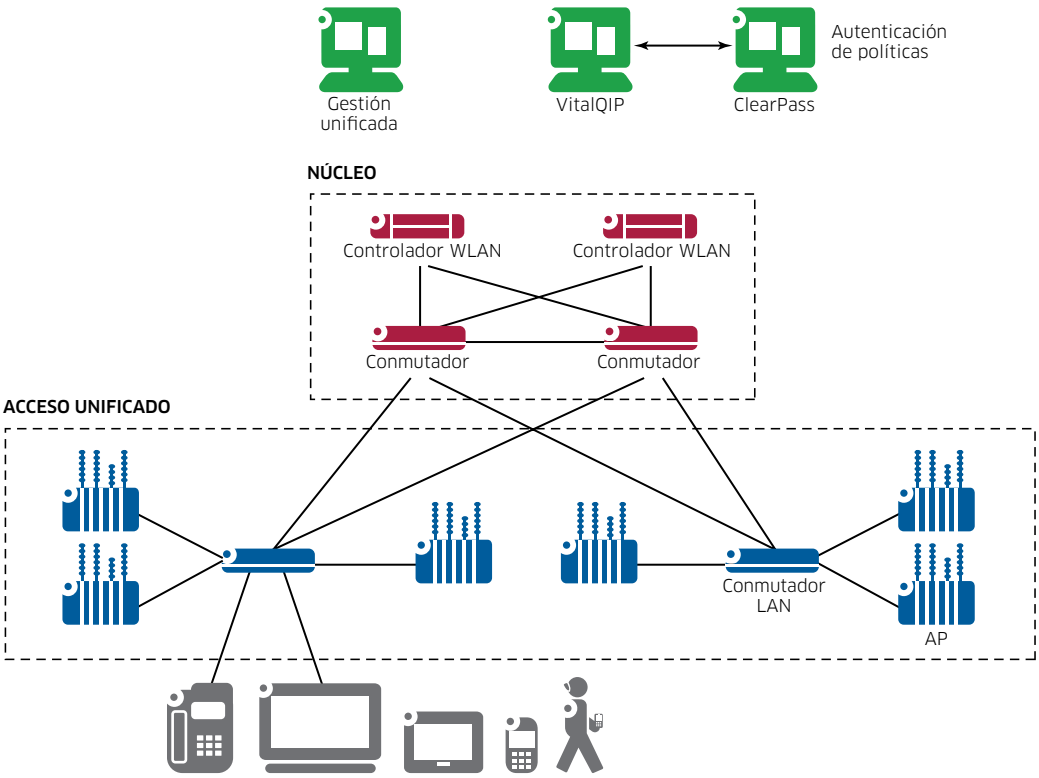
- Un férreo mecanismo de control de accesos y autorización que autentica tanto al usuario como al dispositivo
- Un examen de estado que identifica a cualquier dispositivo no corporativo que intente entrar en la red y que impide a las aplicaciones no autorizadas utilizar el ancho de banda de la red o incumplir las políticas de la empresa. Esto garantiza que los dispositivos que se conecten con la red no contengan virus ni amenazas y que no infecten la red ni a otros dispositivos.
- Un mecanismo de calidad de servicio (QoS) y de priorización que garantiza que todas las aplicaciones aprobadas funcionen correctamente cuando se encuentren en la red y que todo el tráfico se priorice en función del tipo de comunicaciones que genera la aplicación

Con estos tres elementos, el seguimiento de los dispositivos y la gestión de las políticas de BYOD de Alcatel-Lucent gestionan todas las necesidades de control de accesos y notifican también a la infraestructura de red los derechos y el ancho de banda permitidos para un usuario y un dispositivo determinados. Es posible añadir automáticamente dispositivos tales como impresoras, cámaras y escáneres como dispositivos autorizados sin intervención de TI. A partir de ese momento, la infraestructura de la solución Converged Campus Network de Alcatel-Lucent gestiona los derechos de red al tiempo que supervisa continuamente la salud y el cumplimiento de las normas por parte de cada dispositivo. Esto sucede con los empleados, contratistas e invitados cuando estos acceden a la red.

Control de acceso

Las prestaciones de acceso unificado BYOD con la solución Converged Campus Network de Alcatel-Lucent son posibles gracias a Aruba ClearPass™ Policy Manager (CPPM). Esta plataforma proporciona un control de accesos basado en el usuario y en el dispositivo para empleados, contratistas e invitados de cualquier infraestructura de red de cable, inalámbrica o VPN (red privada virtual).

Figura 5. El acceso unificado en la solución Converged Campus Network de Alcatel-Lucent se controla mediante una plataforma de gestión de políticas



Con el CPPM, las políticas de acceso a red gestionadas de forma centralizada ofrecen las prestaciones completas de autenticación necesarias para el personal de movilidad elevada de hoy en día, con independencia del tipo de dispositivo o de a quién pertenezca el dispositivo. Los servicios automatizados permiten a los usuarios integrar sus propios dispositivos de forma segura, registrar dispositivos habilitados para AirPlay y AirPrint para uso compartido y crear credenciales de acceso de invitados. El resultado es una solución de control de accesos de red coherente y escalable que supera los requisitos de seguridad de dispositivos BYOD y gestionados por TI.

El CPPM aplica de forma centralizada todos los aspectos de BYOD basándose en privilegios de acceso a red granulares, concedidos en función del perfil de red del usuario, el tipo de dispositivo, los atributos de gestión de dispositivos, la salud del dispositivo, la ubicación y la hora del día. RADIUS (Remote Authentication Dial In User Service) incorporado, TACACS+ (Terminal Access Controller Access-Control System Plus), la creación de perfiles, la integración, el acceso de invitados y las comprobaciones de estado, así como la capacidad para aprovechar soluciones de gestión de dispositivos móviles de terceros, garantizan una aplicación armonizada de las políticas en toda la red.

Aptitud para aplicaciones

Al gestionar el acceso de esta forma, Alcatel-Lucent es capaz de ofrecer una aptitud completa para aplicaciones. Esto se consigue creando niveles de control de accesos diferenciados para hacer posibles los diferentes intereses de trabajo práctico de diferentes grupos de usuarios.

Por ejemplo, los departamentos funcionales de una organización pueden obtener privilegios de acceso para determinados recursos y aplicaciones. Además, pueden establecerse clases de dispositivos para los usuarios de cada departamento. Con este enfoque, es posible conceder a una clase de dispositivo BYOD diferentes privilegios de acceso que a los dispositivos proporcionados por la empresa.

Pero el acceso diferenciado también permite a los equipos de TI controlar el número de dispositivos que un usuario puede llevar al trabajo. Por ejemplo, los ejecutivos o el personal de ventas pueden estar autorizados a utilizar un máximo de dos dispositivos personales debido a la elevada movilidad y a la constante interacción con los clientes que se espera de este grupo. Por otro lado, los empleados que trabajan desde la oficina pueden tener autorizado un solo dispositivo personal, dado que es probable que pasen la mayor parte del tiempo con un ordenador proporcionado por la empresa.

Los visitantes de la empresa también constituyen un grupo específico con sus propias necesidades de acceso. Puede utilizarse una solución de acceso de invitados para separar el tráfico de los invitados, personalizar la experiencia de cada usuario y ofrecer visibilidad acerca de quién se está conectando. Las soluciones de acceso mixto de este tipo también ofrecen a los equipos de TI los datos necesarios para ajustar los requisitos de ancho de banda para diferentes grupos de usuarios, así como para fines de planificación y auditorías de red basadas en los usuarios. El CPPM también ofrece funciones de gestión de invitados con el fin de simplificar la gestión de los visitantes. La función CPPM Guest™ agiliza los procesos de flujo de trabajo y permite a los operadores y patrocinadores, como recepcionistas, coordinadores de eventos y otro personal ajeno a TI, crear cuentas temporales de acceso a Wi-Fi®.

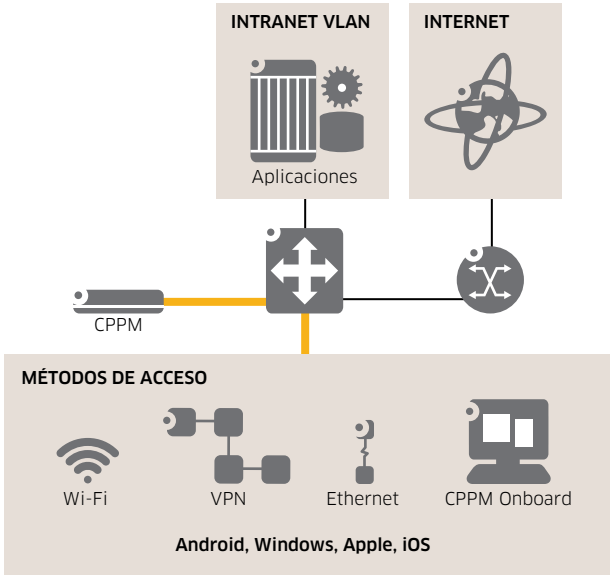
Los invitados también puede registrarse personalmente para acceder a la red. Cuando un usuario se registra, CPPM Guest le envía los datos de identificación para acceder a la cuenta a través de un mensaje de texto (SMS) o de correo electrónico. Las cuentas pueden configurarse para caducar automáticamente después de un número de días u horas específico.

Debido a que funciona fuera de la plataforma CPPM, la función CPPM Guest se habilita mediante el conjunto principal de prestaciones de autenticación, autorización, contabilidad y aplicación de políticas de la plataforma CPPM. El CPPM se adapta de forma armonizada a las redes inalámbricas, de cable y VPN de múltiples fabricantes y admite diversos contenedores de identidad. Por consiguiente, la función CPPM Guest puede adaptarse para atender las necesidades de grandes empresas y de redes multisitio y gestionar el acceso seguro a nivel de usuario de cientos de miles de usuarios simultáneos. Además, con la visibilidad completa de las actividades de acceso a red de cada visitante, CPPM Guest facilita la medición del uso de la red, la identificación de los requisitos de cobertura de Wi-Fi y el cumplimiento de normas corporativas e industriales.

Integración de dispositivos

El CPPM también gestiona la integración de dispositivos. Con el CPPM, la solución es capaz de aprovisionar y configurar los dispositivos móviles personales de un empleado (Windows®, Mac OS® X, iOS® y Android™ 2.2 y superior) y habilitar cada dispositivo para que conecte con la red de forma segura. Esto se consigue con la función CPPM Onboard™ (Figura 6).

Figura 6. El CPPM gestiona la integración de dispositivos con la función Onboard



CPPM Onboard permite a los empleados, contratistas y socios configurar personalmente sus propios dispositivos móviles. El portal de registro de CPPM detecta automáticamente el sistema operativo de un dispositivo y presenta al usuario el paquete de configuración adecuado. Posteriormente, ofrece una forma sencilla de configurar parámetros inalámbricos, de cable y VPN, aplicar credenciales de dispositivo exclusivas y garantizar que los usuarios conecten de forma segura sus dispositivos a redes habilitadas para 802.1X con escasa intervención de TI.

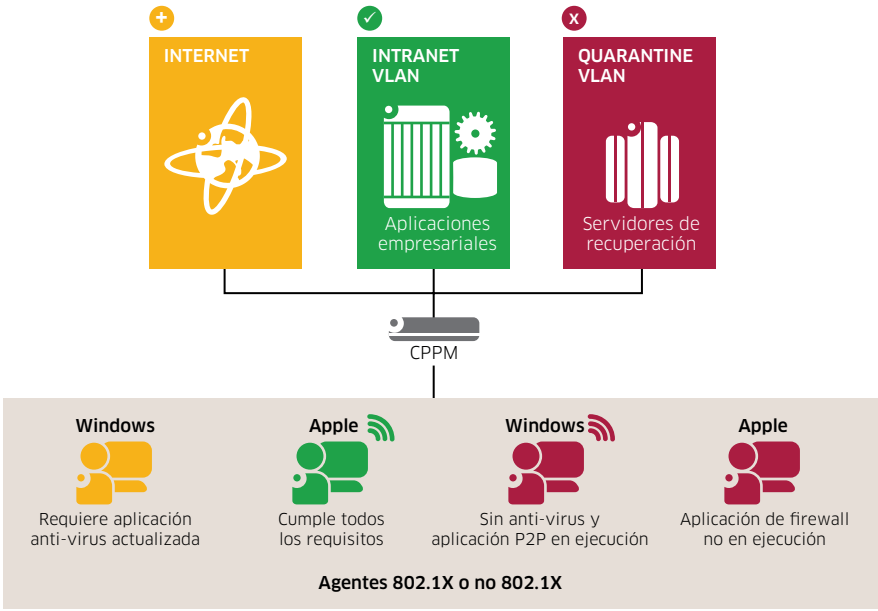
La función CPPM Onboard aprovecha las prestaciones de autorización de certificado de la plataforma CPPM para publicar credenciales exclusivas que incluyan información de certificado y datos del usuario y el dispositivo. La distribución de credenciales de dispositivo publicadas a través de CPPM Onboard protege a las organizaciones que desean adoptar iniciativas BYOD sin implementar una autoridad de certificado externa. Las funciones de búsqueda, fáciles de usar y gestionadas mediante menús, garantizan la revocación y eliminación rápida de certificados para dispositivos móviles específicos si un usuario abandona la empresa o pierde o le roban el dispositivo.

Este sencillo proceso de integración agiliza el flujo de trabajo de los servicios de soporte de TI. Permite al personal de TI automatizar y proteger múltiples procesos necesarios para implantar con éxito iniciativas BYOD, al tiempo que mejora la experiencia del usuario.

Examen de estado

Las evaluaciones de estado y las comprobaciones de salud se gestionan con CPPM OnGuard™. Esta función ofrece protección de categoría empresarial con evaluaciones de estado avanzadas de terminal en los principales sistemas operativos para garantizar el cumplimiento de las normas antes de la conexión de los dispositivos. Estas evaluaciones y comprobaciones se realizan adicionalmente a las comprobaciones anti-virus, anti-spyware y a las auditorías de firewall personal efectuadas por los tradicionales procesos de control de acceso a red (NAC) y protección de acceso a red (NAP). Esto garantiza que la red esté siempre protegida con un nivel superior de cumplimiento de las normas por parte de los terminales (Figura 7).

Figura 7. Las evaluaciones de estado y las comprobaciones de salud se gestionan mediante CPPM OnGuard™



El marco avanzado NAC y NAP de CPPM OnGuard ofrece protección excepcional contra vulnerabilidades. Si hay terminales que no cumplen las normas, el usuario recibe un mensaje acerca del estado de terminal e instrucciones acerca de cómo lograr el cumplimiento si no se utiliza autocorrección. Para mayor protección, las comprobaciones de salud de CPPM OnGuard permiten comprobar datos más granulares que con los agentes NAP estándar. OnGuard también puede utilizarse para evaluar atributos específicos de productos, tales como las versiones de producto, motor y archivo de datos para aplicaciones antivirus.

Gestión de aplicaciones móviles

La gestión de aplicaciones móviles (MAM) se proporciona a través de la aplicación CPPM WorkSpace. Esta función permite a los equipos de TI proteger, distribuir y gestionar aplicaciones empresariales de dispositivos móviles personales. También incluye la aplicación móvil WorkSpace, que permite a los usuarios integrar sus propios dispositivos, organizar y gestionar sus aplicaciones de trabajo y aprovisionar el acceso a red de sus invitados.

WorkSpace facilita a los departamentos de TI de las empresas la creación de políticas que controlen el uso de las aplicaciones y la protección de los datos. Puede iniciarse una sesión automática de VPN cuando se utilicen aplicaciones de trabajo específicas en redes públicas. Las aplicaciones de trabajo también pueden bloquearse basándose en la ubicación o en el estado de seguimiento geográfico.

Para los usuarios, la aplicación móvil WorkSpace ofrece un control sin precedentes para tantos dispositivos personales como tenga autorizados el usuario para su uso en la red. Ofrece visibilidad del estado de política de aplicaciones, acceso a una tienda de aplicaciones empresarial y un inicio de sesión único para aplicaciones de trabajo. También permite a los usuarios crear y gestionar cuentas Wi-Fi temporales de invitados en lugar de que TI o recepción tengan que aprovisionar el acceso de invitados.

WorkSpace admite uno de los mayores ecosistemas de aplicaciones móviles empresariales del sector. TI puede proteger, distribuir y gestionar fácilmente más de 40 aplicaciones de productividad empresarial de terceros, además de aplicaciones desarrolladas internamente. Los controles granulares de políticas y las actualizaciones automáticas permiten a los equipos de TI aplicar cambios en las políticas para cada aplicación sin necesidad de volver a desplegar o empaquetar aplicaciones ya existentes en los dispositivos.

Con la función WorkSpace, los equipos de TI también pueden distribuir y gestionar aplicaciones aprobadas por la empresa desde una tienda de aplicaciones interna. Se utiliza el perfil de red del usuario para determinar qué aplicaciones se envían automáticamente al dispositivo. El departamento de TI también puede controlar qué aplicaciones empresariales se están utilizando y realizar actualizaciones rápidamente en cualquier aplicación sin tocar el dispositivo del usuario.

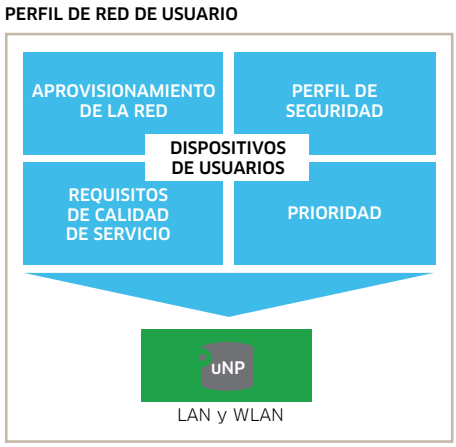
Finalmente, WorkSpace elimina los problemas de responsabilidad corporativa relacionados con privacidad al impedir el acceso de los equipos de TI a la información personal del usuario. Con WorkSpace, los equipos de TI pueden eliminar o bloquear aplicaciones y datos empresariales, pero no pueden ver los datos privados de los usuarios.

Control QoS con User Network Profiles

Ni que decir tiene que todas las comunicaciones que tienen lugar en la red de una empresa deben gestionarse para ofrecer una QoS elevada. La solución Converged Campus Network de Alcatel-Lucent, en combinación con CPPM, garantiza que los usuarios sigan disfrutando de la máxima calidad en sus comunicaciones empresariales y personales mediante la utilización de los atributos exclusivos de User Network Profiles.

Todas las comunicaciones de red en la implementación BYOD de Alcatel-Lucent se gestionan contextualmente utilizando la información exclusiva asociada a cada usuario, aplicación y dispositivo. Esto se consigue mediante la creación de User Network Profiles (uNP) en los que se encuadra cada combinación de empleado/dispositivo/aplicación. El uNP está predefinido para determinar los parámetros de seguridad QoS que deben utilizarse para cada usuario en una situación concreta. Los conmutadores se convierten entonces en los puntos de aplicación de los parámetros de seguridad y QoS. El uNP también puede asignar acreditación de VLAN. (Figura 8).

Figura 8. Las conversaciones de red en la implementación BYOD de Alcatel-Lucent se gestionan con User Network Profiles



Con esta información, la red puede reconocer a los usuarios y dispositivos y vincularlos a un uNP. Esto permite a la red comprender cada comunicación y ajustarse automáticamente a necesidades específicas. La red también es capaz de detectar automáticamente la ubicación de un usuario o dispositivo mediante la supervisión del tráfico en un puerto de conmutador específico. Puede aprovisionar de forma automática el usuario y el dispositivo en el puerto de conmutador en cuestión, incluidos los parámetros iniciales de seguridad y QoS. Asimismo, puede identificar las comunicaciones iniciadas por un usuario concreto en un dispositivo específico que deben medirse para determinar la QoS realmente recibida.

Gestión de accesos y comunicaciones unificados

Los accesos y las comunicaciones unificados basados en uNP se gestionan mediante la arquitectura y la tecnología de virtualización de red simplificadas en las que se basa la solución Converged Campus Network de Alcatel-Lucent (Figura 9). Esta arquitectura está diseñada para mejorar la flexibilidad y optimizar el uso de los recursos de red. Incluye todos los elementos necesarios para hacer posible un acceso unificado eficiente y la aptitud para aplicaciones, lo que incluye:

- Capacidad para gestionar comunicaciones contextualmente con los uNP, que están integrados en los conmutadores de nivel de acceso.
- Conmutadores de nivel de acceso habilitados para detectar y examinar las comunicaciones tras su inicio, así como para gestionar la QoS, según sea necesario, con el fin de lograr una experiencia óptima del usuario final.
- Una capa de coordinación de servicios, que permite a las aplicaciones y los dispositivos detectar servicios de la red y que proporciona un aprovisionamiento de servicios común y un portal de control para garantizar la interoperabilidad entre servicios individuales, incluida la capacidad para compartir un marco de políticas común.

Figura 9. La arquitectura simplificada de la solución Converged Campus Network de Alcatel-Lucent

Los conmutadores de red de área local (LAN) OmniSwitch™ 10K y OmniSwitch 6900 habilitan el núcleo de la arquitectura con velocidad de cable de 10 y 40 GigE. Estos conmutadores analizan y procesan diferentes tipos de tráfico en función de la clasificación granular permitida por los uNP. Como resultado, las empresas pueden asignar prioridad a aplicaciones, a usuarios o a ambos. La arquitectura distribuida procesa el tráfico en la entrada, lo que permite reenviarlo inteligentemente a otros elementos y evitar los embotellamientos en un punto central. También permite a las empresas adaptar su entorno en función de las necesidades crecientes sin que se vean afectados el rendimiento y el ancho de banda.

La red convergente también incluye una capa de acceso unificado en la que se aplican un marco único de políticas, un esquema común de autenticación, una sola base de datos de usuarios y un único conjunto de variables que tienen en cuenta la ubicación tanto para dispositivos de cable como inalámbricos.

El acceso a red de cable se proporciona mediante OmniSwitch 6850E y la serie resistente y apilable OmniSwitch 6855, la serie OmniSwitch 6450 y los conmutadores de LAN de la serie OmniSwitch 6250. El acceso inalámbrico se proporciona mediante puntos de acceso inalámbricos conectados directamente a conmutadores de nivel de acceso, mientras que el control se proporciona mediante los controladores WLAN (red de área local inalámbrica) OmniAccess™ 6000/4000. También se encuentran disponibles tecnologías de punto de acceso instantáneo, con funciones de controlador virtualizado integradas en los puntos de acceso.

CONCLUSIÓN

En un momento en el que crece el número de empresas que estudian cómo utilizar de forma óptima los programas BYOD para mejorar la productividad de los empleados, es importante que los departamentos informáticos cuenten con la flexibilidad necesaria para desarrollar soluciones adaptadas a sus necesidades específicas.

La implementación de BYOD de Alcatel-Lucent con la solución Converged Campus Network de Alcatel-Lucent proporciona la flexibilidad que los directores de TI necesitan para implementar una estrategia BYOD inmediatamente y hacerla evolucionar conforme vayan cambiando las necesidades. Está diseñada para atender todas las necesidades de control de accesos de la empresa y notificar a una infraestructura de red empresarial los derechos y el ancho de banda permitidos para cualquier usuario en cualquier dispositivo. A partir de ese punto, la infraestructura de Alcatel-Lucent gestiona los derechos de red al tiempo que supervisa continuamente la salud y el cumplimiento de las normas por parte de cada dispositivo. Este nivel de control puede configurarse para todos los empleados, contratistas e invitados conforme se incorporen a la red de cable o inalámbrica.

La arquitectura avanzada de Application Fluent Networ que constituye la base de la solución de Alcatel-Lucent para BYOD está diseñada para comunicar directamente con todos los elementos de la red empresarial, recoger información crítica del usuario y proporcionar instrucciones relativas a qué User Network Profile (uNP) debe utilizarse dada la combinación de usuario/dispositivo. El perfil de red puede incorporar parámetros como firewall, gestión de ancho de banda, detección de anomalías en el tráfico, identidad de red de área local virtual (VLAN), etc., lo que garantiza que la red siempre ofrezca una experiencia armonizada a todos los usuarios.

A diferencia de otras soluciones BYOD, la implementación de BYOD de Alcatel-Lucent está plenamente operativa tanto en los dispositivos de cable como inalámbricos que acceden a la red. Ofrece un conjunto completo de opciones para corrección, filtro de aplicaciones, comprobación continua de seguridad y generación de informes de gestión. Asimismo, está diseñada para permitir que los invitados entren en la red de diversas formas, incluido el acceso patrocinado o no patrocinado, garantizando en todo momento un acceso, una seguridad y una gestión adecuados.

Este enfoque escalable funciona con una amplia gama de dispositivos. Ofrece a los usuarios finales mayor libertad, al tiempo que aporta mayor tranquilidad a los administradores de redes.

ACRÓNIMOS

AFN	Application Fluent Network (Red apta para aplicaciones)
BYOD	Bring Your Own Device (Traiga su propio dispositivo)
LAN	Local Area Network (Red de área local)
MAM	Mobile Application Management (Gestión de aplicaciones móviles)
NAC	Network Access Control (Control de acceso a la red)
NAP	Network Access Protection (Protección de acceso a la red)
QoS	Quality of Service (Calidad de servicio)
RADIUS	Remote Authentication Dial-In User Service (Servicio al usuario para la conexión con autenticación remota)
TACACS+	Terminal Access Controller Access-Control System Plus (Cliente de sistema de control de acceso del controlador de acceso a terminales plus)
uNP	User Network Profile (Perfil de red de usuario)
VLAN	Virtual Local Area Network (Red de área local virtual)
VPN	Virtual Private Network (Red privada virtual)
WLAN	Wireless Local Area Network (Red de área local inalámbrica)

Alcatel·Lucent Enterprise