sedian

Seguridad Digital
de Andalucía

Configuración Segura en Windows

- 1ª sesión -

Junta de Andalucía

Unidades didácticas

Sincronización de Hora
Acceso remoto con Direct Access.
Acceso remoto VPN tradicional.
Acceso remoto por medio de Servicios de Escritorio Remoto (RDS)
Windows Defender Firewall con seguridad avanzada.
Protección frente a malware.
Bastionado de sistemas Windows por medio de líneas base.
Protección de las cuentas locales.
El visor de eventos de Windows.
La auditoría de Windows.
Cifrado del almacenamiento secundario.
Implementación del acceso inalámbrico en Windows.

Sincronización de Hora

Cómo funciona el Servicio de Hora de Windows.

La misión del maestro de operaciones de emulación del PDC respecto a la sincronización de hora de los equipos miembros de un dominio de Active Directory.

Sincronización de hora con las herramientas del servicio de hora de Windows (cliente NTP).

Sincronización de Hora

El servicio de hora de Windows (basado en NTP) asegura que los relojes de los equipos de una red sean lo más precisos posible.

Idealmente, todos los relojes de los equipos de un dominio de AD DS están sincronizados con la hora de un equipo autoritativo (PDC)

Antes de Windows Server 2016, el servicio W32Time no estaba diseñado para satisfacer las necesidades de las aplicaciones sujetas a limitaciones temporales. Sin embargo, las actualizaciones de Windows Server 2016 ahora permiten implementar una solución con una precisión de 1 ms en el dominio. Consulte **Hora precisa para Windows Server 2016** y **Límite de compatibilidad para configurar el servicio de hora de Windows para entornos de alta precisión** para obtener más información.

Sincronización de Hora

Los equipos que no están unidos a un dominio están configurados de forma predeterminada para sincronizarse con **time.Windows.com**.

No es posible garantizar la exactitud de la hora en los equipos que tienen conexiones de red intermitentes o sin conexión.

Un bosque de AD DS tiene una jerarquía de sincronización de hora predeterminada.

El servicio de hora de Windows sincroniza la hora entre los equipos de la jerarquía, donde los relojes de referencia más precisos se encuentran en la parte superior.

Sincronización de Hora

Los equipos que son miembros de un dominio funcionan como clientes de hora de forma predeterminada; por lo tanto, en la mayoría de los casos no es necesario configurar el servicio de hora de Windows.

Sin embargo, el servicio de hora de Windows se puede configurar para solicitar la hora desde un origen de la hora de referencia designado (y también puede proporcionar la hora a clientes)

El grado de precisión de la hora de un equipo se denomina "estrato".

El origen de la hora más preciso en una red (por ejemplo, un reloj de hardware) ocupa el nivel de estrato más bajo o el estrato uno.

Este origen de la hora preciso se denomina "reloj de referencia".

Sincronización de Hora

Un servidor NTP que adquiere su hora directamente de un reloj de referencia ocupa un estrato que es un nivel superior al del reloj de referencia.

Los recursos que adquieren la hora del servidor NTP están a dos pasos del reloj de referencia y, por tanto, ocupan un estrato que es dos veces mayor que el origen de la hora más preciso, y así sucesivamente.

A medida que aumenta el número de estrato de un equipo, la hora en el reloj del sistema puede ser menos precisa. Por lo tanto, el nivel de estrato de cualquier equipo es un indicador de cuán sincronizado está ese equipo con el origen de la hora más preciso.

Sincronización de Hora

El Protocolo de tiempo de redes (NTP) es el protocolo de sincronización de hora predeterminado que usa el servicio de hora de Windows en el sistema operativo.

La sincronización de la hora de NTP tiene lugar durante un cierto período e implica la transferencia de paquetes NTP a través de una red.

Los paquetes NTP contienen marcas de tiempo que incluyen una muestra de hora tanto del cliente como del servidor que participan en la sincronización de la hora.

NTP usa la hora universal coordinada (UTC) como estándar universal para la hora actual. La hora UTC es independiente de las zonas horarias y permite usar NTP en cualquier parte del mundo, independientemente de la configuración de la zona horaria.

Sincronización de Hora

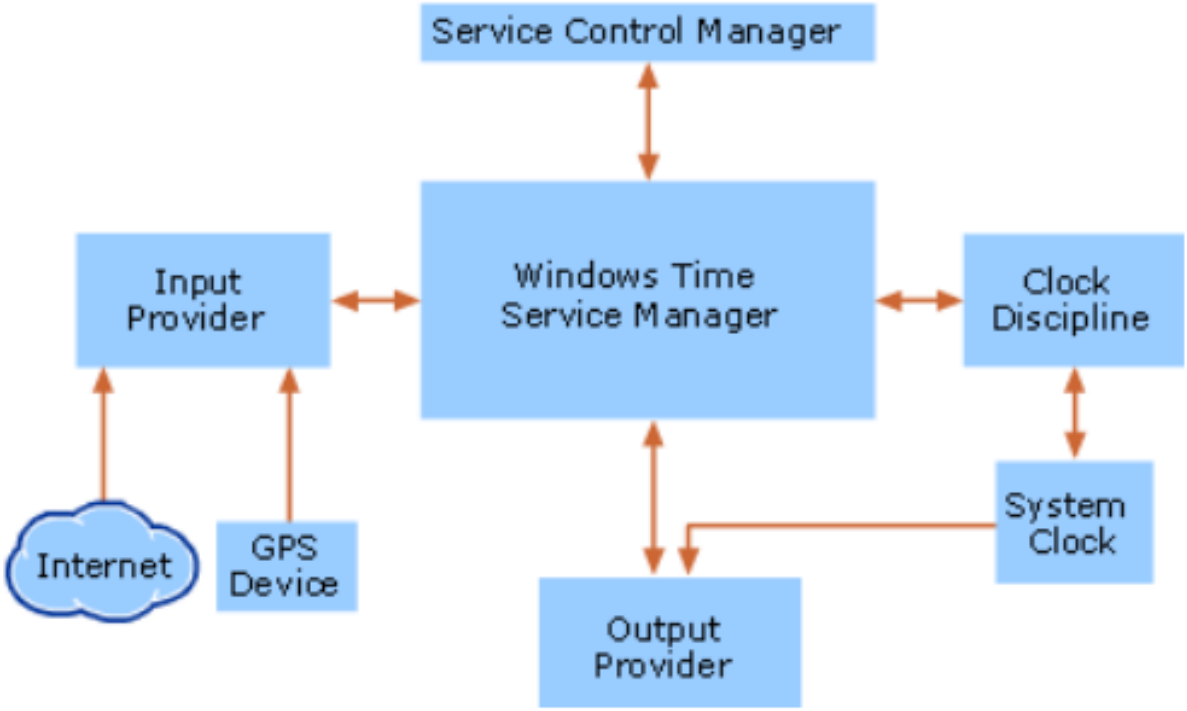
Arquitectura de servicio de hora de Windows

El servicio de hora de Windows consta de los siguientes componentes:

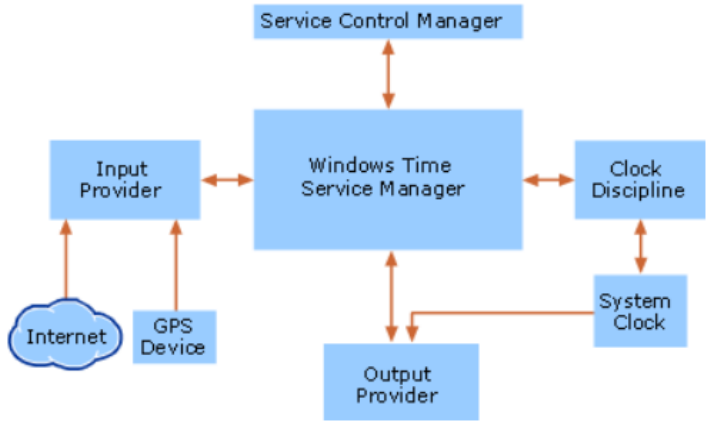
- Administrador de control de servicios
- Administrador del servicio de hora de Windows
- Sincronización de reloj
- Proveedores de hora

Sincronización de Hora

Arquitectura de servicio de hora de Windows



Sincronización de Hora



Service Control Manager Iniciar y detiene el servicio de hora de Windows.

Windows Time Service Manager Iniciar la acción de los proveedores de hora de NTP incluidos con el sistema operativo. Proporcionar información sobre el estado actual del sistema, como el origen de la hora actual o la última vez que se actualizó el reloj del sistema, también es responsable de crear eventos en el registro de eventos.

Sincronización de Hora

El proceso de sincronización de la hora conlleva los siguientes pasos:

1. Los proveedores de entrada solicitan y reciben las muestras de hora de los orígenes de la hora NTP configurados.

2. Estos ejemplos de hora se pasan luego al administrador del servicio de hora de Windows, que recopila todas las muestras y las pasa al subcomponente de sincronización de reloj.

3. El subcomponente de sincronización de reloj aplica los algoritmos NTP, lo que da como resultado la selección de la mejor muestra de hora.

4. El subcomponente de sincronización de reloj ajusta la hora del reloj del sistema a la hora más precisa.

Sincronización de Hora

Los paquetes NTP que se envían entre un equipo miembro del dominio y un controlador de dominio que funciona como servidor de hora se basa en la autenticación de clave compartida.

El servicio de hora de Windows usa la clave de sesión de Kerberos del equipo para crear firmas autenticadas en los paquetes NTP que se envían a través de la red. (¿Qué ocurre si se pierde la relación de confianza?)

Cuando un equipo solicita la hora a un controlador de dominio, el servicio de hora de Windows requiere que se autentique la hora.

El controlador de dominio devuelve la información necesaria en forma de un valor de 64 bits que se ha autenticado con la clave de sesión del servicio Inicio de sesión de red.

Si el paquete NTP devuelto no está firmado con la clave de sesión del equipo o tiene una firma incorrecta, se rechaza la hora. Los errores de autenticación se registran en el Registro de eventos.

Sincronización de Hora

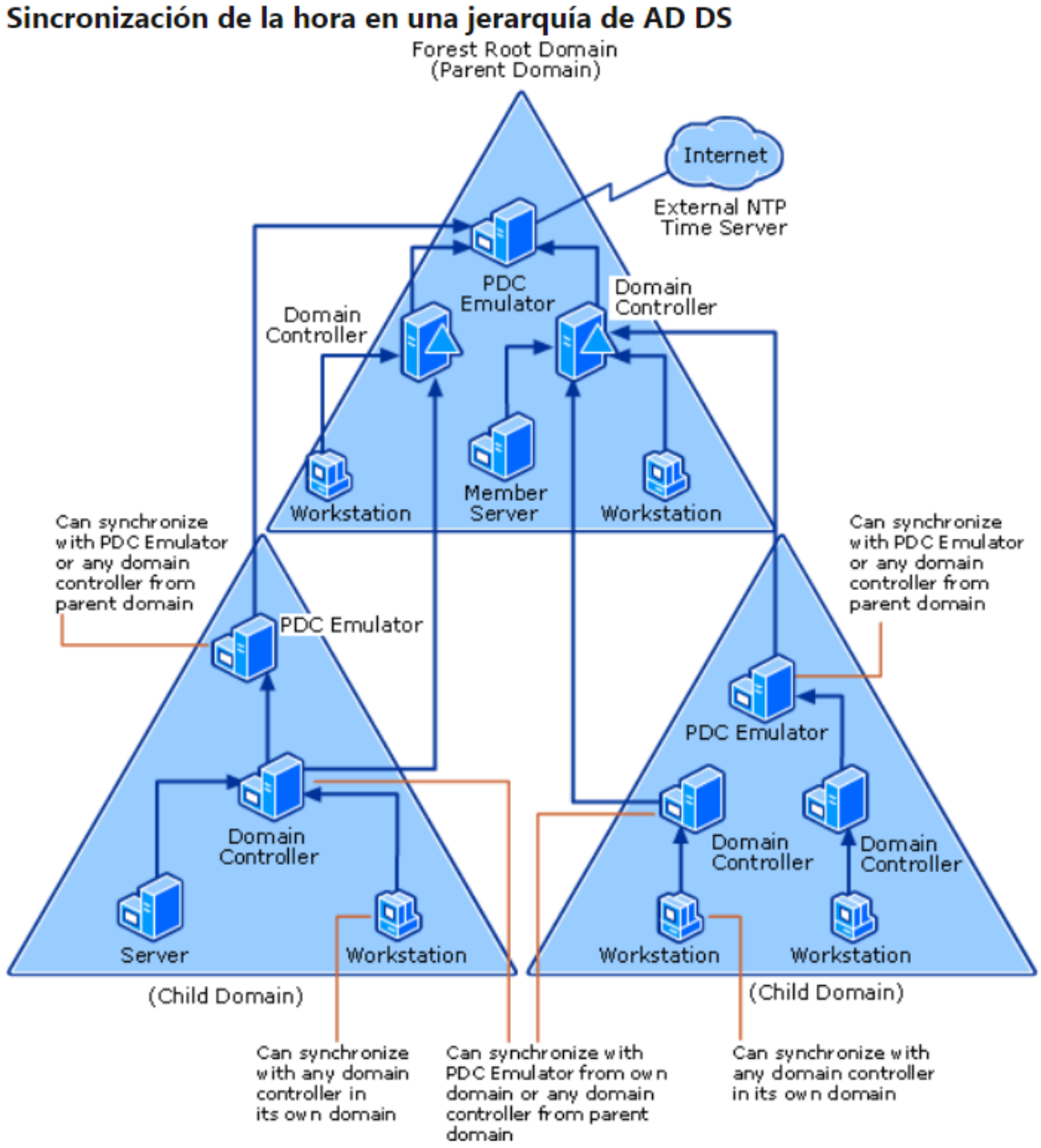
Los clientes de hora de Windows obtienen automáticamente la hora desde controladores de dominio en el mismo dominio.

En un bosque, los controladores de dominio de un dominio secundario sincronizan la hora con los controladores de dominio de sus dominios primarios.

En un bosque de Windows Server 2003 (o superior), el equipo que contiene la FSMO del emulador del controlador de dominio principal (PDC), ubicado en el dominio raíz del bosque, contiene la posición del mejor origen de la hora (el es DC que debemos sincronizar con el servidor NTP)

El resumen de lo descrito puede verse en la siguiente ilustración.

Sincronización de Hora



Sincronización de Hora

Configurar manualmente un origen de tiempo autoritativo en el PDC raíz del bosque

Para configurar el PDC en la raíz de un bosque de Active Directory para sincronizarse con un recurso de hora externo, siga estos pasos:

1. Localizar HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\W32Time\Parameters\Type, editar y poner como valor “NTP”

2. Localiza HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\W32Time\Config\AnnounceFlags, editar y poner valor 5.

3. Habilitar el servidor NTP. Localiza HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\W32Time\TimeProviders\NtpServer, editarlo y cambiar valor a “1”.

4. Especificar los orígenes de hora. Localiza HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\W32Time\Parameters, editamos “NtpServer” y escribimos “Peers”.

Sincronización de Hora

5. Reiniciar el servicio de hora con el commando:

   net stop w32time && net start w32time

Toda la información en detalle

https://support.microsoft.com/es-es/help/816042/how-to-configure-an-authoritative-time-server-in-windows-server

Sincronización de Hora

Planteamientos a discutir:

¿Qué papel tienen los hipervisores vmWare, Hyper-V, en la sincronización de hora?

¿Qué problema se presenta en Kerberos cuando los equipos del dominio no están correctamente sincronizados?

Sincronización de Hora

Para aprender más:

https://docs.microsoft.com/es-es/windows-server/networking/windows-time-service/how-the-windows-time-service-works

https://docs.microsoft.com/es-es/windows-server/networking/windows-time-service/windows-time-service-tools-and-settings

https://docs.microsoft.com/es-es/windows-server/networking/windows-time-service/how-the-windows-time-service-works#network-ports-used-by-windows-time-service

Acceso Remoto con Direct Access

Direct Access es un rol de Active Directory presente desde Windows 2K8R2.

Es un servidor VPN seamless basado en IKEV2.

La diferencia fundamental con otras soluciones de VPN es que DA permite aplicar la directiva de grupo a los equipos que se encuentran en Internet. Esto es un factor diferenciador.

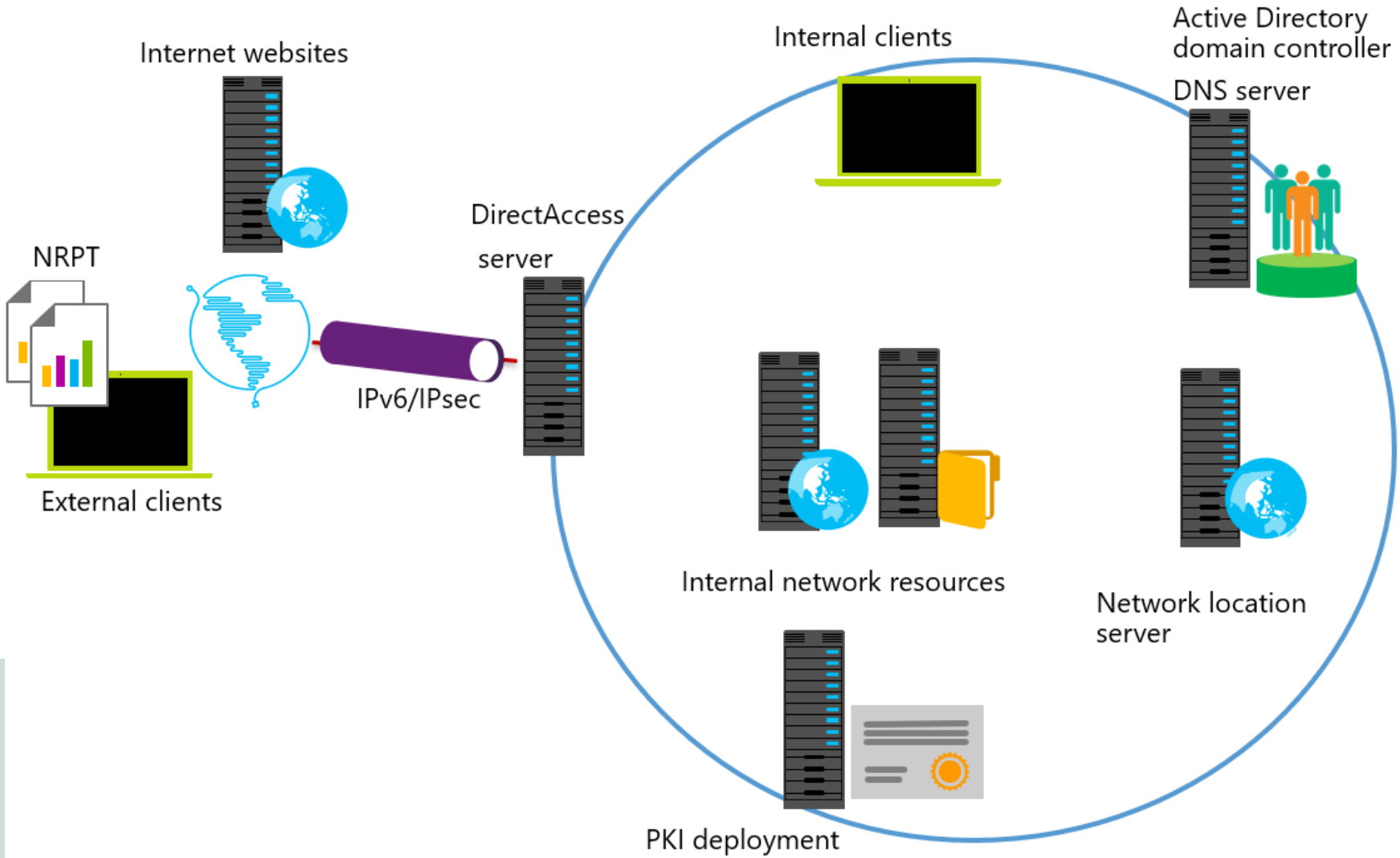
El despliegue es muy sencillo (tanto para la parte servidora como para la cliente) y se hace por GPOs preconfiguradas.

Usa el protocolo IPHTTPS por lo que el tráfico de DA puede ser protegido por los perimetrales con cambios mínimos en las reglas.

El usuario inicia sesión siempre de la misma forma, independientemente de que esté dentro o fuera de la infraestructura física.

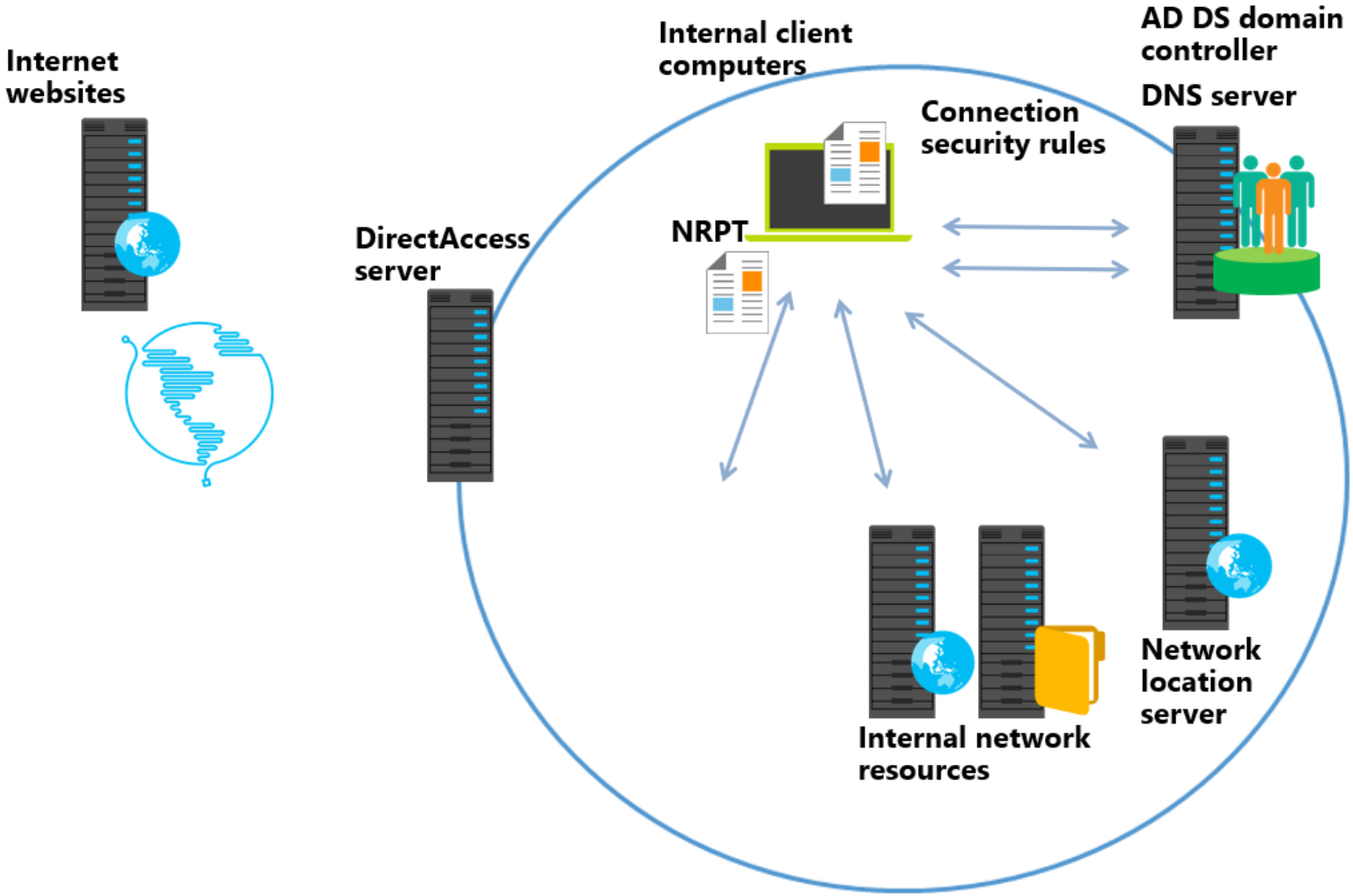
Acceso Remoto con Direct Access

Arquitectura



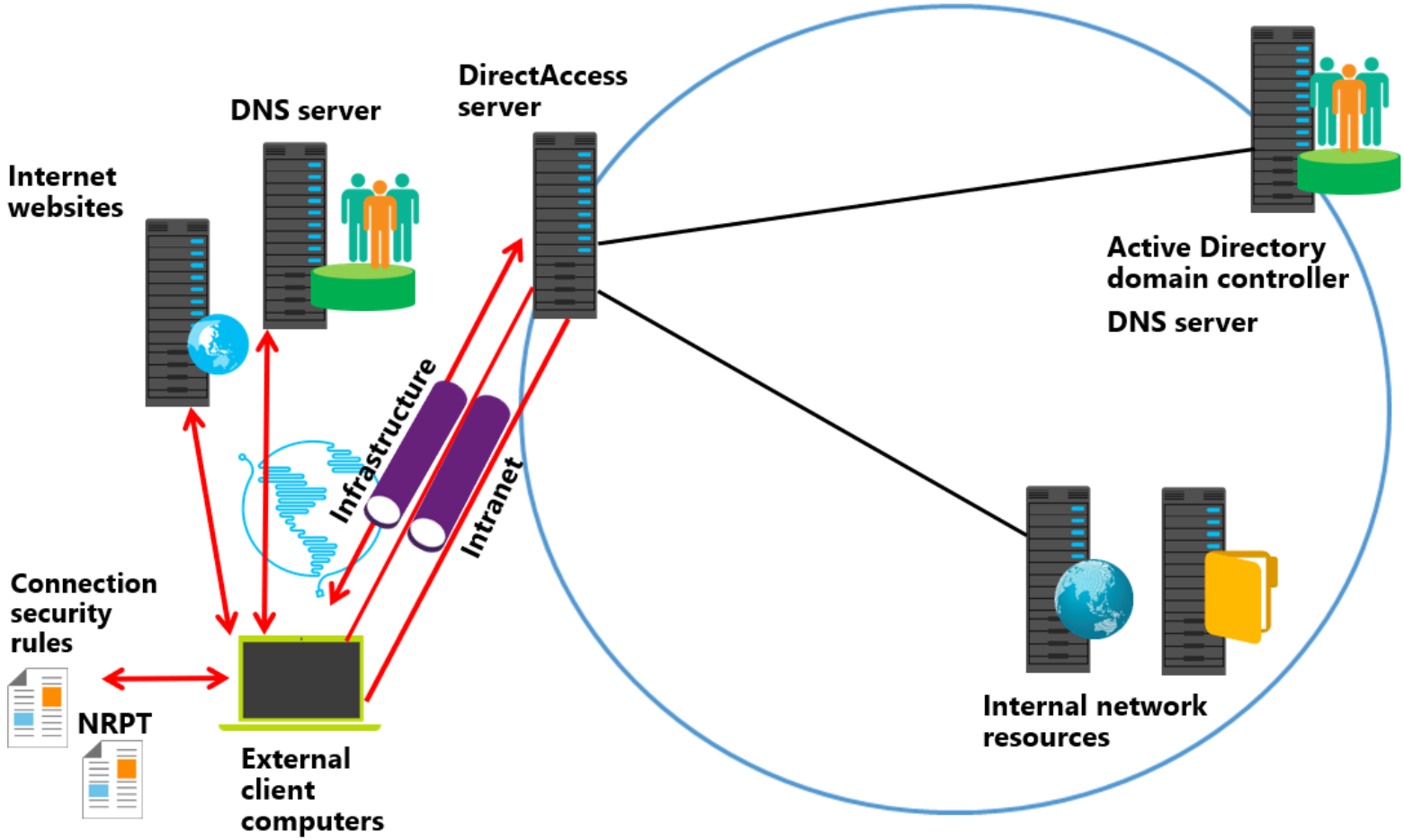
Acceso Remoto con Direct Access

DA cuando el cliente está dentro de la infraestructura.



Acceso Remoto con Direct Access

DA cuando el cliente está fuera de la organización



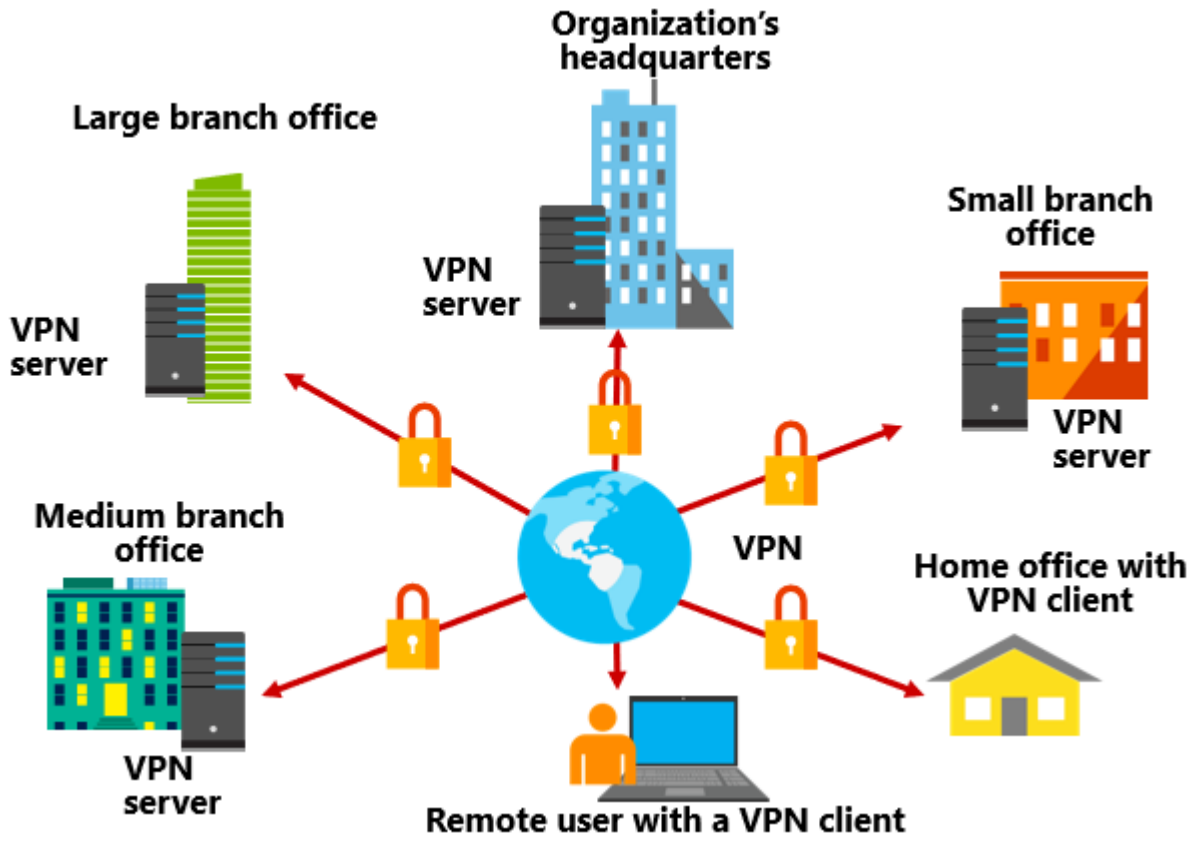
Acceso Remoto con Direct Access

Para aprender más (Ojo, es el primero de una serie de 6 artículos)

https://www.nomizo.fr/2013/03/directaccess-part1-implementing-basic.html

Acceso Remoto VPN tradicional.

Los escenarios VPN



Acceso Remoto VPN tradicional.

VPN de sitio a sitio

Conecta dos partes de una red privada.

Los protocolos más habituales son: PPTP, L2TP e IKEv2

El servidor VPN se suele implementar por medio de soluciones hardware (perimetrales)

Con la llegada de la virtualización es posible usar appliances VPN, también servidores de Microsoft.

Acceso Remoto VPN tradicional.

El servidor de Windows soporta cuatro protocolos de túnel.

Tunneling protocol	Firewall access	Description
PPTP	TCP port 1723	Provides data confidentiality, but not data integrity or data authentication
L2TP/IPsec	UDP port 500, UDP port 1701, UDP port 4500, and IP protocol ID 50	Uses either certificates or preshared keys for authentication; we recommend certificate authentication
SSTP	TCP port 443	Uses SSL to provide data confidentiality, data integrity, and data authentication
IKEv2	UDP port 500	Supports the latest IPsec encryption algorithms to provide data confidentiality, data integrity, and data authentication

Acceso Remoto VPN tradicional.

Las opciones de autenticación disponibles son

Protocol	Description	Security level
PAP	Uses plaintext passwords. Typically used if the remote access client and remote access server cannot negotiate a more secure form of validation.	The least secure authentication protocol. Does not protect against replay attacks, remote client impersonation, or remote server impersonation.
CHAP	A challenge-response authentication protocol that uses the industry-standard MD5 hashing scheme.	An improvement over PAP in that the password is not sent over the PPP link. Requires a plaintext version of the password to validate the challenge response. Does not protect against remote server impersonation.
MS-CHAPv2	An upgrade of MS-CHAP. Provides two-way authentication, also known as mutual authentication. The remote access client receives verification that the remote access server to which it is dialing in to has access to the user's password.	Provides stronger security than CHAP.
EAP	Allows for arbitrary authentication of a remote access connection through the use of authentication schemes, known as EAP types.	Offers the strongest security by providing the most flexibility in authentication variations.

Acceso Remoto VPN tradicional.

¿Qué es la reconexión VPN?

Proporciona conectividad seamless en el roaming de red.

Usa la tecnología IKEv2

Reestablece la conexión VPN cuando se recupera la conectividad.

Es la tecnología que usa Direct Access.

Acceso Remoto VPN tradicional.

¿Qué es CMAK?

Connection Manager Administration Kit

Nos permite crear configuraciones de conexión a servidores VPN

Los perfiles CMAK se pueden distribuir en imágenes del sistema operativo.

Acceso Remoto VPN tradicional.

Despliegue de una solución VPN en Windows.

Para aprender más:

https://support.microsoft.com/es-es/help/20510/windows-10-connect-to-vpn

https://docs.microsoft.com/es-es/windows-server/remote/remote-access/vpn/vpn-top

sedian Seguridad Digital de Andalucía