BeyondTrust y NIST:

Evolución de VPN hacia Confianza Cero

Este documento analiza cómo **BeyondTrust Privileged Remote Access (PRA)** se alinea con los marcos de seguridad del **NIST** (National Institute of Standards and Technology), específicamente bajo el modelo de **Arquitectura de Confianza Cero (ZTA)**, y expone las limitaciones críticas de las **VPN tradicionales** en este contexto.

1. El Desafío de las VPN frente a NIST

Según las directrices del NIST, las **VPN** presentan deficiencias estructurales para el entorno de seguridad actual:

- **Confianza Implícita y Movimiento Lateral**: Las VPN operan típicamente en la capa de red. Una vez que un usuario se autentica, a menudo se le otorga acceso a un segmento completo de la red, lo que permite el **movimiento lateral** de posibles atacantes. NIST[1], señala que las VPN con túneles cifrados dificultan la capacidad de la organización para monitorear el tráfico en busca de código malicioso.

- **Gestión de Dispositivos Personales**: El uso de VPN en dispositivos personales (BYOD) se considera un **riesgo crítico**, ya que la organización no tiene control sobre la higiene del dispositivo (parches, malware), y la VPN actúa como un conducto para que esas amenazas ingresen a la red corporativa.

- **Visibilidad de la Superficie de Ataque**: Las VPN suelen exponer puertos a Internet para su conexión, lo que permite que las aplicaciones y recursos internos sean visibles para actores externos incluso antes de la autenticación.

2. Cumplimiento de NIST mediante BeyondTrust PRA

A diferencia de las VPN, BeyondTrust PRA está diseñado bajo los principios de **NIST Zero Trust**[2] y cumple con los controles de acceso de **NIST**[3]:

- **Acceso de Mínimo Privilegio (AC-6)**: BeyondTrust PRA aplica un control granular a nivel de aplicación, no de red. Los usuarios se conectan solo a los recursos específicos que necesitan, eliminando la exposición de la red corporativa y el riesgo de movimiento lateral.

- **Punto de Ejecución de Políticas (PEP)**: Actúa como el **Punto de Ejecución** de Políticas y Gateway dentro de la arquitectura de NIST, asegurando que ninguna conexión sea directa al recurso. Todas las sesiones se realizan a través de un gateway seguro que solo muestra la actividad de la sesión (pantalla, terminal) al usuario.

- **Monitoreo y Auditoría Automatizados (AC-17)**: PRA cumple con el requisito de monitoreo continuo al grabar todas las sesiones (en video y metadatos de texto). Esto permite la visibilidad en tiempo real de lo que el usuario está haciendo y por qué, permitiendo la revocación inmediata ante comportamientos sospechosos. Esta grabación completa genera documentación detallada.

- **Gestión de Credenciales (IA-5)**: PRA permite la **inyección automática de credenciales** desde un cofre seguro (Vault). De este modo, el usuario accede al sistema sin conocer ni ver la contraseña, cumpliendo con las recomendaciones de NIST sobre protección de mecanismos de autenticación y reducción de fraude de identidad.

- **Acceso Just-In-Time (JIT) y Privilegios Cero**: Cumple con la visión de NIST de eliminar la confianza persistente. El acceso se otorga solo por el tiempo necesario y se revoca automáticamente al completar la tarea o tras un periodo de inactividad.

Comparativa de Cumplimiento

CARACTERÍSTICA	VPN TRADICIONAL	BEYONDTRUST PRA (CUMPLE NIST)
Nivel de Acceso	Capa de Red (Capa 3)	Capa de Aplicación (Granular)
Confianza	Implícita (Perimetral)	Cero (Nunca confiar, siempre verificar)
Visibilidad	Recursos visibles en la red	Recursos ocultos; solo se ve la sesión
Auditoría	Registros de conexión	Grabación completa de la sesión y comandos
Manejo de Credenciales	Expuestas al usuario	Inyectadas desde un Vault (ocultas)

Conclusión: Mientras que las VPN fueron diseñadas para extender un perímetro, BeyondTrust PRA se alinea con la evolución de NIST hacia la **Confianza Cero**, proporcionando un acceso remoto seguro que mitiga el movimiento lateral, protege las credenciales privilegiadas y garantiza una auditoría total de cada acción realizada sobre activos críticos

Ref: (1) NIST SP 800-53 (AC-17), (2) NIST SP 800-207 (Zero Trust), (3) NIST SP 800-53 (AC-17) y 800-171r3