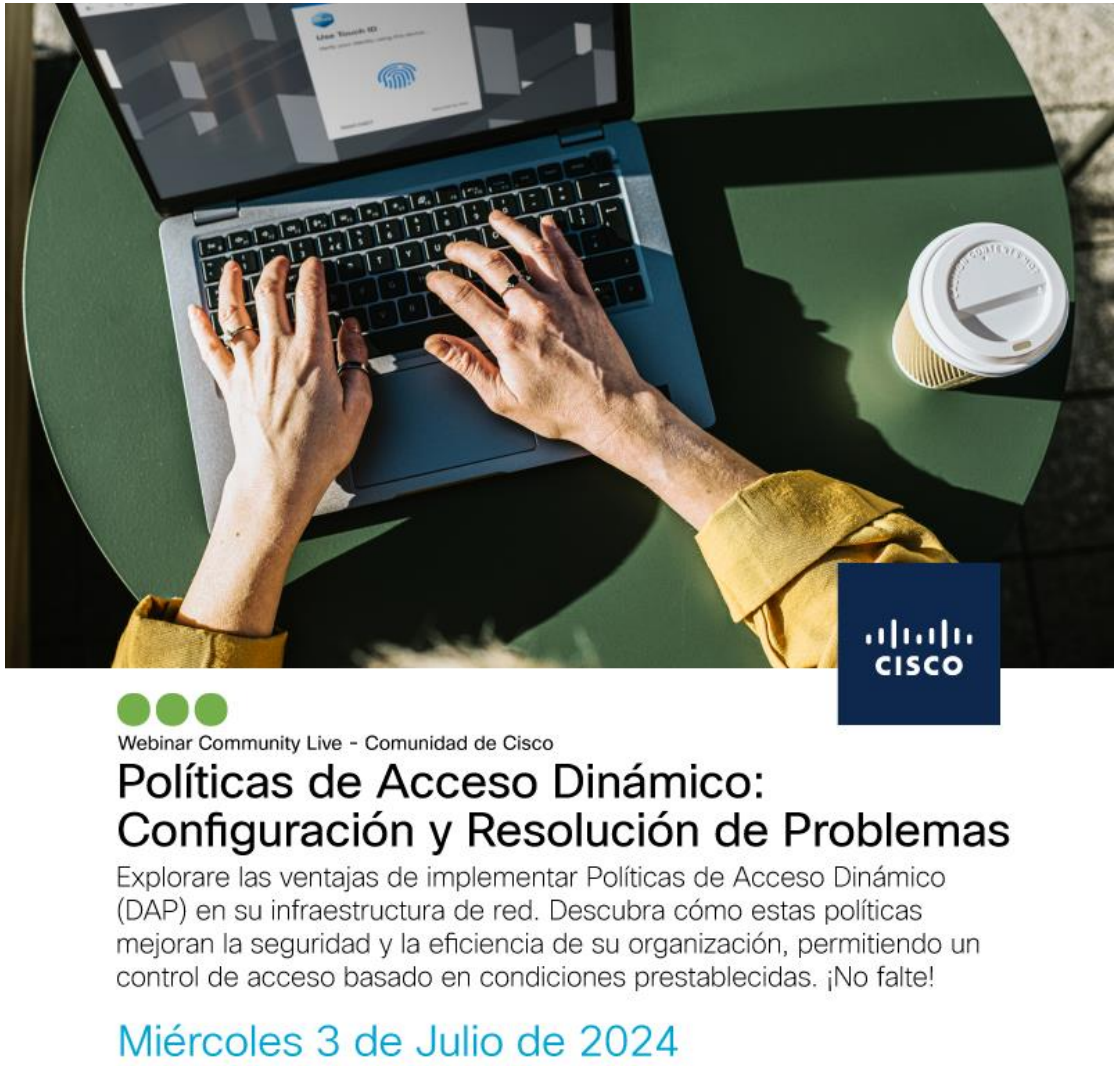
Vista previa de la presentación

Diana Aguilar – Technical Consulting Engineer
Erick Montiel- Technical Consulting Engineer
Luis Suárez - Technical Consulting Engineer



https://bit.ly/CLes-jul24

Políticas de Acceso Dinámico

Utilice las políticas de acceso dinámico para:

- Aplicar políticas específicas en función del usuario o grupo al que pertenezca.

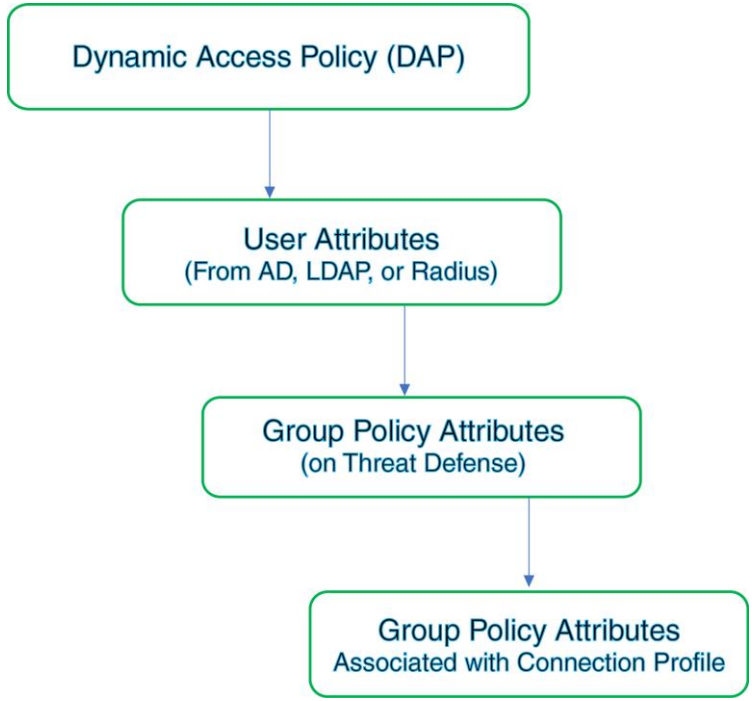
  Por ejemplo: dando más acceso a empleados que a contratistas.

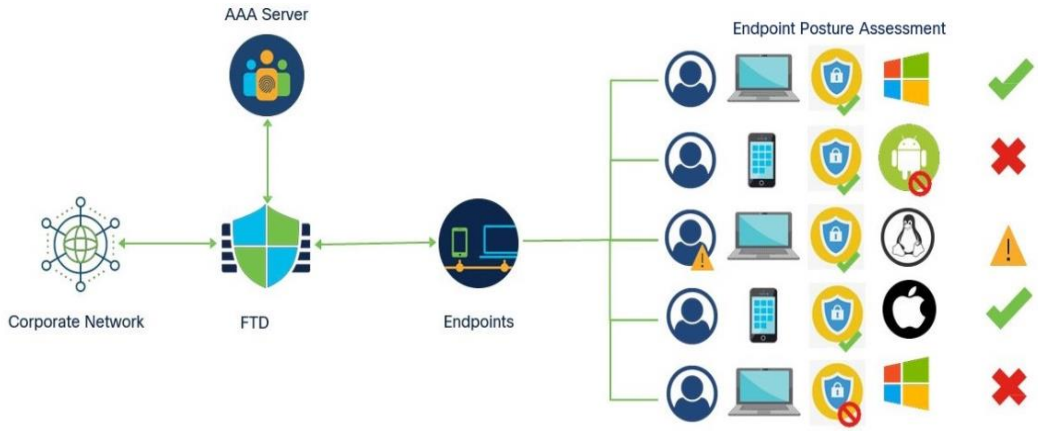
- Verificar que el dispositivo cumpla con las políticas de seguridad antes de establecer la conexión y otorgar acceso a la red.

- Ajustar de manera dinámica los permisos de usuario según el contexto.

  Por ejemplo: más privilegios en una oficina corporativa que en un café internet.

- Personalizar los ajustes de conexión, como establecer tiempos de espera de sesión o aplicar ACLs (Listas de Control de Acceso), dependiendo de los resultados de la política.



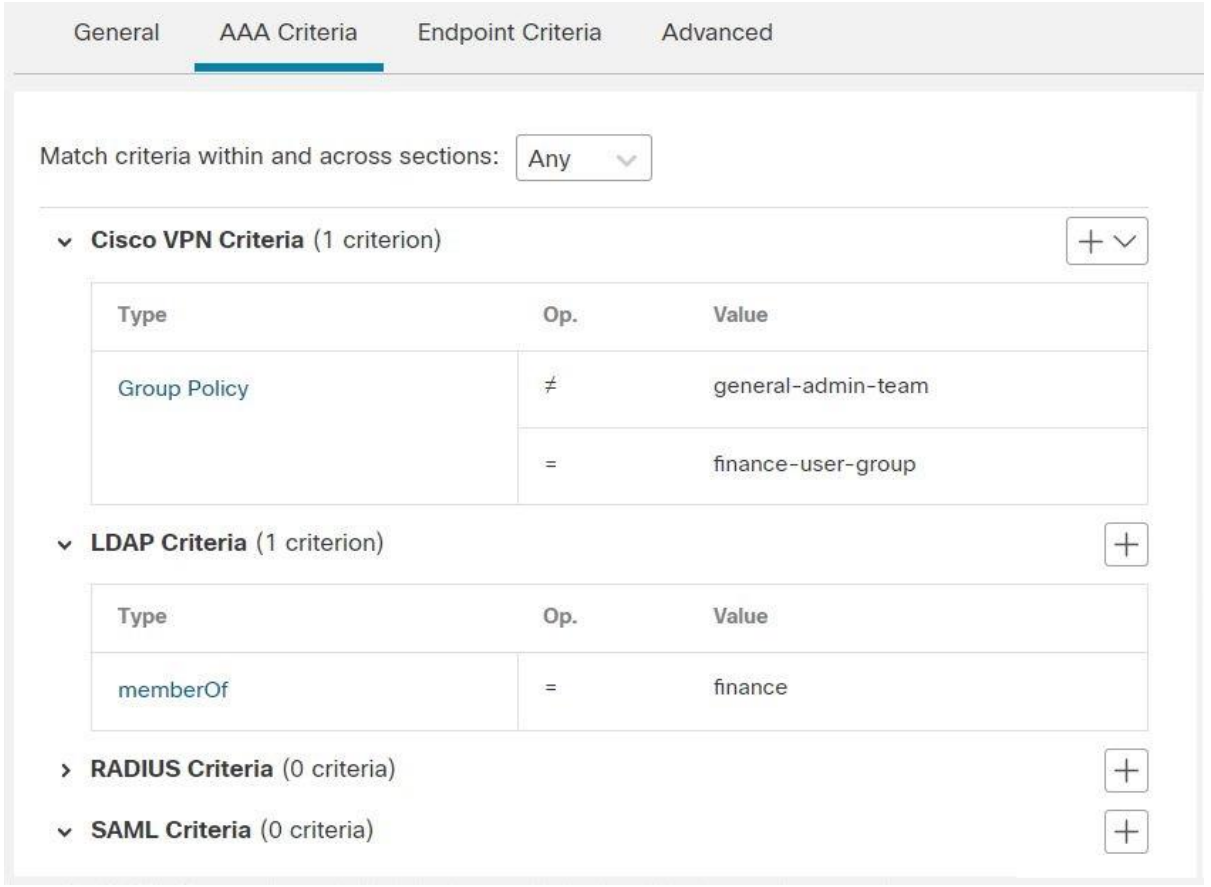


Configuración

La configuración de las políticas de acceso permite la personalización con base en atributos relacionados con AAA, tales como:

- Valores de Autenticación
- Perfiles de Conexión
- Política de Grupo
- Dirección IP
- Nombre de Usuario

Esta integración avanzada fortalece la postura de seguridad, permitiendo un acceso controlado y conforme con las políticas organizacionales, garantizando así una gestión de acceso robusta y centralizada.

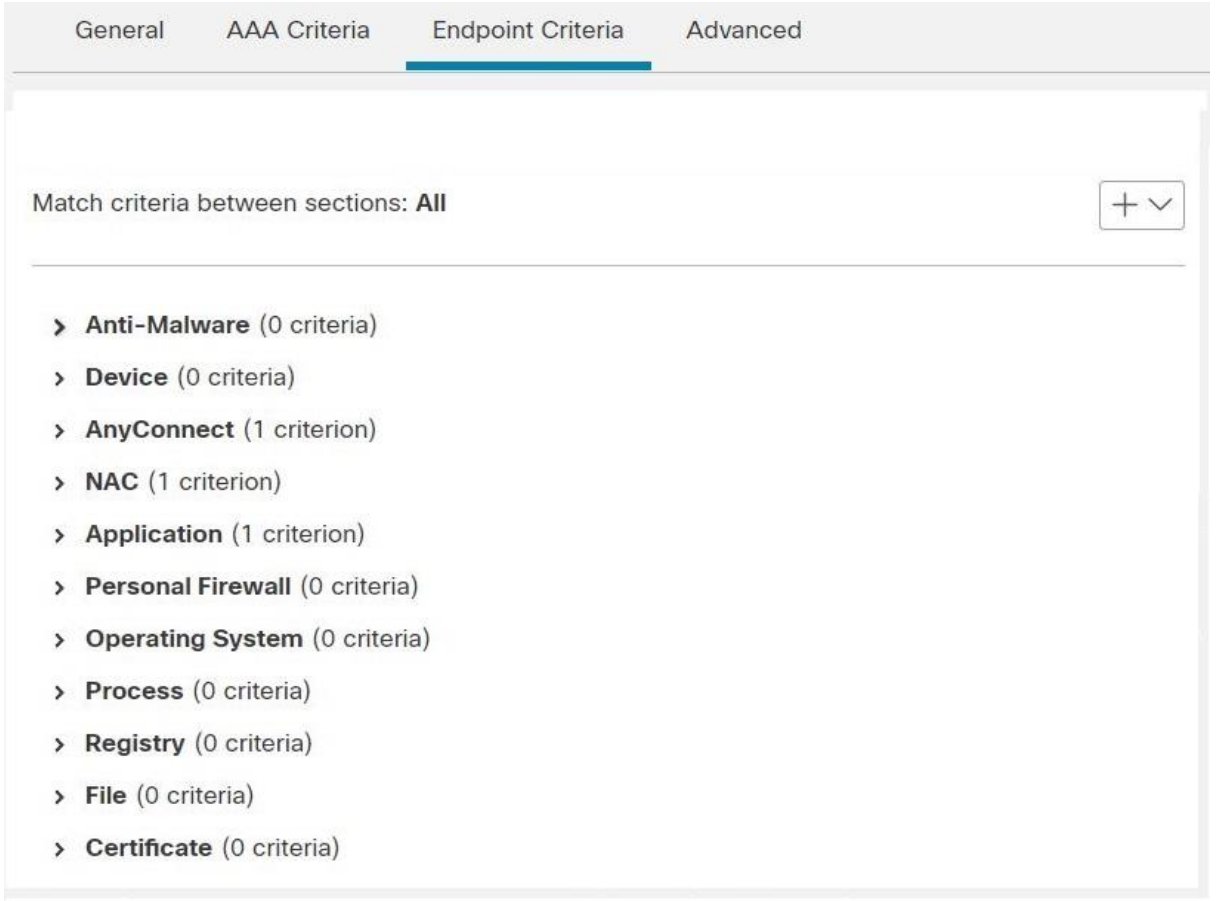


Secure Firewall Posture

Escale la protección de su red implementando Secure Firewall Posture. Esta poderosa combinación permite incorporar criterios de seguridad basados en el estado del dispositivo final, por ejemplo:

- Sistemas operativos.
- Programas de seguridad en ejecución.
- Configuraciones del registro.
- Versiones de aplicaciones.
- Detección de archivos.

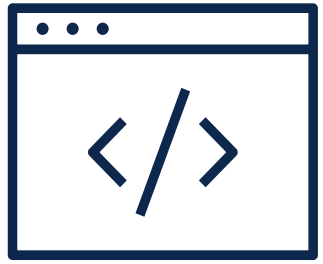
Al hacerlo, no solo se refuerzan los parámetros de conexión, sino que también se asegura que el dispositivo del usuario cumpla con los estándares de seguridad requeridos.



Diagnóstico y Solución de Problemas de DAP

Con el uso de DART (Diagnostics and Reporting Tool) y línea de comandos (CLI) de Secure Firewall, el diagnostico de problemas se vuelve más sencillo, ya que nos permiten:

- Verificar que la configuración sea la deseada.
- Ejecutar comandos de debugs para inspeccionar los atributos que el dispositivo transmite y cómo estos se correlacionan con los récords de DAP configurados.
- Asegurar el acceso adecuado de cada usuario.



Buscamos nuevos expertos para traer más temas...

¡No se pierda nuestro próximo webinar el miércoles 3 de julio!

☞ ¡Inscríbase ahora!

Nuestros eventos anteriores

[Implementación y Configuración de Cisco ISE]

Seguridad / 20 Junio 2024
Avril Alonso y Julio Román

Exploramos las consideraciones clave para realizar actualizaciones exitosas en Cisco Identity Services Engine (ISE) y los Firewall (NGFW) de Cisco. Discutimos las mejores prácticas, los desafíos comunes y las estrategias recomendadas para planificar y ejecutar actualizaciones de manera efectiva. Desde la evaluación de requisitos de hardware y software hasta la gestión de compatibilidad y la mitigación de riesgos, ofreciendo valiosa información para garantizar una transición fluida y segura a las versiones más recientes de Cisco ISE y NGFW.

[Explorando Multicast en Capa 2: IGMP, IGMP Snooping y Consejos para Resolver Problemas]

Routing & Switching / 13 Junio 2024
Aarón Díaz Gutiérrez y Ricardo Bermejo Ochoa

Exploramos diversos aspectos clave en el funcionamiento de multicast en capa 2, centrándonos en Internet Group Management Protocol (IGMP) y su implementación en entornos de redes locales. Analizamos las nociones fundamentales de IGMP, junto con IGMP snooping y su configuración para mejorar la eficiencia de las redes. Además, compartimos con ustedes consejos prácticos para la resolución de problemas relacionados con IGMP, destacando estrategias efectivas para diagnosticar y resolver incidentes comunes.