

¿Cuál es la diferencia entre la autenticación NTLM y LDAP?

Contenido

[Pregunta](#)

[Entorno](#)

[Experiencia del cliente](#)

[Básico](#)

[NTLM \(SSP\)](#)

[Security](#)

[Básico](#)

[NTLM \(SSP\)](#)

Pregunta

¿Cuál es la diferencia entre la autenticación NTLM y LDAP?

Entorno

Dispositivo de seguridad Cisco Web Security Appliance (WSA), todas las versiones de AsyncOS

La autenticación con WSA se puede dividir en las siguientes posibilidades:

Cliente > WSA	WSA > Servidor de autenticación	Tipo de servidor de autenticación
Autenticación básica	autenticación LDAP	Servidor LDAP
Autenticación básica	autenticación LDAP	Servidor de Active Directory con LDAP
Autenticación básica	autenticación básica NTLM	Servidor de Active Directory (NTLM Basic)
autenticación NTLM	autenticación NTLMSSP	Servidor de Active Directory (NTLMSSP)

Nota: NTLMSSP se conoce comúnmente como NTLM.

A continuación se muestra la diferencia notable entre la autenticación básica y la autenticación NTLM.

Experiencia del cliente

Básico

Siempre se le solicitarán al cliente las credenciales. Una vez introducidas las credenciales, los exploradores suelen ofrecer una casilla de verificación para recordar las credenciales proporcionadas. Cada vez que se cierre el explorador, el cliente volverá a preguntar o enviará las credenciales recordadas previamente de nuevo.

Nota: NTLM Basic utiliza la autenticación básica del cliente y, por lo tanto, tendrá las mismas propiedades.

NTLM (SSP)

- El cliente se autenticará de forma transparente utilizando sus credenciales de inicio de sesión de Windows.
- Los únicos casos en los que el cliente solicitará las credenciales son si las credenciales de Windows fallan por primera vez (esto ocurrirá si el cliente ha iniciado sesión localmente en el equipo y no en el dominio utilizado para la autenticación) o si el cliente no confía en el WSA.

Security

Básico

Las credenciales se envían de forma insegura mediante texto sin formato. Una simple captura de paquetes entre el cliente y el WSA revelará el nombre de usuario y la contraseña del usuario.

NTLM (SSP)

Las credenciales se envían de forma segura mediante un intercambio de señales en tres direcciones (autenticación de estilo de resumen). La contraseña NUNCA se envía a través del cable.

El proceso NTLM se ve de la siguiente manera:

1. El cliente envía un paquete de negociación NTLM. Esto indica al WSA que el cliente se propone realizar la autenticación NTLM.
2. El WSA envía una cadena NTLM Challenge al cliente.
3. El cliente utiliza un algoritmo basado en su contraseña para modificar el desafío y envía la respuesta de desafío al WSA.
4. A continuación, el servidor AD verifica que el cliente esté utilizando la contraseña correcta en función de si modificó o no la cadena de desafío de forma adecuada.