目次

[質問](#)
[環境](#)
[クライアント エクスペリエンス](#)
[基本](#)
[NTLM (SSP)](#)
[セキュリティ](#)
[基本](#)
[NTLM (SSP)](#)

質問

NTLM と LDAP 認証の違い

環境

Cisco Web セキュリティ アプライアンス (WSA)、AsyncOS のすべてのバージョン

WSA 認証は、次のように分類できます。

クライアント > WSA	WSA > 認証サーバ	認証サーバ タイプ
基本認証	LDAP 認証	LDAP サーバ
基本認証	LDAP 認証	LDAP を使用する Active Directory サーバ
基本認証	NTLM Basic 認証	Active Directory サーバ (NTLM Basic)
NTLM 認証	NTLMSSP 認証	Active Directory サーバ (NTLMSSP)

注 NTLMSSP は、一般に NTLM とも呼ばれます。

基本認証と NTLM 認証の注目すべき相違点を次に示します。

クライアント エクスペリエンス

基本

クライアントは、常に、クレデンシャルを要求されます。 クレデンシャルを入力すると、一般に、ブラウザにより、入力したクレデンシャルを記憶するためのチェックボックスが提供されます。 ブラウザが閉じられると、クライアントは、クレデンシャルをもう一度要求するか、以前に記

憶したクレデンシャルをもう一度送信します。

注 NTLM Basic ではクライアントからの基本認証を活用しているため、同じプロパティが含まれています。

NTLM (SSP)

- クライアントは、Windows のログオン クレデンシャルを使用して透過的に認証を行います。
- クライアントがクレデンシャルを求める唯一のケースは、Windows クレデンシャルが初めて失敗した場合 (これは、クライアントが、認証に使用するドメインにログインするのではなく、ローカルにコンピュータにログインしているときに発生します) 、またはクライアントが WSA を信頼していない場合です。

セキュリティ

基本

クレデンシャルは、プレーン テキストを使用して、安全ではない状態で送信されます。 クライアントと WSA との間でのシンプルなパケット キャプチャにより、ユーザのユーザ名とパスワードが露呈されます。

NTLM (SSP)

クレデンシャルは、3 ウェイ ハンドシェイク (ダイジェスト形式の認証) で保護されて送信されます。 パスワードが有線ネットワーク上で送信されることはありません。

NTLM プロセスは次のように行われます。

1. クライアントが、NTLM ネゴシエート パケットを送信します。 これにより、WSA に対し、クライアントが NTLM 認証を行う意向であることを伝えます。
2. WSA がクライアントに NTLM チャレンジ文字列を送信します。
3. クライアントが、パスワードに基づくアルゴリズムを使用してチャレンジを変更し、WSA へのチャレンジ応答を送信します。
4. その後、チャレンジ文字列が正しく変更されたかどうかに基づいて、AD サーバは、クライアントが正しいパスワードを使用していることを確認します。