

AXIOLE を用いた Alcatel Lucent OmniSwitch, OminAccess WLAN の認証

2015/10/27

株式会社ネットスプリング 営業本部 営業部 SE

本資料の概要

この資料では、AXIOLE を用いて、Alcatel Lucent OmniSwitch、OmniAccess WLAN の、CaptivePortal、EAP 等による認証を行なう方法について概略を解説します。また、Clear Pass Policy Manager との連携により、AXIOLE の IdP オプションを用いた、SAML 連携による認証を実現しました。

1. EAP、MAC、CaptivePortal(Web)認証

AXIOLE の RADIUS 認証機能を用いることで、下記のとおり各種 LAN 認証に対応できることを確認しました。RADIUS Proxy にも対応しておりますので、eduroam をご利用することも可能です。以下のような構成で動作確認をしております。

認証方式	認証手順	動作確認結果
IEEE802.1X(PEAP, TTLS, TLS)	PEAP : ID/PW TTLS : サーバのみ証明書 ID/PW TLS : サーバ・クライアント相互に 証明書照会	○
MAC 認証	端末の MAC アドレスを照会	○
CaptivePortal(Web 認証)	ブラウザにて ID/PW 入力	○
MAC 認証→Web 認証(and 条件)	MAC 照会後に ID/PW 入力	○
MAC 認証→Web 認証(or 条件)	MAC 照会失敗時 ID/PW 要求	○

2. Clear Pass Policy Manager と連携した SAML 認証

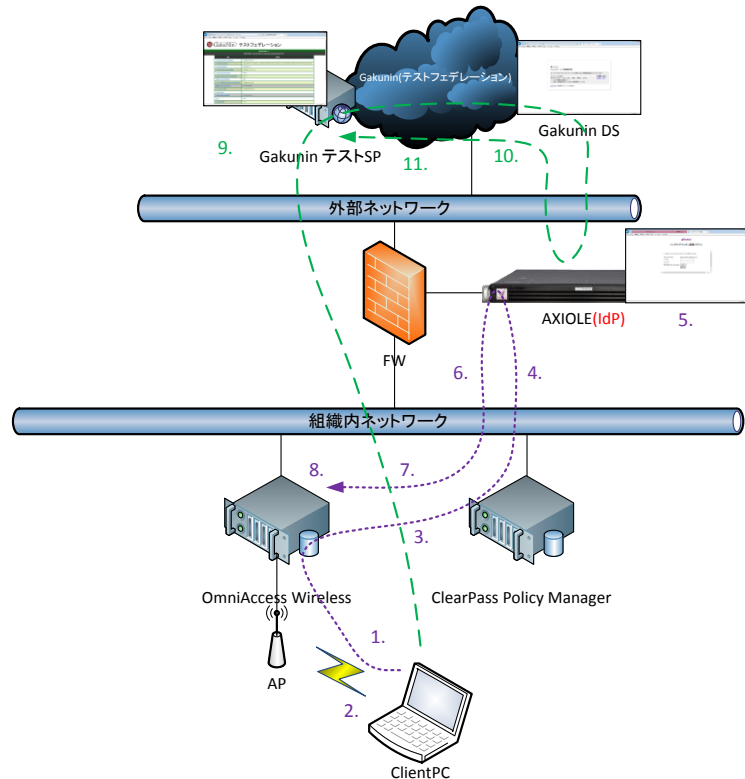
ClearPass Policy Manager を利用することで、OmniSwitch、OmniAccess の Captive Portal 認証を SAML の SP とすることができます。AXIOLE の IdP オプションと組み合わせ、ネットワーク認証を SAML 対応させることができます。

これを利用することで、LAN への認証で学認等の同じく SAML に連携したサービスへのシングルサインオンを実現することができます。

2.1. 利用シナリオ

自組織内の無線 LAN に接続

1. 端末を OmniAccess WLAN(無線 LAN)に接続。
2. 端末ブラウザ起動。
3. Web 認証起動。
→ ClearPass(SP)にリダイレクト。
4. ClearPass から AXIOLE(IdP)にリダイレクト。
5. IdP で認証。
6. 認証に成功したら属性情報と共に ClearPass にリダイレクト。
7. ClearPass が OmniAccess WLAN に該当端末のアクセス許可を発行。
8. 端末はネットワーク利用可能となる。



学認の SP に接続

9. 端末から学認 SP に接続。
10. SP から DS にリダイレクトされ、DS にて自組織選択。
DS から指定された IdP にリダイレクト。
11. 5.~6. で認証済みのため、そのまま学認 SP にシングルサインオン成功。

2.2. 機能を利用するメリット

- ネットワーク接続時の最初の認証が学認と連携。
ネットワーク接続認証と同時に学認サービスにもシングルサインオン可能。
可用性が向上すると共に、セキュリティ強化にも寄与します。
- 利用の容易な Web 認証。
- 自組織のみ、地域フェデレーションなどの利用に最適。

2.3. 導入時に行うこと(概要)

2.3.1. OmniAccess WLAN/OmniSwitch/ClearPass Policy Manager

- CaptivePortal の設定を行い、認証を ClearPass Policy Manager にリダイレクトさせます。
- 認証前のポリシーを作成し、ClearPass Policy Manager、AXIOLE(IdP)、DS 等の認証前にアクセスさせるべきサービスへの通信を許可する。これを対象とする SSID や VLAN に適用させて下さい。
- 認証後のポリシーを設定、適用させて下さい。
- ClearPass Policy Manager を SP に設定して、IdP として AXIOLE を指定します。必要に応じて参照する属性を設定します。

2.3.2. AXIOLE

- IdP オプションを有効にします。
- SP のメタデータを ClearPass Policy Manager より取得。自身のメタデータに取り込みます。
- Relying Party、属性定義、属性フィルタポリシー等各設定をします。
- (学認連携を行う場合は、この後学認テストフェデレーションや本番フェデレーションとの連携設定も行います)

3. まとめ

AXIOLE(IdP)、Alcatel Lucent OmniSwitch、OmniAccess WLAN 各製品による各種認証を実現可能であることを確認しました。また、Alcatel Lucent ClearPass Policy Manager も連携させ、SP として利用することで、SAML 連携によるシングルサインオンを実現することができ、学認などの SAML を使用した認証システムの可用性、安全性の向上をはかることができました。

4. お問い合わせ

株式会社ネットスプリング サポートセンター

TEL: 050-5536-4841 (月～金 9:00～17:00、日曜日・祝祭日・年末年始を除く)

FAX: 050-3737-1458

E-mail: nssc@netspring.co.jp



※1 AXIOLE は、株式会社ネットスプリングの登録商標です。

※2 その他、本書に記載されている会社名、商品名は、各社の商標または登録商標です。