

RADIUSサーバ相互接続情報

Cisco Secure ACS

2009年 8月 6日
アラクサラネットワークス株式会社
ネットワークテクニカルサポート

はじめに

■注意事項

記載した情報は、弊社内の検証環境下で実施した結果です。従って、全ての条件下において結果を保証するものではありません。

■商標一覧

Cisco、Cisco Systems、およびCisco Systemsロゴは、Cisco Systems, Inc.またはその関連会社の米国およびその他の一定の国における登録商標または商標です。

Microsoftは、米国およびその他の国における米国Microsoft Corp.の登録商標です。

Windowsは、米国およびその他の国における米国Microsoft Corp. の登録商標です。

記載の会社名、製品名はそれぞれの会社の商標もしくは登録商標です。

■輸出時の注意

本資料を輸出される場合には、外国為替および外国貿易法ならびに米国の輸出管理関連法規などの規制をご確認の上、必要な手続きをお取りください。なお、ご不明な場合は、弊社担当営業にお問い合わせください。

目次

1. 概要
2. 評価構成
3. 相互接続結果

1. 概要

●本評価の目的

AXシリーズがサポートするネットワーク認証機能(IEEE802.1X認証、Web認証、MAC認証)とRADIUSサーバであるCisco Secure ACS アプライアンス(Cisco 1113 , Secure Access Control Server)の相互接続性を確認する。

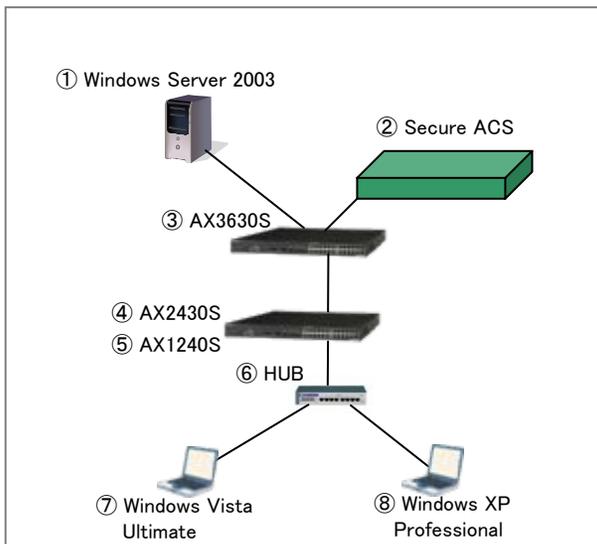
●確認項目

AXシリーズがサポートするネットワーク認証機能との接続確認

- ・認証方式:IEEE802.1X認証、Web認証、MAC認証
- ・マルチステップ認証(MAC認証+Web認証) 、(MAC認証+802.1X認証)
- ・各認証方式における認証モード:固定VLANモード、ダイナミックVLANモード
- ・RADIUS Accounting機能

2. 評価構成

●ネットワーク構成図と使用機器



項番	機器名	役割	Version	備考
①	Windows Server 2003	Active Directory	SP2	・Cisco Secure ACS Remote Agent 4.2をインストール済
		DNSサーバ		
		DHCPサーバ		
		プライベートCA		
②	Cisco Secure ACS アプライアンス (Cisco1113,Secure Access Control Server)	RADIUSサーバ	4.2	サーバ証明書、CAの証明書をインストール済
③	AX3630S	L3スイッチ	11.1.A	DHCP-Relay設定
④	AX2430S	認証スイッチ	11.1.A	ダイナミックVLAN使用時は認証前VLANのDHCPサーバとして動作
⑤	AX1240S		2.1	
⑥	—	Hub	—	EAP透過スイッチ
⑦	Windows Vista Ultimate	クライアントPC	SP1	・IE使用(XPはIE6、VistaはIE7) ・ユーザー証明書、CAの証明書をインストール済
⑧	Windows XP Professional	クライアントPC	SP2	・クライアントPCはDHCPによりIPアドレスを取得

●設定概要

IEEE802.1X認証(EAP)

・IEEE802.1X認証の検証ではWindows Server 2003のActive Directoryおよび証明書サービスとCisco Secure ACSを連携して試験を実施

・EAP-PEAPはPEAP MS-CHAPv2を使用
(ユーザーID、パスワード手入力)

・EAP-TLSにはユーザーの証明書を使用

本資料作成時点では、Cisco Secure ACS (Version4.2)は証明書発行機能がサポートされていないため、証明書ベースのEAP-TLSを使用する場合は、外部CA機関からの証明書発行が必要となります。

Web認証、MAC認証(PAP)

- ・Web認証、MAC認証にはユーザーDBとしてCisco Secure ACSのInternal DBを使用
- ・Web認証のブラウザにはInternet Explorerを使用
- ・プライベートCAにてCA証明書、サーバ証明書を発行
- ・認証前アクセスリストにより認証前に一部プロトコル(DHCP、DNS)を通信許可
- ・URLリダイレクト使用

3. 相互接続結果

● 認証機能相互接続結果

AXシリーズがサポートするネットワーク認証機能(以下の表を参照)とCisco Secure ACSにて相互接続が可能であることを確認しました。

認証方式	認証モード	認証プロトコル	AX1240S	AX2430S	備考
IEEE802.1X認証	固定VLANモード	EAP-PEAP	○	○	ユーザーDBにActive Directoryを使用。
		EAP-TLS	○	○	
	ダイナミックVLANモード	EAP-PEAP	○	○	ユーザーDBにActive Directoryを使用。
		EAP-TLS	○	○	
	RADIUS-Accounting	-	—	○	AX1240S(v2.2以降)にてRADIUS-Accounting機能サポート予定
Web認証	固定VLANモード	PAP	○	○	
	ダイナミックVLANモード	PAP	○	○	
	RADIUS-Accounting	-	—	○	AX1240S(v2.2以降)にてRADIUS-Accounting機能サポート予定
MAC認証	固定VLANモード	PAP	○	○	
	ダイナミックVLANモード	PAP	○	○	
	RADIUS-Accounting	-	—	○	AX1240S(v2.2以降)にてRADIUS-Accounting機能サポート予定
マルチステップ認証 (MAC認証+Web認証)	固定VLANモード	PAP+PAP (MAC+WEB)	○	—	
	ダイナミックVLANモード	PAP+PAP (MAC+WEB)	○	—	
マルチステップ認証 (MAC認証+802.1X認証)	固定VLANモード	PAP+EAP(PEAP) (MAC+1X)	○	—	PAP+EAP(TLS)でも確認
	ダイナミックVLANモード	PAP+EAP(PEAP) (MAC+1X)	○	—	

凡例(○:連携可能 —:AXシリーズ未サポート機能)