データシート

ARUBA CLEARPASS POLICY MANAGER™

最新鋭の統合認証基盤システム

Aruba ClearPass Policy Manager™プラットフォームでは、マルチベンダーの有線、無線、VPNインフラストラクチャを問わず、従業員、契約社員、ゲストのネットワーク・アクセスをロール・ベースとデバイス・ベースでコントロールできます。

コンテキスト・ベースのポリシー・エンジン、RADIUS、TACACS+プロトコルのサポート、デバイス・プロファイリング、総合的なポスチャ・アセスメント、オンボーディング、ゲスト・アクセス・オプションを標準装備するClearPassは、組織のネットワーク・セキュリティ基盤として他の追随を許しません。

ClearPass Exchangeでは、ファイアウォール、EMM、その他の既存ソリューションを利用してセキュリティの範囲を広げるために、サードパーティ製のセキュリティおよびITシステムと連携して脅威からの保護とワークフローを自動化できます。IT部門の手を煩わせることはもうありません。

さらに、ClearPassは、エンド・ユーザーの利便性のためにセキュアなセルフサービス機能をサポートします。ユーザーは、自分のデバイスを企業での使用やインターネット・アクセスのために安全に設定できます。Arubaのワイヤレス製品をご利用のお客様は、AirPlay、AirPrint、DLNA、UPnPのそれぞれに対応したデバイスを登録して共有できます。

これにより、従来のAAAソリューションをはるかに上回る総合的で拡張性の高いポリシー管理プラットフォームが実現し、企業支給のデバイスと個人所有のデバイス(BYOD)のセキュリティ要件を満たす広範なポリシー適用機能が提供されます。

主な特長

- Wi-Fi、有線、VPNのマルチベンダー・ネットワークにロールベースのネットワーク・アクセス権を適用。
- 業界をリードするパフォーマンス、拡張性、高可用性、負荷分散。
- 直感的なポリシー設定テンプレートと可視性に優れたトラブルシューティング・ツール。
- 1つのサービス内で複数の認証/承認ソース(AD、LDAP、SQLデータベース)をサポート。
- 標準装備のBYOD向け認証局(CA)によるセルフサービスのデバイス・オンボーディング。
- 詳細なカスタマイズ機能、ブランディング機能、保証人型承認機能によるゲスト・アクセス。
- モバイル・デバイス・アセスメントのためにNAC、Microsoft NAP、EMM/MDMとの連携に対応。
- SIEM、インターネット・セキュリティ、EMM/MDMなどのサードパーティ製システムとの包括的な連携。
- シングルサインオン(SSO)とSAML v2.0によるAruba自動サインオンをサポート。
- すべての有効ユーザー認証と障害に関する高度なレポート機能。
- DHCPおよびTCPフィンガープリントを利用したプロファイリングを標準装備。
- ESXiおよびHyper-Vのハードウェア・アプライアンスと仮想アプライアンスをサポート。

CLEARPASSの違い

ClearPass Policy Managerは、エンタープライズ・グレードのモビリティとNACのあらゆる側面に一元的に対応する業界唯一のポリシー・ソリューションです。ネットワーク・アクセスは、ユーザーのロール、デバイスのタイプとロール、認証方式、EMM/MDM属性、デバイスの正常性、場所、時間帯に基づいて詳細に適用されます。

卓越した相互運用性を提供するClearPassは、マルチベンダーの無線、有線、VPNインフラストラクチャを広範にサポートするため、IT部門は、どのような環境にもセキュアなモビリティ・ポリシーを簡単にロールアウトできます。

設置の拡張性に優れているため、旧式のAAAソリューションの性能をはるかに上回る数万台のデバイスと認証がサポートされます。組織の規模や環境のタイプ(ローカル、分散)に合わせて、各種オプションが用意されています。

驚くべきシンプルさ

ポリシーは一元的に定義、適用されるため、AAAとポリシー管理のために複数のシステムは必要ありません。これは、企業の全体的なセキュリティ・アーキテクチャの強化にも貢献します。標準装備されている機能を利用することで、IT部門は変化し続けるネットワーク・アクセスの課題に迅速に適合できます。

ClearPassは、優れたセキュリティおよびトラブルシューティング・ツールでもあり、高い可視性によってネットワークの問題と、ポリシーやセキュリティの脆弱性を迅速に特定できます。

高度なポリシー管理

従業員のアクセス

ClearPass Policy Managerでは、802.1X、非802.1X、Webポータルのアクセス方式に基づいた、ユーザーとデバイスのロール・ベースの認証を利用できます。また、さまざまな用途に対応できるように、複数の認証方式を同時に使用できます。

詳細なコントロールを行うために、Microsoft Active Directory、LDAP準拠ディレクトリ、ODBC準拠SQLデータベース、トークン・サーバー、内部データベースなど、複数のドメインにある複数のIDストアの属性を1つのポリシーの中で使用できます。

強化されたデバイス・プロファイリング

標準装備のプロファイリング・サービスは、デバイスのタイプやアクセス方式(有線、無線、VPN)に関係なく、すべてのエンドポイントを検出、分類します。DHCPやTCPなどのフィンガープリント方式を使用してスマートフォン、タブレット、IPカメラなどからコンテキスト・データを取得し、ポリシーを定義できます。

デバイス・プロファイルの変化は、認証権限の動的な変更に使用されます。たとえば、WindowsのノートPCがプリンタとして表示される場合、ClearPassポリシーは自動的にアクセスを失効または拒否できます。

管理対象外エンドポイントのアクセス処理

プリンタ、IPフォン、その他のInternet of Things (IoT)など、管理対象外の非802.1Xデバイスをネットワーク接続時に既知のデバイスまたは未知のデバイスとして識別できます。ネットワーク・アクセス権限と承認は、MAC認証とプロファイリングによって検証されます。

個人用デバイスのセキュアな設定

*ClearPass Onboard*は、ユーザー主導型のセルフガイド・ポータルを通じてWindows、Mac OS X、iOS、Android、Chromebook、Ubuntuデバイスのプロビジョニングを自動化します。承認されたデバイスでは、必要なSSID、802.1X設定、セキュリティ証明書が自動的に設定されます。

カスタマイズ可能なビジター管理

*ClearPass Guest*によってワークフロー・プロセスが簡略化されることで、受付担当者や一般従業員などのIT部門以外のスタッフでも、Wi-Fiや有線でのセキュアなインターネット・アクセスのための一時的なゲスト・アカウントを作成できます。自己登録、保証人型の登録、資格情報の一括作成により、企業、小売店、教育機関、大規模公共施設に求められるゲスト・アクセスをサポートします。

デバイスの正常性チェック

ClearPass OnGuardは、常駐型・非常駐型のOnGuardエージェントまたはMicrosoft NAPを利用して、無線、有線、VPN接続上で高度なエンドポイント・ポスチャ・アセスメントを実行します。OnGuardの正常性チェック機能は、デバイスの接続前にコンプライアンスとネットワークの安全性を確保します。

その他のポリシー管理機能

セキュリティおよびワークフロー・システムとの連携

ClearPass Exchangeの相互運用性には、RESTベースのAPIとsyslogデータ・フローの転送が含まれます。これにより、MDM、SIEM、ファイアウォールPMS、コールセンター、入館システムなどとワークフローを連携させることができます。エンド・ツー・エンドのポリシー適用と可視性のために、コンテキストは各コンポーネント間で共有されます。

接続すれば、業務用アプリの準備はOK

ClearPassの自動サインオン機能を使用すると、モバイル・デバイスでの業務用アプリのアクセスが飛躍的に簡単になります。ネットワーク認証が有効であれば、ユーザーは自動的に業務用モバイル・アプリに接続され、すぐに仕事に着手できます。

SAML 2.0ベースのアプリケーションでのユーザー体験を改善するために、Ping、Okta、その他のID管理ツールでシングルサインオン(SSO)がサポートされます。

仕様

ClearPass Policy Managerアプライアンス

ClearPass Policy Managerには、500、5,000、25,000台のデバイスの認証に対応したハードウェア・アプライアンスと仮想アプライアンスがあります。仮想アプライアンスは、VMware ESX/iとMicrosoft Hyper-Vでサポートされます。

- ESX 4.0、ESXi 4.1～5.5
- Hyper-V 2012 R2およびWindows 2012 R2 Enterprise

拡張と冗長構成は、ハードウェア・アプライアンスだけでなく、仮想アプライアンスをアクティブ/アクティブ・クラスタに設置することによっても実現できます。

プラットフォーム

- AAAサービス(RADIUS、TACACS+、Kerberos)を標準装備
- Web、802.1X、非802.1X、RADIUSの認証と承認
- 高度なレポート、分析、トラブルシューティング・ツール
- マルチベンダーの機器にリダイレクトする外部キャプティブ・ポータル
- ポリシー・シミュレーションとモニター・モードの対話的ユーティリティ
- 複数デバイスの登録ポータル：ゲスト、Aruba AirGroup、BYOD、管理対象外デバイス
- さまざまなネットワーク・タイプ、IDストア、エンドポイントに対応する導入テンプレート
- CACおよびTLS証明書による管理者/オペレータのアクセス・セキュリティ
- IPsecトンネル

フレームワークとプロトコルのサポート

- RADIUS、RADIUS CoA、TACACS+、Web認証、SAML v2.0
- EAP-FAST (EAP-MSCHAPv2、EAP-GTC、EAP-TLS)
- PEAP (EAP-MSCHAPv2、EAP-GTC、EAP-TLS、EAP-PEAP-Public、EAP-PWD)
- TTLS (EAP-MSCHAPv2、EAP-GTC、EAP-TLS、EAP-MD5、PAP、CHAP)
- EAP-TLS
- PAP、CHAP、MSCHAPv1および2、EAP-MD5
- NAC、Microsoft NAP
- Windowsマシン認証
- MAC認証(非802.1Xデバイス)
- 監査(ポートおよび脆弱性スキャンに基づくルール)
- OCSP (Online Certificate Status Protocol)
- SNMP汎用MIB、SNMPプライベートMIB
- CEF (Common Event Format)、LEEF (Log Event Extended Format)

サポートされるIDストア

- Microsoft Active Directory
- RADIUS
- 任意のLDAP互換ディレクトリ
- 任意のODBC互換SQLサーバー
- トークン・サーバー
- 標準装備のSQLストア、静的ホスト・リスト
- Kerberos

RFC標準

- 2246, 2248, 2548, 2759, 2865, 2866, 2869, 2882, 3079, 3576, 3579, 3580, 3748, 4017, 4137, 4849, 4851, 5216, 528, 7030

インターネット・ドラフト

- PEAP（Protected EAP）バージョン0および1、Microsoft CHAP拡張、EAP-FAST、TACACS+による動的プロビジョニング

情報保証確認

- FIPS 140-2：証明書#1747

プロファイリング方式

- DHCP、TCP、MAC OUI、ClearPass Onboard、SNMP、Ciscoデバイス・センサー

	ClearPass Policy Manager-500	ClearPass Policy Manager-5K	ClearPass Policy Manager-25K
アプライアンス仕様			
CPU	(1) デュアルコアPentium	(1) クアッドコアXeon	(2) シックスコアXeon
メモリ	4 GB	8 GB	64 GB
ハードドライブ・ストレージ	(1) 3.5” SATA (7K RPM) 500 GBハードドライブ	(2) 3.5” SATA (7.2K RPM) 1 TB ハードドライブ、RAID-1コントローラー	(6) 2.5” SAS (10K RPM) 600 GBホットプラグ・ハードドライブ、RAID-10コントローラー
アプライアンス拡張性			
最大デバイス数	500	5,000	25,000
フォーム・ファクター			
寸法(幅x高さx奥行)	16.8” x 1.7” x 14”	17.53” x 1.7” x 16.8”	17.53” x 1.7” x 27.8”
重量（開梱後）	14 Lbs	18 Lbs	最大39 Lbs
電源			
消費電力(最大)	最大260W	最大250W	最大750W
電源	シングル	シングル	ホットスワップ対応デュアル (オプション)
AC入力電圧	100/240 VAC自動選択	100/240 VAC自動選択	100/240 VAC自動選択
AC入力周波数	50/60 Hz自動選択	50/60 Hz自動選択	50/60 Hz自動選択
環境仕様			
動作温度	10º C～35º C	10º C～35º C	10º C～35º C
動作振動	5 Hz～350 Hzで0.26 G、5分間	5 Hz～350 Hzで0.26 G、5分間	5 Hz～350 Hzで0.26 G、5分間
動作衝撃	31 Gの衝撃パルス1回、最大2.6ミリ秒間	31 Gの衝撃パルス1回、最大2.6ミリ秒間	31 Gの衝撃パルス1回、最大2.6ミリ秒間
動作高度	-16 m～3,048 m	-16 m～3,048 m	-16 m～3,048 m

* 仮想アプライアンスのサイジングは、ハードウェア・アプライアンスの仕様と一致させる必要があります

ご注文について

ClearPass Policy Managerを注文するための手順は、次のとおりです。

1. 環境で認証するエンドポイント/デバイスの数を決定します。さらに、1日あたりのゲスト数、企業使用向けに設定するBYODデバイスの総数、正常性チェックが必要なコンピューターの総数などのオプション機能を選択します。
2. 環境内で認証を必要とするデバイスとゲストの総数に対応できるサイズの適切なプラットフォーム(仮想またはハードウェア・アプライアンス)を選択します。

注文情報

パーツ・ナンバー	説明
CP-HW-500 または CP-VA-500	最大 500 台の認証デバイスをサポートする Aruba ClearPass Policy Manager 500 ハードウェア・プラットフォーム
CP-HW-5K または CP-VA-5K	最大 5,000 台の認証デバイスをサポートする Aruba ClearPass Policy Manager 5K ハードウェア・プラットフォーム
CP-HW-25K または CP-VA-25K	最大 25,000 台の認証デバイスをサポートする Aruba ClearPass Policy Manager 25K ハードウェア・プラットフォーム
拡張可能アプリケーション・ソフトウェア *	
ClearPass Onboard：デバイスの設定と証明書の管理	
ClearPass OnGuard：エンドポイント・デバイスの正常性	
ClearPass Guest：ビジター・アクセスの管理	
保証	
ハードウェア	1 年間パーツ / 修理保証 **
ソフトウェア	90 日 **

* 拡張可能アプリケーション・ソフトウェアの導入単位： 100、500、1,000、2,500、5,000、10,000、25,000、50,000、100,000

** サポート契約により延長可能です

■ 開発元
アルバネットワークス株式会社
〒105-0004 東京都港区新橋5-27-1 パークプレイス3F
TEL. 03-6809-1540（代表） FAX. 03-6809-1541

■ お問い合わせ