Allied Telesis

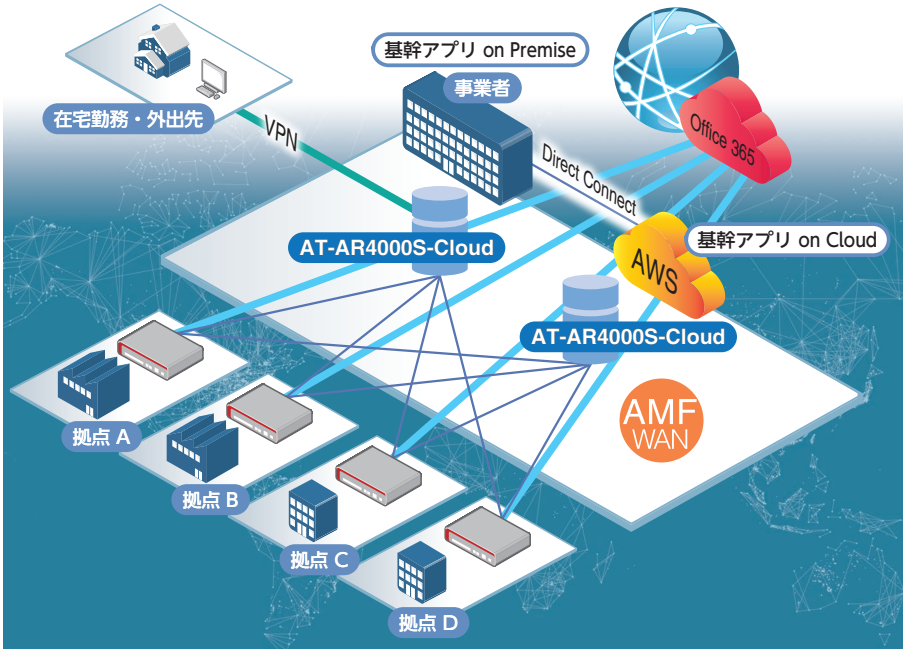
ROUTER Total Networking Solutions

仮想アプライアンスルーター

AT-AR4000S-Cloud

AW Plus　AMF Plus　AMF WAN

Router



AT-AR4000S-Cloudは、AT-AR4050Sと同等のVPN・UTM機能を、仮想化環境やクラウドから提供可能とする仮想アプライアンス製品です。

クラウド、オンプレミスを意識しない業務形態はより進化を遂げています。あわせて、リモートからの業務遂行も止めることはできません。

こうした状況を支えるため、ダイナミックなトラフィックコントロールによるWAN回線の利用効率向上や、管理ポリシーの統一によるセキュリティーの強化を実現できるSD-WANはさらなる普及が進んでいます。

AT-AR4000S-Cloudは、AT-AR4050Sと同様にAMF-WAN（SD-WAN）に対応し、クラウドも含めたSD-WANの導入を強力に推進します。

AT-AR4050Sと同等のVPN・UTM機能をパブリッククラウド上から提供できるため、端末のセキュアなネットワークアクセスを実現するとともに、ローカルネットワークへの設備投資を抑えることができ、導入・運用コストの最適化を可能とします。

特長

●VPN（バーチャル・プライベート・ネットワーク）

IPsec VPN接続を利用した仮想網で、拠点間通信が安全に行えます。IKEv2でよりセキュアなIPsec通信が可能なだけでなく、L2TPv3による柔軟な拠点間通信を実現できます。IPsec通信において最大3000セッションまでサポートし、多拠点ネットワークを構築することが可能です。

●リモートアクセス（OpenVPN、OS標準VPNクライアント）

自宅やホテルなどから社内のPCにアクセスし、リモートでの作業が可能になります。テレワーク/在宅勤務や出張において、オフィスなど一定の場所に縛られずに、いつでもどこでも仕事ができる環境を構築できます。

リモートデスクトップ（RDP）を使って出先から社内にある自分のPCを操作しますので、情報の持ち出しをする必要がなく、万が一PCを紛失しても情報漏洩の心配もありません。

WindowsやiOSに標準搭載しているVPNクライアントソフトに加え、マルチプラットフォームでより高度なセキュリティーに対応したOpenVPNや、AndroidでIPsec IKEv2を用いて接続可能なVPNクライアントソフトstrongSwanと接続検証済みです。

対応バージョンについては弊社ホームページをご参照ください。

2025年2月

特長

●ファイアウォール/UTM

ステートフル・パケット・インスペクション型ファイアウォール（ゾーンベース）やIPSの基本となるセキュリティー機能に加え、レイヤー3ではIPアドレスブラックリスト、レイヤー7ではDPI（ディープパケットインスペクション）やURLフィルターなどに対応。多重構造の強力なセキュリティーで、外部からの脅威や社内からの情報漏洩などを防ぎ、安全なインターネット接続環境を構築できます。UTM機能は以下をご利用いただくことができます。

- ステートフル・パケット・インスペクション型ファイアウォール（ゾーンベース）
  従来のステートフル・パケット・インスペクション型ファイアウォールをゾーンベースに進化させ、ネットワーク環境に合わせた柔軟な設定が可能に。Syn Flood攻撃などの各種攻撃に対する防御のほか、IPv4/IPv6にも対応し、NGNにおいても外部からの脅威から強力にガードすることが可能です。
- IPS（侵入防止）
  プロトコル異常やサービス妨害（DoS）、不正アクセスと思われる異常なイベントなどを検出し、ログ出力や通信を遮断することで、外部からの攻撃を防御することが可能です。
- アプリケーションコントロール（DPI/Sandvine）
  アプリケーションコントロール（DPI＝ディープパケットインスペクション）は、パケットのデータ部分を用いて、どのアプリケーションのトラフィックであるかを判別する機能です。
  200種類以上のアプリケーションを判別可能なデータベースを標準搭載し、さらにSandvine社提供の拡張データベース※1で2000種類以上のアプリケーションの判別が可能になります。
  ビジネスで使用されるさまざまなアプリケーションを特定し、アプリケーションごとに帯域制御やポリシーベースルーティング、インターネットブレークアウト等を行うことで回線帯域を有効利用することができます。また、生産性の低いアプリケーションをフィルターすることで業務効率の向上も図れます。
- Webコントロール（OpenText（Webroot））※2※3
  Webコントロールは、URLを約80種類以上のカテゴリーに分類したデータベースにより、Webブラウザーからのアクセス禁止・許可をコントロールする機能です。クラウド上のビッグデータ分析基盤（AWS/Hadoop/Cassandra）で稼動する機械学習テクノロジーベースの脅威評価エンジンを採用し、リニアにスケールする処理基盤で大量の脅威評価を瞬時に処理することが可能です。人間では処理できない、膨大な量の判定処理を高い精度かつ短い時間で行い、レピュテーションスコアを基に最適な対応（ブロック/アラート等）を取ることができます。
- IPレピュテーション（Emerging Threats）※4※5
  IPレピュテーションは、マルウェア感染ホストやDDoS攻撃元サイトなど、脅威があると判断されたホストのIPアドレスリスト（IPアドレスのブラックリスト）をもとにアクセス制御を行い、外部からの脅威を強力にガードすることが可能です。
- アドバンスドIPS（Emerging Threats）※4※5
  侵入防御（IPS）機能は、サービス妨害（DoS）や不正アクセスと思われる異常なイベントを検出、侵入を防止する機能です。アドバンスドIPSは、IPSの基本機能に加えて、時々刻々と変わる攻撃者の侵入方法に対してさらに幅広く対応、50カテゴリー、6万を超えるパターンを網羅し、より広範な攻撃、侵入に対処することが可能です。

VPNユースケース（VPNコンセントレーター利用）

従業員の働きかた改革を柔軟なコストで実現

我が社は関東一円に広がる支社、工場を持ち、従業員も関東全体に居住している。
Office 365等クラウドアプリケーションの利用は始まっていて、便利に使っている。

1. コロナ禍を通じて、従業員の通勤にかかる時間的負担が特に大きいことが分かってきた。この解決を、在宅ワーク導入で行いたい。
2. とはいえ、在宅ワークのための大型VPN装置を全社員500名分、一斉導入するには負担（費用、運用経験）が不安であり、段階的導入を図りたい。

- **AT-AR4000S-Cloudの出番**
  ライセンスはベース部分と、追加接続部分に分かれて提供されており、追加接続数は10ずつの増強が可能。
  実装するハードウェアも、手持ちのサーバーを利用してスモールスタートが可能。
  運用についても、AT-Vista Manager EXと連携することで、社内構内ネットワークのみならず、WANを含めた網羅的な運用が可能に。

クラウドデプロイユースケース

週末、会社の大会議室を用いてイベントを行うことになった

我が社は映像編集、斬新な動画を作成してエンターテインメント業界に新しい風を起こしている。
今回、動画を豊富に使用したイベントを開催することになった。

1. イベント期間中、来場者へインターネット接続を提供し、自社の提供する動画を楽しんでもらいたい。
2. 来場者数は従業員数の2、3倍を想定。通常設備をそのまま使うと、キャパシティー不足が見込まれる。

- **導入済みAT-AR4000S-Cloudの出番**
  イベント期間中のみ、パブリッククラウドのインスタンスを入れ替え、キャパシティー増強を実施。

  結果：自社設備の入れ替えは行わず、必要な時だけパブリッククラウドの力で性能強化を実現できた。
  バックボーン回線速度の調整も必要だが、結果的に低コストで多くの来場者の満足度を高めることができ、案件をいただくことができた。

特長

※1　Sandvine社提供のデータベースの使用にはUTMライセンス「AT-AR4-UTM-01」が必要です。
※2　UTMライセンス「AT-AR4-UTM-01」が必要です。
※3　Webコントロール機能のURL検索エンジンは、OpenText（Webroot）社のBrightCloudThreat Intelligenceと同じものを使用しています。
※4　UTMライセンス「AT-AR4-UTM-02」が必要です。
※5　Emerging Threats社が提供する33カテゴリーに分類されたIPアドレスブラックリストから、必要なものの選択が可能です。

●GeoIP

特定の国からのアクセス、および特定の国へのアクセスを制御する機能です。これにより、簡易的にセキュリティーを強化することが可能です。

●仮想環境対応/パブリッククラウド

仮想環境との親和性を重視しており、各種ハイパーバイザーや、パブリッククラウド環境での動作をサポート、デプロイを容易にします。

1）仮想化環境

- Microsoft Windows Server Hyper-V
- VirtualBox version6.1※6
- VMware vSphere Hypervisor（ESXi）7.0/8.0※6

2）パブリッククラウド

- さくらインターネット※6
- アマゾン ウェブ サービス（AWS）
- Microsoft Azure
- Oracle Cloud Infrastructure

※6　将来対応予定

●AMF Plusソリューション

ネットワーク上のスイッチやルーターを仮想的な1台の機器として統合管理し、管理運用の「一元化」、「簡素化」、「自律化」によって、管理・運用に関わるコストの削減を実現するネットワーク仮想化機能です。AMF Plusは統合管理を行うAMF Plusマスターと管理されるAMF Plusメンバーからなり、本製品はAMF Plusメンバーに対応しています。

AMF Plusは日々ネットワークの状態を収集分析によって学習し、AT-Vista Manager EXと組み合わせてお使いいただくことで、あらかじめ定義されたポリシーを用いて自動的にネットワークを最適な状態に保ちます。蓄積したデータを数値化することにより、担当者の経験で行われていた業務を平易な作業に落とし込むことができます。

●AlliedWare Plus（AW+）

スイッチ製品「xシリーズ」と共通のOSを採用。機能ごとにモジュール分割されており、単一の障害が与える影響範囲を最小限に抑えることが可能となっています。これにより、旧来の方式の製品と比べシステム全体の可用性が格段に高まります。

●AMF-WAN（SD-WAN）

- インターネットブレークアウト
  回線トラフィックの増大やプロキシーサーバーのセッション数消費問題を解消します。URLオフロードは高速なOffice 365の通信を実現します。また、Webリダイレクト・プロキシーモードでは、Zoomなどを含んだ2000種類以上のアプリケーションをDPIエンジンで自動判別します。
  さらに、ゲートウェイで経路制御するローカルブレークアウトだけでなく、OpenVPN経由で接続するクライアントが直接経路制御を行うターミナルブレークアウトにも対応しています。
- SD-WANロードバランス
  トラフィックを複数WAN回線に負荷分散し、帯域を有効に利用することができます。回線状態を監視し、新たなセッションを結ぶ際に、品質のよい回線を選択してロードバランスをするといった先進的な負荷分散が可能です。IPアドレスやポート番号に加え、アプリケーション単位でロードバランスすることもでき、回線の帯域幅やSLAなどに合わせて柔軟な設定が可能です。
- WANマップ/アプリケーショントラフィックの可視化
  AT-Vista Manager EXを利用することでWANマップを可視化できます。VPNなどの論理回線において、トラフィック状況の可視化やアプリケーション単位の表示が可能です。

●WebベースGUIおよびCLI設定

機器自体の設定や監視・管理をWebブラウザーから簡単に行えます。各種インターネット接続やVPNなどの簡単設定のほか、ダッシュボードでトラフィックやセキュリティーの状態の管理・運用が行えます。操作言語は使用するWebブラウザーの言語設定に応じて日本語/英語の自動切り替えが可能です。
また、業界標準のコマンド体系に準拠したCLIにも対応し、効率よく設定ができます。

●NETCONF/RESTCONF

NETCONF/RESTCONFを使用した機器の、各種情報の取得をサポートしています。

AT-AR4000S-Cloud

製品ラインナップ※1

VPNライセンス（基本ライセンス）※2	
AT-AR4-VPN10S-1Y	Standard用基本ライセンス（10session、1年）
AT-AR4-VPN10S-5Y	Standard用基本ライセンス（10session、5年）
AT-AR4-VPN10S-7Y	Standard用基本ライセンス（10session、7年）
AT-AR4-VPN10S-1Y更新用※3	Standard用基本ライセンス（10session、1年更新用）
AT-AR4-VPN10H-1Y	HighSpeed用基本ライセンス（10session、1年）
AT-AR4-VPN10H-5Y	HighSpeed用基本ライセンス（10session、5年）
AT-AR4-VPN10H-7Y	HighSpeed用基本ライセンス（10session、7年）
AT-AR4-VPN10H-1Y更新用※3	HighSpeed用基本ライセンス（10session、1年更新用）
VPNライセンス（セッション数追加ライセンス）	
AT-AR4-VPN10ADD-1Y	Standard/HighSpeed用追加ライセンス（10session、1年）
AT-AR4-VPN10ADD-5Y	Standard/HighSpeed用追加ライセンス（10session、5年）
AT-AR4-VPN10ADD-7Y	Standard/HighSpeed用追加ライセンス（10session、7年）
AT-AR4-VPN10ADD-1Y更新用※3	Standard/HighSpeed用追加ライセンス（10session、1年更新用）
UTMライセンス（複数ライセンスのバンドルパック）	
AT-AR4-UTM-01：アプリケーションコントロール、Webコントロール	
AT-AR4-UTM-01-1Y-2023	バンドル1年
AT-AR4-UTM-01-5Y-2023	バンドル5年
AT-AR4-UTM-01-1Y-2023更新用※3	バンドル1年更新用
AT-AR4-UTM-02：IPレピュテーション、アドバンスドIPS	
AT-AR4-UTM-02-1Y-2023	バンドル1年
AT-AR4-UTM-02-5Y-2023	バンドル5年
AT-AR4-UTM-02-1Y-2023更新用※3	バンドル1年更新用

※1　1年、5年、7年の利用期限付きライセンスをご購入いただけます。ライセンスのサポートバージョンについてはリリースノートおよびアニュアルライセンスページを参照ください。

※2　物理または仮想インターフェースで利用する最大速度に応じたライセンスをご購入ください。Standard用はNIC速度10Gbps未満、HighSpeed用はNIC速度10Gbps以上となります（チーミング時はその中で最速のインターフェース）。
基本ライセンスの適用により、ルーティング、ファイアウォールを含む本製品の基本機能が利用可能です。VPN接続については10セッションまでが含まれます。

※3　更新専用ライセンスになります。新規購入時の利用可能期間にかかわらず、利用期限付きライセンスを更新する場合は、更新専用ライセンスをご購入ください。

vCPU数に基づくパフォーマンス指標

vCPU数	1※1	2※1	4※1	8※1	12※2
割当メモリー	4GB	8GB	16GB	32GB	32GB
ファイアウォールスループット（UDP）	36,000Mbps	80,000Mbps	100,000Mbps	108,000Mbps	20,000Mbps
IPSecスループット（UDP）	2,000Mbps	4,000Mbps	8,000Mbps	16,000Mbps	8,000Mbps
Next Generation Firewall（UDP）※3	3,000Mbps	7,000Mbps	18,000Mbps	36,000Mbps	18,000Mbps
Advanced Threat Protection（UDP）※4	3,000Mbps	6,000Mbps	12,000Mbps	24,000Mbps	12,000Mbps
ファイアウォールポリシー、ルール数	3,000	5,000	5,000	5,000	5,000
セッション保持数	300,000	1,000,000	1,000,000	1,000,000	1,000,000
ゲートウェイ間VPNトンネル数	1,000	3,000	3,000	3,000	3,000
SSLリモートアクセス（OpenVPN利用）クライアント数	1,000	3,000	3,000	3,000	3,000
Windows & iOS、OS標準VPN（IKEv2）クライアント数	1,000	1,000	1,500	1,500	3,000
Android OS VPN（strongSwan）クライアント数	1,000	1,000	1,500	1,500	3,000

※1　当パフォーマンス指標に使用したサーバーおよびCPUは、Dell EMC PowerEdge R750xsとXeon Gold 6334 Processor 3.60GHzです。Intel Hyper-Threadingで論理分割されたスレッドの うち、AT-AR4000S-Cloudの処理に割り当てたスレッド数（vCPU数）を示します。

※2　当パフォーマンス指標に使用したサーバー CPUは、Intel Core i7-8700K Processor（Coffee Lake）です。Intel Hyper-Threadingで論理分割されたスレッドのうち、AT-AR4000S-Cloudの処理に割り当てたスレッド数（vCPU数）を示します。

※3　アプリケーションコントロールの機能であるDPI Webカテゴライズ機能動作時

※4　アドバンスドIPS機能動作時

仕様

サポート機能	
ルーティング対象プロトコル	IPv4、IPv6
ルーティングプロトコル	RIPv1/v2、RIPng、OSPF、OSPFv3、BGP4、BGP4+、スタティック
マルチキャスト	PIM-SM、IGMPv1/v2/v3※1、IGMPv1/v2/v3プロキシー※1、PIM-SMv6、MLDv1/v2※1
アドレス変換/解決/管理	ダイナミックENAT、スタティックNAT/ENAT、ダブルNAT、サブネットベースNAT、マルチホーミング、NAT46・NAT64、 DNS（リレー、キャッシュ）、PPTP/L2TPパススルー、DNSドメインマッチング
PPP/PPPoE	PPPoEクライアント（マルチセッション、セッションキープアライブ）
ファイアウォール/ セキュリティー	ステートフル・パケット・インスペクション型ファイアウォール（ゾーンベース・IPv4/IPv6）、 アプリケーションコントロール※2、Webコントロール※3、IPレピュテーション※3、アドバンスドIPS※3
VPN（IPsec）	暗号化（ソフトウェア処理）：3DES 暗号化（ハードウェア処理※4）：AES128、AES192、AES256 認証：SHA-1、SHA256、SHA512、AES-GCM IKEv2、IKEv1（メイン/アグレッシブモード）
VPN（IPsec以外）	L2TPv3※5、SSL VPN（OpenVPN）※6、GRE
冗長	Pingポーリング
QoS（クラスベース）	優先制御（PQ/WRR/HTB/LLQ）、帯域制限、輻輳制御（RED）、マーキング（ToS/DSCP/トラフィッククラス）
	分類条件：ToS/DSCP/IPアドレス/IPv6アドレス/TCP、UDPポート番号/出力インターフェース
トンネリング	IPv4 over IPv4、IPv4 over IPv6、IPv6 over IPv6、IPv6 over IPv4
アドレス管理	DHCP（サーバー、クライアント、リレー）、DHCPv6（サーバー、クライアント、リレー）、DHCPv6-PD（サーバー、クライアント）、 ダイナミックDNS※7
その他	AMF Plusメンバー機能、ローカルRADIUSサーバー、RADIUSクライアント、 TACACS+（Accounting/Authentication/Logging）、ブリッジング、Webリダイレクト、IPルートフィルター、 ポリシーベースルーティング、ARP、プロキシー ARP、ローカルプロキシー ARP、ディレクティドブロードキャスト転送制御、 UDPブロードキャストヘルパー、トラフィックシェーピング、SD-WANロードバランス、SD-WANリンクアグリゲーション
管理機能※8	Webベース GUI、SMTP認証、ログ、スクリプト、トリガー、NTP、Secure Shell、NETCONF/RESTCONF、 TFTP/Zmodem/HTTPによるソフトウェア/設定ファイルダウンロード
パッケージ内容	
VPNライセンス（基本ライセンス）	ソフトウェア使用権許諾契約書、ライセンス証書、アニュアルライセンスの発行について、最初にお読みください、CD（ソフトウェア）
VPNライセンス（追加ライセンス）	ソフトウェア使用権許諾契約書、ライセンス証書、アニュアルライセンスの発行について
UTMライセンス	ソフトウェア使用権許諾契約書、ライセンス証書、アニュアルライセンスの発行について、CD（ソフトウェア）

※1　Ethernetインターフェースでのみ使用可能です。

※2　基本ライセンスで製品内蔵データベース利用が可能

※3　UTMライセンスが必要です。

※4　ホストCPUがAES-NIをサポートする場合、自動で有効化されます。

※5　L2TPv3は弊社AW+製品および一部のクラウドサービスとの接続のみをサポートします。

※6　OpenVPNでは、一般的なユーザー名・パスワード認証に加え、ワンタイムパスワード（TOTP/HOTPまたは電子メール）を併用した2要素認証やAES-GCMにも対応しています。また、これらとクライアント証明書による認証も併用可能です。

※7　接続検証済みダイナミックDNSサービスについては、弊社ホームページをご参照ください。

※8　トラップ情報は、弊社ホームページにてご確認ください。

安全のために
ご使用の際は製品に添付されたマニュアルをお読みになり正しくご使用ください。

ネットワーク構築などのご質問やご相談は
0120-860442 テレマーケティング（月～金/9:00～17:30）

製品のくわしい情報は（特長、仕様、構成図、マニュアル等）
ホームページ
http://www.allied-telesis.co.jp/

販売店

アライドテレシス株式会社
〒141-0031 東京都品川区西五反田7-21-11 第2TOCビル
最寄りの営業所の連絡先は下記にてご確認ください
弊社ホームページ≫会社案内≫事業所一覧