AhnLab
NETWORK PLUS

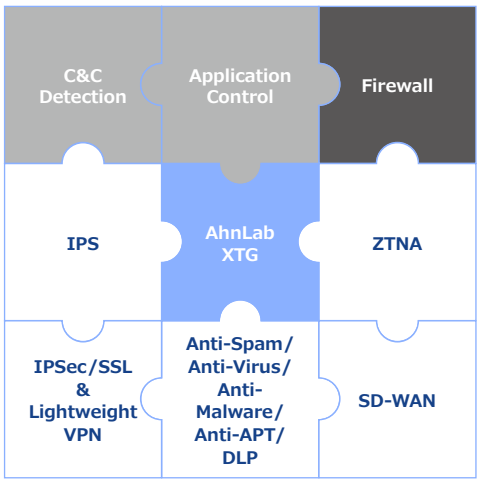
AhnLab XTG

次世代ファイアウォールを超える セキュリティ

AhnLab XTG は、「ファイアウォール / VPN をベースにした高性能ネットワークセキュリティ」と「最新のセキュリティ機能」を兼ね備えた次世代ネットワークセキュリティソリューションです。

製品紹介

AhnLab XTG は、AI ベースの次世代ネットワークセキュリティソリューションであり、複雑化するネットワーク環境と高度化するサイバー脅威に効果的に対応できる統合セキュリティ体制を提供します。また、ZTNA (Zero Trust Network Access)、Light-weight VPN、SD-WAN、ポリシーベースの制御、IPS (Intrusion Prevention System)、アプリケーション制御、URL 制御、C2 の検知・遮断、アンチスパム、DDoS 緩和、DLP (Data Loss Prevention) などの拡張されたネットワークセキュリティ機能を提供し、より安全なビジネス環境を実現します。



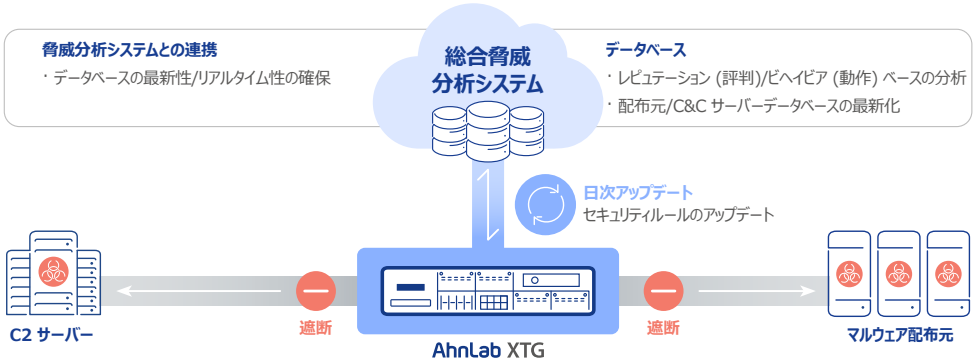
- **差別化された次世代ネットワークセキュリティプラットフォーム**
  - ZTNA ベースのゼロトラスト構築
  - インテリジェントなトラフィック経路の最適化
  - ユーザーおよびデバイスベースのポリシー設定・制御
  - 暗号化トラフィックの検知
  - グローバル / 国内アプリケーションに対する多層防御機能
- **卓越した脅威検知・遮断技術**
  - AI ベースのリアルタイム脅威検知・遮断
  - セキュリティ脅威の検知に特化した多層マルチエンジン構造
  - 脅威インテリジェンスに基づく差別化された脅威検知
  - 社内の脅威分析組織・インフラを保有
- **大容量ファイアウォール処理性能の保証**
  - 高度化された（Advanced）ハードウェアプラットフォーム
  - 高性能マルチコア分散技術
- **長年のノウハウが蓄積されたユーザーインターフェース**
  - ポリシー設定・管理およびシームレスなフロー（Seamless Flow）の提供
  - ドラッグ＆ドロップ方式による柔軟なインターフェースの提供

大容量トラフィック処理に優れた **高性能ファイアウォール**	最新ユースケースに基づく **差別化された次世代セキュリティ**
市場ニーズを反映した **ユーザーインターフェース**	卓越した **脅威検知・対応能力**

次世代ファイアウォール機能

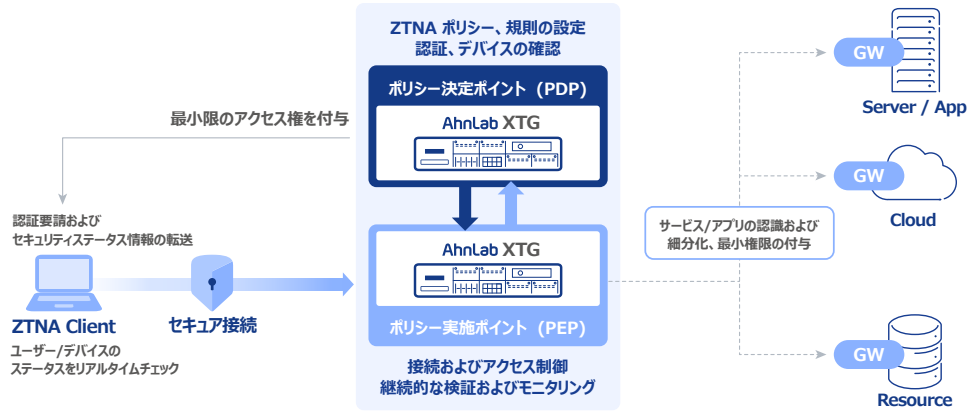
次世代ファイアウォール

インバウンドおよびアウトバウンドトラフィックをユーザー、デバイス、IP アドレス、URL などさまざまな属性に応じて許可または遮断します。
セキュリティの観点から、危険度の高い IP アドレスや Web サイトをリアルタイムで遮断し、内部の重要資産に対する外部からのアクセスを制御することで、ランサムウェアなどのマルウェア感染を防止します。
独自保有する脅威分析システムと C2 ブラックリストデータベースを基に C2 サーバーへのアクセスを検知・遮断し、サイバー脅威からビジネス環境を保護します。



ZTNA アクセス制御

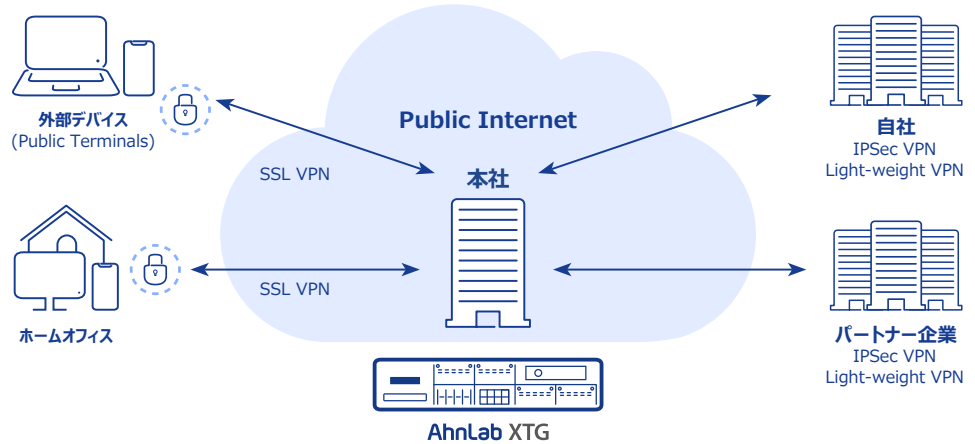
AhnLab XTG ZTNA はネットワークの内部・外部を問わず、すべてのユーザーの身元とデバイスを徹底的に検証し、最小権限の原則を保証します。



外部ユーザーに対するアクセス制御
支社/支店ユーザーに対するアクセス制御
内部ネットワークにおけるアクセス制御
Web を介する接続に対するアクセス制御

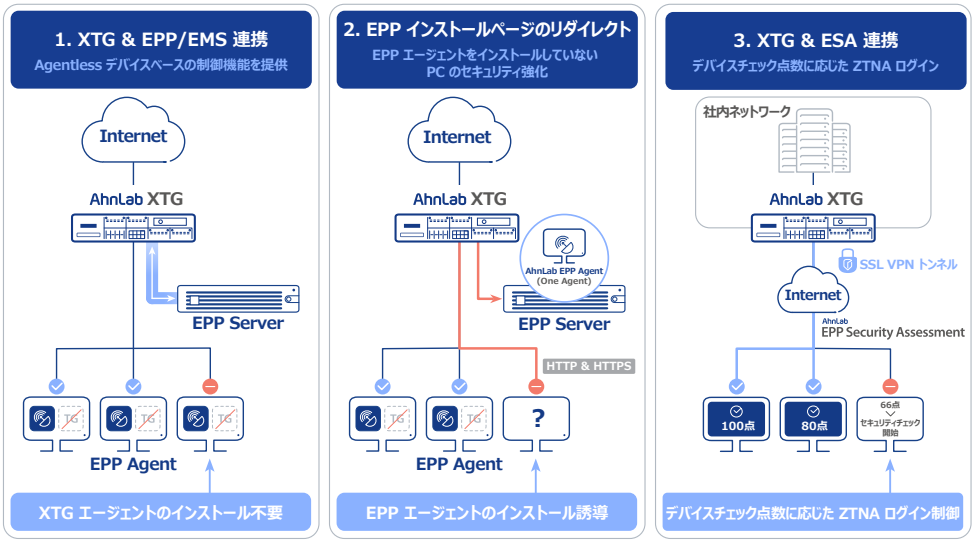
VPN – リモートアクセス

IPSec VPN、SSL VPN、Light-weight VPN に同時対応し、リモートアクセスや本社-支社間のアクセスセキュリティを強化します。さらに、Windows、Mac、Linux、Android、iOS など多様な OS に対応し、モバイル専用 SSL VPN にも対応します。加えて、HA やマルチライン・ロードバランシングなどの技術を活用することで、VPN の安定性と可用性を最大化します。



EPP との連携

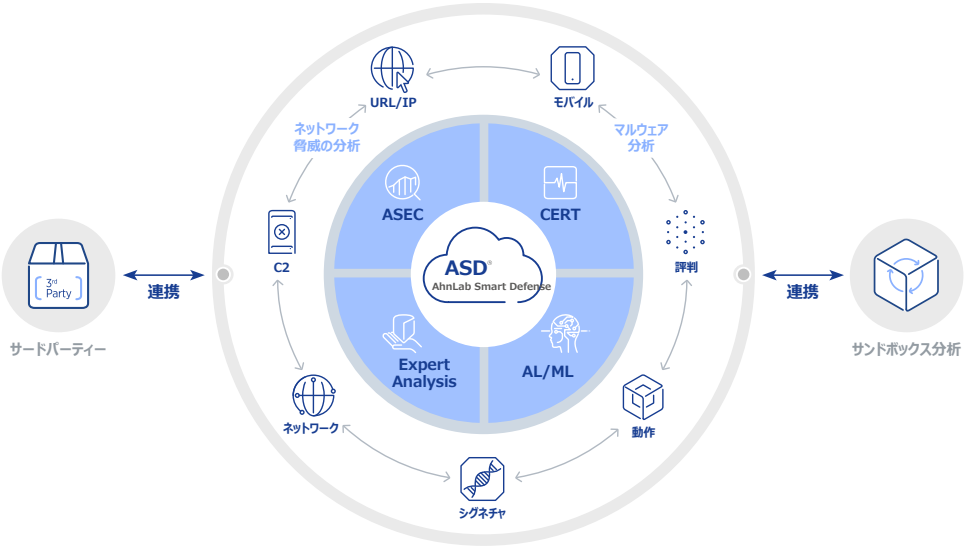
AhnLab XTG と AhnLab EPP を連携させ、安全なデバイスのみが ZTNA に接続できるようにします。EPP との連携により、XTG エージェントをインストールせずにデバイスベースの制御を実現できます。さらに、XTG を通じて EPP エージェントのインストールを誘導し（HTTP/HTTPS）、ESA のデバイスチェック点数を基盤として XTG の ZTNA とログインを制御します。



アンラボのセキュリティインフラ

アンラボの技術力とノウハウが蓄積された AhnLab XTG

アンラボの製品およびサービスの根幹には、数十年間にわたり蓄積された技術力とノウハウが反映されたクラウドベースのエンジン「AhnLab Smart Defense (ASD)」があります。ASD エンジンは、URL/IP、C2、モバイル、ネットワーク、動作、シグネチャ、評判情報に対する分析技術を複合的に適用し、新種の脅威を多次元的に検知・対応します。AhnLab XTG は、このようなアンラボの基盤技術とインフラを活用し、最新のシグネチャ、脆弱性、評判情報、C2 情報を適用することで、顧客を最新のネットワーク脅威から保護します。



製品とサービスの根幹を成す技術力

アンラボは、脅威分析と侵害対応を通じて30年以上にわたり蓄積した膨大なセキュリティデータに基づき、AI セキュリティプラットフォーム「AhnLab AI PLUS」を運営しています。独自のセキュリティデータを学習したアンラボの AI は、脅威の検知と対応能力を高度化し、セキュリティ運用の生産性革新を支援します。

詳細機能

カテゴリ	機能	説明
ネットワーク	インターフェース	· Bridge/Aggregation/VLAN/VXLAN/VRF 対応
	運用モード	· Router/Bridge モードに対応
	ルーティングプロトコル	· Static/Dynamic/Multicasting プロトコルおよびルーティングシミュレーターに対応
	DHCP	· Client/Server/Relay 対応
	SD-WAN	· アプリケーション/サービスパスの最適化、ネットワーク品質モニタリング、ロードバランシングに対応
次世代ファイアウォール	High Availability(HA)	· Active-Standby、Active-Active 対応
	同期	· 管理者設定、ログ設定、ポリシーの同期
	動的情報の同期	· ユーザーおよび FQDN IP アドレス収集情報を別の XTG と同期
	オブジェクト	· クラウド連携機能に対応 · 国ベースのファイアウォールポリシー策定に対応
	QoS	· ポリシー別最小帯域幅の保証および最大帯域幅の制限設定
	アクセス遮断 (Blacklist)	· IPv4/IPv6遮断管理 · L3/L4プロトコル異常スキャン · アクセス遮断ファイル内の IP アドレス重複スキャンツールに対応
	ポリシー除外 (Whitelist)	· IPv4/IPv6除外ポリシーの管理
	重複オブジェクトスキャン	· 重複オブジェクトおよび参照オブジェクトスキャン · 選択したポリシーごとの重複の有無スキャン
	ポリシースキャン	· 重複ポリシーのフィルタリングおよび仮想パケットポリシーの有効性スキャン
	NAT	· Static/Dynamic/Policy based NAT などに対応
	ユーザー認証	· サードパーティ標準認証サーバーとの連携認証 (RADIUS/LDAP/AD/TACACS+/MS-SQL など)
	ポリシーの設定および制御	· IP/MAC、ユーザー、デバイスの設定および制御
	ZTNA	· ユーザーおよびデバイスの識別情報に基づいたアプリケーションおよびリソース別アクセス制御 · Agent および Agentless ZTNA 対応
	仮想パケットの検索	· 仮想パケットを通じた NFGW ポリシーの全体パケット処理シミュレーターに対応
IPSec VPN	構成	· Hub & Spoke、Mesh
	DA (Dynamic Access)	· Hub & Spoke 構成において、Hub 設定の変更なしに Hub-Spoke 間 IPSec VPN トンネルを作成 · Spoke 間通信時に動的にトンネルを生成
	アルゴリズム	· 多様な暗号化アルゴリズムに対応 (AES/SEED/ARIA/LEA/HIGHT など)
	HA	· 本社 VPN の冗長化 (Active-Standby、Active-Active) に対応
	ロードバランシング	· 多様なインターネットマルチ回線のロードバランシング機能に対応
	障害復旧	· DPD スキャンおよび DR 接続に対応
SSL VPN	サポート環境	· Windows、Mac、Linux、Android、iOS など
	ユーザー認証	· サードパーティ標準認証サーバーとの連携認証 (RADIUS/LDAP/AD/DBMS/OTP/FIDO/SMS など)
	アルゴリズム	· 多様な暗号化アルゴリズムに対応 (AES/SEED/ARIA/LEA/HIGHT など)
	エンドポイント連携セキュリティ	· エンドポイントセキュリティ連携 – 接続 PC の事前/事後セキュリティ
	HA	· Active-Standby、Active-Active 構成に対応
	対応デバイス	· モバイルデバイス (スマートフォン/タブレット) およびエンベデッドデバイス (ルーター)
Light-weight VPN	HA	· 本社 VPN の冗長化 (Active-Standby、Active-Active) に対応
	構成	· Gateway-to-Gateway
	デバイス遮断リスト	· 中央デバイスで特定拠点のデバイス遮断リストに対応

カテゴリ	機能	説明
仮想システム	対応方式	· MAC VLAN 方式による最大論理仮想化
	HA	· 仮想システム HA 対応
	通信	· Veth インターフェースを通じた仮想システム間通信
	管理	· 仮想システムを通じたプライベートクラウド、SDN、NFV 管理
IPS	シグネチャ	· 約10,000個以上のシグネチャに対応
	シグネチャのアップデート	· 定期的なシグネチャパターンの自動アップデート
	検知/遮断	· シグネチャ/Anomaly/脆弱性/マルウェアベースの検知・遮断
	シグネチャ管理	· ユーザー定義パターン/Snort Rule (PCRE パターン) の管理
DDoS 防御	攻撃の遮断	· UDP/ICMP/TCP Flooding、Spoofed TCP 攻撃、HTTP 脆弱性攻撃の遮断
アプリケーション制御	対応アプリケーション	· 約3,000個のアプリケーションおよびユーザー定義アプリケーションに対する脅威検知・遮断
	制御	· アプリケーションユーザーの接続とログイン、詳細機能の制御、未知のアプリケーション制御
C2 検知・遮断	検知	· クラウドベースの C2 サーバー接続、未知の悪性ファイル、PUP 内部流入の検知
	遮断	· 独自保有ブラックリストデータベースに基づいた C&C サーバー接続の遮断
アンチマルウェア	エンジン	· 独自のエンジン
	検知/遮断	· Stream-based アンチマルウェアエンジンをベースにマルウェアを検知・遮断
	シグネチャのアップデート	· 最新シグネチャへの対応のため、1日に2回シグネチャをアップデート
	マルウェアスキャン	· HTTP/SMTP/POP3/FTP などの多様なプロトコルおよび圧縮ファイルに対するマルウェアスキャン
アンチスパム	エンジン	· 国際公認のスパムエンジン
	フィルタリング	· RBL (Real-time Blacklist) およびユーザー定義キーワードベースのフィルタリング
	遮断	· 特定時間内に一定数以上のメールまたは特定のメールアカウントを遮断
DLP	制御	· 内部情報の流出およびファイルタイプ・コンテンツ別の制御
	検知/遮断	· 個人情報とキーワードに対するパターン検知・遮断
脅威検知フィルター	データベース	· 独自のマルウェア配布サイト DB、放送通信審議委員会の有害サイト DB および Global Categorized URL DB に対応
自社製品との連携	連携製品	· V3、EPP、MDS、AIPS、DPX、ASTx、ESA、TMS、AIPS など
その他	SSL Inspection	· 暗号化されたトラフィックスキャン
	モニタリング/ログ	· ログストレージ：内蔵 HDD/ログの保存 · ダッシュボード：ウィジェット方式のダッシュボードおよび相関分析 · コンテンツ：トラフィック統合ログおよびカスタムレポート
	遮断	· GeoIP：特定の国/大陸別の遮断
	管理	· 権限：多段階管理者権限 · 接続：Web ベース HTTPS 接続 · 連携：Open API

製品仕様(Specification)

中小企業向け

カテゴリ	40	50	70	100
認証				
CC 認証	EAL4FW+VPN(韓国国内)			
IPv6 認証	IPv6ReadyLogoPhase-2(Router)			
電波法認証	KC			
物理				
プロセッサ	2Core/1.8Ghz	4Core/1.3Ghz	4Core/2.4Ghz	8Core/2.4Ghz
メモリ	8GB	8GB	8GB	8GB
システムストレージ	eMMC9.6GB	eMMC9.6GB	eMMC9.6GB	M.2SSD512GB
ログストレージ	-	-	-	HDD2TB
フォームファクタ	Desktop	19"RackMount/1U	19"RackMount/1U	19"RackMount/1U
外形寸法 (幅×高さ×奥行き mm)	220x44x194.5	438x44x194	438x44x194	430x44x340
電源 (外部電源)	40WSingle	65WSingle	65WSingle	100WSingle
動作温度	0~40°C			
保管温度	-20~70°C			
インターフェース				
Slot	-	-	-	インターフェース
10/100/1000 Base-T	8	8	8	基本 6 / 最大 10
1G Base-X	-	-	-	基本 4 / 最大 8
Bypass	対応			
システムパフォーマンス				
最大同時セッション数 (CC)	1,000,000	1,500,000	2,000,000	3,500,000
1秒あたりの接続数(CPS)	35,000	50,000	50,000	200,000
ファイアウォールスループット (UDP)	4G	6G	8G	12G
ファイアウォールスループット (UDP 64B)	1G	1.5G	2G	3G
VPN Throughput	1G	1.2G	1.4G	1.9G
VPN トンネル数	2,500	5,000	5,000	20,000
ZTNA 同時接続可能な最大デバイス数	50	100	200	300
SSL VPN 同時接続可能なセッション数	500	1,000	1,000	1,000

中堅企業向け

カテゴリ	300	500	1000
認証			
CC 認証	EAL4 FW+VPN (韓国国内)		
IPv6 認証	IPv6 Ready Logo Phase-2 (Router)		
電波法認証	KC		
物理			
プロセッサ	6 Core/3.7Ghz (1each)	8 Core/3.8Ghz (1each)	12 Core/3.7Ghz (1each)
メモリ	8GB	16GB	16GB
システムストレージ	M.2 SSD 512GB		
ログストレージ	HDD 2TB		
フォームファクタ	19" Rack Mount/1U		
外形寸法 (幅×高さ×奥行き mm)	438x44x525		
電源 (外部電源)	350W Single	350W Redundant	350W Redundant
動作温度	0~40°C		
保管温度	-20~70°C		
インターフェース			
Slot	4	4	4
10/100/1000 Base-T	基本 8 / 最大 32	基本 8 / 最大 32	基本 8 / 最大 32
1G Base-X	基本 8 / 最大 32	基本 8 / 最大 32	基本 8 / 最大 32
10G Base-X	-	基本 0 / 最大 8	基本 0 / 最大 8
40G Base-X	-	-	-
100G Base-X	-	-	-
Bypass	対応		
システムパフォーマンス			
最大同時セッション数 (CC)	5,000,000	8,000,000	10,000,000
1秒あたりの接続数(CPS)	300,000	500,000	600,000
ファイアウォールスループット (UDP)	20G	40G	60G
ファイアウォールスループット (UDP 64B)	6G	8G	8G
VPN Throughput	8G	10G	12G
VPN トンネル数	30,000	40,000	40,000
ZTNA 同時接続可能な最大デバイス数	500	1,000	2,000
SSL VPN 同時接続可能なセッション数	2,000	3,000	4,000

大企業
データセンター向け

カテゴリ	2000	5000	10000	20000
認証				
CC 認証	EAL4FW+VPN(韓国国内)			
IPv6 認証	IPv6ReadyLogoPhase-2(Router)			
電波法認証	KC			
物理				
プロセッサ	8Core/3.2Ghz (1each)	12Core/2.4Ghz (2each)	16Core/2.8Ghz (2each)	32Core/2.8Ghz (2each)
メモリ	32GB	64GB	64GB	256GB
システムストレージ	M.2SSD512GB			
ログストレージ	SSD2TB			
フォームファクタ	19"RackMount/2U			
外形寸法 (幅×高さ×奥行き mm)	438x88x602			
電源 (外部電源)	550WRedundant	550WRedundant	1300WRedundant	1300WRedundant
動作温度	0~40°C			
保管温度	-20~70°C			
インターフェース				
スロット	4	8	8	8
10/100/1000 Base-T	基本 8 / 最大32	基本 8 / 最大 64	基本 8 / 最大 64	基本 8 / 最大 64
1G Base-X	基本 8 / 最大 32	基本 8 / 最大 64	基本 8 / 最大 64	基本 8 / 最大 64
10G Base-X	基本 0 / 最大 12	基本 0 / 最大 32	基本 0 / 最大 32	基本 0 / 最大 32
40G Base-X	-	基本 0 / 最大 8	基本 0 / 最大 12	基本 0 / 最大 16
100G Base-X	-	-	基本 0 / 最大 2	基本 0 / 最大 4
Bypass	対応			
システムパフォーマンス				
最大同時セッション数 (CC)	20,000,000	30,000,000	40,000,000	60,000,000
1秒あたりの接続数(CPS)	850,000	1,000,000	1,300,000	1,500,000
ファイアウォールスループット (UDP)	100G	180G	240G	320G
ファイアウォールスループット (UDP 64B)	10G	25G	35G	60G
VPN Throughput	13G	15G	19G	38G
VPN トンネル数	40,000	50,000	60,000	100,000
ZTNA 同時接続可能な最大デバイス数	2,500	5,000	7,500	10,000
SSL VPN 同時接続可能なセッション数	5,000	10,000	15,000	20,000

〒108-0014 東京都港区芝4丁目13-2 田町フロントビル3階
ホームページ: www.ahnlab.com/jp
TEL: +81 3-6453-8315 FAX: +81 3-6453-8316

AhnLab