CISCO
SECUREざっくりシリーズ

The bridge to possible

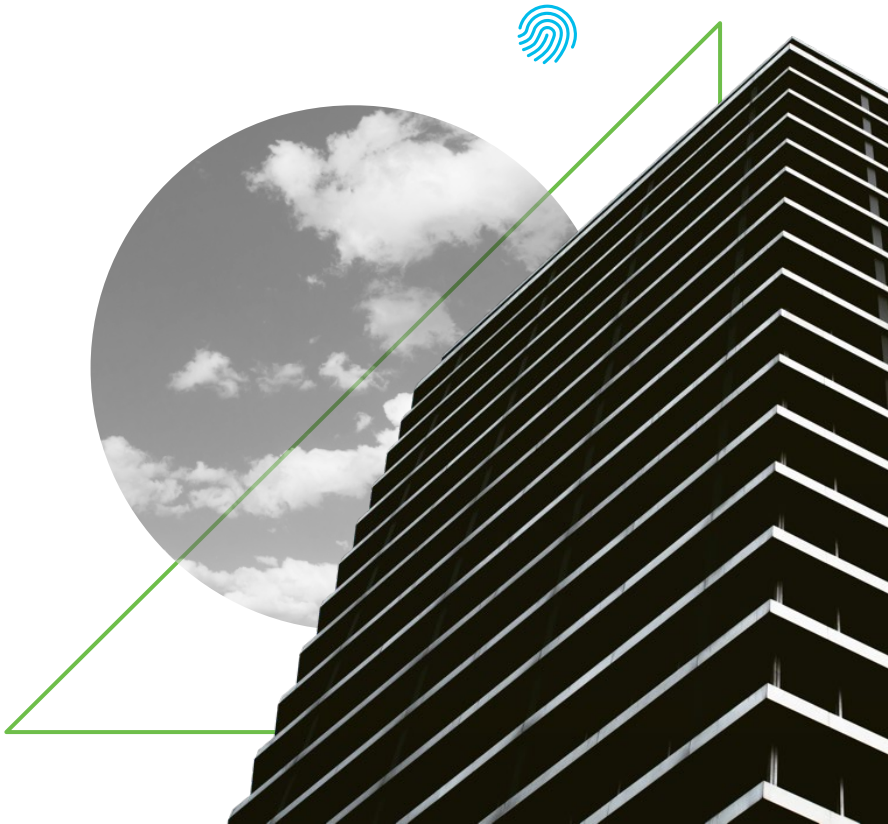
ざっくりAnyConnect (Cisco AnyConnect Secure Mobility Client)

シスコシステムズ合同会社
2022年4月

アジェンダ

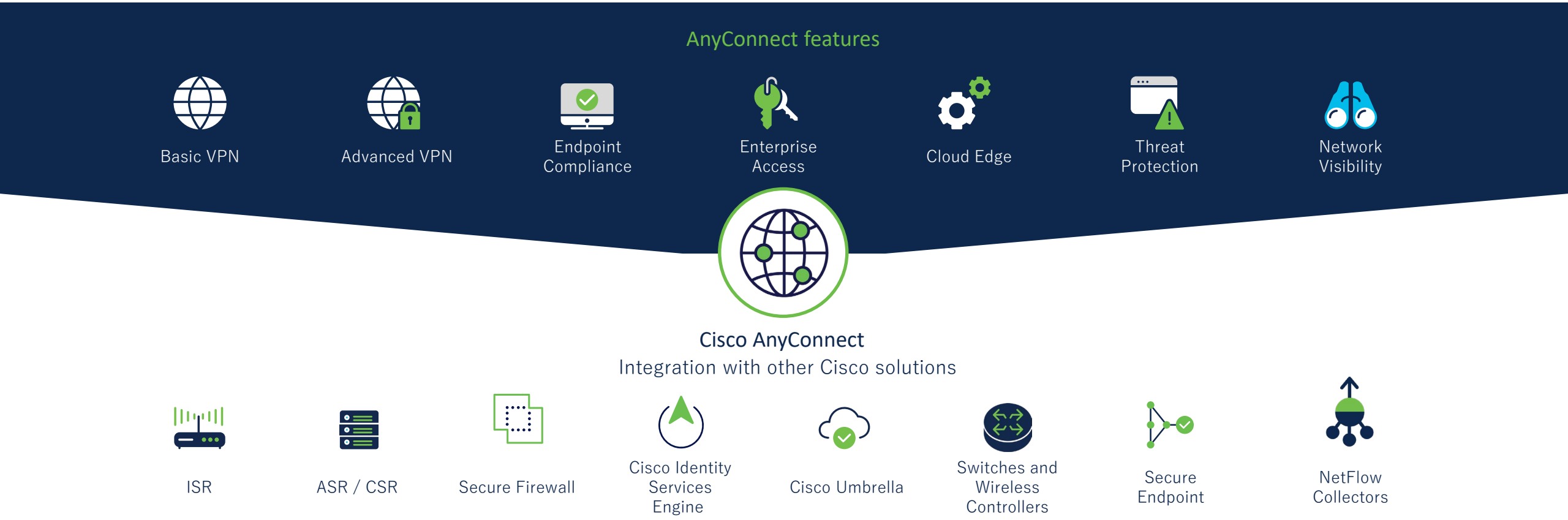
- はじめに
- 前提知識
- AnyConnectが必要になる背景と課題
- ただつなぐだけではないVPNの機能
  - 通信先制御によるローカルブレイクアウト
  - 多様な接続管理
  - 多様な認証オプション
- VPNだけではない、AnyConnectの機能
  - Umbrella Roaming Security Module (RSM)
  - ポスチャモジュール
  - Network Visibility Module (NVM)
  - その他のモジュール
  - 幅広いクライアントOS対応
- 導入シナリオ
- 補足情報

Cisco AnyConnect
Secure Mobility Client



はじめに

様々な機能を有するAnyConnectを幅広いお客様へ紹介いただくための足がかりとして、本資料をご利用いただけますと幸いです。



前提知識

用語	説明
VPN	Virtual Private Network。地点間を「トンネル」と呼ばれる論理的なネットワークを形成して接続し、同一の閉じたネットワーク (Private Network) として扱うための技術。基本的にトンネル内のトラフィックは暗号化し秘匿化される。
RA VPN	Remote Access VPN。VPNの中でも、PCやスマートフォンなどの端末をVPN接続する場合の呼称。
ローカルブレイクアウト	VPN接続された拠点/端末からのトラフィックは、データセンター (DC) などに集約された後にインターネットへ抜ける構成になっていたが、クラウドの発展によりインターネット区間の帯域の逼迫が問題となる。信頼できるクラウドへのトラフィックを、VPNを介さず直接インターネットと通信させるようにすることを指す。
ゼロトラスト	利用者や端末、エリアなどを無条件に信頼せずに、リソースやデータへのアクセスに際して、継続的に認証・認可を行うセキュリティモデル。
MFA	Multi-Factor Authentication。認証時に、IDとパスワード以外に、本人を特定する要素を付加することで、万が一、IDとパスワードが漏洩した際にも、不正アクセスを防止する手法。

AnyConnectが必要となる背景と課題

VPNによる安全な接続

クラウドシフトが進んでいるが、過渡期であり、かつ社内ネットワーク上のリソースがなくなるわけではないため、VPNを用いた安全な接続が必要。

トラフィック可視化

クライアント端末のトラフィックを監視することで、インシデント発生の兆候を検知したり、発生時にトラフィック履歴の監査から被害状況の把握をおこなう。

ローカルブレークアウトの必要性

クラウドサービスの利用増加に伴い、VPNトンネルを経由して社外に抜けるトラフィックにより、インターネット接続回線が逼迫する状態が発生。ローカルブレークアウトによる、トラフィック分散の必要性が増加。

端末のコンプライアンス

社内ネットワークに接続する端末が、セキュリティに対する要件（AntiVirus、Firewall、パッチ適用などの状態）に適合するか否かを確認し、状態によりアクセス制限や修復を行い、コンプライアンス違反の端末によるセキュリティリスクを低減する。

Multi OS対応

現在の企業活動では、様々な種類の端末（Windows [Intel/ARM], Mac, Linux, Apple iOS, Android, Chrome OSなど）が利用されており、それらに対して同一のサービスを提供することが求められる。

強度の高い認証

パスワードなどの認証情報漏えいリスクに対する耐性を高めるため、多要素認証 (MFA) を用いた強度の高い認証が必要とされる。

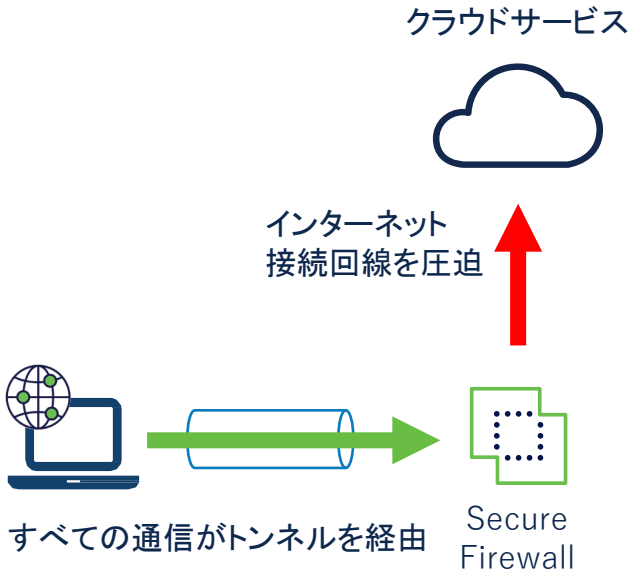
ただつなぐだけではない
VPNの機能

Plus
VPN Only
Apex

通信先制御によるローカルブレイクアウト
トラフィック分散でリソースの最適化

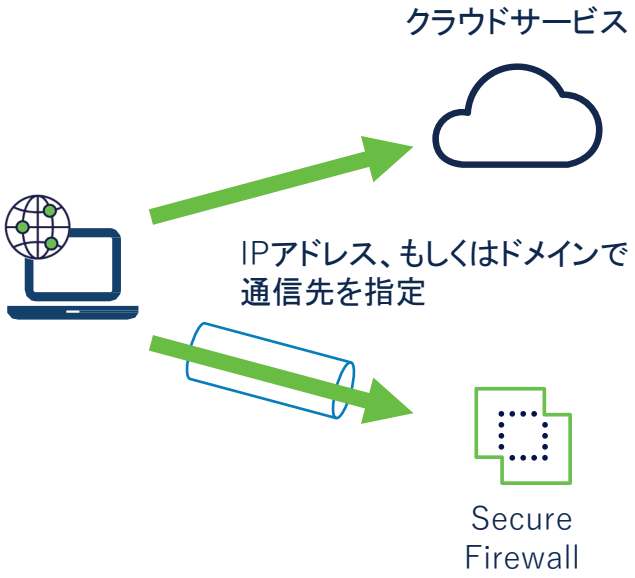
従来の接続手法

Full Tunnel
すべての通信をトンネル経由で行う。
信頼出来るクラウド宛の通信などが増えている昨今の通信環境においては、VPNを収容しているデータセンターなどの拠点の**インターネット接続回線を圧迫**する状況が発生する。

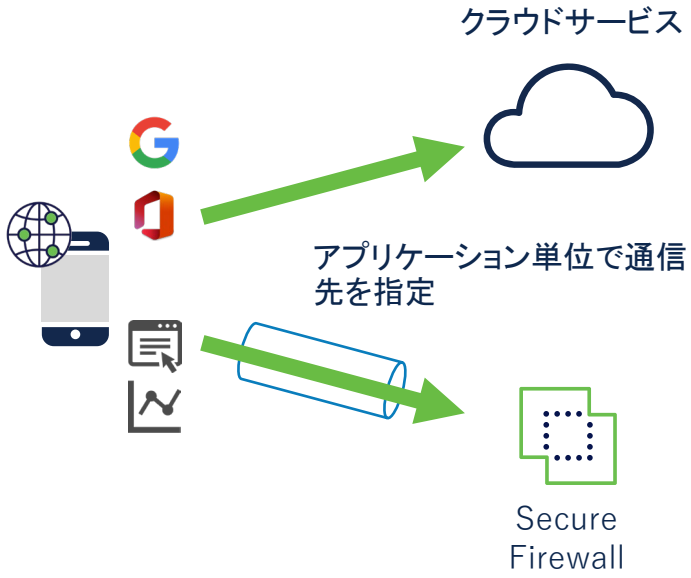


ローカルブレークアウトによるトラフィック分散

Split Tunnel
トンネルを経由する通信先を限定し、信頼できるクラウドサービスを除外したり、社内宛の通信に限定したりすることで、トラフィックの分散を図る。
IPアドレス、もしくはドメインで通信先を指定することができ、ドメイン指定の場合は**Dynamic Split Tunnel**として区別される。



PerApp VPN
アプリケーションを指定し、トラフィックをトンネル向きにするかを決定する。
(Apple iOS/Androidのみ)

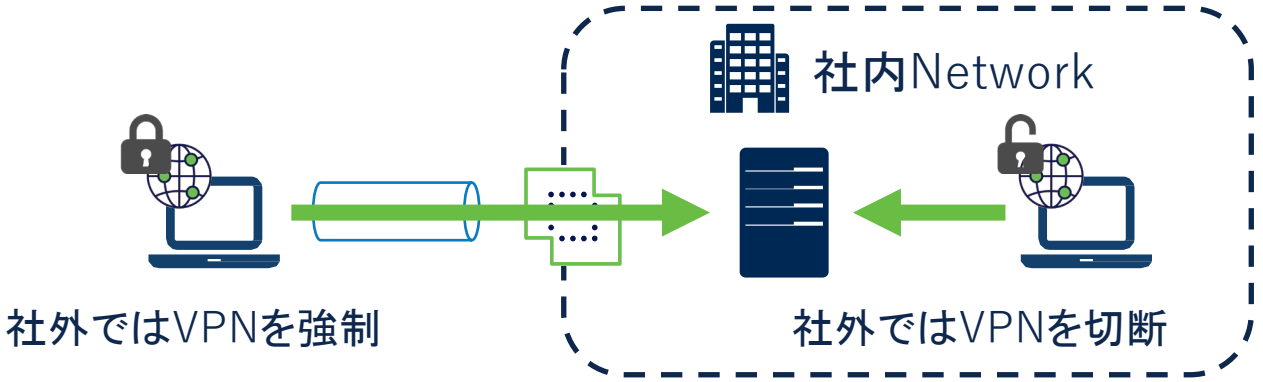


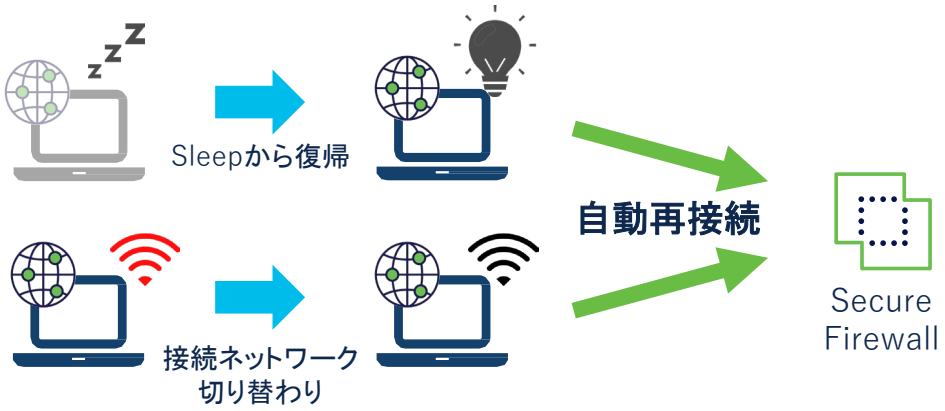
Plus
VPN Only
Apex

多様な接続管理
ユーザエクスペリエンスの向上

Trusted Network Detection (TND) / Always-On

TNDにより、接続しているネットワークの状態（DNSの設定内容）からVPN接続の要否を決定、Always-OnによりVPN接続を強制する。
クライアント端末及びVPNヘッドエンドにおける、リソースの最適化とセキュリティの確保を両立する。



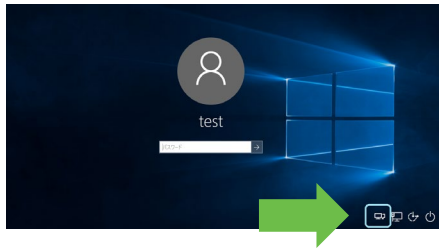


自動再接続

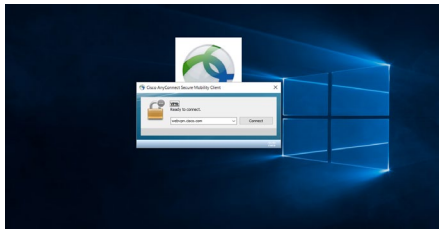
接続状態でSleepになった場合のResume後や、端末が接続するネットワークの切り替わりなどにより再接続が必要になった場合、状態変化前のVPNセッション情報を引き継ぎ、ユーザの操作無しで自動的に再接続する。

Start Before Logon (SBL)

ログオン前にVPN接続を確立させることで、キャッシュログオンが無効な場合でも、社外ネットワークからADドメインに対するログオンを実施することが出来る。
(Windowsのみ対応)



「ネットワークサインイン」ボタンをクリック

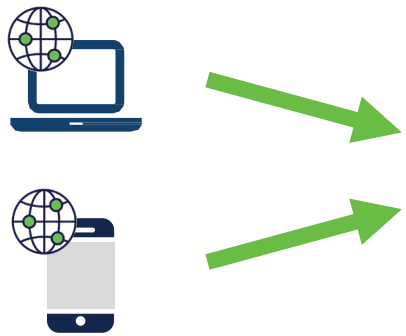


VPN接続を実行

Plus
VPN Only
Apex

多様な認証オプション
強度の高い認証を実現

AnyConnectにおけるAAA（認証/認可/アカウンティング）
AAAは以下の三要素から構成され、認証後のアクセス権の制御（認可）や、アクセス履歴の管理（アカウンティング）などを行うことができる。
- 利用者が誰なのか（Authentication:認証）
- 利用者ができることは何か（Authorization:認可）
- 利用者の行動履歴（Accounting:アカウンティング）



認証ソース
- 証明書（複数証明書利用可）
- RADIUS
- LDAP/Active Directory
- TACACS+
- RSA SecureID（SDI）
- HTTP Form
- Kerberos
- Local DB
- SAML

幅広い認証ソースをサポート。

ゼロトラストによる認証強化
SAML連携で、生体や所有要素を用いるMFA利用することで、さらなるセキュリティの強化を図ることが可能。

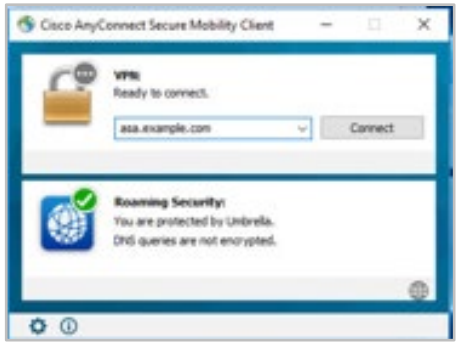
VPNだけではない AnyConnectの機能

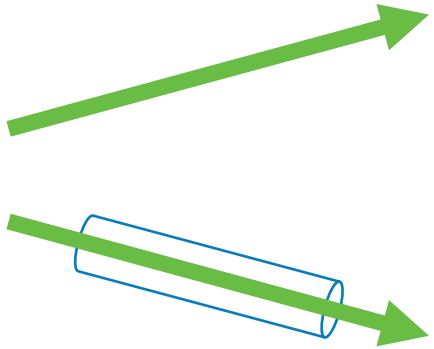
Plus

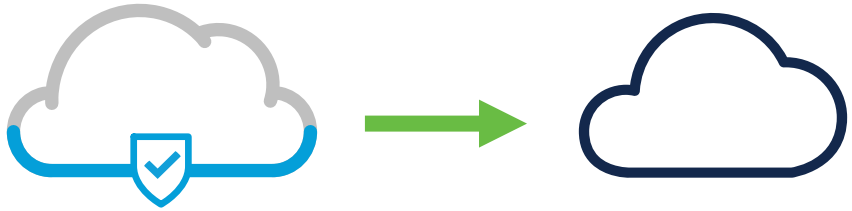
Apex

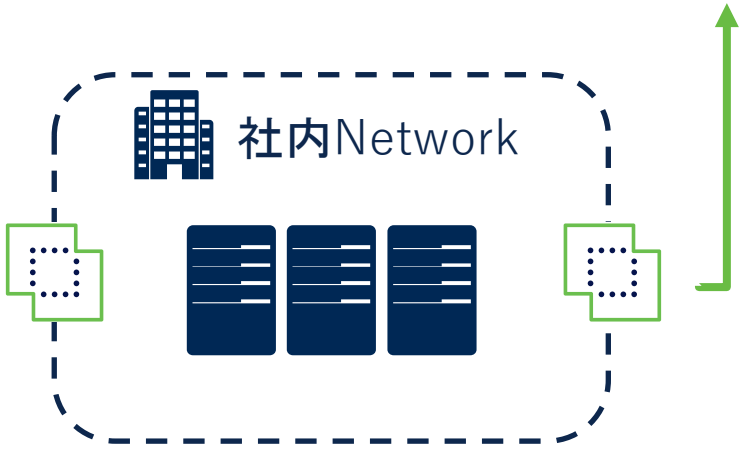
Umbrella Roaming Security Module (RSM)

DNS/Web (TCP/80,443)はUmbrellaで検査し、
セキュリティを確保。
VPNの接続状態に関わらず、これらのトラフィック
を保護対象とすることができる。









社内宛通信および、DNS/Web以外
はVPNトンネル経由で通信。

DNS/Web (TCP/80,443) の通信はローカルブレークアウトされ、
Umbrellaで処理されるため、社内Networkからインターネットに
接続される経路の帯域消費は削減される。

ポスチャモジュール

ポスチャとは？

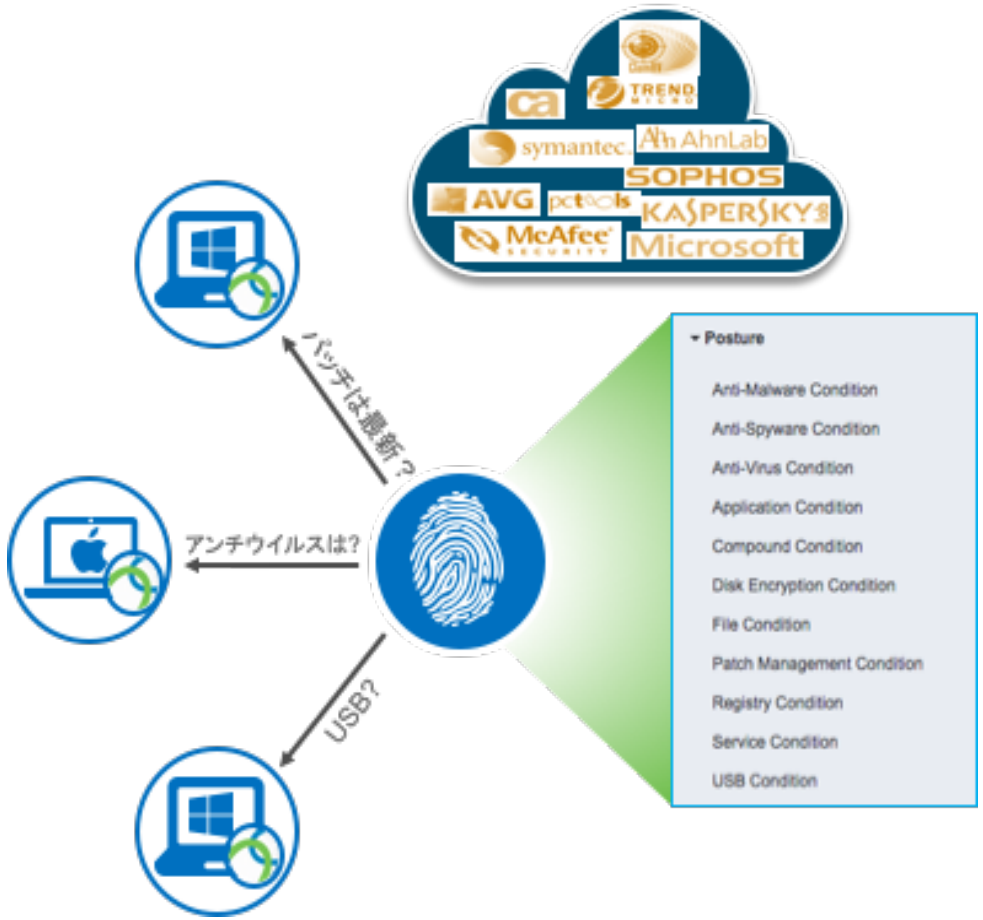
ネットワークに接続するエンドポイントのセキュリティポリシーに対するコンプライアンスに関するステートのこと。
パッチの適用状況や、アンチウィルスソフトの状態など、エンドポイント内の各種状態を検査対象とし、結果によりアクセス制限や修復を実行する。

2つのポスチャモジュール

AnyConnectでは、2 種類のポスチャモジュールをにより、ホストにインストールされた AV, AS, FW S/W などについてエンドポイントのコンプライアンスを評価可能。

- VPNポスチャ (Hostscan)
  VPN接続時に実行される、AnyConnectとVPNヘッドエンド(ASA/FTD)のみで利用可能なポスチャモジュール。

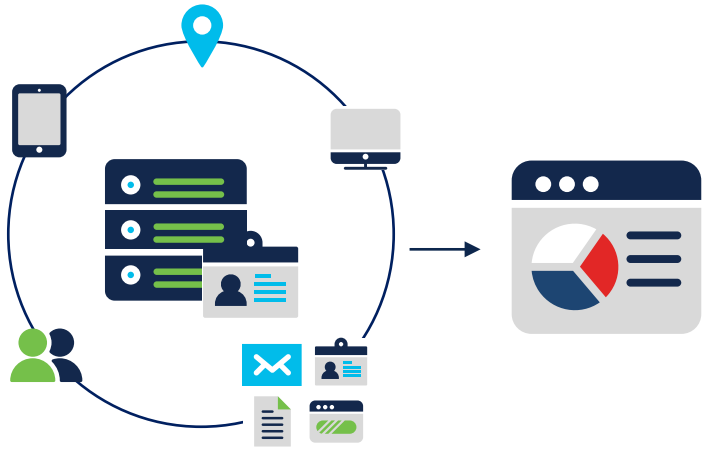
- ISEポスチャ
  Identity Services Engine (ISE) をポリシーエンジンとして動作するポスチャモジュール。VPN接続時のみならず、社内LAN接続時にもコンプライアンスチェックの評価を実行。



Network Visibility Module (NVM)

トラフィック可視化

- エンドポイントからのネットワークフローの詳細を取り込み、Cisco Secure Network Analytics (Stealthwatch)などのネットワーク可視化ソリューションと連携
- フロー情報はNetFlow v10 (IPFIX)に則り、従来のNetFlowの情報に加え、デバイスID、デバイス名、プロセス情報などの情報を付加し、可視性を強化
- VPN接続の有無を問わずフロー情報の収集が可能
- Windows / macOS / Linux / Android (Samsung Knox)をサポート



NVMのユースケース

- AD ユーザ/グループ（誰）がどのアプリケーションにアクセスしているのか
- どの AD グループ/ユーザ間で通信を行っているのか。ラテラル ムーブメントはあるのか
- どんなデバイスの種類がアプリケーションにアクセスしているのか
- ユーザはどこから SaaS アプリケーションにアクセスしていて、その SaaS アプリケーションは何なのか
- ユーザは許可されたアプリケーションを使っているのか？それとも脆弱性のあるバージョンのアプリケーションを使っているのか

AnyConnect NVMでユーザ ログ分析を楽にしませんか
https://gblogs.cisco.com/jp/2018/12/anyconnect-nvm-makes-user-activity-log-analysis-easier/

その他のモジュール

Network Access Manager (NAM, Windowsのみ対応)

Plus Apex

- 有線/無線LANのコネクティビティを提供
  - IEEE 802.1xサプリカント/IEEE 802.11設定/MACSEC

AMP Enabler (Windows/macOSのみ対応)

Plus Apex

- Cisco Secure Endpoint (AMP for Endpoint)をAnyConnectユーザに展開するモジュール

Diagnostics And Reporting Tool (DART)

Plus VPN Only Apex

- TACにサービスリクエスト(SR)を起票する際に使用する、ログバンドルを生成するモジュール

幅広いクライアントOS対応

モジュール	Windows (Intel)	Windows (ARM)	macOS	Linux	Apple iOS	Android	Chrome	Windows (UWP)
VPN core	✓	✓	✓	✓	✓	✓	✓	✓
Umbrella Roaming Security Module (RSM)	✓		✓			✓		
ポスチャ	✓	✓	✓	✓	ACIDex	ACIDex	ACIDex	ACIDex
Network Visibility Module (NVM)	✓		✓	✓		✓		
Network Access Manager (NAM)	✓							
AMP Enabler	✓		✓					
DART	✓	✓	✓	✓	✓	✓	✓	✓

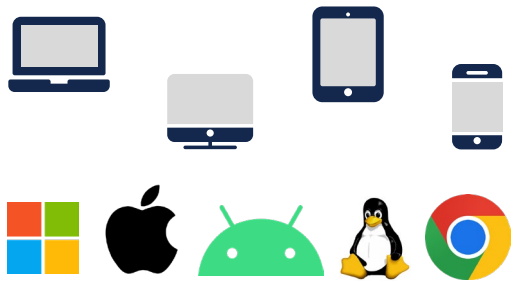
*ACIDex: AnyConnect Identity Extensions
https://www.cisco.com/c/ja_jp/support/docs/security/anyconnect-secure-mobility-client/118944-technote-anyconnect-00.html

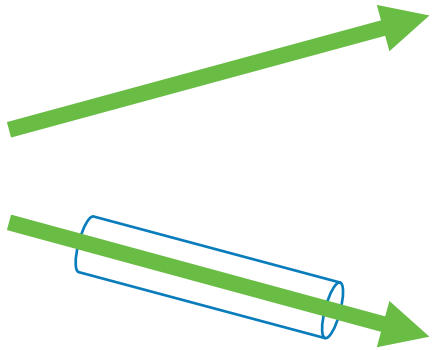
導入シナリオ

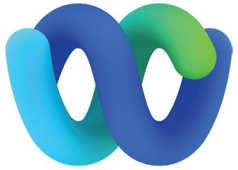
均一なVPNサービスの提供

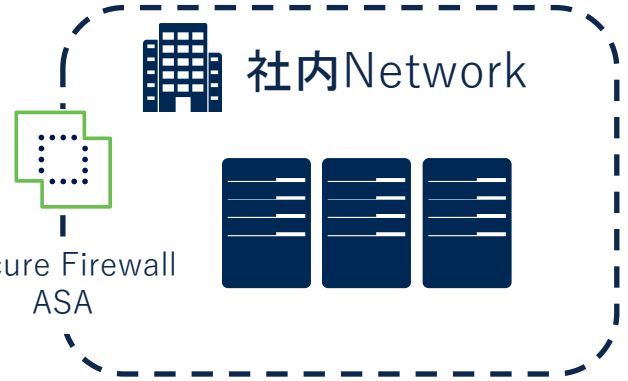
Split Tunnel

Cisco Webex及び、Microsoft 365へのトラフィックは、Split tunnelで除外し、トンネルを経由せず直接通信









幅広いクライアントOS対応

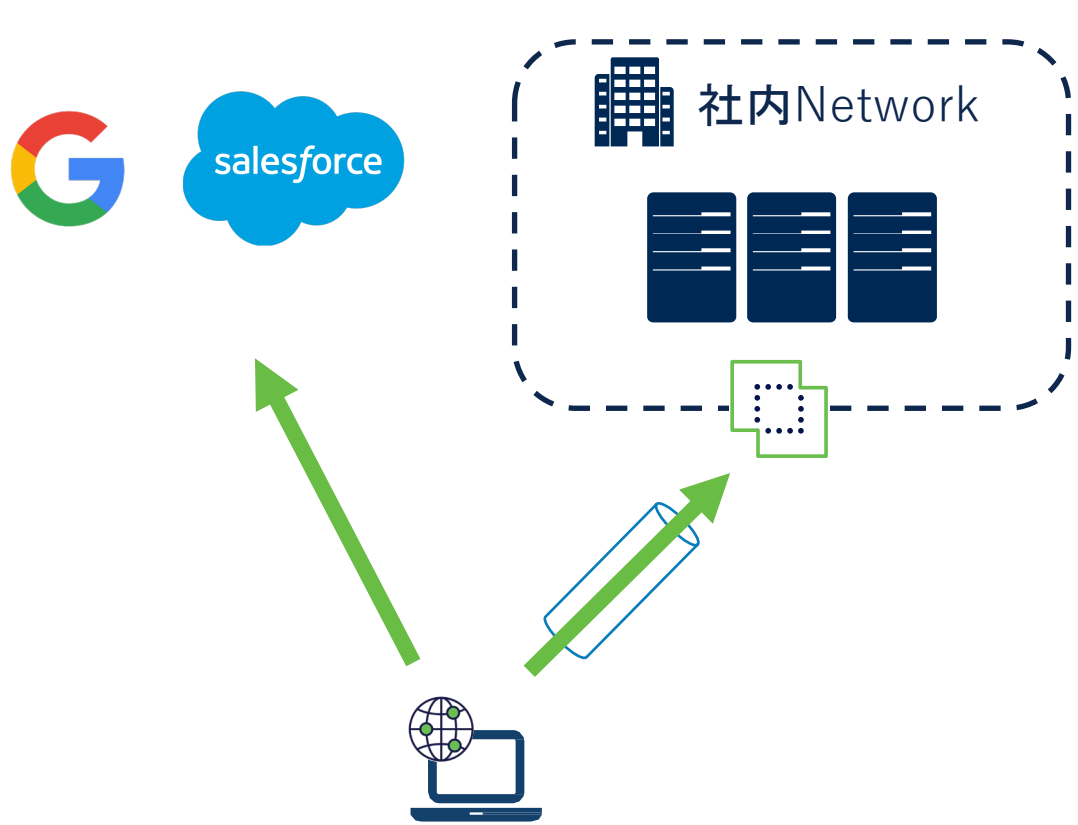
クライアントOSに依らず、均一なVPNサービスを提供する

Microsoft Office 365およびCisco Webex用のAnyConnectスプリットトンネルの最適化
https://www.cisco.com/c/ja_jp/support/docs/security/anyconnect-secure-mobility-client/215343-optimize-anyconnect-split-tunnel-for-off.html

ローカルブレイクアウト

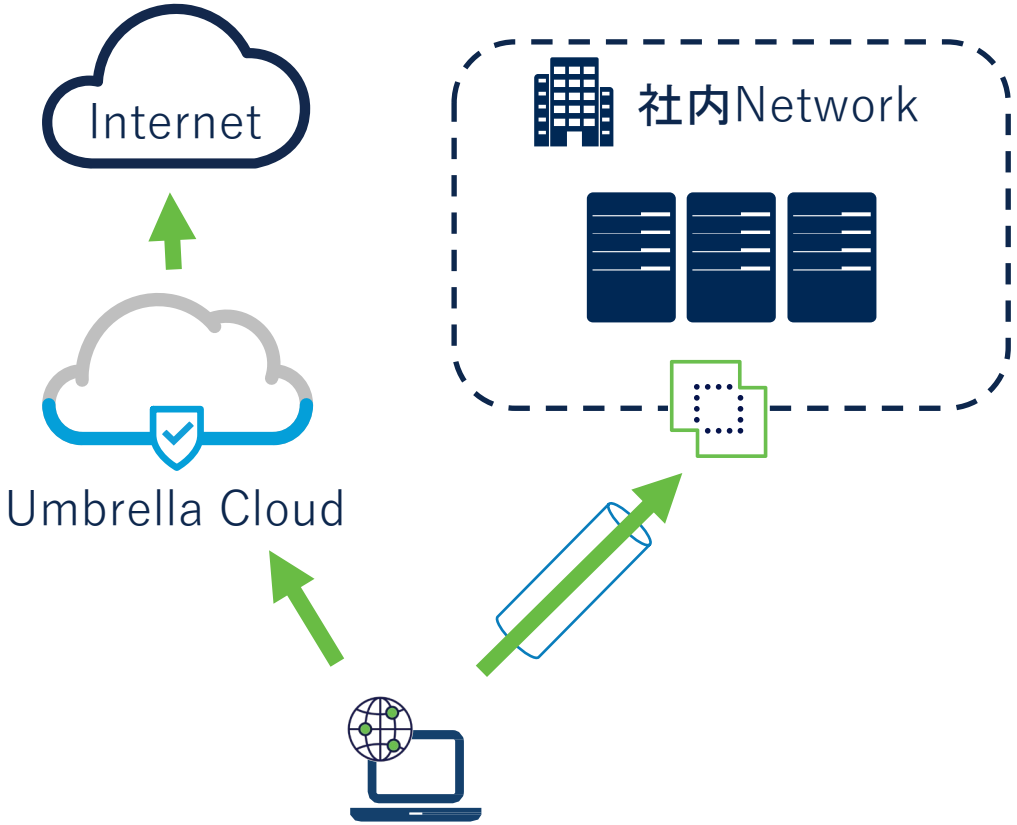
Dynamic Split Tunnel

クラウドアプリケーションをドメイン指定でトンネルから除外し、社内ネットワークを経由せずに直接通信



Umbrella Roaming Security

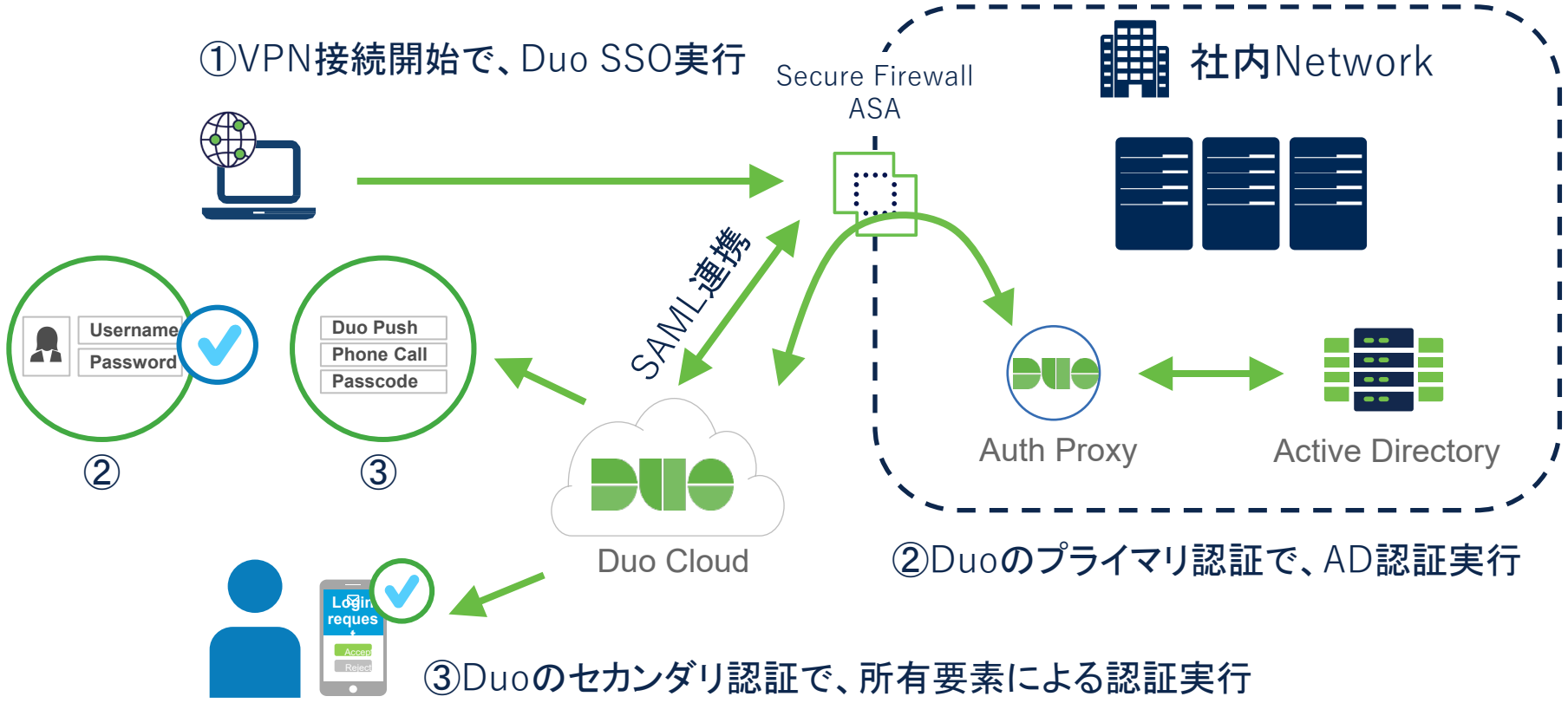
DNS / Web (TCP/80, 443)をUmbrella経由として、社内ネットワーク経由のインターネット宛通信を削減



ゼロトラスト

Duo MFAにより接続ごとに本人確認を実行

ゼロトラストの原則である「決して信頼せず、常に検証する (Never Trust, Always Verify)**」を、**
Duo MFAを用いて実現する。



補足情報

構成要素

クライアントOS

- Windows (Intel/ARM/UWP)
- macOS
- Linux
- Apple iOS
- Android
- Chrome OS

Secure Firewall

- ASA
  終端装置としてのFull Featureを利用可能
- FTD
  利用可能な機能に制限あり

Cisco Umbrella

- Roaming Security Module (RSM) で連携し、DNS / Web (TCP/80,443) トラフィックのクラウドセキュリティ化

Cisco Secure Access by Duo

- SAML、もしくはDuo Authentication Proxy (DAP)による連携でMFA実行

Cisco Identity Services Engine

- ISEポスチャのポリシーエンジン
- VPN接続及び、Network Access Manager (NAM)におけるRADIUS認証サーバ

NetFlow Collectors

- Network Visibility Module (NVM) で連携し、フロー情報収集
- Cisco製品の場合には、Cisco Secure Network Analytics (Stealthwatch)が該当

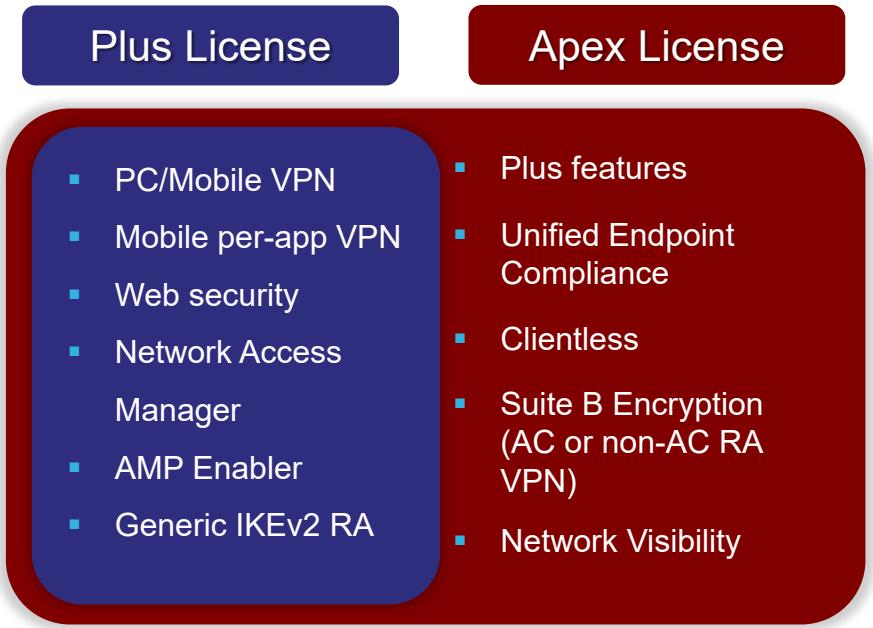
Secure Endpoint (AMP for Endpoint)

- AMP Enablerでソフトウェア展開

ライセンス

2種類のライセンス形態が存在

利用ユーザ数に応じたライセンス



OR

Head end (ASA/FTD)に関連付ける、
VPN同時接続数に応じたライセンス

AnyConnect VPN Only

詳細は AnyConnect 4.10 ライセンスオプション 参照

参考資料

- Sales Connect セキュリティ資料　AnyConnect及び他セキュリティ製品に関するコンテンツがまとまっています

製品情報

- PSU-VoD-SEC-Anyconnect-01 概要のご紹介
- PSU-VoD-SEC-Anyconnect-02 機能のご紹介

Duo連携

- CTU-Plus-SEC-DuoAC-01-DuoとAnyconnectハンズオントレーニング Duo講義
- CTU-Plus-SEC-DuoAC-02-DuoとAnyconnectハンズオントレーニング Anyconnect講義
- CTU-Plus-SEC-DuoAC-03-DuoとAnyconnectハンズオントレーニング ラボ演習

その他

- Cisco AnyConnect 発注ガイド
- AnyConnect セキュア モビリティ クライアント リリース 4.10 の機能、ライセンス、および OS
- AnyConnect モバイルプラットフォームおよび機能ガイド

SECURE