セッションに関するご質問

アンケートフォームにご記入ください。

担当営業やシスココンタクトセンターまでにお問い合わせください。

今後のシスコセキュリティウェビナー

https://www.cisco.com/c/ja_jp/training-events/events-webinars/webinars.html

毎週木曜日開催を予定。当面の予定は以下となります。

2020/6/4	木	14:00-14:30	30分でわかる最新の多要素認証 (Duo Security)
2020/6/4	木	15:00-15:30	30分でわかるマイクロセグメンテーション
2020/6/11	木	14:00-14:30	30分でわかるVPN（AnyConnect）
2020/6/11	木	15:00-15:30	30分でわかるクラウドセキュリティ（Umbrella）
2020/6/18	木	14:00-14:30	30分でわかるメールセキュリティ
2020/6/18	木	15:00-15:30	30分でわかるエンドポイントセキュリティ（AMP）
2020/6/25	木	14:00-14:30	30分でわかる認証基盤（ISE）
2020/6/25	木	15:00-15:30	30分でわかる可視化と脅威検出（StealthWatch）

cisco Secure

30分でわかるリモートアクセスVPN (AnyConnect)

2020年6月11日
シスコシステムズ合同会社
セキュリティ事業
テクニカルソリューションズアーキテクト
小林 達哉 (tatskoba@cisco.com)

“アフターコロナ”でのテレワークの必要性

- 新型コロナウイルス感染拡大に伴い、日本でも政府による緊急事態宣言が発令され、多くの企業がテレワークを緊急的に導入
- 結果的に、日本でも WebEX 等の Web 会議で仕事を行うことへの心理的ハードルが大きく下がった
- 緊急事態宣言終結後の “アフターコロナ” の世界でも、働き方改革の一貫として、テレワークは継続して行うという企業も多い

- 経済再生相 経済3団体と連合にテレワークや時差出勤の継続要請

https://www3.nhk.or.jp/news/html/20200601/k10012453761000.html

- 緊急事態宣言解除後の日本企業、テレワーク活用の「新しい生活様式」広がる

https://www.newsweekjapan.jp/stories/business/2020/05/post-93511.php

セキュアなテレワーク

安全なリモートアクセスVPN

Cisco AnyConnect

外部から社内ネットワークへ安全に接続するためのクライアント ソフトウェアであり、幅広い端末に対応し、DNS Web セキュリティ（Umbrella連携）を提供

セキュアインターネットゲートウェイ

Cisco Umbrella

あらゆる場所で、あらゆるユーザ、あらゆるデバイスを保護できる、簡単かつ迅速に導入可能なクラウド提供型のセキュリティサービス（DNS、Web、クラウドFW、クラウドアプリ可視化・制御等）

ゼロトラスト/多要素認証

Cisco DUO Security

信頼できるユーザとデバイスだけをアプリケーションに接続する適応型多要素認証（MFA）サービスであり、情報漏えいが起きるリスクを軽減

エンドポイントを保護

Cisco AMP for Endpoint

マルウェアを検出・可視化し、高度な脅威を防御・対応するソフトウェアであり、リモートワーカーのデバイスを安全な状態に維持し、生産性を向上

セキュアなテレワーク

インターネット

クラウド
サービス

ビデオ会議・イベントWeb
ミーティング

チャット・ファイル共有
電話・ホワイトボード

内部サーバ
アプリ

Webex
Meeting

Webex
Teams

DNG

Umbrella

Cisco Umbrella
VPNを使わないテレワークへの対応
迅速に導入可能な
クラウドセキュリティ

VPN終端用
ASA/FTD

Cisco Duo Security
VPNレス社内アクセス
多要素認証
パスワード漏洩を守る
デバイスの健全性を検証

Cisco AnyConnect
VPNでの業務にアクセス
幅広い端末に対応

AnyConnect

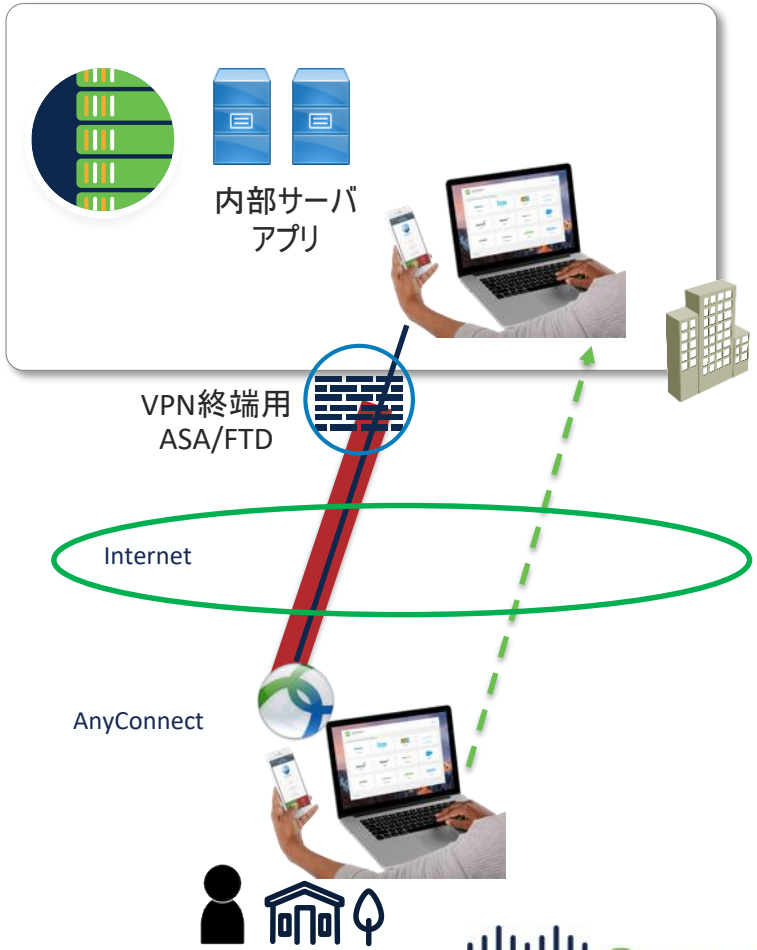
Duo

AMP

Cisco AMP for Endpoints
デバイスを安全な状態に維持
マルウェアを検出・可視化し、高度な脅
威を防御・対応

リモートアクセス VPN

- PC やスマートフォンに専用アプリケーション (Cisco AnyConnect) をインストールし、VPN 終端装置 (Cisco ASA / FTD 等) まで安全な VPN トンネル (SSL-VPN / IPsec IKEv2) を張る
- PC やスマートフォンがあたかも VPN 終端装置の内側に存在するようになる
- フルトンネルの VPN (AnyConnect 利用時) であれば、IP (v4 / v6 どちらも可) 通信すべてに対応
- Firewall で守られていたり、そもそもプライベートアドレスのためにインターネットから直接のアクセスが不可な内部ネットワークに、安全にアクセスすることが可能
- 長い間使われてきた接続方法



cisco Secure

これからの時代は “VPN レス”?

- 業務で利用するすべてのサーバがクラウドにあるならば…

→確かに VPN での内部への安全なアクセスは不要

→ただし、Umbrella 等を使ってクラウドへのアクセスを安全に保つ必要がある

- 内部ネットワークで使うアプリケーション (プロトコル) が特定のものだけであれば…

→ Duo Network Gateway のようなソリューションを使うことで VPN アクセスは不要

上記のどちらかが満たせていない限り、リモートアクセス VPN は必要

シスコはこれらすべてに対してソリューションがある

cisco Secure

シスコのリモートアクセス VPN に必要なもの

- クライアントソフトウェア
  - AnyConnect ソフトウェア + ライセンス (後述)

    OS 標準 VPN クライアントもサポートしているが、接続の問題発生時の切り分けに手間がかかるため、非推奨

- VPN 終端装置 (VPN サーバ)
  - Cisco ASA – Basic Firewall- (ASA on Firepower, ASAv) (ASA5500-X は一部モデルを除き販売終了アナウンス済み)
  - Cisco Firepower Threat Defense (通称 FTD) – Next Gen Firewall

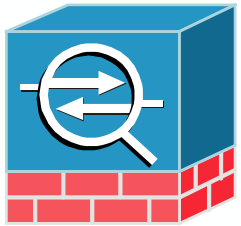
    NGFW (アプリケーション制御, IPS, Malware 対策) 機能と同時に行いたい場合に FTD を検討、ただしリモートアクセス VPN は ASA の方が安価で機能が豊富。IOS ルータも VPN 終端装置として動作可能だが、ASA や FTD の方が機能豊富で管理が容易なため、ここでは扱わない

- その他オプション
  - Umbrella ライセンス、Duo ライセンス等

ASA と AnyConnect

- ASA の特長
  - CLI で操作できる Basic Firewall
  - リモートアクセス VPN 終端装置として豊富な機能
  - 多量の ACL でも安価に実現
  - 16年目のロングセラー

    (PIX まで遡ると27年!)



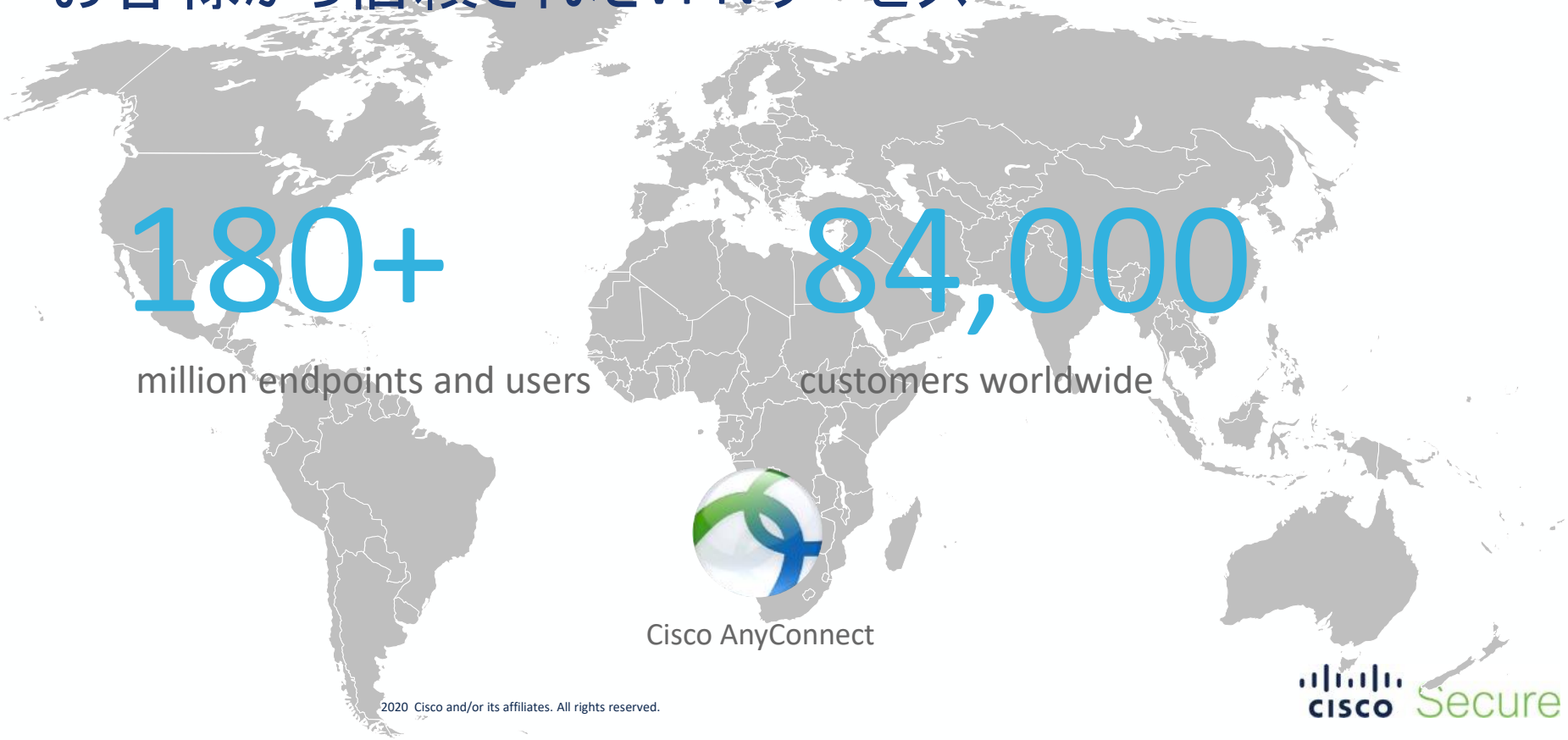
- AnyConnect の特長
  - どこからでも安全なアクセスを提供
  - IPsec でも SSLでも利用可能なフルトンネル VPN
  - PC だけでなくスマートフォンでも利用可能
  - VPN 以外の機能も豊富 (NAM, NVM, AMP enabler, Umbrella)
  - 14年目のロングセラー

    (Cisco VPN Client まで遡ると21年!)

どちらもまだまだシスコのセキュリティ製品の中核かつ主力

cisco Secure

数千社のお客様での利用実績
お客様から信頼されたVPNサービス



180+

million endpoints and users

84,000

customers worldwide

Cisco AnyConnect

cisco Secure

ASA 製品ラインナップ

- Firepower シリーズに ASA ソフトウェアをインストールして利用することが可能
- 仮想環境用、IaaS 向けのソフトウェアも選択可能

物理アプライアンス

Firepower 41x5
(4112, 4115, 4125,4145)

Firepower 9300
(*SM-24,36,44*)
(SM-40,48,56)

Firepower 4100
(4110, *4120, 4140, 4150*)

Firepower 2100
(2110, 2120,
2130, 2140)

Firepower 1120 /
1140 / 1150

Firepower 1010

ASA 5516-X

ASA 5508-X

仮想アプライアンス

ASAv5, ASAv10, ASAv30, ASAv50, ASAv100

(注) ASAv100 は AWS / Azure には未対応

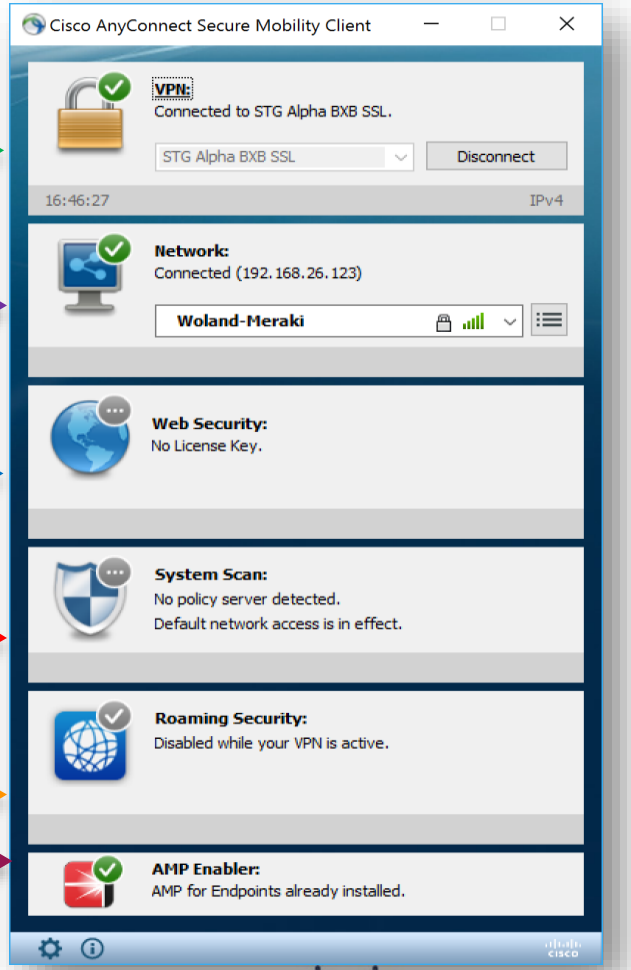
Teleworker | Branch Office | Internet Edge | Campus | Data Center

赤字のモデルは新製品、斜字のモデルは販売終了アナウンス済み

cisco Secure

AnyConnect の様々なモジュール

- VPN Module (Core)
- Network Access Manager (NAM)
- Web Security (CWS)
- Posture
- Umbrella Module
- HostScan (aka: ASA posture) (No UI)
- Network Visibility Module (NVM) (No UI)
- AMP Enabler Module
- Diagnostics and Reporting Tool (DART)



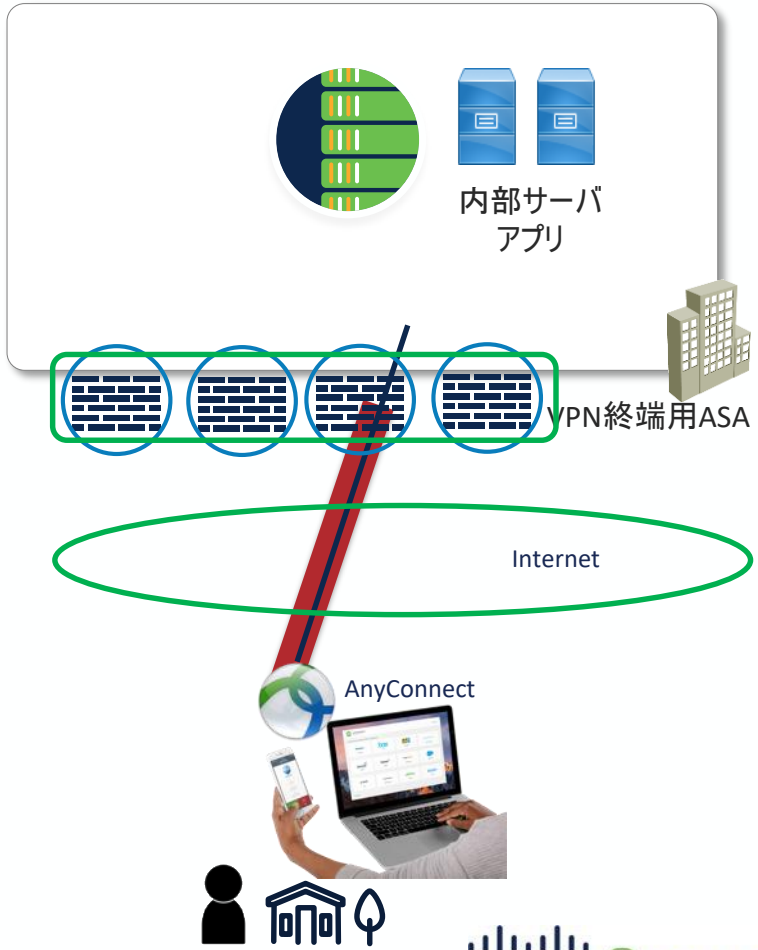
VPN 以外にも様々なクライアントセキュリティ機能を提供

cisco Secure

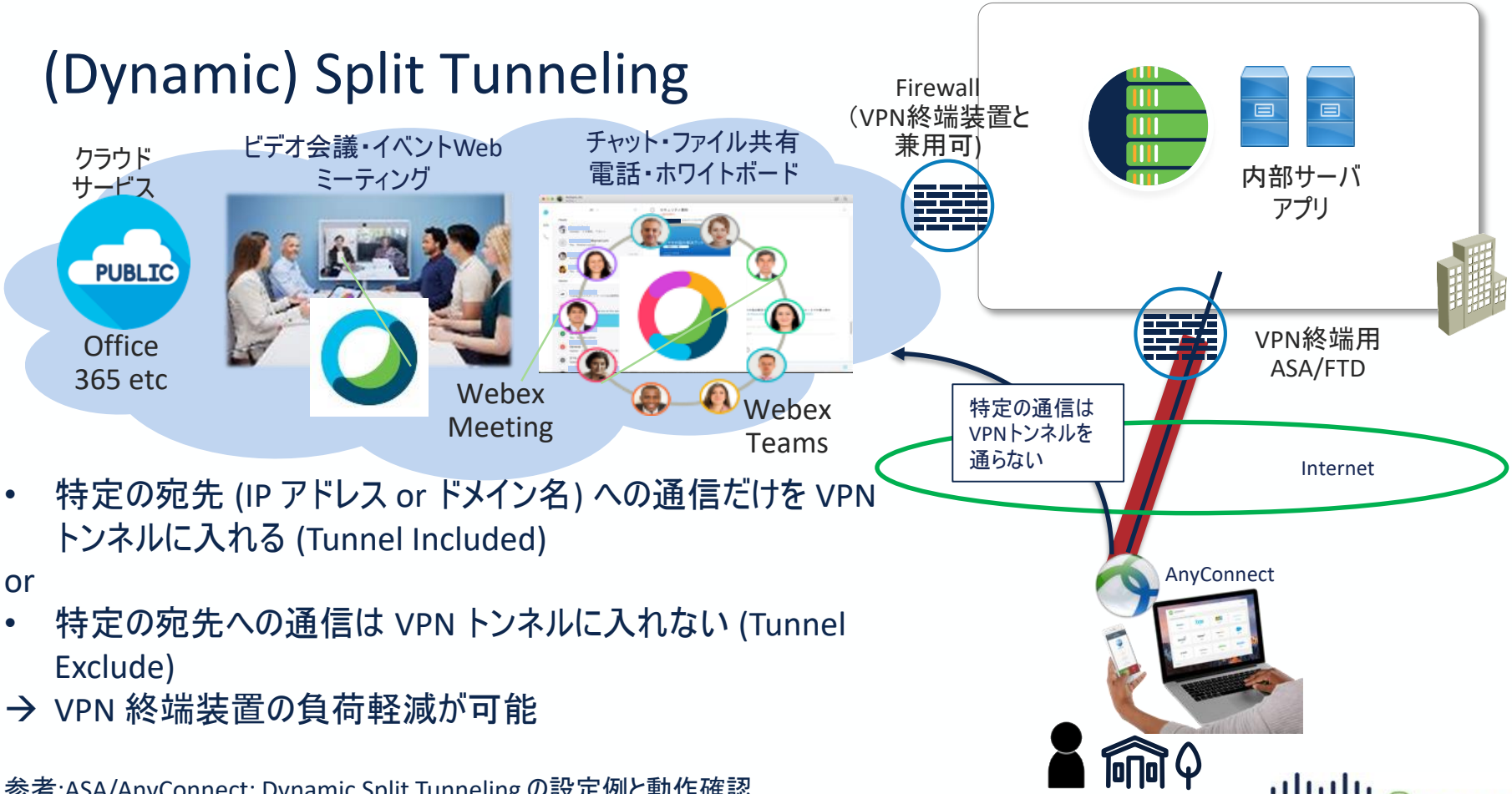
VPN ロードバランス

- 複数の ASA を並べて、1つの大きな VPN 終端装置に見せる機能 (FTD は不可)
- ASA ネイティブな機能であり、外部ロードバランサ不要
- ASA はモデルもソフトウェアバージョンも合わせる必要なし (ただし、サポートの観点からはソフトウェアバージョンは合わせた方が良い)
- VPN3000 の時代から使われている非常に枯れた安定した技術であり、実績多数

参考その1: ASA: リモートアクセスVPN パフォーマンス最適化のためのベストプラクティス (AnyConnect)
https://community.cisco.com/t5/-/-/ta-p/4061565
参考その2: [温故知新] Cisco ASA の VPN ロードバランスをもう一度楽しんでみる
https://qiita.com/tatskoba27/items/7133fd9957106e97db8b



(Dynamic) Split Tunneling



- 特定の宛先 (IP アドレス or ドメイン名) への通信だけを VPN トンネルに入れる (Tunnel Included)

or

- 特定の宛先への通信は VPN トンネルに入れない (Tunnel Exclude)

→ VPN 終端装置の負荷軽減が可能

参考:ASA/AnyConnect: Dynamic Split Tunneling の設定例と動作確認
https://community.cisco.com/t5/-/-/ta-p/4054529

※ Dynamic Split Tunneling (ドメイン名で振り分け) は Apple iOS 未サポート

cisco Secure

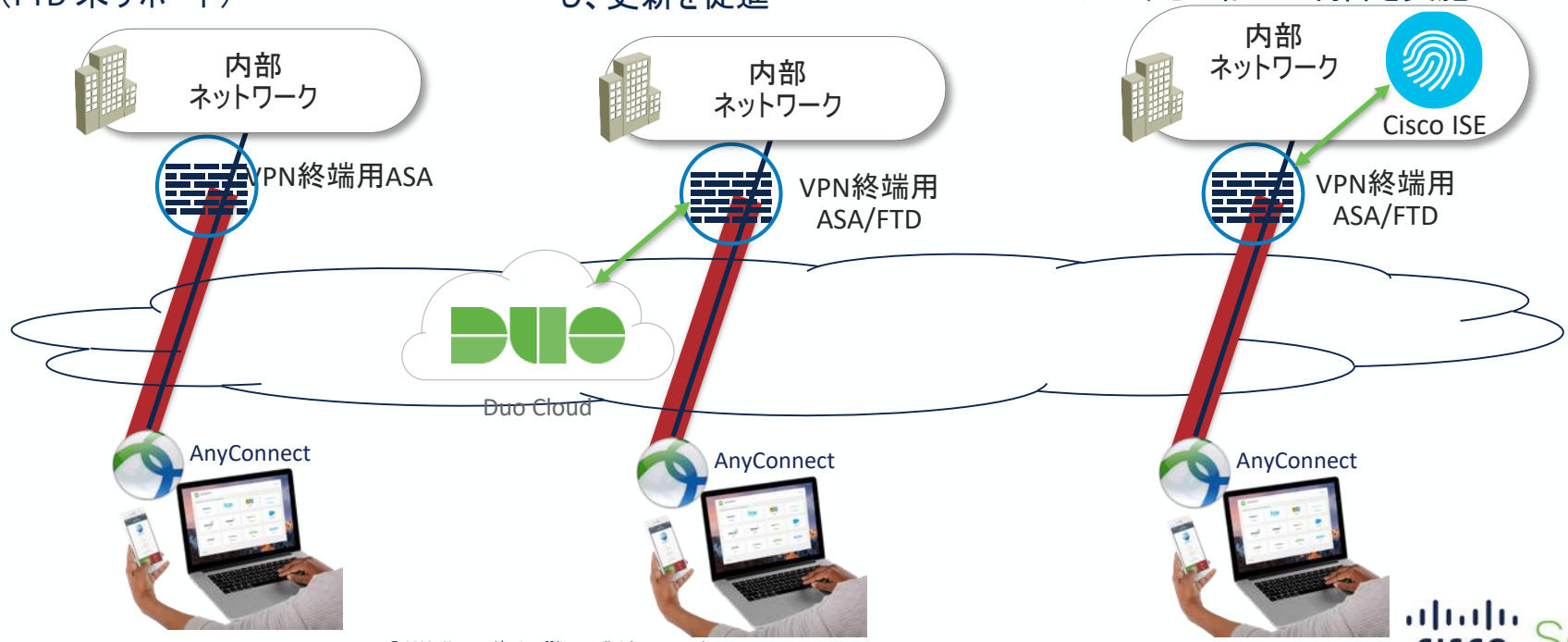
Posture (検疫)

3つのタイプのソリューションが存在
ニーズに合わせて選択

ASA と AnyConnect の
hostscan だけで行う簡易検疫
（FTD 未サポート）

VPN 認証時に Duo と連携
古い OS やアプリケーションを検知し、更新を促進

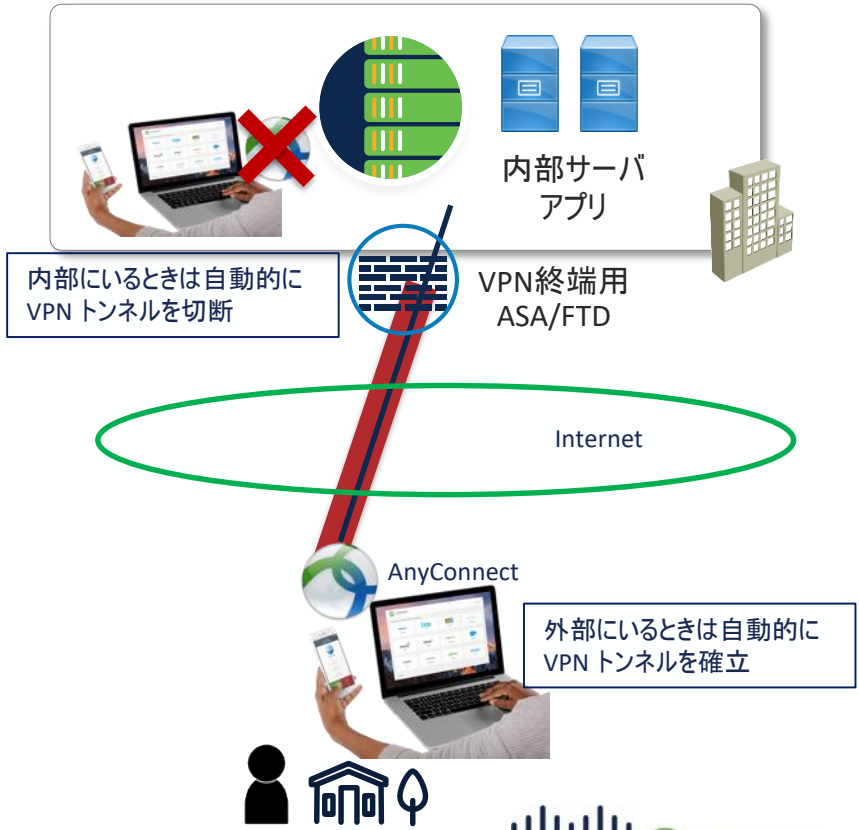
VPN 認証時に ISE と連携
古い OS やアプリケーション、違反な設定を検知し、きめ細かい制御を実施



cisco Secure

Always On & Trusted Network Detection

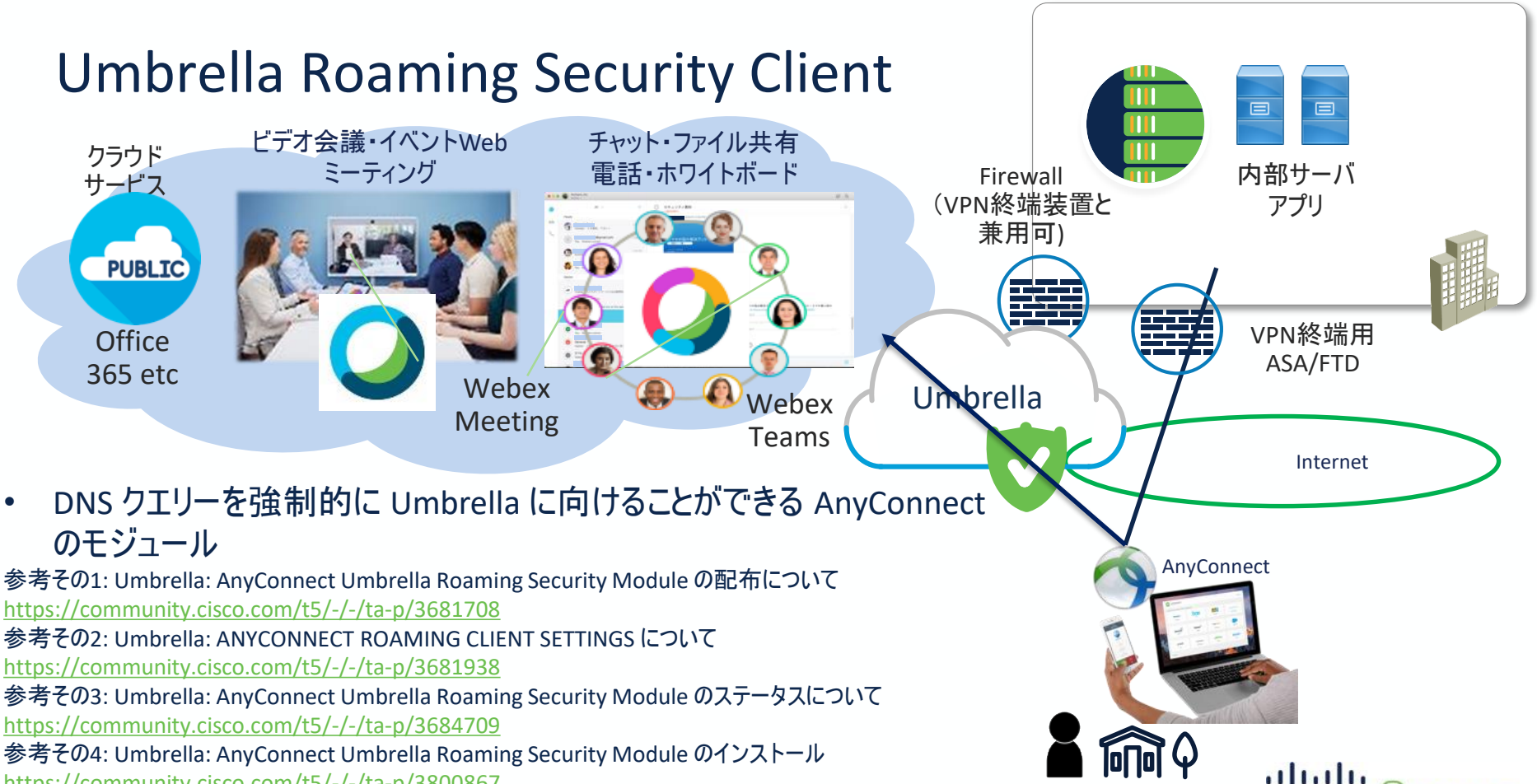
- AnyConnect が動作している PC が、外部ネットワークに存在しているときには、自動的に VPN トンネルを確立され、内部ネットワークに存在しているときには、自動的に VPN トンネルを切断する機能
- エンドユーザが VPN 接続、切断を意識することなく、シームレスな VPN の利用が可能
- 内部ネットワーク or 外部ネットワークの判断は、以下の仕組みを利用
  - 付与されたドメイン名および参照 DNS サーバが信頼されたものであれば内部ネットワークと判断
  - 信頼される内部サーバへの疎通があれば内部ネットワークと判断



※ Apple iOS では未サポート。代わりに Connect on Demand という特定のドメイン宛ての通信発生時に自動的に VPN トンネルを張る機能がある

cisco Secure

Umbrella Roaming Security Client



- DNS クエリーを強制的に Umbrella に向けることができる AnyConnect のモジュール

参考その1: Umbrella: AnyConnect Umbrella Roaming Security Module の配布について
https://community.cisco.com/t5/-/-/ta-p/3681708
参考その2: Umbrella: ANYCONNECT ROAMING CLIENT SETTINGS について
https://community.cisco.com/t5/-/-/ta-p/3681938
参考その3: Umbrella: AnyConnect Umbrella Roaming Security Module のステータスについて
https://community.cisco.com/t5/-/-/ta-p/3684709
参考その4: Umbrella: AnyConnect Umbrella Roaming Security Module のインストール
https://community.cisco.com/t5/-/-/ta-p/3800867

cisco Secure

シスコ社員の AnyConnect 利用方法

VPN 切断時には Umbrella RSM が有効になり、VPN 接続時には (クライアントは社内にいるときと同じセキュリティが担保されるので) Umbrella RSM が無効化される

[注] VPN 接続時の認証には Duo Security の MFA も利用しているがここでは割愛

cisco Secure

AnyConnect ライセンスの選択方法

- 基本的な機能 (後述) だけで良い

  → Plus ライセンスを利用ユーザ数でオーダー (同時接続数やデバイスの数、ASA 等の VPN 終端装置の数は一切気にしない)

- 高度な機能 (後述) まで使いたい

  → APEX ライセンスを利用ユーザ数でオーダー (同時接続数やデバイスの数、AS A等の VPN 終端装置の数は一切気にしない)

- 機能はともかく利用ユーザ数は多いが同時に VPN 接続する人数は多くないので Plus や APEX のようなユーザ数ライセンスだと価格的に辛い

  → VPN-Only ライセンスを VPN 終端装置毎に最大同時接続数でオーダー

- [注] AnyConnect 3.x までの Essentials や Premium, Shared Premium ライセンスは、ASA 等の VPN 終端装置更新時に持ち越すことはできない

AnyConnect Plus / APEX / VPN-Only ライセンス

Plus License

- PC/Mobile VPN
- Mobile per-app VPN
- Web security
- Network Access Manager
- AMP Enabler
- Generic IKEv2 RA

APEX License

- Plus features
- Unified Endpoint Compliance
- Clientless
- Suite B Encryption (AC or non-AC RA VPN)
- Network Visibility

ユーザ単位、5/3/1 年単位のサイトライセンス
Plus は Perpetual ライセンスも選択可能

VPN-Only License

機能は APEX と同じ

同時接続数、ASA / FTD 1台 (もしくは Failover ペア) あたりのライセンス
Perpetual のみ対応
移管および追加不可

通常は Plus / APEX を選択
利用ユーザ数は多いが同時に VPN 接続する人数は多くない場合に、VPN-Only も検討

ASA-VPN バンドル

- 組織の規模に応じて事前にサイジング済みの VPN バンドル

- DTLS Any Connect の実世界でのパフォーマンス
- アプライアンスのトンネル容量
- リモートワーカーがメール、音声・ビデオ会議、ウェブサーフィンを利用することを想定
- ユーザーによって複数のデバイスを持っている想定
- リモートアクセスのために高可用性が必要

Bundle Names By Employee Count

- ASA-VPN-75-BUN
- ASA-VPN-300-BUN
- ASA-VPN-600-BUN
- ASA-VPN-2K-BUN
- ASA-VPN-6K-BUN
- ASA-VPN-10K-BUN
- ASA-VPN-15K-BUN

従業員数 (利用者数) でカウント

SMB

VPN aggregate throughput
240-550 Mbps

ASA-VPN-75-BUN
FPR1010 (2 HA)
Any Con Plus
Any Con Apx
Sec-Plus HA Lic
Encryption Lic

ASA-VPN-300-BUN
FPR1140 (2 HA)
Any Con Plus
Any Con Apx
Encryption Lic

Mid-Cap/Commercial

VPN aggregate throughput
550 Mbps – 1 Gbps

ASA-VPN-600-BUN
FPR1150 (2 HA)
Any Con Plus
Any Con Apx
Encryption Lic

ASA-VPN-2K-BUN
FPR2140 (2 HA)
Any Con Plus
Any Con Apx
Encryption Lic

Large Enterprises

VPN aggregate throughput
6.5 - 12 Gbps

ASA-VPN-6K-BUN
FPR4110 (2HA)
Any Con Plus
Any Con Apx
Encryption Lic

ASA-VPN-15K-BUN
FPR4125 (2 HA)
Any Con Plus
Any Con Apx
Encryption Lic

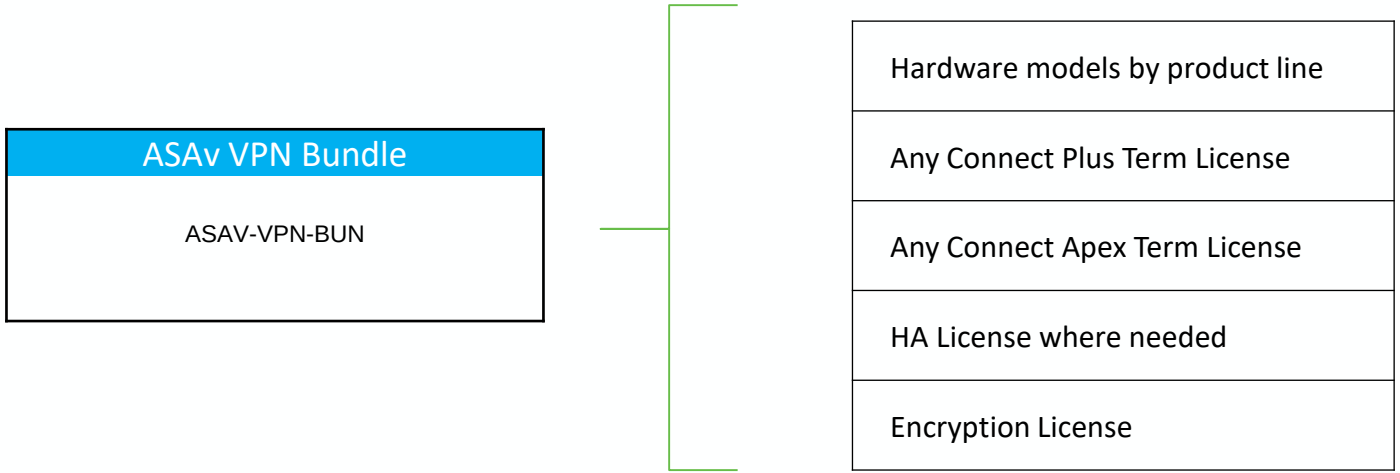
ASA-VPN-10K-BUN
FPR4115 (2 HA)
Any Con Plus
Any Con Apx
Encryption Lic

cisco Secure

ASAv-VPN バンドル

仮想 ASA のために VPN の発注を簡素化するために設計

- ユーザー数によりサイジングされたものではなく、VPN に必要な要素をバンドルした型番
- サイジング・数量などは個別選択する必要あり

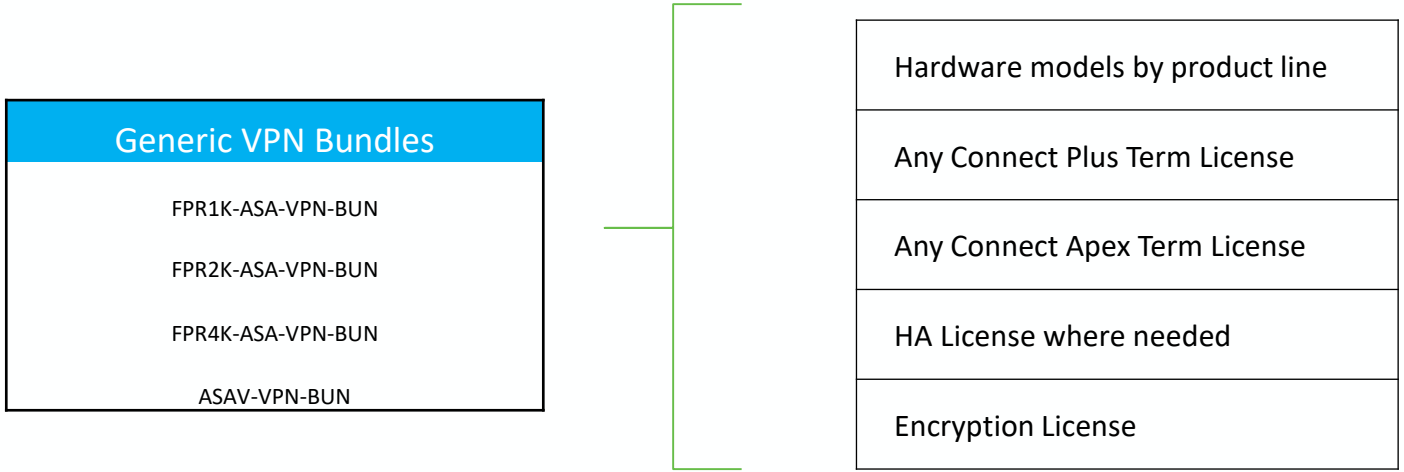


cisco Secure

Generic VPN Bundles

大規模環境向け VPN の発注を簡素化するために設計

- ユーザー数によりサイジングされたものではなく、VPN に必要な要素をバンドルした型番
- サイジング・数量などは個別選択する必要あり



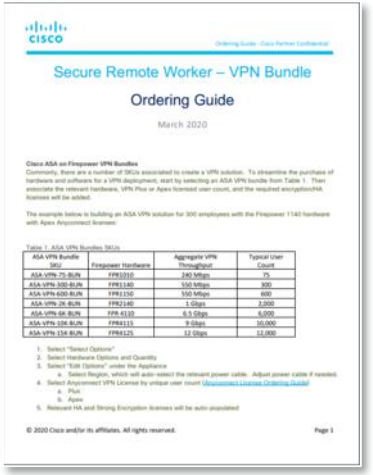
cisco Secure

VPN バンドル各種ガイド

オーダー方法詳細は以下ガイドを参照

Ordering Guide URL

https://www.cisco.com/c/dam/en/us/products/se/2020/3/Collateral/secure-remote-worker-vpn-bundle-og.pdf

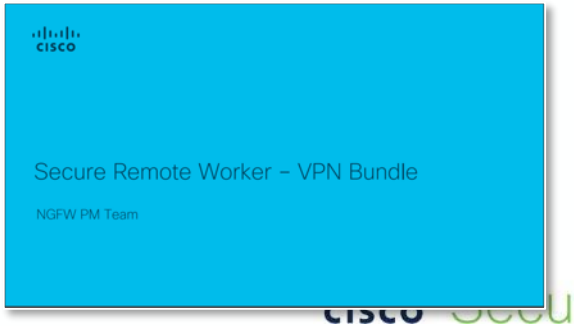

Secure Remote Worker – VPN Bundle

Ordering Guide

March 2020

Partner Guide

https://www.cisco.com/c/dam/en/us/products/se/2020/3/Collateral/secure-remote-worker-offer-vpn-bundle-partner-guide.pdf



セキュアリモートワーク支援オファー AnyConnect 関連

オファーの詳細:

- AnyConnect をご利用のお客様:オファー期間中、購入したユーザ数の上限に関係なくクライアントを追加してインストールが可能。オファー期間終了時に、上限を超えているユーザアカウントを購入する、もしくはクライアントのアンインストールが必要
- ASA/Firepower をご利用で AnyConnect をまだ使用していないお客様:AnyConnect の 90 日間トライアルの評価。オファー期間終了時に、試用した AC ライセンスを購入する、もしくはクライアントのアンインストールが必要
- 新規のお客様:ASAv30 の大幅な割引プログラム。AnyConnect の 90 日間トライアルの評価。オファー期間終了時に、試用した AC ライセンスを購入する、もしくはクライアントのアンインストールが必要

サポート:シスコ セキュリティ パートナー セールス スペシャリスト、
シスコアカウントマネージャへ問い合わせ。ライセンスのリクエストについては、
licensing@cisco.com へ電子メールを送信

AnyConnect

ASAv
ファイアウォール

cisco Secure

© 2020 Cisco and/or its affiliates. All rights reserved.

まとめ

- “アフターコロナ”の新しい生活様式においても、テレワークの整備および継続利用は必要
- テレワークにおける VPN は、“VPN レス”が可能な環境であれば不要だが、まだまだ必要な環境は多い
- シスコは長年に渡ってリモートアクセス VPN の製品をリリース
- VPN を繋ぐときのセキュリティ対策はもちろん、VPN を繋いでいないときのセキュリティ対策が重要
- シスコからはこれらを実現できるソリューションを提供
- シスコは、わかりやすい VPN バンドルや、セキュアリモートワーク支援のオファーがある

今後のテレワーク整備でのリモートアクセス VPN はシスコにご相談を!!

cisco Secure


cisco Secure

シスコ コンタクトセンター

自社導入をご検討されているお客様へのお問い合わせ窓口です。

製品に関して ｜ サービスに関して ｜ 各種キャンペーンに関して ｜ お見積依頼 ｜ 一般的なご質問

お問い合わせ先

お電話での問い合わせ

平日10:00-12:00, 13:00-17:00

0120-092-255

お問い合わせフォーム

https://www.cisco.com/jp/go/vdc_callback