COVID-19 対策に向けた AnyConnect の導入およびパフォーマンス/拡張リファレンス情報

内容

概要
実装
ライセンス
AnyConnect 初期設定クイックスタートガイド
完全な設定ガイド
証明書インストールガイド
パフォーマンスと拡張性に関する問題
問題の現象と特定
CPU 使用率が高い。
最大 VPN 接続数
データシートリファレンス
考えられる緩和策
スプリット トンネリングの有効化
VPN ロードバランシングの実装（ASA のみ）
構成の最適化
トンネルプロトコルの選択
トンネル単位のQoSの適用（FTDのみ）
暗号エンジン アクセラレータ バイアスの実装（ASA のみ）
FAQ
ライセンス
コンフィギュレーション
モニタリング
トラブルシューティング
追加サポートについて
参考資料

概要

世界中の国々が COVID-19 のパンデミックと闘う中、感染の拡散防止策としてリモートワークを導入する企業が増えています。その結果、従業員が社内のリソースにアクセスできるようにするためのリモートアクセス VPN（RAVPN）の需要が高まっています。本記事では、ネットワーク内に RAVPN を迅速に設定したり、パフォーマンスや拡張性に関する問題を特定して対処したりするためのコンフィギュレーション ガイドのリファレンス情報を提供します。

実装

次のセクションでは、シスコの各種プラットフォームで AnyConnect リモートアクセスを設定および展開する方法について詳しく説明します。また、証明書インストールガイドも紹介します。証明書の導入は RAVPN の証明書認証の要件であるため、シスコのリモート アクセス ソリューシ

ョンに不可欠な要素です。

ライセンス

デバイスで RAVPN 接続を終了するには、ライセンスが必要です。ASA プラットフォームでは、ライセンスがない場合は 2 つの VPN ピアのみサポートされます。FTD プラットフォームでは、ライセンスがなければ、AnyConnect の設定をデバイスに展開できません。COVID-19 の感染拡大を受けて、シスコは無料の一時ライセンスを提供し、シスコデバイスへの RAVPN 実装を支援しています。この件に関する詳細については、以下を参照してくださいCOVID-19 対策向け AnyConnect 緊急ライセンスの取得

AnyConnect 初期設定クイックスタートガイド

最も一般的な設定で AnyConnect Remote Access を実装するには、次のクイックスタートガイドに従ってください。

- ASA でのスプリット トンネリングによる AnyConnect セキュア モビリティ クライアントの設定
- FTD での AnyConnect Remote Access VPN の設定
- FMCによって管理されるFTDの初期AnyConnect設定（ビデオ）

完全な製品設定ガイドについては、以下を参照してください。

完全な設定ガイド

ASA：

- ASA ASDM の設定
- ASA CLI の設定

FTD：

- FDM によって管理されている FTD
- FMC によって管理されている FTD

IOS/IOS-XE：

- SSLVPN 用の IOS ルータ
- SSL VPN 用の IOS XE ルータ（CSR のみ）
- IKEv2 VPN 用の IOS/IOS XE ルータ

証明書インストールガイド

- ASA
- FTD FDM
- FTD FMC
- IOS/IOS-XE

パフォーマンスと拡張性に関する問題

RAVPN の使用量が大幅に増加すると、AnyConnect ユーザがパフォーマンスの問題に直面する可

能性があります。こうした問題を特定して、対処するための緩和策を決定する方法については、以下を参照してください。

問題の現象と特定

CPU 使用率が高い。

CPU 使用率は、VPN ユーザのパフォーマンスに直接影響します。デバイスによって処理される暗号化または復号トラフィックが多くなると、CPU 使用率が高くなります。プラットフォームで処理可能な最大 VPN スループットに近づくと、デバイスの CPU 使用率が高くなる可能性があります。CPU 使用率が高くなるのは、デバイスがオーバーサブスクライブされているためか、あるいは別の問題が原因であるのかを判断する必要があります。

デバイスの CPU 使用率が高くなっているかを確認するには、次のコマンドを実行することをお勧めします。

show process cpu-usage non-zero

show cpu usage

出力例：

```
asa# show processes cpu-usage non-zero
PC         Thread       5Sec     1Min     5Min   Process
0x00000000019da592   0x00007fffd808b040     0.0%     0.0%     0.5%   Logger
0x0000000000844596   0x00007fffd807bd60     0.0%     0.0%     0.1%   CP Processing
0x0000000000c0dc8c   0x00007fffd8074960     0.1%     0.1%     0.1%   ARP Thread
   -          -        43.8%    43.8%    40.3%   DATAPATH-0-2209
   -          -        43.9%    43.8%    40.3%   DATAPATH-1-2210

asa# show cpu usage
CPU utilization for 5 seconds = 88%; 1 minute: 88%; 5 minutes: 82%
```

上記の例では、DATAPATH-0 と DATAPATH-1 で合計 CPU 使用率の 87.7% を占めていることがわかります。この場合、ASA がオーバーサブスクライブされており、この現象の原因が大量のトラフィックの暗号化と復号化によるものかを判断する必要があります。その際、プラットフォームのデータシートに記載されている VPN スループット値と比較できます。

デバイスを通過する 1 秒あたりの VPN の合計トラフィック量を計算するには、***show crypto accelerator statisticsコマンドの Global Statistics セクションで Input bytes と Output bytes を追加します。***ASA または FTD で、*clear crypto accelerator statistics* コマンドを使用して、***show crypto accelerator statistics の出力をクリアします。***一定時間待ってから、以下に示すように ***show crypto accelerator statistics コマンドを実行します。***

```
asa# show crypto accelerator statistics

Crypto Accelerator Status
-------------------------
[Capability]
   Supports hardware crypto: True
   Supports modular hardware crypto: False
   Max accelerators: 2
   Max crypto throughput: 1000 Mbps
   Max crypto connections: 5000
```

```
[Global Statistics]
   Number of active accelerators: 2
   Number of non-operational accelerators: 0
   Input packets: 257353
   Input bytes: 271730225                          <----------------
   Output packets: 2740
   Output error packets: 0
   Output bytes: 57793                             <----------------
[…]
```

特定の間隔でスナップショットをいくつか取り、ビット/秒（bps）に変換可能なバイト単位の平均スループットを取得します。 計算式は以下のとおりです。

$$\frac{[InputBytes + OutputBytes] * 8}{1,000,000 * seconds} = Mbps$$

前述した例では、***clear crypto accelerator statistics コマンドが 0 秒時点で発行されています。***10 秒後に ***show crypto accelerator statistics コマンドが発行され、10 秒間隔で合計バイト数が取得されました。***これらの値を使用して、10 秒間隔で処理された 217Mbps の bps を計算します。より正確な平均値を得るには、複数のスナップショットが必要になることがあります。

これらの値は、暗号化や復号化されたすべてのトラフィック（HTTPS、SSL、IPsec、SSH など）で増加することに注意してください。 この値を使用して、平均 VPN スループットを特定し、データシートと比較できます。平均スループットが、プラットフォームのデータシートに表示される値とほぼ同じである場合、デバイスは暗号化および復号化されたトラフィックによってオーバーサブスクライブされています。

さらに、VPN トラフィックのカウンタが増加しないため、この方法で Firepower 2100 プラットフォームの VPN スループットを判断することはできません。これはCSCvt46830で追跡されています .

最大 VPN 接続数

VPN 接続が最大数に達した場合、接続が中断されてユーザが接続できなくなる可能性があります。AnyConnect Plus または Apex ライセンスをアクティブにすると、VPN ピアに設定されている最大数のロックは解除されますが、最大数に達している間、他のユーザはデバイスへの接続が許可されません。

デバイスにおける最大 VPN 接続可能数を確認するには、***show vpn-sessiondb*** の出力結果を確認します。

```
asa# show vpn-sessiondb
----------------------------------------------------------------------------
VPN Session Summary
----------------------------------------------------------------------------
                            Active : Cumulative : Peak Concur : Inactive
                           ----------------------------------------------
AnyConnect Client             :      10 :         218 :           11 :         0
  SSL/TLS/DTLS                :      10 :         218 :           11 :         0
Clientless VPN                :       0 :          73 :            4
  Browser                     :       0 :          73 :            4
----------------------------------------------------------------------------
Total Active and Inactive     :      10              Total Cumulative :     291
Device Total VPN Capacity     :     250
Device Load                   :      4%
----------------------------------------------------------------------------
```

```
-------------------------------------------------------------------------------
Tunnels Summary
-------------------------------------------------------------------------------
                              Active : Cumulative : Peak Concurrent
                             ------------------------------------------
Clientless                   :      0 :         73 :               4
AnyConnect-Parent            :     10 :        218 :              11
SSL-Tunnel                   :     10 :         77 :              10
DTLS-Tunnel                  :     10 :         65 :              10
-------------------------------------------------------------------------------
Totals                       :     30 :        433
-------------------------------------------------------------------------------
```

プラットフォームでサポートされているユーザ数の合計を確認するには、以下にあるデバイスのデータシートを確認してください。

デバイスが VPN ユーザの最大数に達していないにもかかわらず VPN ユーザが接続できない場合は、TAC からサポートを受けてください。

データシートリファレンス

次のデータシートでは、プラットフォームでサポートされる VPN ユーザの最大数とテストに基づく最大 VPN スループットが共に強調表示されています。IKEv2 および DTLS AnyConnect では、各セクションに記載されている IPsec VPN スループットと同様の合計（集約）スループットが予想されます。

- ASAv
- ASA 5500
- ASA 5585
- Firepower 1000
- Firepower 2100
- FirePOWER 4100
- FirePOWER 9300

考えられる緩和策

スプリット トンネリングの有効化

デフォルトでは、ASA および FTD のグループポリシーでは tunnelall が実装されます。これにより、RA クライアントで生成されたすべてのトラフィックが VPN 経由で送信されて、ヘッドエンドによって処理されます。パケットの暗号化と復号化は CPU 使用率に直接関係するため、企業のセキュリティポリシーにしたがって必要なトラフィックのみが、VPN ヘッドエンドによって処理されるようにすることが重要です。フルトンネルではなくスプリットトンネルポリシーを採用して、不要な負荷から VPN ヘッドエンドを保護することを検討してください。

- ASA スプリットトンネリングガイド
- FTD（FMC）スプリットトンネリングガイド

注：Tunnel All により、企業全体のパラメータ セキュリティ ポリシーが実装されます。スプリットトンネリングはクライアントデバイスに依存して、ユーザのインターネットトラフィックの保護をサポートします。シスコでは、スプリットトンネルポリシー向けに、Umbrella といった VPN ユーザを保護するための付加的セキュリティツールを提供しています。

VPN ロードバランシングの実装（ASA のみ）

VPN ロードバランシングは、ASA プラットフォームに搭載されている機能です。2 つ以上の ASA が VPN セッションの負荷を共有できるようにします。両方のデバイスが 500 VPN ピアをサポートしている場合、それらの間に VPN ロードバランシングを設定することで、合計 1000 個の VPN ピアがデバイス間でサポートされます。この機能を使用すると、単一のデバイスが処理可能な数を超えて、同時 VPN ユーザ数を増やすことができます。ロードバランシングアルゴリズムを含むVPNロードバランシングの詳細については、次を参照してください。VPN ロードバランシング

構成の最適化

プラットフォームで有効になっている付加的サービスによって、デバイスの処理と負荷が増加します。たとえば、IPS、SSL 暗号解読、NAT などが挙げられます。VPN セッションの終了のみを実行する VPN コンセントレータとしてデバイスを設定することを検討してください。

トンネルプロトコルの選択

デフォルトでは、DTLS トンネルを確立するように ASA のグループポリシーが設定されています。VPN ヘッドエンドと AnyConnect クライアントの間で UDP 443 トラフィックがブロックされている場合、TLS に自動的にフォールバックします。VPN スループットパフォーマンスを最大化するには、DTLS または IKEv2 を使用することをお勧めします。DTLS は、プロトコルオーバーヘッドが小さいため、TLS よりもパフォーマンスが向上します。IKEv2 を使用した場合でも TLS より高いスループットが実現します。さらに、AES-GCM暗号を使用すると、パフォーマンスが若干向上する可能性があります。これらの暗号は、TLS 1.2、DTLS 1.2、およびIKEv2で使用できます。

トンネル単位のQoSの適用（FTDのみ）

QoS を実装すると、アウトバウンド方向の AnyConnect ユーザに送信されるトラフィック量を制限できます。これにより、VPN ヘッドエンドは、各リモートアクセスクライアントで出力帯域幅が均等に共有されるようにできます。詳細については、次のサイトを参照してください。FTD の設定

暗号エンジン アクセラレータ バイアスの実装（ASA のみ）

暗号エンジン アクセラレータ バイアスを使用すると、暗号コアを再割り当てして、一方の暗号化プロトコルをもう一方（SSL や IPsec）より優先的に使用できるようになります。 この目的は、VPNトンネルの大部分がIPsecまたはSSLを使用する場合のAnyConnectスループットの最適化です。このコマンドを実装すると、サービスが中断する可能性があるため、メンテナンス時間が必要です。また、パフォーマンス（AnyConnectのスループットとCPU使用率）の向上は、トラフィックプロファイルによって異なる場合があります。VPN ヘッドエンドで SSL セッションのみ、または IPsec セッションのみが終了する場合は、このコマンドを使用すると VPN ヘッドエンドをさらに最適化できる可能性があります。コマンドリファレンスは、以下で確認できます。コマンド リファレンス

現在の暗号コア割り当てを確認するには、コマンド***show crypto accelerator load-balanceを実行します***。このコマンドは、デバイスが処理できる暗号使用率の総量を示しません。これは、各コアに割り当てられているsslまたはipsecトラフィックの比率を示します。デバイスの使用率の概算を求めるには、上記の「**CPU高使用率」の項を参照し**て、計算された値をプラットフォームのデー

タシートの値と比較してください。

リモートアクセスSSLVPNを主に終端するASAプラットフォームでは、crypto engine accelerator-bias sslコマンドを使用してSSLを優先するように暗号化コア割り当てを調整することを推奨***します***。

次の例は、***crypto engine accelerator-bias ssl***コマンドを使用してAnyConnect SSLクライアントに対応するASA5555のコア割り当てを示しています。

```
asa# sh run all crypto engine
crypto engine accelerator-bias ssl
asa# show crypto accelerator load-balance

[..]
                  Crypto SSL Load Balancing Stats:
                  ================================

Engine      Crypto Cores             SSL Sessions            Active Session
                                                             Distribution (%)
======     ==============      ============================   ================
  0        IPSEC 1, SSL 7      Total: 166714  Active:   205         100.0%
[..]
```

アクティブなセッション分散は、プラットフォームの現在の暗号使用率に関係なく、常に100 %になります。

注：暗号化コア再分散ができるのは、次のプラットフォームです。ASA 5585、5580、5545/5555、4110、4120、4140、4150、SM-24、SM-36、SM-44、および ASASM

FAQ

ライセンス

Q：AnyConnect ソフトウェアをダウンロードできませんが、どうしてでしょうか？

A：AnyConnect クライアントをダウンロードできるようにするには、AnyConnect Plus または Apex ライセンスを購入する必要があります。購入後に権限が付与されるはずです。AnyConnect Apex や Plus ライセンスを購入しても権限が付与されない場合は、権限付与についてのケースをオープンして、問題を解決してください。

Q：スマート ライセンス アカウントで AnyConnect ライセンスを 99999 購入済みと表示されるのはどうしてですか？

A：これは、AnyConnect Plus 永久ライセンス、非バンド AnyConnect Plus、Apex ライセンスなどの特定の AnyConnect ライセンスで想定されます。

Q：「使用中」のライセンスが減分されるのは、どのようなときですか？

A：この値は、AnyConnect ライセンスを使用しているデバイスが登録されるたびに減分されます。たとえば、FMC を登録してから、AnyConnect Plus ライセンスをデバイスに追加すると、AnyConnect Plus ライセンスの使用中の値が減分されます。この値は、現在のユーザセッションに基づいては減分**されません。**ASAv デバイスを登録しても、「使用中」の数は減分**されません**

。これは既知の表面的な問題です。購入した承認ユーザ数より多くのデバイスは登録できません。

Q：購入金額はどのように決定されますか。

A：購入金額は、ライセンスで購入された承認ユーザ数によって決まります。たとえば、ユーザ数が 25 の AnyConnect Plus ライセンスには 25 件の購入分が含まれます。

Q：強力な暗号化を実装するにはどうすればよいですか？

A：強力な暗号化を実装するには、登録トークンを作成する際に [このトークンで登録される製品でエクスポート制御機能を許可する（Allow export-controlled functionality on the products registered with this token）] チェックボックスをオンにします。

Q：PAK からスマートライセンスに移行するにはどうすればよいですか？

A：ライセンスについてのケースをオープンする必要があります。

Q：「X」個のユーザライセンスを所有している場合、「X + 1」人以上のユーザがデバイスに接続するとどうなりますか？

A：Apex および Plus ライセンスでは、デバイスの VPN 最大ユーザ数のロックが解除されています。最大 VPN ユーザ数に達していない限り、デバイスは引き続き接続を許可します。VPN ユーザセッションについてデバイスで強制されるものはなく、信用ベースとなっています。VPN のセッション使用数を増やす必要がある場合は、各自の責任で承認ユーザのライセンスを追加購入します。デバイスでサポートされている最大ユーザ数を確認するには、シスコの Web サイトでデバイスのデータシートを確認するか、***show vpn-sessiondb コマンドを実行して、「Device Total VPN Capacity」を確認します。***ASA の場合は、***show version または show vpn-sessiondb license-summary コマンドを実行することもできます。***

Q：ライセンスがデバイスで有効になっているかどうかを確認するにはどうすればよいですか？

A：FTD では、ライセンスがアクティブ化されていない限り AnyConnect の設定を展開できません。ASA では、***show version または show vpn-sessiondb license summary コマンドを実行すると、承認ユーザ数を確認できます。***アクティブ化されたライセンスがない場合、最大ユーザ数は 2 名です。なお ASA では、前述のコマンドに Plus/Apex のライセンス情報は表示されません。これは、機能強化要求 CSCuw74731 で追跡されています。

コンフィギュレーション

Q:VPNのロードバランシングにはどのASAプラットフォームを使用できますか。VPN ロードバランシングクラスタで異なる ASA ハードウェア プラットフォームやソフトウェアバージョンを使用できますか。

A：はい。VPNロードバランシングクラスタは、ASAvを含むさまざまな物理または仮想ASAモデルで構成できます。ただし、通常はクラスタの種類を同じにすることをお勧めします。VPN ロードバランシングクラスタで異なるソフトウェアバージョンが使用されている場合は、IPsec セッ

ションのみがサポートされます。詳細については、「VPNロードバランシングのガイドラインと制限事項」を参照してください。

Q：スプリットトンネリングの設定方法を教えてください。また、スプリットトンネルの設定で特定の種類のアプリケーション トラフィック（Office 365 など）がトンネリングされないようにすることはできますか。

A：さまざまな使用例の設定例については、シスコ コミュニティの記事「AnyConnect スプリットトンネリング（AnyConnect Split Tunneling）」を参照してください。また、スプリットトンネリングとダイナミック スプリットトンネリングを組み合わせてアプリケーションベースのスプリットトンネリングを行うこともできます。Office 365 と Webex に合わせて AnyConnect スプリットトンネリングを最適化する方法の例については、「Microsoft Office365 と Cisco Webex の接続に合わせて AnyConnect を最適化する方法（How to optimize Anyconnect for Microsoft Office365 and Cisco Webex connections）」を参照してください。

Q：AnyConnect を使用して ASA ヘッドエンドに接続すると、「信頼できない証明書の警告」というエラーが表示されます。原因

A：このエラーは、ヘッドエンドが自己署名証明書を使用していることが原因である可能性があります。このエラーを修正するには、認証局から SSL 証明書を購入してヘッドエンド ASA にインストールします。実装の詳細な手順については、「ASAの設定：SSL デジタル証明書のインストールと更新」を参照してください。

Q：Cisco RAVPN ヘッドエンドでワイルドカード証明書はサポートされていますか。

A：はい。ワイルドカードと DNS サブジェクト代替名（SAN）を持つ証明書がサポートされています。

Q：単一のデバイスでロードバランシングとフェールオーバーの両方を使用できますか。

A：アクティブ/スタンバイフェールオーバーは、VPN ロード バランシングでサポートされています。アクティブユニットで障害が発生した場合、スタンバイデバイスが VPN トンネルに影響を与えることなくすぐに引き継ぎを行います。VPN ロードバランシングは、アクティブ/アクティブフェールオーバー構成ではサポートされていません。

モニタリング

Q:ASA CPUの使用状況を監視するために使用できるSNMP MIBはどれですか。

A: CISCO-PROCESS-MIBを使用して、ASAのCPU使用率を監視できます。サポートされるMIBの完全なリストについては、『適応型セキュリティアプライアンスMIBサポートリスト』を参照してください。また、特定の ASA に対してサポートされている SNMP MIB および OID のリストを取得するには、次のコマンドを発行します。***show snmp-server oidlist***

Q：現在 VPN ヘッドエンドに接続しているユーザの数を監視する方法を教えてください。

A：CLI から show vpn-sessiondb を使用して、ASA か FTD、または SNMP MIB の現在のユーザ数を確認します。

CISCO-REMOTE-ACCESS-MONITOR-MIB

トラブルシューティング

Q：一部の AnyConnect VPN ユーザの接続が頻繁に切れているようです。このような問題をトラブルシューティングする方法を教えてください。

A：**VPNの接続解除やその他の一般的なAnyConnectの問題のトラブルシューティングについては**、『AnyConnect VPN Clientトラブルシューティングガイド – 一般的な問題』を参照してください。

Q：一定数のユーザが VPN ヘッドエンドに接続すると、それ以上ユーザが接続できなくなります。ライセンスはデバイスでアクティブ化されており、***show vpn-sessiondb にはデバイスでさらに多くのユーザを処理できると示されます。***何が問題なのでしょうか。

A：それらのユーザの VPN ローカルアドレスプールで接続中のユーザの数が使用可能なアドレスの数を超えていないことを確認します。これは ***show ip local pool [pool-name]*** コマンドで確認できます。別の原因としては、古いプラットフォームで ***vpn-sessiondb max-anyconnect-premium-or-essentials-limit*** コマンドの値が低く設定されていることが考えられます。これについては、***show run all vpn-sessiondb*** コマンドで確認できます。これが問題の場合は、値を増やすか、こうした制限を回避するためにコマンドを削除します。

追加サポートについて

詳細については、TACにお問い合わせください。有効なサポート契約が必要です。各国のシスコサポートの連絡先

Cisco VPN コミュニティには、ここからアクセスすることもできます。

また、TAC Security Show Podcastsも確認できます

参考資料

AnyConnect の導入や COVID-19 関連の一般的な問題への対応に役立つその他のリソースへの追加リンクについては、以下をご覧ください。

- シスコセキュリティがリモートワーカーの増加に対応（Cisco Security Responds to Increase in Remote Workers）：シスココミュニティ
- AnyConnect Ordering Guide（AnyConnect 発注ガイド）
- AnyConnect ライセンスに関する FAQ（よくある質問）
- AnyConnect VPN, ASA, and FTD FAQ for Secure Remote Workers