ASA：マルチコンテキスト モードのリモート アクセス（AnyConnect）VPN

概要

このドキュメントでは、CLIを使用して、Cisco適応型セキュリティアプライアンス(ASA)ファイアウォールでリモートアクセス(RA)仮想プライベートネットワーク(VPN)をマルチコンテキスト(MC)モードで設定する方法について説明します。マルチコンテキストモードのCisco ASAでサポート/サポートされていない機能と、RA VPNに関するライセンス要件が表示されます。

前提条件

要件

次の項目に関する知識があることが推奨されます。

- ASA AnyConnect SSLの設定
- ASAマルチコンテキスト設定

使用するコンポーネント

このドキュメントの情報は、次のソフトウェアとハードウェアのバージョンに基づいています。

- AnyConnectセキュアモビリティクライアントバージョン4.4.00243
- ASAソフトウェアバージョン9.6(2)を搭載したASA5525 X 2

注：AnyConnect VPN Clientパッケージは、Cisco Software Download（登録ユーザ専用）からダウンロードしてください。

注：このドキュメントの情報は、特定のラボ環境にあるデバイスに基づいて作成されました。このドキュメントで使用するすべてのデバイスは、初期（デフォルト）設定の状態から起動しています。対象のネットワークが実稼働中である場合には、どのようなコマンドについても、その潜在的な影響について確実に理解しておく必要があります。

背景説明

マルチコンテキストは、アプリケーションの複数の独立したコピーを同じハードウェア上で同時に実行し、各コピー（または仮想デバイス）を個別の物理デバイスとしてユーザに表示する仮想化の形態です。これにより、1つのASAを複数の独立したユーザに対して複数のASAとして認識できます。ASAファミリは、初期リリース以降、仮想ファイアウォールをサポートしています。ただし、ASAではリモートアクセスの仮想化サポートはありませんでした。9.0リリースでは、マルチコンテキストのVPN LAN2LAN(L2L)サポートが追加されました。

注：9.5.2からASAへのVPNリモートアクセス(RA)接続に対するマルチコンテキストベース

の仮想化サポート。

9.6.2**以降ではフラッシュ**仮想化がサポートされています。つまり、コンテキストごとにAnyconnectイメージを使用できます。

マルチコンテキストの機能履歴

ASA 9.6(2)で追加された新機能

機能
マルチコンテキストモードのプリフィル/ユーザ名/証明書からの機能
リモートアクセスVPNのフラッシュ仮想化
マルチコンテキストデバイスでサポートされるAnyConnectクライアントプロファイル
マルチコンテキストモードでのAnyConnect接続のステートフルフェールオーバー
リモートアクセスVPNダイナミックアクセスポリシー(DAP)は、マルチコンテキストモードでサポートさ
リモートアクセスVPN CoA（認可変更）は、マルチコンテキストモードでサポートされています
リモートアクセスVPNローカリゼーションは、マルチコンテキストモードでサポートされています
コンテキストごとのパケットキャプチャストレージがサポートされます。

ASA 9.5(2)の機能

機能	
AnyConnect 4.x以降(SSL VPNのみ。IKEv2サポートなし)	ASAへのVPNリモートアクセス(RA)接続に対するマルチコ
一元化されたAnyConnectイメージ設定	• フラッシュストレージは仮想化されません。 • AnyConnectイメージは管理コンテキストでグローバル
AnyConnectイメージのアップグレード	AnyConnectクライアントプロファイルは、マルチコンテキ Secure Mobility Clientリリース4.2.00748または4.3.03013
AnyConnect接続のコンテキストリソース管理	• コンテキストごとの最大ライセンス使用量を制御可能 • コンテキストごとのライセンスバーストを可能にする

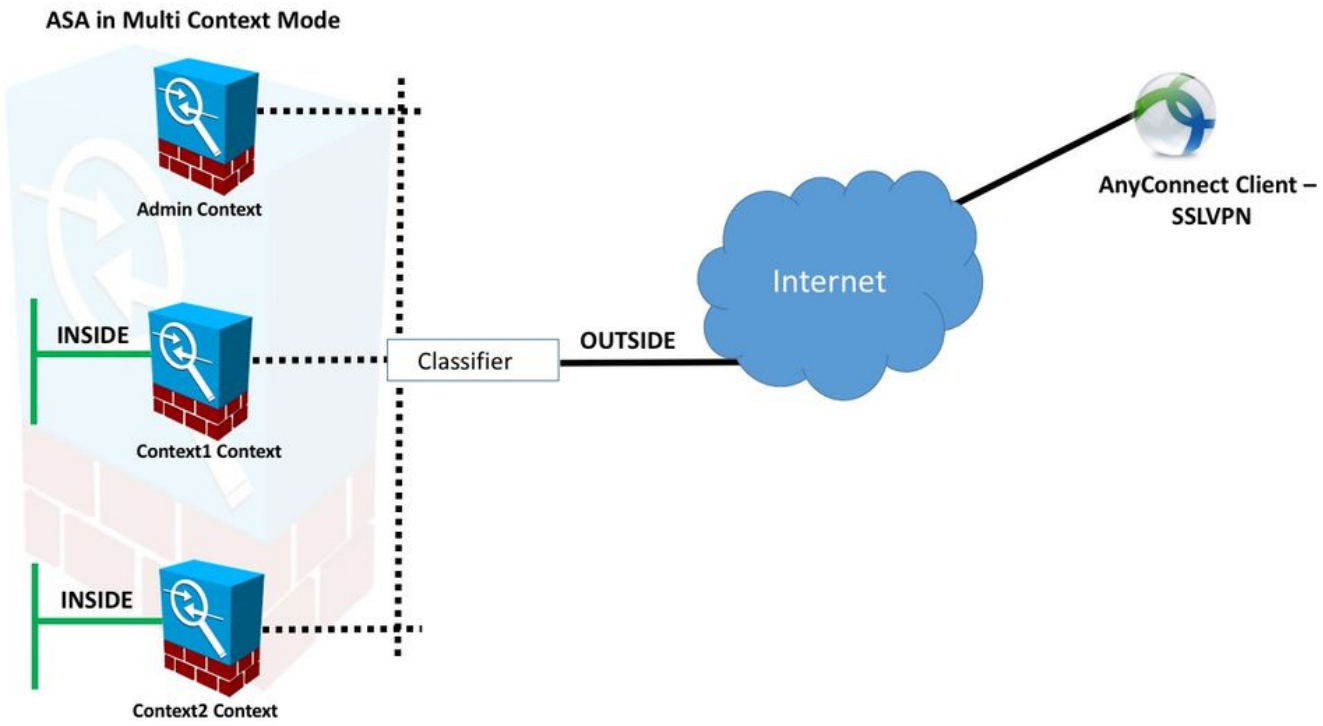
ライセンス

- AnyConnect Apexライセンスが必要
- Essentialsライセンスは無視されるか、許可されない
- コンテキストごとの最大ライセンス使用量を制御可能な構成
- コンテキストごとのライセンスバーストを可能にする設定

設定

注：このセクションで使用されるコマンドの詳細については、Command Lookup Tool（登録ユーザ専用）を使用してください。

ネットワーク図



注： この例の複数のコンテキストはインターフェイス(OUTSIDE)を共有し、分類子はインターフェイス固有の（自動または手動の）MACアドレスを使用してパケットを転送します。セキュリティアプライアンスが複数のコンテキストでパケットを分類する方法の詳細については、『ASAによるパケットの分類方法』を参照してください

次の設定手順は、ASA 9.6.2以降のバージョンを使用しており、利用可能な新機能の一部を示しています。9.6.2(および9.5.2)より前のASAバージョンの設定手順の違いは、このドキュメントの「付録A」に記載されています。

リモートアクセスVPNのセットアップに必要なシステムコンテキストとカスタムコンテキストの設定を次に示します。

システムコンテキストの初期設定

まず、システムコンテキストで、フェールオーバー、VPNリソース割り当て、カスタムコンテキスト、およびApexライセンス検証を設定します。手順と設定については、このセクションと次のセクションで説明します

ステップ1：フェールオーバーの構成。

```
 !! Active Firewall

failover
failover lan unit primary
failover lan interface LAN_FAIL GigabitEthernet0/3
failover link LAN_FAIL GigabitEthernet0/3
failover interface ip LAN_FAIL 10.1.1.1 255.255.255.252 standby 10.1.1.2
failover group 1
failover group 2

 !! Secondary Firewall
```

```
failover
failover lan unit secondary
failover lan interface LAN_FAIL GigabitEthernet0/3
failover link LAN_FAIL GigabitEthernet0/3
failover interface ip LAN_FAIL 10.1.1.1 255.255.255.252 standby 10.1.1.2
failover group 1
failover group 2
```

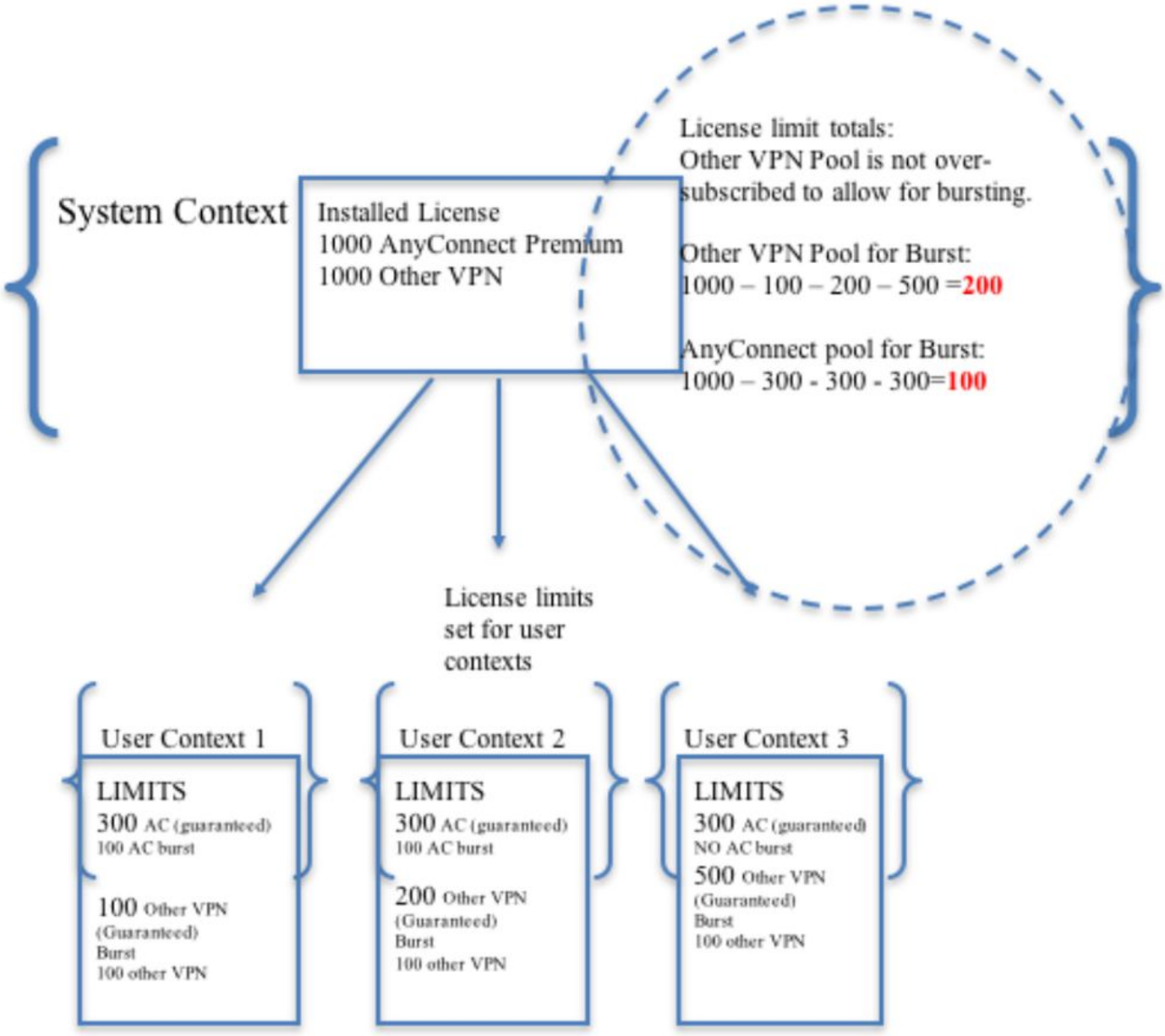
ステップ2:VPNリソースの割り当て

既存のクラス設定で設定されます。ライセンスは、ライセンス数またはコンテキストごとの合計に対する割合で許可されます

MC RAVPNに導入された新しいリソースタイプ：

- VPN AnyConnect:コンテキストに対して保証され、オーバーサブスクライブされる可能性がある
- VPNバーストAnyConnect:保証された制限を超えるコンテキスト追加ライセンスを許可します。バーストプールは、コンテキストに対して保証されていないライセンスで構成され、先着順でバーストコンテキストに許可されます

VPNライセンスプロビジョニングモデル：



注：ASA5585は最大10,000のCisco AnyConnectユーザセッションを提供します。この例では、コンテキストごとに4000のCisco AnyConnectユーザセッションが割り当てられます。

```
class resource02
 limit-resource VPN AnyConnect 4000
 limit-resource VPN Burst AnyConnect 2000

class resource01
 limit-resource VPN AnyConnect 4000
 limit-resource VPN Burst AnyConnect 2000
```

ステップ3：コンテキストを設定し、リソースを割り当てます。

注：この例では、GigabitEthernet0/0がすべてのコンテキストで共有されています。

```
admin-context admin
```

```
context admin
  allocate-interface GigabitEthernet0/0
  config-url disk0:/admin

context context1
  member resource01
  allocate-interface GigabitEthernet0/0
  allocate-interface GigabitEthernet0/1
  config-url disk0:/context1
  join-failover-group 1

context context2
  member resource02
  allocate-interface GigabitEthernet0/0
  allocate-interface GigabitEthernet0/2
  config-url disk0:/context2
  join-failover-group 2
```

ステップ4: ApexライセンスがASAにインストールされていることを確認します。詳細については、次のリンクを参照してください。

アクティベーションキーのアクティブ化または非アクティブ化

ステップ5:Anyconnectイメージパッケージを設定します。使用されているASAバージョンに応じて、Anyconnectイメージをロードし、RA VPNを設定する方法が2つあります。バージョンが9.6.2以上の場合は、フラッシュ仮想化を使用できます。9.6.2より古いバージョンについては、付録Aを参照してください

> **注：**9.6.2以降では、フラッシュ仮想化がサポートされています。つまり、コンテキストごとにAnyconnectイメージを使用できます。

フラッシュ仮想化

リモートアクセスVPNでは、AnyConnectパッケージ、ホストスキャンパッケージ、DAP設定、プラグイン、カスタマイズ、ローカリゼーションなどのさまざまな設定やイメージのフラッシュストレージが必要です。9.6.2より前のマルチコンテキストモードでは、ユーザコンテキストはフラッシュのどの部分にもアクセスできず、フラッシュは管理され、システムコンテキストからのみシステム管理者にアクセスできます。

この制限を解決するため、フラッシュ上のファイルのセキュリティとプライバシーを維持し、コンテキスト間でフラッシュを公平に共有できるようにするため、マルチコンテキストモードのフラッシュに仮想ファイルシステムを作成します。これにより、ユーザごとに異なるAnyConnectイメージをインストールできます。また、AnyConnectイメージを共有できるようにすることで、これらのイメージが消費するメモリ量を削減できます。共有ストレージは、すべてのコンテキストに共通するファイルやパッケージを保存するために使用されます。

> **注：** システム管理者は、ディレクトリ構造を作成し、すべてのプライベートファイルと共有ファイルを別々のディレクトリに編成して、コンテキストが共有ストレージとしてアクセスできるように設定する必要があります。

すべてのコンテキストは、独自のプライベート・ストレージに対する読み取り/書き込み/削除の権限を持ち、共有ストレージに対する読み取り専用アクセス権を持ちます。共有ストレージへの書き込みアクセス権を持つのは、システムコンテキストだけです.

次の構成では、プライベート・ストレージを示すようにカスタム・コンテキスト1が構成され、共有ストレージを示すようにカスタム・コンテキスト2が構成されます。

プライベートストレージ

コンテキストごとに1つのプライベート記憶域を指定できます。このディレクトリは、コンテキスト内（およびシステム実行スペースから）読み取り/書き込み/削除が可能です。 指定されたパスの下に、ASAはコンテキストの後にサブディレクトリを作成します。

たとえば、context1でパスにdisk0:/private-storageを指定すると、ASAはこのコンテキストのサブディレクトリをdisk0:/private-storage/context1/に作成します。

共有ストレージ

コンテキストごとに1つの読み取り専用の共有ストレージ領域を指定できます。すべてのコンテキスト（AnyConnectパッケージなど）で共有できる一般的な大きなファイルの重複を減らすために、共有ストレージ領域を使用できます。

プライベートストレージ領域を使用するための設定

```
!! Create a directory in the system context.
ciscoasa(config)# mkdir private_context1

!! Define the directory as private storage url in the respective context.

ciscoasa(config)# context context1 ciscoasa(config-ctx)# storage-url private
disk0:/private_context1 context1

!! Transfer the anyconnect image in the sub directory.
ciscoasa(config)# copy flash:/anyconnect-win-4.2.01035-k9.pkg flash:/private_context1/context1
```

共有ストレージスペースを使用するための設定

```
!! Create a directory in the system context.

ciscoasa(config)# mkdir shared

!! Define the directory as shared storage url in the respective contexts.

ciscoasa(config)# context context2 ciscoasa(config-ctx)# storage-url shared disk0:/shared shared

!! Transfer the anyconnect image in the shared directory.
ciscoasa(config)# copy disk0:/anyconnect-win-4.3.05019-k9.pkg disk0:/shared
```

それぞれのコンテキストでイメージを確認します

```
!! Custom Context 1 configured for private storage.

ciscoasa(config)#changeto context context1
ciscoasa/context1(config)# show context1:
213 19183882 Jun 12 2017 13:29:51 context1:/anyconnect-win-4.2.01035-k9.pkg

!! Custom Context 2 configured for shared storage.

ciscoasa(config)#changeto context context2
```

```
ciscoasa/context2(config)# show shared:
195 25356342 May 24 2017 08:07:02 shared:/anyconnect-win-4.3.05017-k9.pkg
```

ステップ6:上記のフラッシュ仮想化設定を含むシステムコンテキストの設定の要約を次に示します。

システムコンテキスト

```
context context1
member resource01
allocate-interface GigabitEthernet0/0
 storage-url private disk0:/private_context1 context1
config-url disk0:/context1.cfg
join-failover-group 1
!
context context2
member resource02
allocate-interface GigabitEthernet0/1
storage-url shared disk0:/shared shared
config-url disk0:/context2.cfg
join-failover-group 2
```

手順 7：次に示すように、2つのカスタムコンテキストを設定します

カスタムコンテキスト1

```
!! Enable WebVPN on respective interfaces

webvpn
enable outside
anyconnect image context1:/anyconnect-win-4.2.01035-k9.pkg 1
anyconnect enable
tunnel-group-list enable

!! IP pool and username configuration

ip local pool mypool 192.168.1.1-192.168.50.1 mask 255.255.0.0
username cisco password cisco

!! Configure the required connection profile for SSL VPN

access-list split standard permit 192.168.1.0 255.255.255.0

group-policy GroupPolicy_MC_RAVPN_1 internal
group-policy GroupPolicy_MC_RAVPN_1 attributes
banner value "Welcome to Context1 SSLVPN"
wins-server none
dns-server value 192.168.20.10
vpn-tunnel-protocol ssl-client
split-tunnel-policy tunnelspecified
split-tunnel-network-list value split
default-domain value cisco.com

tunnel-group MC_RAVPN_1 type remote-access
tunnel-group MC_RAVPN_1 general-attributes
address-pool mypool
default-group-policy GroupPolicy_MC_RAVPN_1
tunnel-group MC_RAVPN_1 webvpn-attributes
group-alias MC_RAVPN_1 enable
```

カスタムコンテキスト2

```
!! Enable WebVPN on respective interfaces

webvpn
enable outside
anyconnect image shared:/anyconnect-win-4.3.05017-k9.pkg 1
anyconnect enable
tunnel-group-list enable

!! IP pool and username configuration

ip local pool mypool 192.168.51.1-192.168.101.1 mask 255.255.0.0
username cisco password cisco

!! Configure the required connection profile for SSL VPN

access-list split standard permit 192.168.1.0 255.255.255.0

group-policy GroupPolicy_MC_RAVPN_2 internal
group-policy GroupPolicy_MC_RAVPN_2 attributes
banner value "Welcome to Context2 SSLVPN"
wins-server none
dns-server value 192.168.60.10
vpn-tunnel-protocol ssl-client
split-tunnel-policy tunnelspecified
split-tunnel-network-list value split
default-domain value cisco.com
!
!
tunnel-group MC_RAVPN_2 type remote-access
tunnel-group MC_RAVPN_2 general-attributes
address-pool mypool
default-group-policy GroupPolicy_MC_RAVPN_2
tunnel-group MC_RAVPN_2 webvpn-attributes
group-alias MC_RAVPN_2 enable
```

確認

ここでは、設定が正常に機能しているかどうかを確認します。

Apexライセンスがインストールされているかどうかを確認する

ASAはAnyConnect Apexライセンスを特に認識しませんが、次のようなApexライセンスのライセンス特性を適用します。

- プラットフォームの制限に対するAnyConnect Premiumライセンス
- モバイル向けAnyConnect
- AnyConnect for Cisco VPN Phone
- Advanced Endpoint Assessment

AnyConnect Apexライセンスがインストールされていないため、接続がブロックされると、syslogが生成されます。

AnyConnectパッケージがカスタムコンテキスト(9.6.2以降)で使用可能かどうかを確認します。

```
! AnyConnect package is available in context1

 ciscoasa/context1(config)# show context1:

213 19183882 Jun 12 2017 13:29:51 context1:/anyconnect-win-4.2.01035-k9.pkg

ciscoasa/pri/context1/act# show run webvpn
webvpn
enable outside
anyconnect image context1:/anyconnect-win-4.2.01035-k9.pkg 1
anyconnect enable
tunnel-group-list enable
```

カスタムコンテキストの下にイメージが存在しない場合は、Anyconnectイメージの設定(9.6.2以降)を参照してください。

ユーザがカスタムコンテキストでAnyConnect経由で接続できるかどうかを確認する

ヒント：より良い表示のために、下のビデオをフルスクリーンで見る。

```
!! One Active Connection on Context1

ciscoasa/pri/context1/act# show vpn-sessiondb anyconnect

Session Type: AnyConnect

Username : cisco Index : 5
Assigned IP : 192.168.1.1 Public IP : 10.142.168.102
Protocol : AnyConnect-Parent SSL-Tunnel DTLS-Tunnel
License : AnyConnect Premium, AnyConnect for Mobile
Encryption : AnyConnect-Parent: (1)none SSL-Tunnel: (1)AES-GCM-256 DTLS-Tunnel: (1)AES256
Hashing : AnyConnect-Parent: (1)none SSL-Tunnel: (1)SHA384 DTLS-Tunnel: (1)SHA1
Bytes Tx : 3186 Bytes Rx : 426
Group Policy : GroupPolicy_MC_RAVPN_1 Tunnel Group : MC_RAVPN_1
Login Time : 15:33:25 UTC Thu Dec 3 2015
Duration : 0h:00m:05s
Inactivity : 0h:00m:00s
VLAN Mapping : N/A VLAN : none
Audt Sess ID : 0a6a2c2600005000566060c5
Security Grp : none

!! Changing Context to Context2

ciscoasa/pri/context1/act# changeto context context2

!! One Active Connection on Context2

ciscoasa/pri/context2/act# show vpn-sessiondb anyconnect

Session Type: AnyConnect

Username : cisco Index : 1
Assigned IP : 192.168.51.1 Public IP : 10.142.168.94
Protocol : AnyConnect-Parent SSL-Tunnel DTLS-Tunnel
License : AnyConnect Premium
```

```
Encryption : AnyConnect-Parent: (1)none SSL-Tunnel: (1)AES256 DTLS-Tunnel: (1)AES256
Hashing : AnyConnect-Parent: (1)none SSL-Tunnel: (1)SHA1 DTLS-Tunnel: (1)SHA1
Bytes Tx : 10550 Bytes Rx : 1836
Group Policy : GroupPolicy_MC_RAVPN_2 Tunnel Group : MC_RAVPN_2
Login Time : 15:34:16 UTC Thu Dec 3 2015
Duration : 0h:00m:17s
Inactivity : 0h:00m:00s
VLAN Mapping : N/A VLAN : none
Audt Sess ID : 0a6a2c2400001000566060f8
Security Grp : none

!! Changing Context to System

ciscoasa/pri/context2/act# changeto system

!! Notice total number of connections are two (for the device)

ciscoasa/pri/act# show vpn-sessiondb license-summary
----------------------------------------------------------------------------
VPN Licenses and Configured Limits Summary
----------------------------------------------------------------------------
Status : Capacity : Installed : Limit
---------------------------------------
AnyConnect Premium : ENABLED : 10000 : 10000 : NONE
Other VPN (Available by Default) : ENABLED : 10000 : 10000 : NONE
AnyConnect for Mobile : ENABLED(Requires Premium or Essentials)
Advanced Endpoint Assessment : ENABLED(Requires Premium)
AnyConnect for Cisco VPN Phone : ENABLED
VPN-3DES-AES : ENABLED
VPN-DES : ENABLED
----------------------------------------------------------------------------

----------------------------------------------------------------------------
VPN Licenses Usage Summary
----------------------------------------------------------------------------
Local : Shared : All : Peak : Eff. :
In Use : In Use : In Use : In Use : Limit : Usage
-------------------------------------------------
AnyConnect Premium : 2 : 0 : 2 : 2 : 10000 : 0%
AnyConnect Client : : 2 : 2 : 0%
AnyConnect Mobile : : 2 : 2 : 0%
Other VPN : : 0 : 0 : 10000 : 0%
Site-to-Site VPN : : 0 : 0 : 0%
----------------------------------------------------------------------------

!! Notice the resource usage per Context

ciscoasa/pri/act# show resource usage all resource VPN AnyConnect
Resource Current Peak Limit Denied Context
AnyConnect 1 1 4000 0 context1
AnyConnect 1 1 4000 0 context2
```

トラブルシュート

ここでは、設定のトラブルシューティングに使用できる情報を示します。

AnyConnectのトラブルシューティング

ヒント：ASAにApexライセンスがインストールされていない場合、AnyConnectセッションは次のsyslogで終了します。

%ASA-6-725002:デバイスはTLSv1セッションのクライアント
OUTSIDE:10.142.168.86/51577 ~ 10.106.44.38/443とのSSLハンドシェイクを完了しました
%ASA-6-113012:AAA user authentication Successful :ローカルデータベース：ユーザ= cisco
%ASA-6-113009:ユーザのAAA取得デフォルトグループポリシー (GroupPolicy_MC_RAVPN_1) = cisco
%ASA-6-113008:AAAトランザクションステータスACCEPT:ユーザ= cisco
%ASA-3-716057:グループユーザIP <10.142.168.86>セッションが終了しました。AnyConnect Apexライセンスはありません
%ASA-4-113038:グループユーザIP <10.142.168.86> AnyConnect親セッションを作成できません。

付録A:9.6.2より前のバージョンのAnyconnectイメージ設定

AnyConnectイメージは、ASAバージョン9.6.2より前の管理コンテキストでグローバルに設定されます(この機能は9.5.2から使用できます)。これは、フラッシュストレージが仮想化されておらず、システムコンテキストからのみアクセスできるためです。

ステップ5.1:システムコンテキストでAnyConnectパッケージファイルをフラッシュにコピーします。

システムコンテキスト：

```
ciscoasa(config)# show flash:

195 25356342 May 24 2017 08:07:02 anyconnect-win-4.3.05017-k9.pkg
```

ステップ 5.2： Anyconnectイメージの設定 Adminコンテキストで実行します。

管理コンテキスト：

```
webvpn
anyconnect image disk0:/anyconnect-win-4.3.05017-k9.pkg 1
anyconnect enable
```

注：Anyconnectイメージは、管理コンテキストでのみ設定できます。すべてのコンテキストが、このグローバルAnyconnectイメージ設定を自動的に参照します。

カスタムコンテキスト1:

```
 !! Shared interface configuration - OUTSIDE (GigabitEthernet0/0)

interface GigabitEthernet0/0
nameif OUTSIDE
security-level 0
ip address 10.106.44.38 255.255.255.0 standby 10.106.44.39

!! Enable WebVPN on respective interfaces

webvpn
enable OUTSIDE
anyconnect enable
```

```
!! IP pool and username configuration

ip local pool mypool 192.168.1.1-192.168.50.1 mask 255.255.0.0

username cisco password cisco

!! Configure the require connection profile for SSL VPN

group-policy GroupPolicy_MC_RAVPN_1 internal
group-policy GroupPolicy_MC_RAVPN_1 attributes
banner value "Welcome to Context1 SSLVPN"
wins-server none
dns-server value 192.168.20.10
vpn-tunnel-protocol ssl-client
split-tunnel-policy tunnelspecified
split-tunnel-network-list value split
default-domain value cisco.com

tunnel-group MC_RAVPN_1 type remote-access
tunnel-group MC_RAVPN_1 general-attributes
address-pool mypool
default-group-policy GroupPolicy_MC_RAVPN_1
tunnel-group MC_RAVPN_1 webvpn-attributes
group-alias MC_RAVPN_1 enable
group-url https://10.106.44.38/context1 enable
```

カスタムコンテキスト2:

```
!! Shared interface configuration - OUTSIDE (GigabitEthernet0/0)

interface GigabitEthernet0/0
nameif OUTSIDE
security-level 0
ip address 10.106.44.36 255.255.255.0 standby 10.106.44.37

!! Enable WebVPN on respective interface

webvpn
enable OUTSIDE
anyconnect enable

!! IP pool and username configuration

ip local pool mypool 192.168.51.1-192.168.101.1 mask 255.255.0.0

username cisco password cisco

!! Configure the require connection profile for SSL VPN

group-policy GroupPolicy_MC_RAVPN_2 internal
group-policy GroupPolicy_MC_RAVPN_2 attributes
banner value "Welcome to Context2 SSLVPN"
wins-server none
dns-server value 192.168.60.10
vpn-tunnel-protocol ssl-client
split-tunnel-policy tunnelspecified
split-tunnel-network-list value split
default-domain value cisco.com

tunnel-group MC_RAVPN_2 type remote-access
tunnel-group MC_RAVPN_2 general-attributes
address-pool mypool
```

```
default-group-policy GroupPolicy_MC_RAVPN_2
tunnel-group MC_RAVPN_2 webvpn-attributes
group-alias MC_RAVPN_2 enable
group-url https://10.106.44.36/context2 enable
```

AnyConnectパッケージが管理コンテキストにインストールされていて、カスタムコンテキスト(9.6.2より前)で使用できるかどうかを確認します。

```
!! AnyConnect package is installed in Admin Context

ciscoasa/pri/admin/act# show run webvpn
webvpn
anyconnect image disk0:/anyconnect-win-3.1.10010-k9.pkg 1
anyconnect enable

ciscoasa/pri/admin/act# show webvpn anyconnect
1. disk0:/anyconnect-win-3.1.10010-k9.pkg 1 dyn-regex=/Windows NT/
CISCO STC win2k+
3,1,10010
Hostscan Version 3.1.10010
Wed 07/22/2015 12:06:07.65

1 AnyConnect Client(s) installed

!! AnyConnect package is available in context1

ciscoasa/pri/admin/act# changeto context context1

ciscoasa/pri/context1/act# show run webvpn
webvpn
enable OUTSIDE
anyconnect enable
tunnel-group-list enable

ciscoasa/pri/context1/act# show webvpn anyconnect
1. disk0:/anyconnect-win-3.1.10010-k9.pkg 1 dyn-regex=/Windows NT/
CISCO STC win2k+
3,1,10010
Hostscan Version 3.1.10010
Wed 07/22/2015 12:06:07.65

1 AnyConnect Client(s) installed
```

参考資料

リリース ノート：9.5(2)

リリース ノート：9.6(2)

関連情報

- Cisco ASA 5500 シリーズ適応型セキュリティ アプライアンス
- AnyConnect VPN クライアントのトラブルシューティング ガイド - 一般的な問題
- AnyConnect セッションの管理、モニタリング、およびトラブルシューティング
- テクニカル サポートとドキュメント – Cisco Systems
- https://www.cisco.com/c/en/us/td/docs/security/asa/roadmap/asa_new_features.pdf