Cisco ASA 5500 から Cisco Adaptive Security Virtual Appliance への移行

2014 年 4 月 24 日

目次

概要

ASAv は Cisco ASA 5500 と共通のソフトウェア基盤を共有しますが、ASAv で ASA 5500 の設定を直接使用することはできません。ASA 5500 の設定を変更し、ASAv ではサポートされないすべての機能の設定を削除する必要があります。

移行がサポートされるプラットフォーム

8.4（x）以降のソフトウェアがインストールされているすべての ASA ハードウェア デバイスを移行できます。

Cisco Systems, Inc.
www.cisco.com

サポートされない機能

ASAv は、次の ASA 機能をサポートしません。

- クラスタ
- マルチ コンテキスト モード
- アクティブ / アクティブ フェールオーバー
- EtherChannel
- Advanced Inspection and Prevention Security Services Module（AIP SSM）
- Content Security and Control Security Services Module（CSC SSM）
- Context Security（CX）Module
- AnyConnect Premium（共有）ライセンス

Cisco ASA 5500 設定から ASAv 設定への変更

ASA 5500 設定を ASAv 設定に移行するには、次のガイドラインに従ってください。

ガイドライン

- CLI または ASDM を使用して移行を実行できます。
- ASDM を使用するには、ASAv の HTTP アクセスを設定する必要があります。
- ASAv のソース コンフィギュレーション ファイルを変更するには、テキスト エディタを使用します。
- ASAv はマルチ コンテキスト モードをサポートしませんが、セキュリティ コンテキストの設定を ASAv の設定に変換できます。
- ASAv は ASA クラスタリングをサポートしません。したがって、ASAv で使用する前に、クラスタ関連のインターフェイス設定を削除する必要があります。

（注） ASAv に未変更のハードウェア構成をコピーできます。ただし、このバージョンの仮想プラットフォームでサポートされないコマンドには、「無効な入力」などのエラーや警告が表示されます。

手順の詳細

次の表に、ASA 5500 の設定を ASAv の設定に変更するために必要な手順を示します。

ステップ	タスクの説明	参照先
1.	ASA 5500 設定をバージョン 9.2(1) にアップグレードするには、組み込みの ASAv の移行ツールを活用できます。スタートアップ コンフィギュレーションが以前の ASA バージョンと一致する場合、再起動時にこのツールがアクティブになります。バージョン 9.2(1) は、スタートアップ コンフィギュレーションに最初に保存されていたバージョンから変更されている機能関連のコマンドを移行します。	設定の移行に関する詳細情報とアップグレードのガイドラインについては、ASA のリリース ノートを参照してください。
2.	ASA 5500 ファイアウォール コンフィギュレーション ファイルをソース デバイスから取得し、ローカル ファイル システムに保存します。	『General Operations CLI Configuration Guide（CLI コンフィギュレーション ガイド（一般的な操作））』の「Managing Software and Configurations（ソフトウェアとコンフィギュレーションの管理）」の章を参照してください。

ステップ	タスクの説明	参照先
3.	次の 2 つのオプションのいずれかを選択してください。 **CLI の使用** 次の VPN コンフィギュレーション ファイルをエクスポートします。 • クライアントレス Secure Socket Layer（SSL）のカスタマイズまたはプラグイン。 • AnyConnect、Cisco Secure Desktop および ASA 5500 からのホスト スキャン イメージ。 • ASA 5500 からのアイデンティティ証明書の PKCS12 ファイル。 （注） コンフィギュレーションで指定されたパスにファイルが配置されていることを確認してください。	『VPN CLI Configuration Guide（VPN CLI コンフィギュレーション ガイド）』の「Clientless SSL VPN Overview（クライアントレス SSL VPN の設定）」の章を参照してください。 『VPN CLI Configuration Guide（VPN CLI コンフィギュレーション ガイド）』の「Configuring AnyConnect VPN Client Connections（AnyConnect VPN Client 接続の設定）」の章を参照してください。 『Cisco Secure Desktop Configuration Guide for Cisco ASA 5500 Series Administrators（Cisco ASA 5500 Series 管理者用 Cisco Secure Desktop コンフィギュレーション ガイド）』の「Installing and Enabling CSD（CSD のインストールおよびイネーブル）」の章を参照してください。 『VPN CLI Configuration Guide（VPN CLI コンフィギュレーション ガイド）』の「Configuring AnyConnect Host Scan（AnyConnect ホスト スキャンの設定）」の章を参照してください。 『General Operations CLI Configuration Guide（CLI コンフィギュレーション ガイド（一般的な操作））』の「Configuring Digital Certificates（デジタル証明書の設定）」の章を参照してください。 『VPN CLI Configuration Guide（VPN CLI コンフィギュレーション ガイド）』の「Configuring Policy Groups（グループ ポリシーの設定）」の章を参照してください。
	ASDM の使用 このプロセスを効率化するには、ASDM のバックアップ ユーティリティを使用し、ソース ファイルを保存することを勧めています。これらの VPN 固有ファイルには、すべてのセキュリティ イメージ、アイデンティティ証明書、VPN 事前共有キー、すべての SSL VPN 設定が含まれる場合があります。 （注） バックアップ プロセスから除外する実行コンフィギュレーションとスタートアップ コンフィギュレーションのチェックボックスをオフにしてください。	『General Operations ASDM Configuration Guide（ASDM コンフィギュレーション ガイド（一般的な操作））』の「Managing Software and Configurations（ソフトウェアとコンフィギュレーションの管理）」の章を参照してください。
4.	次に示すように ASA 5500 の設定を ASAv の設定に変更します。	—
a.	インターフェイスの設定を変更して、ASAv の使用可能なインターフェイスに一致させます：Management 0/0 および GigabitEthernet 0/0 - 0/8（10 インターフェイスの展開の場合）。 EtherChannel インターフェイスを削除します。	『General Operations CLI Configuration Guide（CLI コンフィギュレーション ガイド（一般的な操作））』の「Starting Interface Configuration（ASA 5510 and Higher）（インターフェイス コンフィギュレーションの開始（ASA 5510 以降）」を参照してください。

ステップ	タスクの説明	参照先
b.	Content Security and Control Security Services Module コンフィギュレーションを削除します（インストールされている場合）。	『Firewall CLI Configuration Guide（ファイアウォール CLI コンフィギュレーション ガイド）』の「Configuring the ASA CSC Module（ASA CSC モジュールの設定）」の章を参照してください。
c.	Advanced Inspection and Prevention Security Services Module コンフィギュレーションを削除します（インストールされている場合）。	『Firewall CLI Configuration Guide（ファイアウォール CLI コンフィギュレーション ガイド）』の「Configuring the ASA IPS Module（ASA IPS モジュールの設定）」の章を参照してください。
d.	CX モジュール コンフィギュレーションを削除します（インストールされている場合）。	『Configuring the ASA IPS Module（ファイアウォール CLI コンフィギュレーション ガイド）』の「Configuring the ASA CX Module（ASA CX モジュールの設定）」の章を参照してください。
e.	次のサポートされていない機能を削除します。 • マルチ コンテキスト モード • クラスタリング：**ip address** コマンドから **cluster-pool** および **mgmt-pool** キーワードと引数を削除します。 • アクティブ / アクティブ フェールオーバー	『General Operations CLI Configuration Guide（CLI コンフィギュレーション ガイド（一般的な操作））』の「Configuring Multiple Context Mode（マルチ コンテキスト モードの設定）」の章を参照してください。 『General Operations CLI Configuration Guide（CLI コンフィギュレーション ガイド（一般的な操作））』の「Configuring a Cluster of ASAs（ASA のクラスタの設定）」の章を参照してください。 『General Operations CLI Configuration Guide（CLI コンフィギュレーション ガイド（一般的な操作））』の「Configuring Failover（フェールオーバーの設定）」の章を参照してください。
5.	ASAv を配置します。ASDM 接続をイネーブル化するには、OVF テンプレートのインターフェイス マッピングを含む適切なプロパティを設定する必要があります。 VMware vSphere Client を使用して VM に ASAv をインストールします。	『Cisco Adaptive Security Virtual Appliance（ASAv）Quick Start Guide（Cisco Adaptive Security Virtual Appliance（ASAv）クイック スタート ガイド）』の「Deploying the Cisco Adaptive Security Virtual Appliance（Cisco Adaptive Security Virtual Appliance の展開）」の章を参照してください。
6.	ASAv に接続し、SSH または Telnet の基本的な接続を設定します。 CLI から、**telnet**、**ssh**、または **http** コマンドを使用します。 ASDM で **[Configuration] > [Device Management] > [Management Access] > [ASDM/HTTPS/Telnet/SSH]** を選択します。	『Cisco Adaptive Security Virtual Appliance（ASAv）Quick Start Guide（Cisco Adaptive Security Virtual Appliance（ASAv）クイック スタート ガイド）』の「Deploying the Cisco Adaptive Security Virtual Appliance（Cisco Adaptive Security Virtual Appliance の展開）」の章を参照してください。

ステップ	タスクの説明	参照先
7.	ASAv のシリアル番号を確認して、ASAv を標準モードで実行するために必要な新しいライセンスを取得します。 CLI で、**show version** または **show inventory** コマンドを入力します。 ASDM では、**[Help] > [About the Cisco ASA]** を選択します。 また、ASA ハードウェアの設定内容に応じて、その他の機能のライセンスも要求する必要があります。	『Cisco Adaptive Security Virtual Appliance（ASAv）Quick Start Guide（Cisco Adaptive Security Virtual Appliance（ASAv）クイック スタート ガイド）』の「Deploying the Cisco Adaptive Security Virtual Appliance（Cisco Adaptive Security Virtual Appliance の展開）」の章を参照してください。
8.	ステップ 3. で取得した VPN 固有ファイルをインポートします。ASDM のバックアップ zip ファイルを取得した場合は、ASAv にそれを復元できます。 ASDM で、**[Tools] > [Restore Configurations]** を選択します。 （注） **anyconnect-essentials** コマンドまたは **no anyconnect-essentials** コマンドを発行した場合は、次のメッセージが表示されます。 「`ERROR: Command required AnyConnect Essentials license`」	『VPN CLI Configuration Guide（VPN CLI コンフィギュレーション ガイド）』の「Clientless SSL VPN Overview（クライアントレス SSL VPN の設定）」の章を参照してください。 『VPN CLI Configuration Guide（VPN CLI コンフィギュレーション ガイド）』の「Configuring AnyConnect VPN Client Connections（AnyConnect VPN Client 接続の設定）」の章を参照してください。 『Cisco Secure Desktop Configuration Guide for Cisco ASA 5500 Series Administrators（Cisco ASA 5500 Series 管理者用 Cisco Secure Desktop コンフィギュレーション ガイド）』の「Installing and Enabling CSD（CSD のインストールおよびイネーブル）」の章を参照してください。
9.	ASAv のスタートアップ コンフィギュレーションに、変更された ASA 5500 のコンフィギュレーションをコピーします。次に、**reload noconfirm** コマンドを入力して ASAv をリロードし、コピーしたスタートアップ コンフィギュレーションを保持します。 コピー アンド ペーストまたはファイルの読み取りのメソッドは、バージョン 9.2(1) で保存され、前の手順で変更されたファイルでのみ使用できます。これらのメソッドは、インターフェイスをシャットダウン状態のままにし、実行コンフィギュレーションと競合する場合があり、ASA 移行ツールをトリガーしません。 VMware vSphere Client コンソール ウィンドウでは、情報をコピー アンド ペーストすることはできません。CLI から **configure net** または **copy running-config** のいずれかのコマンドを入力して、TFTP、HTTP、または FTP サーバを使用して変更されたコンフィギュレーション ファイルを転送する必要があります。	『General Operations CLI Configuration Guide（CLI コンフィギュレーション ガイド（一般的な操作））』の「Configuring Management Access（管理アクセスの設定）」の章を参照してください。 コマンド リファレンスの **reload noconfirm** コマンドを参照してください。 『General Operations CLI Configuration Guide（CLI コンフィギュレーション ガイド（一般的な操作））』の「Configuring Digital Certificates（デジタル証明書の設定）」の章を参照してください。 コマンド リファレンスの **configure net** または **copy running-config** コマンドを参照してください。

ステップ	タスクの説明	参照先
10.	ASAv の変更された設定を次のようにして確認します。	—
a.	ASAv の起動時に検出されたエラーを表示するには、CLI から、**show startup-config errors** コマンドを使用します。 ASDM で、**[Tools] > [Command Line Interface]** を選択します。	コマンド リファレンスの **show startup-config errors** コマンドを参照してください。 『General Operations ASDM Configuration Guide（ASDM コンフィギュレーション ガイド（一般的な操作））』の「Managing Software and Configurations（ソフトウェアとコンフィギュレーションの管理）」の章を参照してください。
b.	ディセーブルにすることができないインターフェイスの設定が、ディセーブル化されていないことを確認します。 CLI から、**no shutdown** コマンドを入力します。 ASDM で、**[Configuration] > [Device Management] > [Interfaces]** を選択します。	コマンド リファレンスの **no shutdown** コマンドを参照してください。 『General Operations ASDM Configuration Guide（ASDM コンフィギュレーション ガイド（一般的な操作））』の「Completing Interface Configuration（Routed Mode）（インターフェイス コンフィギュレーションの実行（ルーテッド モード））」の章を参照してください。
c.	アクセス リスト、インターフェイス、インスペクションが正しいことを確認します。 CLI で、**show running-config** コマンドを使用して、ASAv の設定が正しいことを確認します。 ASDM で、**[Tools] > [Command Line Interface]** を選択します。	『General Operations ASDM Configuration Guide（ASDM コンフィギュレーション ガイド（一般的な操作））』の「Using the ACL Manager（ACL マネージャの使用）」の章を参照してください。 『General Operations ASDM Configuration Guide（ASDM コンフィギュレーション ガイド（一般的な操作））』の「Starting Interface Configuration (ASA 5510 and Higher)（インターフェイス コンフィギュレーションの開始（ASA 5510 以降））」の章を参照してください。 『Firewall ASDM Configuration Guide（ファイアウォール ASDM コンフィギュレーション ガイド）』の「Getting Started with Application Layer Protocol Inspection（アプリケーション レイヤ プロトコル インスペクションの準備）」の章を参照してください。 コマンド リファレンスの **show running-config** コマンドを参照してください。
d.	本番環境に導入する前に、ASAv で変更された設定が目的の動作を行うかどうかをテストします。 CLI から、**packet-tracer** コマンドを使用します。 ASDM で、**[Tools] > [Packet Tracer]** を選択します。	コマンド リファレンスの **packet tracer** コマンドを参照してください。 『General Operations ASDM Configuration Guide（ASDM コンフィギュレーション ガイド（一般的な操作））』の「Troubleshooting（トラブルシューティング）」の章を参照してください。

サンプル コンフィギュレーション ファイル

移行前の基本設定

次に示すのは、ASAv への移行前の ASA 5525-X からの基本サンプル コンフィギュレーション ファイルです。

```
Admin context:

: Saved
:
ASA Version 9.1(3) <context>
!
hostname admin
enable password 2KFQnbNIdI.2KYOU encrypted
passwd 2KFQnbNIdI.2KYOU encrypted
names
ip local pool outside_pool 10.1.2.2-10.1.2.10 mask 255.255.255.0
ip local pool inside_pool 10.1.1.2-10.1.1.10 mask 255.255.255.0
ip local pool mgmt-pool 172.16.1.241-172.16.1.245
!
interface Management0/0
 management-only
 nameif mgmt
 security-level 0
 ip address 172.16.1.240 255.255.255.0
!
interface GigabitEthernet0/0
 nameif inside
 security-level 100
 ip address 10.1.1.1 255.255.255.0
 ospf hello-interval 1
 ospf dead-interval 2
!
interface GigabitEthernet0/1
 nameif outside
 security-level 0
 ip address 10.1.2.1 255.255.255.0
 ospf hello-interval 1
 ospf dead-interval 2
!
same-security-traffic permit inter-interface
access-list global extended permit icmp any any
access-list global extended permit ip any any
pager lines 24
logging console warnings
logging buffered debugging
logging asdm informational
mtu mgmt 1500
mtu inside 1500
mtu outside 1500
icmp unreachable rate-limit 1 burst-size 1
icmp permit any inside
icmp permit any outside
no asdm history enable
arp timeout 14400
access-group global in interface inside
access-group global in interface outside
access-group global global
!
router ospf 1
 network 10.1.1.0 255.255.255.0 area 0
 network 10.1.2.0 255.255.255.0 area 0
```

```
 timers spf 1 1
 timers lsa-group-pacing 1
 log-adj-changes
!
route outside 0.0.0.0 0.0.0.0 10.1.2.200 200
route inside 10.10.140.0 255.255.255.0 10.1.1.200 200
timeout xlate 3:00:00
timeout pat-xlate 0:00:30
timeout conn 1:00:00 half-closed 0:10:00 udp 0:02:00 icmp 0:00:02
timeout sunrpc 0:10:00 h323 0:05:00 h225 1:00:00 mgcp 0:05:00 mgcp-pat 0:05:00
timeout sip 0:30:00 sip_media 0:02:00 sip-invite 0:03:00 sip-disconnect 0:02:00
timeout sip-provisional-media 0:02:00 uauth 0:05:00 absolute
timeout tcp-proxy-reassembly 0:01:00
timeout floating-conn 0:00:00
user-identity default-domain LOCAL
http server enable
http 0.0.0.0 0.0.0.0 mgmt
no snmp-server location
no snmp-server contact
crypto ipsec security-association pmtu-aging infinite
telnet timeout 5
ssh timeout 5
ssh key-exchange group dh-group1-sha1
no threat-detection statistics tcp-intercept
!
class-map inspection_default
 match default-inspection-traffic
!
!
policy-map type inspect dns preset_dns_map
 parameters
  message-length maximum client auto
  message-length maximum 512
policy-map global_policy
 class inspection_default
  inspect dns preset_dns_map
  inspect ftp
  inspect ip-options
  inspect netbios
  inspect rsh
  inspect esmtp
  inspect sqlnet
  inspect sunrpc
  inspect tftp
  inspect xdmcp
  inspect icmp
!
service-policy global_policy global
Cryptochecksum:0e8178ab18e3d553aabeee98f2192418
: end
```

移行後の基本設定

次に示すのは、ASAv への移行後の ASA 5525-X からの基本サンプル コンフィギュレーション ファイルです。

```
admin# show running-config
hostname admin
enable password 2KFQnbNIdI.2KYOU encrypted
xlate per-session deny tcp any4 any4
xlate per-session deny tcp any4 any6
xlate per-session deny tcp any6 any4
xlate per-session deny tcp any6 any6
```

```
xlate per-session deny udp any4 any4 eq domain
xlate per-session deny udp any4 any6 eq domain
xlate per-session deny udp any6 any4 eq domain
xlate per-session deny udp any6 any6 eq domain
passwd 2KFQnbNIdI.2KYOU encrypted
names
ip local pool outside_pool 10.1.2.2-10.1.2.10 mask 255.255.255.0
ip local pool inside_pool 10.1.1.2-10.1.1.10 mask 255.255.255.0
!
interface GigabitEthernet0/0
 shutdown
 nameif inside
 security-level 100
 ip address 10.1.1.1 255.255.255.0
 ospf hello-interval 1
 ospf dead-interval 2
!
interface GigabitEthernet0/1
 shutdown
 nameif outside
 security-level 0
 ip address 10.1.2.1 255.255.255.0
 ospf hello-interval 1
 ospf dead-interval 2
!
interface GigabitEthernet0/2
 shutdown
 no nameif
 no security-level
 no ip address
!
interface GigabitEthernet0/3
 shutdown
 no nameif
 no security-level
 no ip address
!
interface GigabitEthernet0/4
 shutdown
 no nameif
 no security-level
 no ip address
!
interface GigabitEthernet0/5
 shutdown
 no nameif
 no security-level
 no ip address
!
interface GigabitEthernet0/6
 shutdown
 no nameif
 no security-level
 no ip address
!
interface GigabitEthernet0/7
 shutdown
 no nameif
 no security-level
 no ip address
!
interface GigabitEthernet0/8
 shutdown
 no nameif
```

```
 no security-level
 no ip address
!
interface Management0/0
 management-only
 nameif mgmt
 security-level 0
 ip address 172.16.1.240 255.255.255.0
!
ftp mode passive
same-security-traffic permit inter-interface
access-list global extended permit icmp any any
access-list global extended permit ip any any
pager lines 24
logging console warnings
logging buffered debugging
logging asdm informational
mtu mgmt 1500
mtu inside 1500
mtu outside 1500
no failover
icmp unreachable rate-limit 1 burst-size 1
icmp permit any inside
icmp permit any outside
no asdm history enable
arp timeout 14400
no arp permit-nonconnected
access-group global in interface inside
access-group global in interface outside
access-group global global
router ospf 1
 network 10.1.1.0 255.255.255.0 area 0
 network 10.1.2.0 255.255.255.0 area 0
 log-adj-changes
!
route outside 0.0.0.0 0.0.0.0 10.1.2.200 200
route inside 10.10.140.0 255.255.255.0 10.1.1.200 200
timeout xlate 3:00:00
timeout pat-xlate 0:00:30
timeout conn 1:00:00 half-closed 0:10:00 udp 0:02:00 icmp 0:00:02
timeout sunrpc 0:10:00 h323 0:05:00 h225 1:00:00 mgcp 0:05:00 mgcp-pat 0:05:00
timeout sip 0:30:00 sip_media 0:02:00 sip-invite 0:03:00 sip-disconnect 0:02:00
timeout sip-provisional-media 0:02:00 uauth 0:05:00 absolute
timeout tcp-proxy-reassembly 0:01:00
timeout floating-conn 0:00:00
dynamic-access-policy-record DfltAccessPolicy
user-identity default-domain LOCAL
http server enable
http 0.0.0.0 0.0.0.0 mgmt
no snmp-server location
no snmp-server contact
crypto ipsec security-association pmtu-aging infinite
crypto ca trustpool policy
telnet timeout 5
ssh timeout 5
ssh key-exchange group dh-group1-sha1
console timeout 0
threat-detection basic-threat
threat-detection statistics access-list
no threat-detection statistics tcp-intercept
!
class-map inspection_default
 match default-inspection-traffic
!
```

```
!
policy-map type inspect dns preset_dns_map
 parameters
  message-length maximum client auto
  message-length maximum 512
policy-map global_policy
 class inspection_default
  inspect ftp
  inspect h323 h225
  inspect h323 ras
  inspect rsh
  inspect rtsp
  inspect esmtp
  inspect sqlnet
  inspect skinny
  inspect sunrpc
  inspect xdmcp
  inspect sip
  inspect netbios
  inspect tftp
  inspect ip-options
  inspect dns preset_dns_map
  inspect icmp
!
service-policy global_policy global
prompt hostname context
no call-home reporting anonymous
call-home
 profile CiscoTAC-1
  no active
  destination address http https://tools.cisco.com/its/service/oddce/services/DDCEService
  destination address email callhome@cisco.com
  destination transport-method http
  subscribe-to-alert-group diagnostic
  subscribe-to-alert-group environment
  subscribe-to-alert-group inventory periodic monthly 8
  subscribe-to-alert-group configuration periodic monthly 8
  subscribe-to-alert-group telemetry periodic daily
Cryptochecksum:ab49a0b37aa11997ffb6cadaaf2c5fe4
: end
admin#
```

移行前の VPN での設定

移行の前に、次の 2 つの要件が満たされていることを確認してください。

- ***** を持つ事前共有キーに実際のキーが存在する。
- vCPU および AnyConnect Essentials 機能のライセンスが追加されている。

次に示すのは、ASAv への移行前の ASA 5515-X からの VPN を使用したサンプル コンフィギュレーション ファイルです。

```
ciscoasa# show running-config
: Saved
:
ASA Version 9.2(0)3
!
hostname ciscoasa
enable password 2KFQnbNIdI.2KYOU encrypted
xlate per-session deny tcp any4 any4
xlate per-session deny tcp any4 any6
xlate per-session deny tcp any6 any4
xlate per-session deny tcp any6 any6
xlate per-session deny udp any4 any4 eq domain
```

```
xlate per-session deny udp any4 any6 eq domain
xlate per-session deny udp any6 any4 eq domain
xlate per-session deny udp any6 any6 eq domain
passwd 2KFQnbNIdI.2KYOU encrypted
names
ip local pool RASSLVPN 10.20.20.101-10.20.20.110 mask 255.255.255.0
!
interface GigabitEthernet0/0
 nameif Outside
 security-level 0
 ip address 10.30.30.1 255.255.255.0
 no shutdown
!
interface GigabitEthernet0/1
 nameif Inside
 security-level 100
 ip address 10.20.20.2 255.255.255.0
 no shutdown
!
interface GigabitEthernet0/2
 shutdown
 no nameif
 no security-level
 no ip address
!
interface GigabitEthernet0/3
 shutdown
 no nameif
 no security-level
 no ip address
!
interface GigabitEthernet0/4
 shutdown
 no nameif
 no security-level
 no ip address
!
interface GigabitEthernet0/5
 shutdown
 no nameif
 no security-level
 no ip address
!
interface GigabitEthernet0/6
 shutdown
 no nameif
 no security-level
 no ip address
!
interface GigabitEthernet0/7
 shutdown
 no nameif
 no security-level
 no ip address
!
interface GigabitEthernet0/8
 shutdown
 no nameif
 no security-level
 no ip address
!
interface Management0/0
 management-only
 nameif management
```

```
 security-level 100
 ip address 10.0.0.152 255.255.0.0
!
ftp mode passive
dns domain-lookup management
dns domain-lookup Outside
dns domain-lookup Inside
access-list ACL-OUTSIDE extended permit icmp any any
access-list Inside_cryptomap extended permit ip 10.30.30.0 255.255.255.0 10.10.10.0
255.255.255.0
access-list bla extended permit ip any any
access-list block extended deny ip any any
pager lines 23
logging enable
logging console debugging
logging asdm informational
mtu management 1500
mtu Outside 1500
mtu Inside 1500
no failover
icmp unreachable rate-limit 1 burst-size 1
no asdm history enable
arp timeout 14400
no arp permit-nonconnected
access-group block in interface Outside
route management 0.0.0.0 0.0.0.0 10.0.0.1 200
route Inside 10.10.0.0 255.255.0.0 10.20.20.1 1
route Inside 192.168.0.0 255.255.0.0 10.20.20.1 1
timeout xlate 3:00:00
timeout pat-xlate 0:00:30
timeout conn 1:00:00 half-closed 0:10:00 udp 0:02:00 icmp 0:00:02
timeout sunrpc 0:10:00 h323 0:05:00 h225 1:00:00 mgcp 0:05:00 mgcp-pat 0:05:00
timeout sip 0:30:00 sip_media 0:02:00 sip-invite 0:03:00 sip-disconnect 0:02:00
timeout sip-provisional-media 0:02:00 uauth 0:05:00 absolute
timeout tcp-proxy-reassembly 0:01:00
timeout floating-conn 0:00:00
dynamic-access-policy-record DfltAccessPolicy
user-identity default-domain LOCAL
aaa authentication ssh console LOCAL
http server enable
http 10.0.0.0 255.255.0.0 management
http 0.0.0.0 0.0.0.0 Outside
http 0.0.0.0 0.0.0.0 management
no snmp-server location
no snmp-server contact
crypto ipsec ikev1 transform-set ESP-AES-128-SHA esp-aes esp-sha-hmac
crypto ipsec ikev1 transform-set ESP-AES-128-MD5 esp-aes esp-md5-hmac
crypto ipsec ikev1 transform-set ESP-AES-192-SHA esp-aes-192 esp-sha-hmac
crypto ipsec ikev1 transform-set ESP-AES-192-MD5 esp-aes-192 esp-md5-hmac
crypto ipsec ikev1 transform-set ESP-AES-256-SHA esp-aes-256 esp-sha-hmac
crypto ipsec ikev1 transform-set ESP-AES-256-MD5 esp-aes-256 esp-md5-hmac
crypto ipsec ikev1 transform-set ESP-AES-128-SHA-TRANS esp-aes esp-sha-hmac
crypto ipsec ikev1 transform-set ESP-AES-128-SHA-TRANS mode transport
crypto ipsec ikev1 transform-set ESP-AES-128-MD5-TRANS esp-aes esp-md5-hmac
crypto ipsec ikev1 transform-set ESP-AES-128-MD5-TRANS mode transport
crypto ipsec ikev1 transform-set ESP-AES-192-SHA-TRANS esp-aes-192 esp-sha-hmac
crypto ipsec ikev1 transform-set ESP-AES-192-SHA-TRANS mode transport
crypto ipsec ikev1 transform-set ESP-AES-192-MD5-TRANS esp-aes-192 esp-md5-hmac
crypto ipsec ikev1 transform-set ESP-AES-192-MD5-TRANS mode transport
crypto ipsec ikev1 transform-set ESP-AES-256-SHA-TRANS esp-aes-256 esp-sha-hmac
crypto ipsec ikev1 transform-set ESP-AES-256-SHA-TRANS mode transport
crypto ipsec ikev1 transform-set ESP-AES-256-MD5-TRANS esp-aes-256 esp-md5-hmac
crypto ipsec ikev1 transform-set ESP-AES-256-MD5-TRANS mode transport
crypto ipsec ikev1 transform-set ESP-3DES-SHA esp-3des esp-sha-hmac
```

```
crypto ipsec ikev1 transform-set ESP-3DES-MD5 esp-3des esp-md5-hmac
crypto ipsec ikev1 transform-set ESP-3DES-SHA-TRANS esp-3des esp-sha-hmac
crypto ipsec ikev1 transform-set ESP-3DES-SHA-TRANS mode transport
crypto ipsec ikev1 transform-set ESP-3DES-MD5-TRANS esp-3des esp-md5-hmac
crypto ipsec ikev1 transform-set ESP-3DES-MD5-TRANS mode transport
crypto ipsec ikev1 transform-set ESP-DES-SHA esp-des esp-sha-hmac
crypto ipsec ikev1 transform-set ESP-DES-MD5 esp-des esp-md5-hmac
crypto ipsec ikev1 transform-set ESP-DES-SHA-TRANS esp-des esp-sha-hmac
crypto ipsec ikev1 transform-set ESP-DES-SHA-TRANS mode transport
crypto ipsec ikev1 transform-set ESP-DES-MD5-TRANS esp-des esp-md5-hmac
crypto ipsec ikev1 transform-set ESP-DES-MD5-TRANS mode transport
crypto ipsec ikev2 ipsec-proposal DES
 protocol esp encryption des
 protocol esp integrity sha-1 md5
crypto ipsec ikev2 ipsec-proposal 3DES
 protocol esp encryption 3des
 protocol esp integrity sha-1 md5
crypto ipsec ikev2 ipsec-proposal AES
 protocol esp encryption aes
 protocol esp integrity sha-1 md5
crypto ipsec ikev2 ipsec-proposal AES192
 protocol esp encryption aes-192
 protocol esp integrity sha-1 md5
crypto ipsec ikev2 ipsec-proposal AES256
 protocol esp encryption aes-256
 protocol esp integrity sha-1 md5
crypto ipsec security-association pmtu-aging infinite
crypto map Inside_map 1 match address Inside_cryptomap
crypto map Inside_map 1 set peer 10.20.20.1
crypto map Inside_map 1 set ikev1 transform-set ESP-AES-128-SHA ESP-AES-128-MD5
ESP-AES-192-SHA ESP-AES-192-MD5 ESP-AES-256-SHA ESP-AES-256-MD5 ESP-3DES-SHA ESP-3DES-MD5
ESP-DES-SHA ESP-DES-MD5
crypto map Inside_map 1 set ikev2 ipsec-proposal AES256 AES192 AES 3DES DES
crypto map Inside_map interface Inside
crypto ca trustpool policy
crypto ikev2 policy 1
 encryption aes-256
 integrity sha
 group 5 2
 prf sha
 lifetime seconds 86400
crypto ikev2 policy 10
 encryption aes-192
 integrity sha
 group 5 2
 prf sha
 lifetime seconds 86400
crypto ikev2 policy 20
 encryption aes
 integrity sha
 group 5 2
 prf sha
 lifetime seconds 86400
crypto ikev2 policy 30
 encryption 3des
 integrity sha
 group 5 2
 prf sha
 lifetime seconds 86400
crypto ikev2 policy 40
 encryption des
 integrity sha
 group 5 2
 prf sha
```

```
 lifetime seconds 86400
crypto ikev2 enable Inside
crypto ikev1 policy 10
 authentication crack
 encryption aes-256
 hash sha
 group 2
 lifetime 86400
crypto ikev1 policy 20
 authentication rsa-sig
 encryption aes-256
 hash sha
 group 2
 lifetime 86400
crypto ikev1 policy 30
 authentication pre-share
 encryption aes-256
 hash sha
 group 2
 lifetime 86400
crypto ikev1 policy 40
 authentication crack
 encryption aes-192
 hash sha
 group 2
 lifetime 86400
crypto ikev1 policy 50
 authentication rsa-sig
 encryption aes-192
 hash sha
 group 2
 lifetime 86400
crypto ikev1 policy 60
 authentication pre-share
 encryption aes-192
 hash sha
 group 2
 lifetime 86400
crypto ikev1 policy 70
 authentication crack
 encryption aes
 hash sha
 group 2
 lifetime 86400
crypto ikev1 policy 80
 authentication rsa-sig
 encryption aes
 hash sha
 group 2
 lifetime 86400
crypto ikev1 policy 90
 authentication pre-share
 encryption aes
 hash sha
 group 2
 lifetime 86400
crypto ikev1 policy 100
 authentication crack
 encryption 3des
 hash sha
 group 2
 lifetime 86400
crypto ikev1 policy 110
 authentication rsa-sig
```

```
 encryption 3des
 hash sha
 group 2
 lifetime 86400
crypto ikev1 policy 120
 authentication pre-share
 encryption 3des
 hash sha
 group 2
 lifetime 86400
crypto ikev1 policy 130
 authentication crack
 encryption des
 hash sha
 group 2
 lifetime 86400
crypto ikev1 policy 140
 authentication rsa-sig
 encryption des
 hash sha
 group 2
 lifetime 86400
crypto ikev1 policy 150
 authentication pre-share
 encryption des
 hash sha
 group 2
 lifetime 86400
telnet 0.0.0.0 0.0.0.0 management
telnet timeout 5
ssh 0.0.0.0 0.0.0.0 management
ssh timeout 5
ssh key-exchange group dh-group1-sha1
console timeout 0
threat-detection basic-threat
threat-detection statistics port
threat-detection statistics protocol
threat-detection statistics access-list
no threat-detection statistics tcp-intercept
webvpn
 enable Outside
 no anyconnect-essentials
 anyconnect image disk0:/anyconnect-win-3.1.05152-k9.pkg 1
 anyconnect enable
 tunnel-group-list enable
 internal-password enable
group-policy DfltGrpPolicy attributes
 vpn-tunnel-protocol ikev1 l2tp-ipsec ssl-client ssl-clientless
 webvpn
  url-list value Bookmark
group-policy "GroupPolicy_AnyConnect RA SSL VPN" internal
group-policy "GroupPolicy_AnyConnect RA SSL VPN" attributes
 wins-server none
 dns-server none
 vpn-tunnel-protocol ssl-client
 default-domain none
group-policy GroupPolicy_10.20.20.1 internal
group-policy GroupPolicy_10.20.20.1 attributes
 vpn-tunnel-protocol ikev2
username admin password 2KFQnbNIdI.2KYOU encrypted privilege 15
tunnel-group "AnyConnect RA SSL VPN" type remote-access
tunnel-group "AnyConnect RA SSL VPN" general-attributes
 address-pool RASSLVPN
 default-group-policy "GroupPolicy_AnyConnect RA SSL VPN"
```

```
tunnel-group "AnyConnect RA SSL VPN" webvpn-attributes
 group-alias "AnyConnect RA SSL VPN" enable
tunnel-group 10.20.20.1 type ipsec-l2l
tunnel-group 10.20.20.1 general-attributes
 default-group-policy GroupPolicy_10.20.20.1
tunnel-group 10.20.20.1 ipsec-attributes
 ikev1 pre-shared-key Cisco1
 ikev2 remote-authentication pre-shared-key Cisco2
 ikev2 local-authentication pre-shared-key Cisco3
tunnel-group ClientlessVPN type remote-access
tunnel-group ClientlessVPN webvpn-attributes
 group-alias ClientlessVPN enable
!
class-map inspection_default
 match default-inspection-traffic
!
!
policy-map type inspect dns preset_dns_map
 parameters
  message-length maximum client auto
  message-length maximum 512
policy-map global_policy
 class inspection_default
  inspect rtsp
  inspect sunrpc
  inspect xdmcp
  inspect netbios
  inspect tftp
  inspect ip-options
  inspect dns preset_dns_map
  inspect ftp
  inspect h323 h225
  inspect h323 ras
  inspect rsh
  inspect esmtp
  inspect sqlnet
  inspect sip
  inspect skinny
!
service-policy global_policy global
prompt hostname context
no call-home reporting anonymous
call-home
 profile CiscoTAC-1
  no active
  destination address http https://tools.cisco.com/its/service/oddce/services/DDCEService
  destination address email callhome@cisco.com
  destination transport-method http
  subscribe-to-alert-group diagnostic
  subscribe-to-alert-group environment
  subscribe-to-alert-group inventory periodic monthly 2
  subscribe-to-alert-group configuration periodic monthly 2
  subscribe-to-alert-group telemetry periodic daily
Cryptochecksum:7359004446ef826e734dc5413e1c669d
: end
ciscoasa#
```

移行後の VPN での設定

次に示すのは、ASAv への移行後の ASA 5515-X からの VPN を使用したサンプル コンフィギュレーション ファイルです。

```
ciscoasa# show running-config
```

```
: Saved
:
ASA Version 9.2(0)3
!
hostname ciscoasa
enable password 2KFQnbNIdI.2KYOU encrypted
xlate per-session deny tcp any4 any4
xlate per-session deny tcp any4 any6
xlate per-session deny tcp any6 any4
xlate per-session deny tcp any6 any6
xlate per-session deny udp any4 any4 eq domain
xlate per-session deny udp any4 any6 eq domain
xlate per-session deny udp any6 any4 eq domain
xlate per-session deny udp any6 any6 eq domain
passwd 2KFQnbNIdI.2KYOU encrypted
names
ip local pool RASSLVPN 10.20.20.101-10.20.20.110 mask 255.255.255.0
!
interface GigabitEthernet0/0
 nameif Outside
 security-level 0
 ip address 10.30.30.1 255.255.255.0
!
interface GigabitEthernet0/1
 nameif Inside
 security-level 100
 ip address 10.20.20.2 255.255.255.0
!
interface GigabitEthernet0/2
 shutdown
 no nameif
 no security-level
 no ip address
!
interface GigabitEthernet0/3
 shutdown
 no nameif
 no security-level
 no ip address
!
interface GigabitEthernet0/4
 shutdown
 no nameif
 no security-level
 no ip address
!
interface GigabitEthernet0/5
 shutdown
 no nameif
 no security-level
 no ip address
!
interface GigabitEthernet0/6
 shutdown
 no nameif
 no security-level
 no ip address
!
interface GigabitEthernet0/7
 shutdown
 no nameif
 no security-level
 no ip address
!
```

```
interface GigabitEthernet0/8
 shutdown
 no nameif
 no security-level
 no ip address
!
interface Management0/0
 management-only
 nameif management
 security-level 100
 ip address 10.0.0.152 255.255.0.0
!
ftp mode passive
dns domain-lookup management
dns domain-lookup Outside
dns domain-lookup Inside
access-list ACL-OUTSIDE extended permit icmp any any
access-list Inside_cryptomap extended permit ip 10.30.30.0 255.255.255.0 10.10.10.0
255.255.255.0
access-list bla extended permit ip any any
access-list block extended deny ip any any
pager lines 23
logging enable
logging console debugging
logging asdm informational
mtu management 1500
mtu Outside 1500
mtu Inside 1500
no failover
icmp unreachable rate-limit 1 burst-size 1
no asdm history enable
arp timeout 14400
no arp permit-nonconnected
access-group block in interface Outside
route management 0.0.0.0 0.0.0.0 10.0.0.1 200
route Inside 10.10.0.0 255.255.0.0 10.20.20.1 1
route Inside 192.168.0.0 255.255.0.0 10.20.20.1 1
timeout xlate 3:00:00
timeout pat-xlate 0:00:30
timeout conn 1:00:00 half-closed 0:10:00 udp 0:02:00 icmp 0:00:02
timeout sunrpc 0:10:00 h323 0:05:00 h225 1:00:00 mgcp 0:05:00 mgcp-pat 0:05:00
timeout sip 0:30:00 sip_media 0:02:00 sip-invite 0:03:00 sip-disconnect 0:02:00
timeout sip-provisional-media 0:02:00 uauth 0:05:00 absolute
timeout tcp-proxy-reassembly 0:01:00
timeout floating-conn 0:00:00
dynamic-access-policy-record DfltAccessPolicy
user-identity default-domain LOCAL
aaa authentication ssh console LOCAL
http server enable
http 10.0.0.0 255.255.0.0 management
http 0.0.0.0 0.0.0.0 Outside
http 0.0.0.0 0.0.0.0 management
no snmp-server location
no snmp-server contact
crypto ipsec ikev1 transform-set ESP-AES-128-SHA esp-aes esp-sha-hmac
crypto ipsec ikev1 transform-set ESP-AES-128-MD5 esp-aes esp-md5-hmac
crypto ipsec ikev1 transform-set ESP-AES-192-SHA esp-aes-192 esp-sha-hmac
crypto ipsec ikev1 transform-set ESP-AES-192-MD5 esp-aes-192 esp-md5-hmac
crypto ipsec ikev1 transform-set ESP-AES-256-SHA esp-aes-256 esp-sha-hmac
crypto ipsec ikev1 transform-set ESP-AES-256-MD5 esp-aes-256 esp-md5-hmac
crypto ipsec ikev1 transform-set ESP-AES-128-SHA-TRANS esp-aes esp-sha-hmac
crypto ipsec ikev1 transform-set ESP-AES-128-SHA-TRANS mode transport
crypto ipsec ikev1 transform-set ESP-AES-128-MD5-TRANS esp-aes esp-md5-hmac
crypto ipsec ikev1 transform-set ESP-AES-128-MD5-TRANS mode transport
```

```
crypto ipsec ikev1 transform-set ESP-AES-192-SHA-TRANS esp-aes-192 esp-sha-hmac
crypto ipsec ikev1 transform-set ESP-AES-192-SHA-TRANS mode transport
crypto ipsec ikev1 transform-set ESP-AES-192-MD5-TRANS esp-aes-192 esp-md5-hmac
crypto ipsec ikev1 transform-set ESP-AES-192-MD5-TRANS mode transport
crypto ipsec ikev1 transform-set ESP-AES-256-SHA-TRANS esp-aes-256 esp-sha-hmac
crypto ipsec ikev1 transform-set ESP-AES-256-SHA-TRANS mode transport
crypto ipsec ikev1 transform-set ESP-AES-256-MD5-TRANS esp-aes-256 esp-md5-hmac
crypto ipsec ikev1 transform-set ESP-AES-256-MD5-TRANS mode transport
crypto ipsec ikev1 transform-set ESP-3DES-SHA esp-3des esp-sha-hmac
crypto ipsec ikev1 transform-set ESP-3DES-MD5 esp-3des esp-md5-hmac
crypto ipsec ikev1 transform-set ESP-3DES-SHA-TRANS esp-3des esp-sha-hmac
crypto ipsec ikev1 transform-set ESP-3DES-SHA-TRANS mode transport
crypto ipsec ikev1 transform-set ESP-3DES-MD5-TRANS esp-3des esp-md5-hmac
crypto ipsec ikev1 transform-set ESP-3DES-MD5-TRANS mode transport
crypto ipsec ikev1 transform-set ESP-DES-SHA esp-des esp-sha-hmac
crypto ipsec ikev1 transform-set ESP-DES-MD5 esp-des esp-md5-hmac
crypto ipsec ikev1 transform-set ESP-DES-SHA-TRANS esp-des esp-sha-hmac
crypto ipsec ikev1 transform-set ESP-DES-SHA-TRANS mode transport
crypto ipsec ikev1 transform-set ESP-DES-MD5-TRANS esp-des esp-md5-hmac
crypto ipsec ikev1 transform-set ESP-DES-MD5-TRANS mode transport
crypto ipsec ikev2 ipsec-proposal AES256
 protocol esp encryption aes-256
 protocol esp integrity sha-1 md5
crypto ipsec ikev2 ipsec-proposal AES192
 protocol esp encryption aes-192
 protocol esp integrity sha-1 md5
crypto ipsec ikev2 ipsec-proposal AES
 protocol esp encryption aes
 protocol esp integrity sha-1 md5
crypto ipsec ikev2 ipsec-proposal 3DES
 protocol esp encryption 3des
 protocol esp integrity sha-1 md5
crypto ipsec ikev2 ipsec-proposal DES
 protocol esp encryption des
 protocol esp integrity sha-1 md5
crypto ipsec security-association pmtu-aging infinite
crypto map Inside_map 1 match address Inside_cryptomap
crypto map Inside_map 1 set peer 10.20.20.1
crypto map Inside_map 1 set ikev1 transform-set ESP-AES-128-SHA ESP-AES-128-MD5
ESP-AES-192-SHA ESP-AES-192-MD5 ESP-AES-256-SHA ESP-AES-256-MD5 ESP-3DES-SHA ESP-3DES-MD5
ESP-DES-SHA ESP-DES-MD5
crypto map Inside_map 1 set ikev2 ipsec-proposal AES256 AES192 AES 3DES DES
crypto map Inside_map interface Inside
crypto ca trustpool policy
crypto ikev2 policy 1
 encryption aes-256
 integrity sha
 group 5 2
 prf sha
 lifetime seconds 86400
crypto ikev2 policy 10
 encryption aes-192
 integrity sha
 group 5 2
 prf sha
 lifetime seconds 86400
crypto ikev2 policy 20
 encryption aes
 integrity sha
 group 5 2
 prf sha
 lifetime seconds 86400
crypto ikev2 policy 30
 encryption 3des
```

```
 integrity sha
 group 5 2
 prf sha
 lifetime seconds 86400
crypto ikev2 policy 40
 encryption des
 integrity sha
 group 5 2
 prf sha
 lifetime seconds 86400
crypto ikev2 enable Inside
crypto ikev1 policy 10
 authentication crack
 encryption aes-256
 hash sha
 group 2
 lifetime 86400
crypto ikev1 policy 20
 authentication rsa-sig
 encryption aes-256
 hash sha
 group 2
 lifetime 86400
crypto ikev1 policy 30
 authentication pre-share
 encryption aes-256
 hash sha
 group 2
 lifetime 86400
crypto ikev1 policy 40
 authentication crack
 encryption aes-192
 hash sha
 group 2
 lifetime 86400
crypto ikev1 policy 50
 authentication rsa-sig
 encryption aes-192
 hash sha
 group 2
 lifetime 86400
crypto ikev1 policy 60
 authentication pre-share
 encryption aes-192
 hash sha
 group 2
 lifetime 86400
crypto ikev1 policy 70
 authentication crack
 encryption aes
 hash sha
 group 2
 lifetime 86400
crypto ikev1 policy 80
 authentication rsa-sig
 encryption aes
 hash sha
 group 2
 lifetime 86400
crypto ikev1 policy 90
 authentication pre-share
 encryption aes
 hash sha
 group 2
```

```
 lifetime 86400
crypto ikev1 policy 100
 authentication crack
 encryption 3des
 hash sha
 group 2
 lifetime 86400
crypto ikev1 policy 110
 authentication rsa-sig
 encryption 3des
 hash sha
 group 2
 lifetime 86400
crypto ikev1 policy 120
 authentication pre-share
 encryption 3des
 hash sha
 group 2
 lifetime 86400
crypto ikev1 policy 130
 authentication crack
 encryption des
 hash sha
 group 2
 lifetime 86400
crypto ikev1 policy 140
 authentication rsa-sig
 encryption des
 hash sha
 group 2
 lifetime 86400
crypto ikev1 policy 150
 authentication pre-share
 encryption des
 hash sha
 group 2
 lifetime 86400
telnet 0.0.0.0 0.0.0.0 management
telnet timeout 5
ssh 0.0.0.0 0.0.0.0 management
ssh timeout 5
ssh key-exchange group dh-group1-sha1
console timeout 0
threat-detection basic-threat
threat-detection statistics port
threat-detection statistics protocol
threat-detection statistics access-list
no threat-detection statistics tcp-intercept
webvpn
 enable Outside
 no anyconnect-essentials
 anyconnect enable
 tunnel-group-list enable
 internal-password enable
group-policy DfltGrpPolicy attributes
 vpn-tunnel-protocol ikev1 l2tp-ipsec ssl-client ssl-clientless
group-policy "GroupPolicy_AnyConnect RA SSL VPN" internal
group-policy "GroupPolicy_AnyConnect RA SSL VPN" attributes
 wins-server none
 dns-server none
 vpn-tunnel-protocol ssl-client
 default-domain none
group-policy GroupPolicy_10.20.20.1 internal
group-policy GroupPolicy_10.20.20.1 attributes
```

```
 vpn-tunnel-protocol ikev2
username admin password 2KFQnbNIdI.2KYOU encrypted privilege 15
tunnel-group "AnyConnect RA SSL VPN" type remote-access
tunnel-group "AnyConnect RA SSL VPN" general-attributes
 address-pool RASSLVPN
 default-group-policy "GroupPolicy_AnyConnect RA SSL VPN"
tunnel-group "AnyConnect RA SSL VPN" webvpn-attributes
 group-alias "AnyConnect RA SSL VPN" enable
tunnel-group 10.20.20.1 type ipsec-l2l
tunnel-group 10.20.20.1 general-attributes
 default-group-policy GroupPolicy_10.20.20.1
tunnel-group 10.20.20.1 ipsec-attributes
 ikev1 pre-shared-key *****
 ikev2 remote-authentication pre-shared-key *****
 ikev2 local-authentication pre-shared-key *****
tunnel-group ClientlessVPN type remote-access
tunnel-group ClientlessVPN webvpn-attributes
 group-alias ClientlessVPN enable
!
class-map inspection_default
 match default-inspection-traffic
!
!
policy-map type inspect dns preset_dns_map
 parameters
  message-length maximum client auto
  message-length maximum 512
policy-map global_policy
 class inspection_default
  inspect dns preset_dns_map
  inspect ftp
  inspect h323 h225
  inspect h323 ras
  inspect rsh
  inspect rtsp
  inspect esmtp
  inspect sqlnet
  inspect skinny
  inspect sunrpc
  inspect xdmcp
  inspect sip
  inspect netbios
  inspect tftp
  inspect ip-options
!
service-policy global_policy global
prompt hostname context
no call-home reporting anonymous
call-home
 profile CiscoTAC-1
  no active
  destination address http https://tools.cisco.com/its/service/oddce/services/DDCEService
  destination address email callhome@cisco.com
  destination transport-method http
  subscribe-to-alert-group diagnostic
  subscribe-to-alert-group environment
  subscribe-to-alert-group inventory periodic monthly 2
  subscribe-to-alert-group configuration periodic monthly 2
  subscribe-to-alert-group telemetry periodic daily
Cryptochecksum:96fc251e97bea6a4223f8f3d2de3ae15
: end
ciscoasa# %ASA-7-111009: User 'enable_15' executed cmd: show running-config
```

関連資料

ASA 5500 および ASAv に関する詳細については、次の URL にアクセスしてください。

http://www.cisco.com/go/asadocs

マニュアルの入手方法およびテクニカル サポート

マニュアルの入手方法、テクニカル サポート、その他の有用な情報について、次の URL で、毎月更新される『*What's New in Cisco Product Documentation（Cisco 製品資料の更新情報）*』を参照してください。シスコの新規および改訂版の技術マニュアルの一覧も示されています。
http://www.cisco.com/c/en/us/td/docs/general/whatsnew/whatsnew.html

『*What's New in Cisco Product Documentation（Cisco 製品資料の更新情報）*』は、シスコの新規および改訂版の技術マニュアルの一覧も示し、RSS フィードとして購読できます。また、リーダー アプリケーションを使用してコンテンツをデスクトップに配信することもできます。RSS フィードは無料のサービスです。