SDM によるルータ設定の基礎

目次

はじめに

このドキュメントでは、Cisco Security Device Manager（SDM）を使用して、ルータの基本的な設定を行う方法について説明します。 基本的な設定には、IP アドレス、デフォルト ルーティング、スタティック ルーティングおよびダイナミック ルーティング、スタティック NAT およびダイナミック NAT、ホスト名、バナー、シークレット パスワード、ユーザ アカウントなどの設定が含まれます。 Cisco SDM では、使いやすい Web ベースの管理インターフェイスを使用して、Small Office Home Office（SOHO）、Branch Office（BO; 営業所）、支店、中央サイト、本社など、さまざまなネットワーク環境内のルータを設定できます。

前提条件

要件

このドキュメントでは、Cisco ルータが完全に動作しており、Cisco SDM で設定変更できるように設定されていることを想定しています。

注: SDM でルータを設定できるようにするには、『SDM 用の HTTPS アクセスの許可』を参照してください。

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くものです。

- Cisco IOS? ソフトウェア リリース 12.4(8) が稼働中の Cisco 3640 ルータ
- Cisco Security Device Manager（SDM）バージョン 2.3.1

本書の情報は、特定のラボ環境にあるデバイスに基づいて作成されたものです。 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。 稼働中のネットワークで作業を行う場合、コマンドの影響について十分に理解したうえで作業してください。

注: シスコのサービス統合型ルータ（ISR）を使用する場合、より強力な機能を含む同様の設定の詳細については、「Cisco Configuration Professional を使用した基本的なルータの設定」を参照してください。 Cisco CP でサポートされているルータについては、『*Release Notes for Cisco Configuration Professional 2.5*』の「Supported Routers」の項を参照してください。

表記法

ドキュメント表記の詳細は、『シスコ テクニカル ティップスの表記法』を参照してください。

設定

このセクションでは、ネットワーク内にあるルータの基本的な設定を行うための情報を提供します。

ネットワーク図

このドキュメントでは、次のネットワーク構成を使用しています。

注: この設定で使用している IP アドレス スキームは、インターネット上で正式にルーティング可能なものではありません。 これらは、ラボ環境で使用された RFC 1918 のアドレスです。

インターフェイスの設定

Cisco ルータのインターフェイスを設定するには、次の手順を実行します。

1. Home をクリックして、SDM Home ページに移動します。SDM Home ページでは、ルータのハードウェアやソフトウェア、機能の可用性、および設定の概略などの情報が提供されています。 緑色の円はこのルータでサポートされている機能、赤色の円はサポートされていない機能を示しています。
2. [Configure] > [Interfaces and Connections] > [Create Connection] を選択して、インターフェイスの WAN 接続を設定します。例として、シリアル インターフェイス 2/0 の場合は、[Serial] オプションを選択して [Create New Connection] をクリックします。**注:** Ethernet などの別の種類のインターフェイスの場合は、対応するインターフェイス タイプを選択して [Create New Connection] ボタンをクリックします。
3. 選択したインターフェイスが表示されたら、Next をクリックして次に進みます。
4. [Available Interfaces] のオプションから [Serial interface 2/0]（目的のインターフェイス）を選択して、[Next] をクリックします。

5. シリアル インターフェイスのカプセル化の種類を選択して、[Next] をクリックします。
6. インターフェイスの固定 IP アドレスと対応するサブネット マスクを指定して、[Next] をクリックします。
7. ISP から提供されるネクストホップ IP アドレス (ネットワーク ダイアグラムでは、192.168.1.2) などのオプション パラメータを使用してデフォルト ルーティングを設定し、[Next] をクリックします。次のウィンドウが表示され、ユーザが行った設定の要約が表示されます。 **[Finish] をクリックします。**次のウィンドウが表示され、ルータへのコマンド転送状況が表示されます。 非互換コマンドや非サポート機能によりコマンド転送が失敗した場合は、エラーが表示されます。
8. [Configure] > [Interfaces and Connections] > [Edit Interfaces/Connections] を選択して、さまざまなインターフェイスの追加/編集/削除を行います。インターフェイスの設定を編集または変更するには、変更するインターフェイスを強調表示して [Edit] をクリックします。 ここでは既存の固定 IP アドレスを変更できます。

NAT の設定

ダイナミック NAT の設定

Cisco ルータでダイナミック NAT を設定するには、次の手順を実行します。

1. [Configure] > [NAT] > [Basic NAT] を選択し、[Launch the selected task] をクリックして、基本的な NAT を設定します。
2. [Next] をクリックします。
3. インターネットまたは ISP に接続するインターフェイスを選択し、インターネット アクセスで共有する IP アドレス範囲を選択します。
4. 次のウィンドウが表示され、ユーザが行った設定の要約が表示されます。 **[Finish] をクリックします。**
5. Edit NAT Configuration ウィンドウが表示され、設定されたダイナミック NAT 設定と、オーバーロード変換 (PAT) された変換後の IP アドレスが表示されます。 ダイナミック NAT にアドレス プールを設定する場合は、[Address Pool] をクリックします。
6. [Add] をクリックします。ここでは、プール名、IP アドレス範囲、ネットマスクなどの情報を指定します。 プール内のほとんどのアドレスが割り当てられ、IP アドレス プールをほぼ使い果たしてしまうことがあります。 このような場合には、PAT を使用して 1 つの IP アドレスで複数の IP アドレス要求に対応することができます。 アドレス プールが枯渇しそうになったときにルータで PAT が使用されるようにするには、Port Address Translation (PAT) にチェックマークを付けます。
7. [Add] をクリックします。
8. [Edit] をクリックします。
9. [Type] フィールドで [Address Pool] を選択し、[Address Pool] に **pool1** という名前を入力して [OK] をクリックします。
10. 次のウィンドウが表示され、アドレス プールを使用したダイナミック NAT の設定が表示されます。 Designate NAT Interfaces をクリックします。次のウィンドウを使用して、NAT 変換で使用する内部インターフェイスと外部インターフェイスを指定します。 NAT では変換ルールを解釈する際に、内部と外部の指定を参照します。これは、変換が内部から外部、外部から内部の両方向で行われるためです。指定すると、すべての NAT 変換ルールでこれらのインターフェイスが使用されます。 指定したインターフェイスは、メインの NAT ウィンドウの変換ルール リストの上部に表示されます。

スタティック NAT の設定

Cisco ルータでスタティック NAT を設定するには、次の手順を実行します。

1. [Configure] > [NAT] > [Edit NAT Configuration] を選択し、[Add] をクリックして、スタティック NAT を設定します。
2. [Direction] で、[From inside to outside] または [From outside to inside] を選択し、[Translate from Interface] で変換する内部 IP アドレスを指定します。 [Translate to Interface] エリアで、タイプを選択します。**変換元のアドレス**を [IP Address] フィールドで指定した IP アドレスに変換する場合は、[IP Address] を選択します。**変換元のアドレス**で、ルータのインターフェイスのアドレスが使用されるようにするには、[Interface] を選択します。 Translate from のアドレスが、インターフェイス フィールドで指定したインターフェイスに割り当てられている IP アドレスに変換されます。変換に内部デバイスのポート情報を含めるには、[Redirect Port] にチェックマークを入れます。 これにより、各デバイスに指定されたポートが同一でない限り、複数のデバイスで 1 つのパブリック IP アドレスを使用できるようになります。 この変換先アドレスの各ポート マッピングについて、エントリを作成する必要があります。 TCP ポート番号の場合は [TCP]、UDP ポート番号の場合は [UDP] をクリックします。 Original Port フィールドに、内部デバイスのポート番号を入力します。 Translated Port フィールドに、ルータがこの変換で使用するポート番号を入力します。 「インターネットから内部デバイスにアクセスできるようにする場合」セクション (『ネットワーク アドレス変換の設定： 『内部デバイスのアクセスにインターネットを許可』を参照してください。次のウィンドウに、ポート リダイレクトをイネーブルにしたスタティック NAT の設定が表示されます。

ルーティングの設定

スタティック ルーティングの設定

Cisco ルータでスタティック ルーティングを設定するには、次の手順を実行します。

1. [Configure] > [Routing] > [Static Routing] を選択し、[Add] をクリックして、スタティック ルーティングを設定します。
2. 宛先ネットワーク アドレスとマスクを入力し、発信インターフェイスまたはネクストホップ IP アドレスのいずれかを選択します。次のウィンドウに、10.1.1.0 ネットワークへのスタティック ルートが表示されています。ネクストホップ IP アドレスは 192.168.1.2 です。

ダイナミック ルーティングの設定

Cisco ルータでダイナミック ルーティングを設定するには、次の手順を実行します。

1. [Configure] > [Routing] > [Dynamic Routing] を選択します。
2. [RIP] を選択し、[Edit] をクリックします。
3. [Enable RIP] にチェックマークを付け RIP のバージョンを選択し、[Add] をクリックします。
4. アドバタイズするネットワーク アドレスを指定します。
5. [OK] をクリックします。
6. [Deliver] をクリックして、コマンドをルータに転送します。次のウィンドウに、ダイナミック RIP ルーティングの設定が表示されます。

その他の設定

Cisco ルータでその他の基本的な設定を行うには、次の手順を実行します。

1. ルータのホスト名、ドメイン名、バナー、およびイネーブル シークレット パスワードのプロパティを変更する場合は、[Configure] > [Additional Tasks] > [Router Properties] を選択して、[Edit] をクリックします。
2. [Configure] > [Additional Tasks] > [Router Access] > [User Accounts/View] を選択して、ルータに対するユーザ アカウントの追加/編集/削除を行います。
3. [File] > [Save Running Config to PC...] を選択して、設定内容をルータの NVRAM および PC に保存し、現在の設定をデフォルト（工場出荷時）設定にリセットします。
4. タスク バーに移動し、[Edit] > [Preferences] を選択して、次のユーザ設定オプションを有効にします。ルータへの転送前にコマンドをプレビューする。シグニチャ ファイルをフラッシュに保存する。SDM を終了する前に確認する。モード/タスクの切り替え時に、インターフェイスのステータスのモニタリングを継続する。
5. 次の操作を行う場合は、タスク バーから View を選択します。Home、Configure、または Monitor ページを表示する。ルータの実行コンフィギュレーションを表示する。さまざまな **show コマンド**を表示する。SDM のデフォルトの規則を表示する。CLI で設定されたルータ設定がある場合に、Refresh を選択して、ルータの設定を SDM に同期させる。

CLI 設定

ルータの設定

```
Router#show run
Building configuration...

Current configuration : 2525 bytes
!
version 12.4
service timestamps debug datetime msec
service timestamps log datetime msec
no service password-encryption
!
hostname Router
!
boot-start-marker
boot-end-marker
!
no logging buffered
enable password cisco
!
no aaa new-model
!
resource policy
!
!
!
ip cef
!
!
!
!--- RSA certificate generated after you enable the !---
ip http secure-server command.
```

```
crypto pki trustpoint TP-self-signed-392370502
 enrollment selfsigned
 subject-name cn=IOS-Self-Signed-Certificate-392370502
 revocation-check none
 rsakeypair TP-self-signed-392370502
!
!
crypto pki certificate chain TP-self-signed-392370502
 certificate self-signed 01
  3082023C 308201A5 A0030201 02020101 300D0609 2A864886
F70D0101 04050
  30312E30 2C060355 04031325 494F532D 53656C66 2D536967
6E65642D 43657
  69666963 6174652D 33393233 37303530 32301E17 0D303530
39323330 34333
  375A170D 32303031 30313030 30303030 5A303031 2E302C06
03550403 13254
  532D5365 6C662D53 69676E65 642D4365 72746966 69636174
652D3339 32333
  35303230 819F300D 06092A86 4886F70D 01010105 0003818D
00308189 02818
  C86C0F42 84656325 70922027 EF314C2F 17C8BBE1 B478AFA3
FE2BC2F2 3C272
  A3B5E13A 1392A158 73D8FE0D 20BFD952 6B22890C 38776830
241BE259 EE2AA
  CF4124EA 37E41B46 A2076586 2F0F9A74 FDB72B3B 6159EEF7
0DEC7D44 BE489
  9E351BF7 F5C808D9 2706C8B7 F5CE4B73 39ED8A61 508F455A
68245A6B D072F
  02030100 01A36630 64300F06 03551D13 0101FF04 05300301
01FF3011 06035
  11040A30 08820652 6F757465 72301F06 03551D23 04183016
80148943 F2369
  ACD8CCA6 CA04EC47 C68B8179 E205301D 0603551D 0E041604
148943F2 36910
  D8CCA6CA 04EC47C6 8B8179E2 05300D06 092A8648 86F70D01
01040500 03818
  3B93B9DC 7DA78DF5 6D1D0D68 6CE075F3 FFDAD0FB 9C58E269
FE360329 2CEE3
  D8661EB4 041DEFEF E14AA79D F33661FC 2E667519 E185D586
13FBD678 F52E1
  E3C92ACD 52741FA4 4429D0B7 EB3DF979 0EB9D563 51C950E0
11504B41 4AE79
  0DD0BE16 856B688C B727B3DB 30A9A91E 10236FA7 63BAEACB
5F7E8602 0C33D
  quit
!
!
!
!
!
!
!
!
!
!
!--- Create a user account named sdmsdm with all
privileges.

username sdmsdm privilege 15 password 0 sdmsdm
!
!
!
!
```

```
!
!
interface Ethernet0/0
 no ip address
 shutdown
 half-duplex
!
!--- The LAN interface configured with a private IP
address. interface FastEthernet1/0 ip address 172.16.1.2
255.255.255.0 !--- Designate that traffic that
originates from behind !--- the interface is subject to
Network Address Translation (NAT).  ip nat inside
 ip virtual-reassembly
 duplex auto
 speed auto
!
!--- This is the WAN interface configured with a
routable (public) IP address. interface Serial2/0 ip
address 192.168.1.1 255.255.255.0 !--- Designate that
this interface is the !--- destination for traffic that
has undergone NAT. ip nat outside
 ip virtual-reassembly
!
interface Serial2/1
 no ip address
 shutdown
!
interface Serial2/2
 no ip address
 shutdown
!
interface Serial2/3
 no ip address
 shutdown
!
!--- RIP version 2 routing is enabled. router rip
version 2 network 172.1.0.0 no auto-summary !--- This is
where the commands to enable HTTP and HTTPS are
configured. ip http server ip http secure-server ! !---
This configuration is for dynamic NAT.

!
!--- Define a pool of outside IP addresses for NAT. ip
nat pool pool1 192.168.1.3 192.168.1.10 netmask
255.255.255.0 !--- In order to enable NAT of the inside
source address, !--- specify that traffic from hosts
that match access list 1 !--- are NATed to the address
pool named pool1. ip nat inside source list 1 pool pool1
! !--- Access list 1 permits only 172.16.1.0 network to
be NATed. access-list 1 remark SDM_ACL Category=2
access-list 1 permit 172.16.1.0 0.0.0.255 ! !--- This
configuration is for static NAT

!--- In order to translate the packets between the real
IP address 172.16.1.1 with TCP !--- port 80 and the
mapped IP address 192.168.1.1 with TCP port 500. ip nat
inside source static tcp 172.16.1.1 80 192.168.1.3 500
extendable
!
!

!
!
!--- The default route is configured and points to
```

```
192.168.1.2. ip route 0.0.0.0 0.0.0.0 192.168.1.2 ! ! !--
-- The static route is configured and points to
192.168.1.2. ip route 10.1.1.0 255.255.255.0 192.168.1.2
! ! control-plane ! ! ! ! ! ! ! ! ! line con 0 line
aux 0 !--- Telnet enabled with password as sdmsdm. line
vty 0 4 password sdmsdm login ! ! end
```

確認

[Configure] > [Interface] & [Connections] > [Edit Interface Connections] > [Test Connection] の順に選択して、エンドツーエンド接続をテストします。 リモート エンドの IP アドレスを指定するには、[User-specified] オプション ボタンをクリックします。

トラブルシューティング

Output Interpreter Tool（OIT）（登録ユーザ専用）では、特定の **show** コマンドがサポートされています。 OIT を使用して、**show** コマンド出力の解析を表示できます。

注: debug コマンドを使用する前に、『デバッグ コマンドの重要な情報』を参照してください。

次の方法をトラブルシューティングに使用できます。

- タスク バーから [Tools] > [Update SDM] を選択して、SDM に対する ping、Telnet、および最新バージョンへのアップグレードを行います。 Cisco.com、ローカル PC、または CD からアップグレードできます。
- [Help] > [About this Router] を選択して、ルータのハードウェア設定に関する情報を表示します。次のウィンドウに、ルータに保存されている IOS イメージに関する情報が表示されます。
- [Help] オプションでは、ルータの設定に使用できる SDM のさまざまなオプションに関する情報が表示されます。

SDM の 64 ビット OS との互換性

SDM は 64 ビット OS マシンではサポートされていません。 ルータに SDM をインストールし、Web ブラウザからアクセスする必要があります。

ルータへの SDM ファイルのインストールに関する詳細については、「タスク 4： SDM ファイルのインストール」を参照してください。

Web ブラウザから SDM を起動できない

問題

Web ブラウザを使用して SDM を使用すると、SDM の起動エラー メッセージが表示されます。

解決策 1

問題は Java のバージョンである可能性があります。 Java の更新プログロムは SDM のバージョンと互換性がない場合があります。 Java のバージョンが Java 6 update 12 の場合、**そのバージョンをアンインストールして、Java 6 update 3 をインストールします。** これで問題が解消され

ます。 互換性に関する詳細については、「SDM 2.5 Release Note」の「Web Browser Versions and Java Runtime Environment Versionsの項を参照してください。 SDM バージョン 2.5 は Java バージョン 6 の update 2 および 3 で動作します。

解決策 2

問題を解決するために、Internet Explorer オプションの [Allow active content to run in files on My Computer] を有効にします。

1. Internet Explorer を開き、[Tools] > [Internet Options] > [Advanced] を選択します。
2. セキュリティのセクションで、[Allow active content to run in files on my computer] オプションと [Allow active content to install software even if the signature is invalid] オプションのチェックボックスをオンにします。
3. 変更を有効にするには、[OK] をクリックして、ブラウザを再起動します。

エラー： java.bling のスタック オーバーフロー

問題

SDM に接続できず、次のエラー メッセージが表示されます。

```
Router#show run
Building configuration...

Current configuration : 2525 bytes
!
version 12.4
service timestamps debug datetime msec
service timestamps log datetime msec
no service password-encryption
!
hostname Router
!
boot-start-marker
boot-end-marker
!
no logging buffered
enable password cisco
!
no aaa new-model
!
resource policy
!
!
!
ip cef
!
!
!
!--- RSA certificate generated after you enable the !--- ip http secure-server command.

crypto pki trustpoint TP-self-signed-392370502
 enrollment selfsigned
 subject-name cn=IOS-Self-Signed-Certificate-392370502
 revocation-check none
 rsakeypair TP-self-signed-392370502
!
```

```
!
crypto pki certificate chain TP-self-signed-392370502
 certificate self-signed 01
  3082023C 308201A5 A0030201 02020101 300D0609 2A864886 F70D0101 04050
  30312E30 2C060355 04031325 494F532D 53656C66 2D536967 6E65642D 43657
  69666963 6174652D 33393233 37303530 32301E17 0D303530 39323330 34333
  375A170D 32303031 30313030 30303030 5A303031 2E302C06 03550403 13254
  532D5365 6C662D53 69676E65 642D4365 72746966 69636174 652D3339 32333
  35303230 819F300D 06092A86 4886F70D 01010105 0003818D 00308189 02818
  C86C0F42 84656325 70922027 EF314C2F 17C8BBE1 B478AFA3 FE2BC2F2 3C272
  A3B5E13A 1392A158 73D8FE0D 20BFD952 6B22890C 38776830 241BE259 EE2AA
  CF4124EA 37E41B46 A2076586 2F0F9A74 FDB72B3B 6159EEF7 0DEC7D44 BE489
  9E351BF7 F5C808D9 2706C8B7 F5CE4B73 39ED8A61 508F455A 68245A6B D072F
  02030100 01A36630 64300F06 03551D13 0101FF04 05300301 01FF3011 06035
  11040A30 08820652 6F757465 72301F06 03551D23 04183016 80148943 F2369
  ACD8CCA6 CA04EC47 C68B8179 E205301D 0603551D 0E041604 148943F2 36910
  D8CCA6CA 04EC47C6 8B8179E2 05300D06 092A8648 86F70D01 01040500 03818
  3B93B9DC 7DA78DF5 6D1D0D68 6CE075F3 FFDAD0FB 9C58E269 FE360329 2CEE3
  D8661EB4 041DEFEF E14AA79D F33661FC 2E667519 E185D586 13FBD678 F52E1
  E3C92ACD 52741FA4 4429D0B7 EB3DF979 0EB9D563 51C950E0 11504B41 4AE79
  0DD0BE16 856B688C B727B3DB 30A9A91E 10236FA7 63BAEACB 5F7E8602 0C33D
  quit
!
!
!
!
!
!
!
!
!
!
!--- Create a user account named sdmsdm with all privileges.

username sdmsdm privilege 15 password 0 sdmsdm
!
!
!
!
!
!
interface Ethernet0/0
 no ip address
 shutdown
 half-duplex
!
!--- The LAN interface configured with a private IP address. interface FastEthernet1/0 ip
address 172.16.1.2 255.255.255.0 !--- Designate that traffic that originates from behind !---
the interface is subject to Network Address Translation (NAT).  ip nat inside
 ip virtual-reassembly
 duplex auto
 speed auto
!
!--- This is the WAN interface configured with a routable (public) IP address. interface
Serial2/0 ip address 192.168.1.1 255.255.255.0 !--- Designate that this interface is the !---
destination for traffic that has undergone NAT. ip nat outside
 ip virtual-reassembly
!
interface Serial2/1
 no ip address
 shutdown
!
interface Serial2/2
 no ip address
```

```
 shutdown
!
interface Serial2/3
 no ip address
 shutdown
!
!--- RIP version 2 routing is enabled. router rip version 2 network 172.1.0.0 no auto-summary !-
-- This is where the commands to enable HTTP and HTTPS are configured. ip http server ip http
secure-server ! !--- This configuration is for dynamic NAT.

!
!--- Define a pool of outside IP addresses for NAT. ip nat pool pool1 192.168.1.3 192.168.1.10
netmask 255.255.255.0 !--- In order to enable NAT of the inside source address, !--- specify
that traffic from hosts that match access list 1 !--- are NATed to the address pool named pool1.
ip nat inside source list 1 pool pool1 ! !--- Access list 1 permits only 172.16.1.0 network to
be NATed. access-list 1 remark SDM_ACL Category=2 access-list 1 permit 172.16.1.0 0.0.0.255 ! !-
-- This configuration is for static NAT

!--- In order to translate the packets between the real IP address 172.16.1.1 with TCP !--- port
80 and the mapped IP address 192.168.1.1 with TCP port 500. ip nat inside source static tcp
172.16.1.1 80 192.168.1.3 500 extendable
!
!

!
!
!--- The default route is configured and points to 192.168.1.2. ip route 0.0.0.0 0.0.0.0
192.168.1.2 ! ! !--- The static route is configured and points to 192.168.1.2. ip route 10.1.1.0
255.255.255.0 192.168.1.2 ! ! control-plane ! ! ! ! ! ! ! ! ! line con 0 line aux 0 !---
Telnet enabled with password as sdmsdm. line vty 0 4 password sdmsdm login ! ! end
```

解決策

この問題は通常、Java コード バージョン 1.5.0_06 が使用されているときに発生します。 この問題を解決する方法については、「The user is unable to connect to Security Device Manager (SDM) and receives the java.bling stack over flow error message.」を参照してください。

関連情報

- Cisco Security Device Manager インストール ガイド
- Cisco 製品に関するサポートページ：ルータ
- Cisco Configuration Professional のサポート ページ
- NAT に関するサポートページ
- テクニカル サポートとドキュメント – Cisco Systems