

Cisco Start Router

設定マニュアル ポートフォワーディング Cisco 841M J

2016年2月19日
第1.0版



www.networld.co.jp

株式会社ネットワールド



Networld



Cisco Start Router

設定マニュアル ポートフォワーディング Cisco 841M J



改訂履歴

版番号	改訂日	改訂者	改訂内容
1.0	2016年2月19日	ネットワーク	● 新規



免責事項

- 本書のご利用は、お客様ご自身の責任において行われるものとします。本書に記載する情報については、株式会社ネットワーク（以下 弊社）が慎重に作成および管理いたしますが、弊社がすべての情報の正確性および完全性を保証するものではありません。
- 弊社は、お客様が本書からご入手された情報により発生したあらゆる損害に関して、一切の責任を負いません。また、本書および本書にリンクが設定されている他の情報元から取得された各種情報のご利用によって生じたあらゆる損害に関しても、一切の責任を負いません。
- 弊社は、本書に記載する内容の全部または一部を、お客様への事前の告知なしに変更または廃止する場合がございます。なお、弊社が本書を更新することをお約束するものではありません。



表記規則

表記	表記の意味
「」 (括弧記号)	キー、テキストボックス、ラジオボタンなどのオブジェクト
bold (ボールド文字)	入力または選択するシステム定義値
<i><italic></i> (イタリック文字)	入力または選択するユーザー定義値
□ (囲み線)	入力または選択するオブジェクト
"" (二重引用符記号)	表示されるメッセージ
[] (蛍光マーカー)	確認するメッセージ

表記の例)

(1) 「Exec」ラジオボタンを選択します。

(2) テキストボックスに以下のコマンドを入力します。

copy running-config <file name>

(3) 「コマンドを実行」ボタンをクリックします。正常に実行されれば、画面に「[OK]」が表示されます。

Destination filename [startup-config]?

Building configuration...

[OK]

1

2

3

CLIによる設定

CLI機能はルータのコマンドプロンプトで実行可能な設定や、全てのIOS CLIコマンドを入力できます

Exec
 Configure

copy running-config startup-config

Destination filename [startup-config]?
Building configuration...

[OK]



目次

1. はじめに.....	1
1.1 対象製品.....	1
1.2 CCP Express のシステム要件.....	1
1.3 クイックリンク.....	2
2. システム構成.....	3
2.1 使用した機材.....	4
3. 設定手順.....	5
3.1 ゾーンの設定.....	5
3.1.1 WAN ゾーンの設定.....	5
3.1.2 LAN ゾーンの設定.....	8
3.2 ポートフォワーディングの設定.....	9
3.3 ポリシーの設定.....	11
3.3.1 WAN-LAN ゾーンのパリシーの設定.....	11
4. 設定ファイル.....	16



1. はじめに

本書は、Cisco Configuration Professional Express（以下 CCP Express）のアドバンスドセットアップを使用して Cisco 841M J シリーズのポートフォワーディングの設定を実行する手順を説明した資料です。本書では、IP アドレスとポート番号を変換する NAT デバイスとして、製品を設定します。CCP Express は、Web UI を備えた組み込みのデバイス管理ツールです。CCP Express のアドバンスドセットアップを使用すると、WAN、LAN、およびセキュリティなど、製品の詳細設定を簡単に実行できます。ポートフォワーディングの設定が完了すると、インターネットなどのパブリックネットワークのホストが、LAN などのプライベートネットワークの特定のホストで許可された特定のサービスに接続できるようになります。

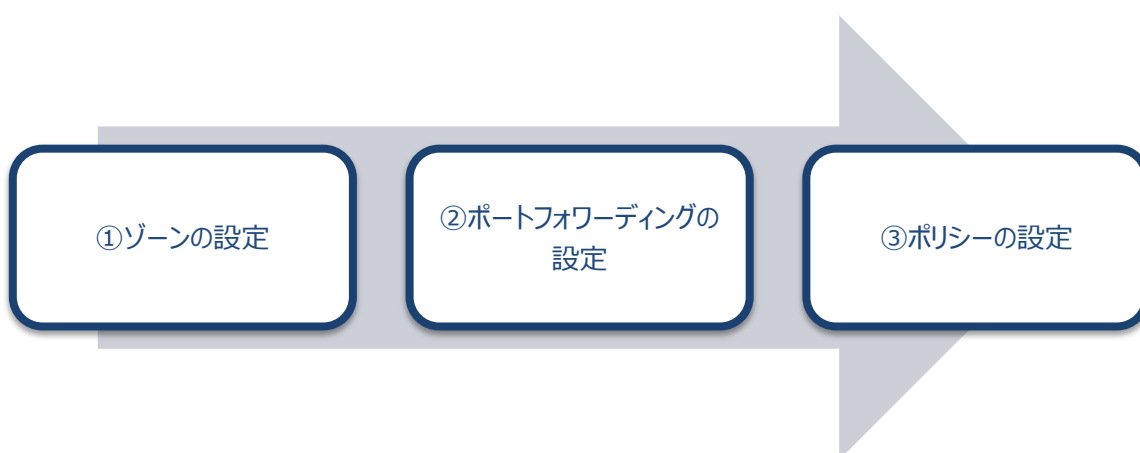


図 1 本書で実行する設定

1.1 対象製品

本書を使用してポートフォワーディングの設定を実行できる製品は、以下のとおりです。

表 1 本書の対象製品

C841M-4X-JSEC/K9	C841M-4X-JAIS/K9	C841M-8X-JAIS/K9
☑	☑	☑

1.2 CCP Express のシステム要件

CCP Express を使用できる Cisco IOS および Web ブラウザーは、次のとおりです。なお、本書では CCP Express のセキュリティ機能（ゾーン、ポリシー、VPN などのセキュリティ設定）を使用するため、製品にバージョン 15.5(1)T 以上の Cisco IOS がインストールされている必要があります。

- Cisco IOS 15.2(4)M2～、または 15.3(1)T～、セキュリティ機能は 15.5(1)T～



- Microsoft Internet Explorer 10
- Google Chrome 17～
- Mozilla Firefox 10～

1.3 クイックリンク

Cisco 841M J シリーズの公式の情報は、以下の URL から入手できます。

- Cisco Start Router ホーム:
<http://www.cisco.com/web/JP/smb/c800m/index.html>
- 製品カタログ:
http://www.cisco.com/web/JP/product/catalog/pdf/1082_en_start_catalog.pdf
- データシート:
http://www.cisco.com/web/JP/smb/c800m/docs/c800mj_data_sheet_c78-732678.pdf
- サポートコミュニティ:
<https://supportforums.cisco.com/ja/start>
- よくある質問:
<http://www.cisco.com/web/JP/smb/c800m/c800m-faq.html>
- サポート窓口:
<http://www.cisco.com/web/JP/smb/c800m/c800m-support.html>



2. システム構成

ポートフォーワーディングの設定の手順は、以下の構成で説明します。

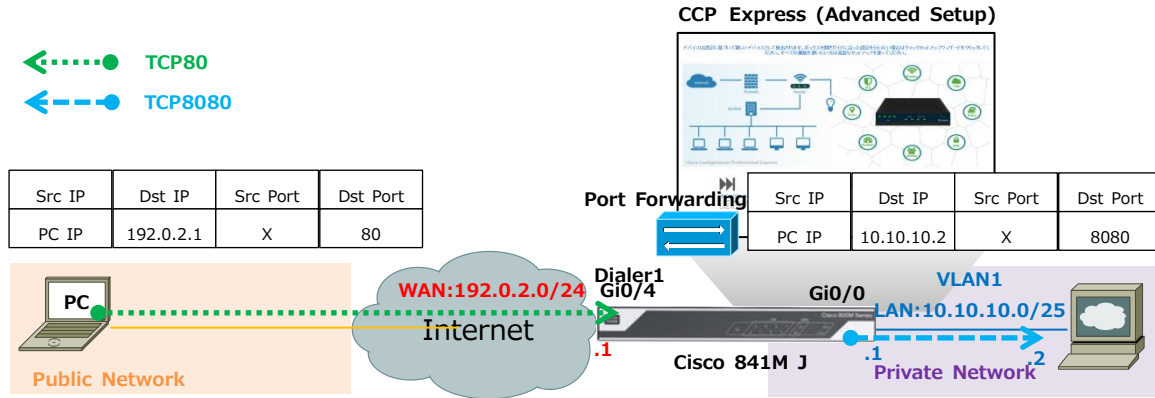


図 2 ポートフォーワーディングの設定で構成するシステム

製品は、内部グローバルアドレス（自身のパブリック IP アドレスと宛先ポート番号）と内部ローカルアドレス（ホストのプライベート IP アドレスと宛先ポート番号）を 1 対 1 に対応付けして宛先を変換することで、パブリックネットワークからプライベートネットワークへの透過的な接続を実現します。プライベートネットワークのホストは、プライベート IP アドレスと TCP8080 番を使用するサービスを提供します。パブリックネットワークのホストは、TCP80 番と製品のパブリック IP アドレスを宛先に指定することで、プライベートネットワークのサービスに接続します。なお、本書では、製品はクイックセットアップウィザードを使用したインターフェースや VLAN などの LAN 側の基本設定、PPPoE、デフォルトルート、NAT などの WAN 側の基本設定、およびインターネット接続用の標準的なファイアウォール設定が完了しているものとします。クイックセットアップウィザードを使用した製品の初期セットアップについては、クイックスタートガイドをご参照ください。

- Cisco Start Router 設定マニュアル クイックスタートガイド Cisco 841M J:
http://www.networkworld.co.jp/download_file/4574/7266/



2.1 使用した機材

本書で使用した機材は、以下のとおりです。

表 2 本書で使用した機材

機材	製品型番または名称	備考
Cisco 841M J シリーズ	C841M-4X-JAIS/K9 15.5(3)M	
デバイス管理ツール	CCP Express 3.1.2	
PC	Windows 7 x64 Professional	
(Public Network)	SP1	
Web ブラウザー	Internet Explorer x64 11.0.9600.18163	
サーバー	CentOS x64 6.5	
サービスアプリケーション (Private Network)	Apache HTTP Server x64 2.2.15-31	TCP8080 番で待ち受け



3. 設定手順

Cisco 841M J シリーズのポートフォワーディングの設定を実行します。

3.1 ゾーンの設定

既定の WAN ゾーンと LAN ゾーンに、ポートフォワーディングで使用するインターフェースを割り当てます。ゾーンはポリシーの前提条件で、ポリシーはゾーンのペアに対して適用されます。パブリックネットワークのホストがポートフォワーディングによってプライベートネットワークのホストに接続されるためには、ポートフォワーディングで使用するインターフェースが所属するゾーンに対して、接続を許可するポリシーを設定する必要があります。ゾーンに対してポリシーが割り当てられていない場合、既定ですべてのトラフィックが破棄（Drop）されます。

3.1.1 WAN ゾーンの設定

既定の WAN ゾーンに、ポートフォワーディングで使用する WAN 側インターフェースを割り当てます。

(1) インターフェースの設定画面に移動します。「インターフェイスと接続」ボタンをクリックします。ホーム画面が表示されていない場合は、「ホーム」ボタンをクリックするか、またはショートカットメニューから「インターフェイス」ボタンをクリックしてください。



<p>インターフェイスと接続 LAN/WANインターフェイスを含め、すべてのデバイスのインターフェイスを設定します。DSL、イーサネット、3G/4Gリンク、またはVLAN/ループバックインターフェイスを作成し、インターフェイス属性を設定します。</p>	<p>1</p> <p>DNS/DHCP/ホスト名 デバイスのホスト名、ドメイン名、DNSサーバ、IPv4のDHCPプールを設定します。</p>	<p>アイデンティティ 指定された特権レベルで新しいユーザーを構成し、エンドユーザービューを管理します。</p>
<p>静的ルーティング IPv4とIPv6の静的ルートを設定します。</p>	<p>ルータの診断 ルータに関する基本的な診断情報を表示します。ルータのバージョン、インターフェイス、ソフトウェアバージョンなどをフラッシュやCPUの利用統計と共に表示します。</p>	<p>プラグアンドプレイサーバの設定 プラグアンドプレイサーバをセットアップし、デバイスを自動設定します。</p>
<p>トラブルシューティング PingまたはTracerouteを使用し、他のIPv4またはIPv6の宛先への接続性をトラブルシューティングします。</p>	<p>任意のコマンド IOSコマンドを設定し、showコマンドを実行します。</p>	<p>シスコアクティブアドバイザー ハードウェアおよびソフトウェア製品の使用情報をCiscoに送信します。</p>
<p>セキュリティ ファイアウォール、侵入防御、VPN、およびコンテンツセキュリティ機能を備えた攻撃防御の主要コンポーネントを含む包括的なソリューション。</p>	<p>クイックセットアップ・ウィザード このウィザードを使用すると簡単にWAN/LAN接続の設定が可能です。すでに設定済みのルータには使用しないでください。</p>	

図 3 CCP Express のホーム（インターフェイスと接続）



図 4 CCP Express のショートカット（ホームとインターフェイス）

(2) WAN 側インターフェイスを編集します。「GigabitEthernet0/4」ラベル内の「編集」ボタンをクリックします。



インターフェイス

ループバックの追加 VLANの追加 編集 削除

プライマリWAN: GigabitEthernet0/4(Dialer1)
 バックアップWAN: 未構成
 [ゾーン](#)

*注意: 複数選択できません。

インターフェイス	IPv4 アドレス	IPv6 アドレス	管理状態	操作状態	説明	アクション
構成可能なインターフェイス						
<input type="checkbox"/>	GigabitEthernet0/0		↑	up		
<input type="checkbox"/>	GigabitEthernet0/1		↑	down		
<input type="checkbox"/>	GigabitEthernet0/2		↑	down		
<input type="checkbox"/>	GigabitEthernet0/3		↑	down		
<input type="checkbox"/>	GigabitEthernet0/4		↑	up		
<input type="checkbox"/>	GigabitEthernet0/5		↓	down		
<input type="checkbox"/>	Vlan1	10.10.10.1	↑	up	\$ETH_LAN\$	
読み取り専用のインターフェイス						
<input type="checkbox"/>	NV10		↑	up		
<input type="checkbox"/>	Virtual-Access1		↑	up		
<input type="checkbox"/>	Virtual-Access2		↑	up		
<input type="checkbox"/>	Dialer1	192.0.2.1	↑	up		

図 5 インターフェイスの編集

(3) WAN 側インターフェイスを既定の WAN ゾーンに割り当てます。「WAN ゾーンに移動」チェックボックスにチェックを入れます。「はい」ボタンをクリックします。この設定はプライマリ WAN インターフェイスの既定の設定のため、ほとんどの場合、当該インターフェイスはすでに WAN ゾーンに割り当てられています。

編集 GigabitEthernet0/4 インターフェイス

▼ プライマリセカンダリインターフェイス

なし
 プライマリWANインターフェイス
 バックアップWANインターフェイス

1 WANゾーンに移動

▶ 接続
 ▶ IPv4 アドレス
 ▶ IPv6 アドレス
 ▶ 認証

2



図 6 インターフェイスの編集 (詳細)

3.1.2 LAN ゾーンの設定

既定の LAN ゾーンに、ポートフォワーディングで使用する LAN 側インターフェースを割り当てます。

(1) セキュリティの設定画面に移動します。「セキュリティ」ボタンをクリックします。ホーム画面が表示されていない場合は、「ホーム」ボタンをクリックするか、またはショートカットメニューから「セキュリティ」ボタンをクリックしてください。



図 7 CCP Express のホーム (セキュリティ)



図 8 CCP Express のショートカット (ホームとセキュリティ)

(2) LAN 側インターフェースを既定の LAN ゾーンに割り当てます。「ゾーン」タブをクリックします。「使用可能なインターフェイス」リスト内の「Vlan1」ラベルをドラッグし、「ゾーン LAN」リストにドロップします。「適用する」ボタンをクリックします。この設定は初期セットアップにクイックセットアップウィザードを使用した



場合の既定の設定のため、ほとんどの場合、当該インターフェースはすでにLANゾーンに割り当てられています。

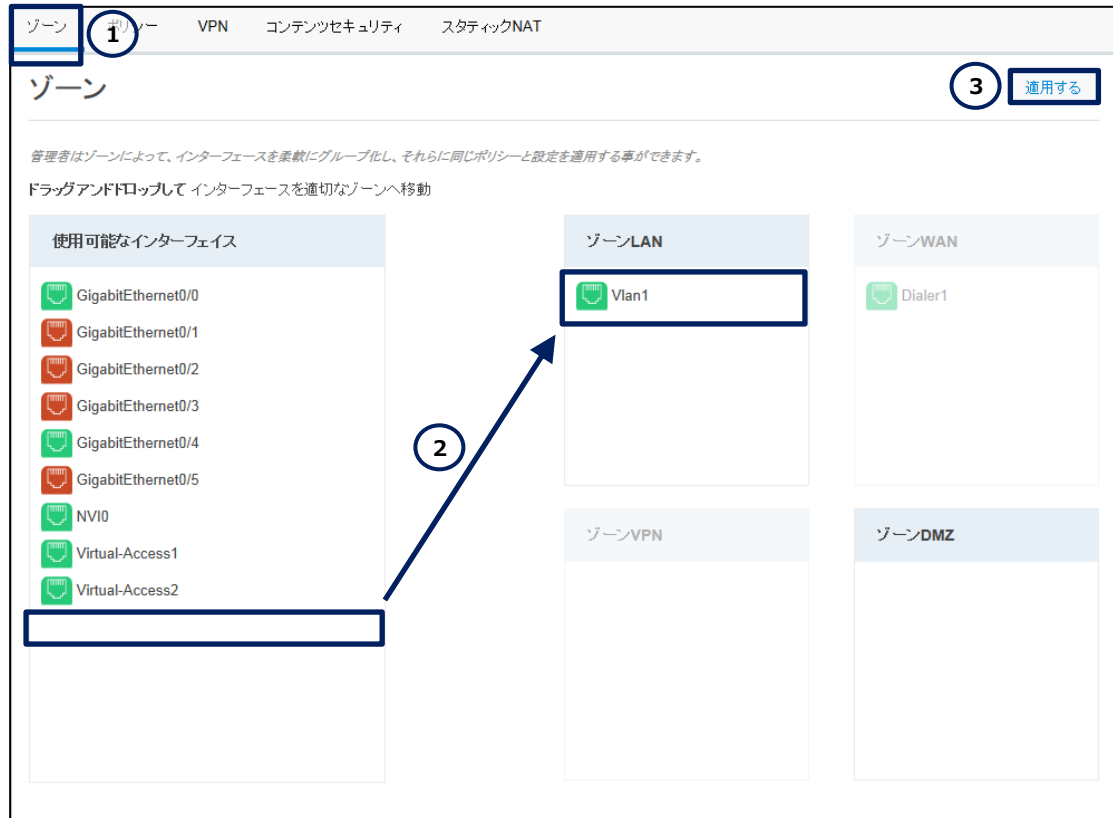


図 9 セキュリティの編集 (ゾーン)

3.2 ポートフォワーディングの設定

内部ローカルアドレスと内部グローバルアドレスを関連付けます。

(1) セキュリティの設定画面に移動します。「セキュリティ」ボタンをクリックします。ホーム画面が表示されていない場合は、「ホーム」ボタンをクリックするか、またはショートカットメニューから「セキュリティ」ボタンをクリックしてください。



インターフェイスと接続
LAN/WANインターフェイスを含め、すべてのデバイスのインターフェイスを設定します。DSL、イーサネット、3G/4Gリンク、またはVLAN/ループバックインターフェイスを作成し、インターフェイス属性を設定します。

DNS/DHCP/ホスト名
デバイスのホスト名、ドメイン名、DNSサーバ、IPv4のDHCPプールを設定します。

アイデンティティ
指定された特権レベルで新しいユーザーを構成し、エンドユーザービューを管理します。

静的ルーティング
IPv4とIPv6の静的ルートを設定します。

ルータの診断
ルータに関する基本的な診断情報を表示します。ルータのバージョン、インターフェイス、ソフトウェアバージョンなどをフラッシュやCPUの利用統計と共に表示します。

プラグアンドプレイサーバの設定
プラグアンドプレイサーバをセットアップし、デバイスを自動設定します。

トラブルシューティング
PingまたはTracerouteを使用し、他のIPv4またはIPv6の宛先への接続性をトラブルシューティングします。

任意のコマンド
IOSコマンドを設定し、showコマンドを実行します。

シスコアクティブアドバイザー
ハードウェアおよびソフトウェア製品の使用情報をCiscoに送信します。

セキュリティ
ファイアウォール、侵入防御、VPN、およびコンテンツセキュリティ機能を備えた攻撃防御の主要コンポーネントを含む包括的なソリューション。

クイックセットアップ・ウィザード
このウィザードを使用すると簡単にWAN/LAN接続の設定が可能です。すでに設定済みのルータには使用しないでください。

図 10 CCP Express のホーム (セキュリティ)



図 11 CCP Express のショートカット (ホームとセキュリティ)

(2) スタティック NAT を追加します。ポートフォワーディングは、スタティック NAT の一種です。

- ① 「スタティック NAT」タブをクリックします。
- ② 「追加」ボタンをクリックします。

ゾーン ポリシー VPN コンテンツセキュリティ **スタティック NAT**

スタティック NAT 追加

スタティック NAT は、実アドレスからマッピングされたアドレスへの固定的変換を作成します。

データが見つかりません

図 12 スタティック NAT の編集



(3) ポートフォワーディングを設定します。「*」ラベルが記載された設定は、必須の設定です。

- ① 「内部 IP」テキストボックスにプライベートネットワークのホストの IP アドレス（内部ローカルアドレス）である **10.10.10.2** を入力します。
- ② 「外部 IP/インターフェース」テキストボックスに製品の WAN 側インターフェースの IP アドレス（内部グローバルアドレス）である **192.0.2.1** を入力します。IP アドレスを固定できない場合は、WAN 側インターフェースのインターフェース名を内部グローバルアドレスとして設定できます。
- ③ 「ポートフォワーディングを有効にする」チェックボックスにチェックを入れます。
- ④ 「TCP」ラジオボタンをクリックします。
- ⑤ 「内部ポート」テキストボックスにプライベートネットワークのホストのサービスのポート番号である **8080** を入力します。
- ⑥ 「外部ポート」テキストボックスに製品のポートフォワーディング用の待ち受けポート番号である **80** を入力します。
- ⑦ 「はい」ボタンをクリックします。




図 13 スタティック NAT の編集（詳細）

3.3 ポリシーの設定

ポートフォワーディングで使用するインターフェースが所属するゾーンに対して、ポリシーを設定します。

3.3.1 WAN-LAN ゾーンポリシーの設定

既定の WAN ゾーンから既定の LAN ゾーンに向かうゾーンペアに対して、特定の IP アドレスとポート番号への接続を許可するポリシーを設定します。

(1) セキュリティの設定画面に移動します。「セキュリティ」ボタンをクリックします。ホーム画面が表示され



ていない場合は、「ホーム」ボタンをクリックするか、またはショートカットメニューから「セキュリティ」ボタンをクリックしてください。



図 14 CCP Express のホーム（セキュリティ）



図 15 CCP Express のショートカット（ホームとセキュリティ）

(2) ポリシーを追加します。

- ① 「ポリシー」タブをクリックします。
- ② 「追加」ボタンをクリックします。



図 16 ポリシーの編集

(3) 既定の WAN ゾーンから既定の LAN ゾーンに向かう特定のトラフィックに対するポリシーを設定します。

- ① 「ポリシー名」テキストボックスにポリシー名を入力します。
- ② 必要に応じて、「ポリシーの説明」テキストボックスにポリシーの説明を入力します。
- ③ 「送信元ゾーン」ドロップダウンリストで **WAN** を選択します。
- ④ 「宛先ゾーン」ドロップダウンリストで **LAN** を選択します。
- ⑤ 「アクション」ドロップダウンリストで **許可** を選択します。
- ⑥ 「ネットワーク」タブをクリックします。
- ⑦ 「宛先ネットワーク」テキストボックスにプライベートネットワークのホストの IP アドレス（内部ローカルアドレス）である **10.10.10.2/32** を入力します。このテキストボックスでは、ネットワークアドレス、IP アドレスとサブネットマスク、またはネットワークアドレスの範囲（ハイフン区切り）を使用できます。
- ⑧ 「+」ボタンをクリックします。なお、ひとつでも宛先ネットワークを追加すると、既定の Any ポリシーは削除されます。
- ⑨ 「ポート」タブをクリックします。
- ⑩ 「宛先ポート」ドロップダウンリストでプライベートネットワークのホストのサービスプロトコルである **TCP** を選択します。
- ⑪ 「宛先ポート」テキストボックスにプライベートネットワークのホストのサービスポート番号である **8080** を入力します。
- ⑫ 「+」ボタンをクリックします。なお、ひとつでも宛先ポートを追加すると、既定の Any ポリシーは削除されます。
- ⑬ 「セーブ」ボタンをクリックします。



セキュリティポリシーウィザード

ポリシー名 **1** PortForwarding ポリシーの説明 **2** ポリシーの説明 アクショ **5** 許可

送信元ゾーン **3** WAN 宛先ゾーン **4** LAN

ネットワーク アプリケーション ポート ドメインフィルタリング ユーザグループ

6 送信元ネットワーク

宛先ネットワーク

送信元ネットワークアドレス + **7** 10.10.10.2/32 x + **8**

例: 192.168.0.0, IP サブネット: 192.168.0.0/8 または 範囲: 192.168.0.0 - 192.200.0.0

セーブ キャンセル

図 17 ポリシーの編集（詳細 - ネットワーク）



セキュリティポリシーウィザード

ポリシー名: PortForwarding ポリシーの説明: ポリシーの説明 アクション: 許可

送信元ゾーン: WAN 宛先ゾーン: LAN

ネットワーク アプリケーション **9** **ポート** ドメインフィルタリング ユーザグループ

ドラッグアンドドロップして ポートを送信元または宛先ポートへ移動

利用可能なポート

bgp	chargen	cmd	daytime	discard (tcp)
discard (udp)	domain (tcp)	domain (udp)	drip	echo (tcp)
echo (udp)	exec	finger	ftp	ftp-data

送信元ポート

宛先ポート

TCP 送信元ポート + **10** TCP 8080 × + **12**

例: TCP:40, UDP:60 または 範囲: UDP:1000 - 2000, TCP:2000 - 3000

13 **保存** キャンセル

図 18 ポリシーの編集 (詳細 - ポート)

設定は以上です。Web ブラウザー等を使用して、パブリックネットワークのホストがプライベートネットワークの特定のホストの TCP8080 ベースのサービスに接続できることを確認してください。



4. 設定ファイル

本書で追加または変更される設定（クイックスタートガイドを使用した設定との差分）は、以下のとおりです。

```
001: object-group service INTERNAL_UTM_SERVICE
002: object-group network portforwarding_dst_net
003: host 10.10.10.2
004: object-group network portforwarding_src_net
005: any
006: object-group service portforwarding_svc
007: tcp eq 8080
008: class-map type inspect match-all portforwarding
009: match access-group name portforwarding_acl
010: class-map type inspect match-any INTERNAL_DOMAIN_FILTER
011: match protocol msnmsgr
012: match protocol ymsgr
013: policy-map type inspect WAN-LAN-POLICY
014: class type inspect portforwarding
015: inspect
016: class type inspect INTERNAL_DOMAIN_FILTER
017: inspect
018: class class-default
019: drop log
020: zone security VPN
021: zone security DMZ
022: zone-pair security WAN-LAN source WAN destination LAN
023: service-policy type inspect WAN-LAN-POLICY
024: ip nat inside source static tcp 10.10.10.2 8080 192.0.2.1 80 extendable
025: ip access-list extended portforwarding_acl
026: permit object-group portforwarding_svc object-group
portforwarding_src_net object-group portforwarding_dst_net
```

お問い合わせ

Q 製品のご購入に関するお問い合わせ

<https://info-networld.smartseminar.jp/public/application/add/152>

Q ご購入後の製品導入に関するお問い合わせ

弊社担当営業にご連絡ください。

Q 製品の保守に関するお問い合わせ

保守開始案内に記載されている連絡先にご連絡ください。

本書に記載されているロゴ、会社名、製品名、サービス名は、一般に各社の登録商標または商標です。本書では、®、™、©マークを省略しています。

www.networld.co.jp

株式会社ネットワーク

