Cisco ASA 5500-Xシリーズ Firewall 設定ガイド

シスコシステムズ合同会社

2011年05月

目次

- はじめに
- 全体構成およびソフトウェアバージョン
- 設定概要
- インターフェイスの設定
- ルーティングの設定
- NAT の設定
- フィルタリングの設定
- インスペクション設定
- Logging の設定

はじめに

資料の内容・目的

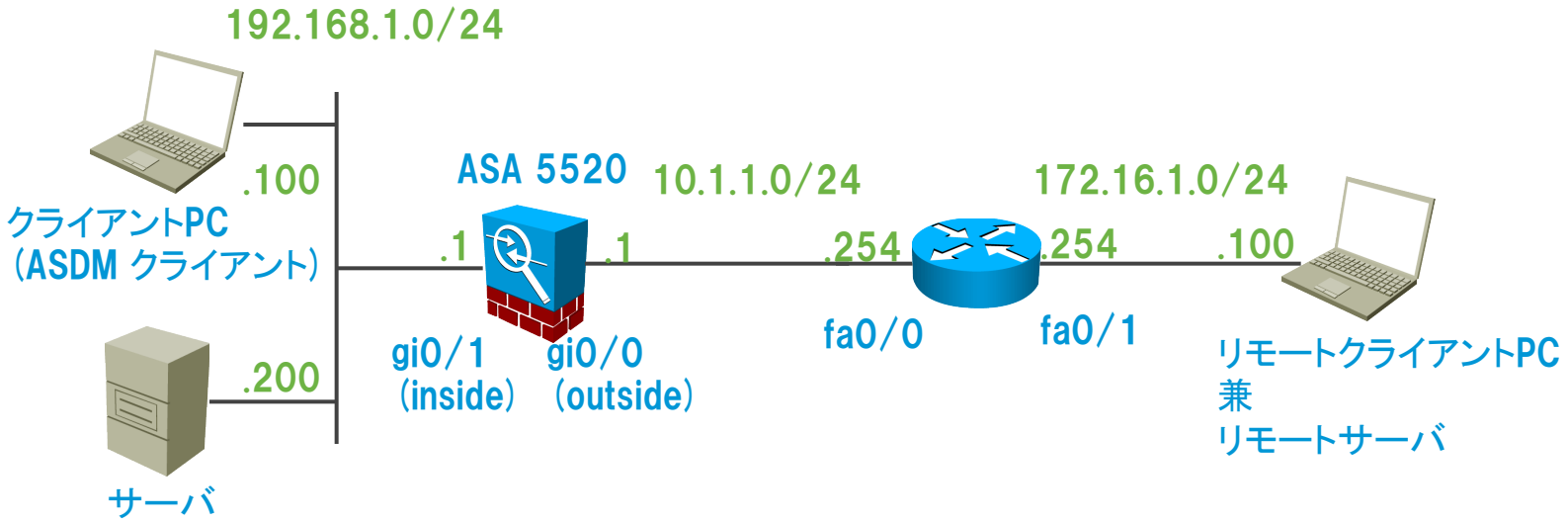
- 本資料ではASA 8.4 におけるファイアウォールの設定を紹介します。

内容に関する保証について

- 本資料は Single Context を前提に設定されています。そのため、Multi Context 環境とは設定内容が異なります。
- 本資料で紹介する技術情報は、2011年5月現在の情報です。
- 本資料に記載されている仕様および製品に関する情報は、予告なしに変更されることがあります。
- シスコは、本資料に関して、その正確性又は完全性について一切の責任を負わないこととします。
- シスコは、本資料が十分な品質を有すること、特定の目的に対する適合性を有すること、又は第三者の知的財産権、プライバシー権等その他の一切の権利に対する侵害がないことを、明示にも黙示にも表明又は保証しません。

全体構成およびソフトウェアバージョン

全体構成図



ASAソフトウェアバージョン

ASA：8.4（1）
ASDM：6.4（1）

初期設定(ASDM 端末の設定)

- 管理ネットワークの設定と、GUI 管理ツール(ASDM)アクセス端末のIPアドレスの指定をセットアップウィザードで設定することが可能であるが、管理ネットワークの利用が前提となる。この例では管理ネットワークを用いず inside ネットワークから管理を行い、その為の設定をコンソールから行う。

```
ciscoasa> enable
Password:
ciscoasa# write erase
Erase configuration in flash memory? [confirm]
[OK]
ciscoasa# reload
System config has been modified. Save? [Y]es/[N]o:
Proceed with reload? [confirm]
ciscoasa#
***
*** --- START GRACEFUL SHUTDOWN ---
                (略)
Rebooting.....
                (略)
[Pre-configure Firewall now through interactive prompts [yes]? No
ciscoasa> enable
ciscoasa# conf t
ciscoasa(config)# hostname ASA5520-L02-02
ASA5520-L02-02(config)# int g0/1
ASA5520-L02-02(config-if)# nameif inside
INFO: Security level for "inside" set to 100 by default.

ASA5520-L02-02(config-if)# ip address 192.168.1.1 255.255.255.0
ASA5520-L02-02(config-if)# no shut
ASA5520-L02-02(config-if)# asdm image disk0:/asdm-641.bin
ASA5520-L02-02(config)# http server enable
ASA5520-L02-02(config)# http 0.0.0.0 0.0.0.0 inside
ASA5520-L02-02(config)# write mem
```

コンソールセットアップ例

設定の消去

セットアップウィザードを行わない

ホスト名

インターフェース g0/1 にinside を割当て

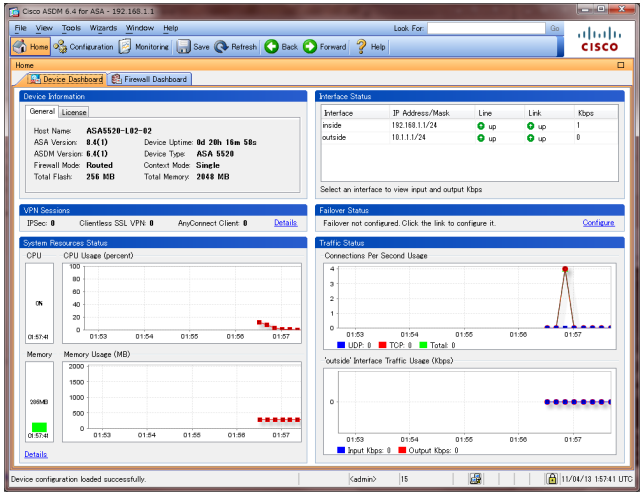
192.168.1.1/24

インターフェース有効

利用する asdm イメージを指定

http サービス有効

http/asdm アクセス端末指定

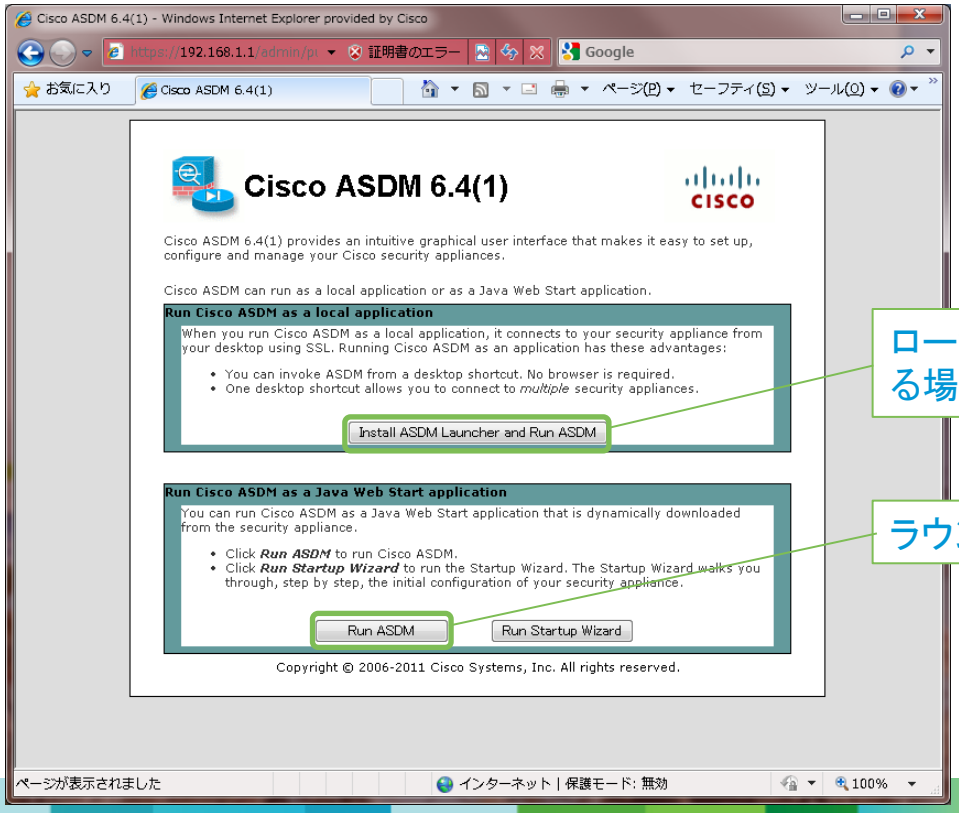


ASDM アクセス画面

ASDMラウンチャインストール

- 以降の設定は ASDM(Adaptive Security Device Manager)を用いて設定を行う。
- ASDM を起動するには、ブラウザから、下記を実行

  https://<ASA に割り当てた IP アドレス>
- ASDM ラウンチャをインストールした場合は、次回以降ラウンチャから起動可

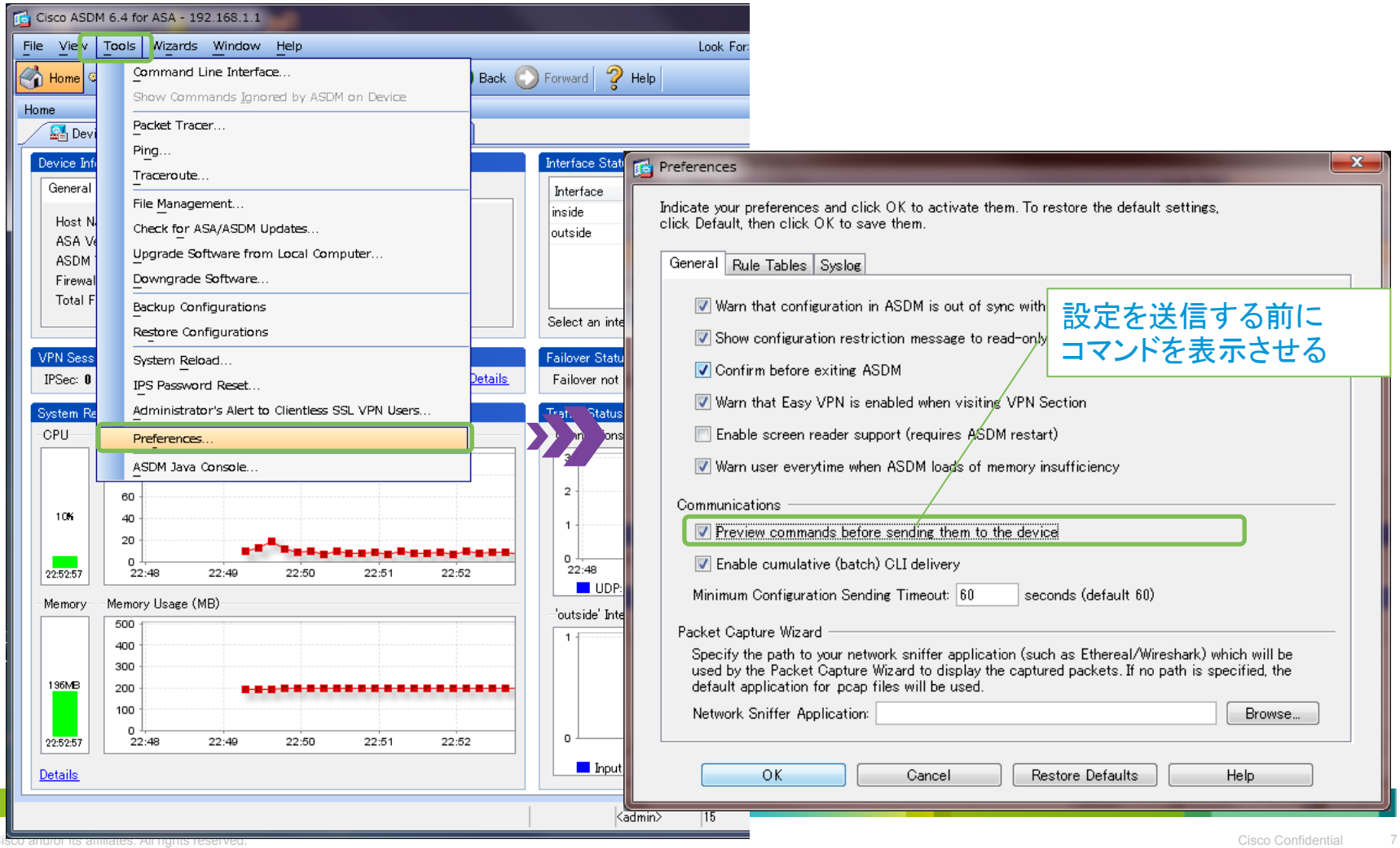


ローカルにラウンチャをインストールして実行する場合

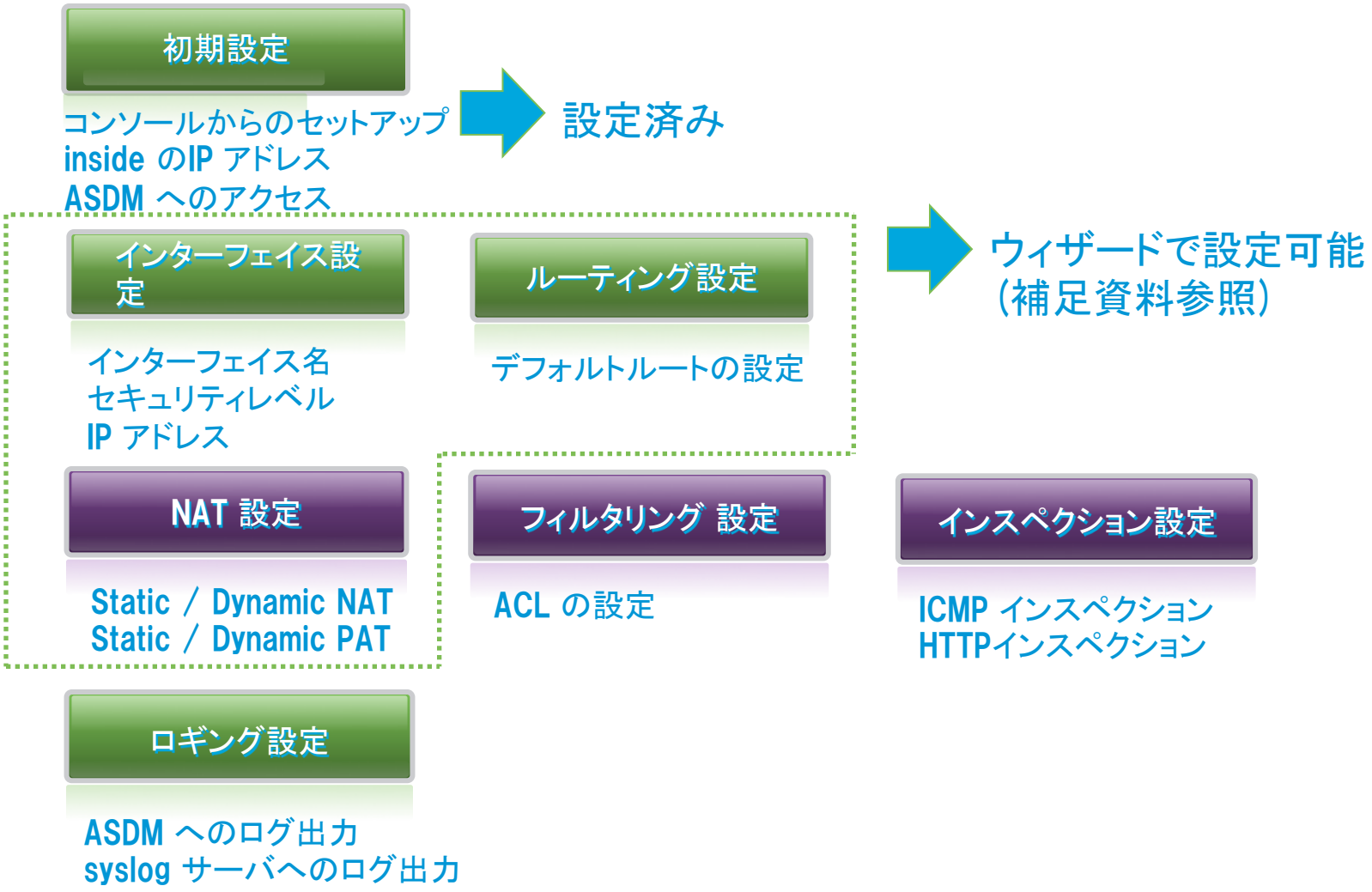
ラウンチャをインストールせず実行する場合

設定内容を事前表示するための設定

- ASDM で設定変更を行う際、ASA への適用時にCLI での設定内容を表示させることが可能

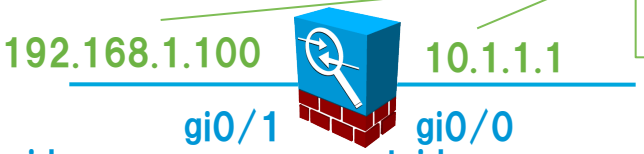


設定概要



インターフェイスの設定

インターフェイス設定概要



各インターフェイスにIP アドレスを設定する

各インターフェイスにインターフェイス名を設定する。名前は任意の文字列が可能だが一般的にinside、outside、DMZ 等が使用される。

各インターフェイスに0-100 の範囲でセキュリティレベルを設定する。
通常inside には100、outside には0 、DMZ には1-99 の値を設定する

セキュリティレベル

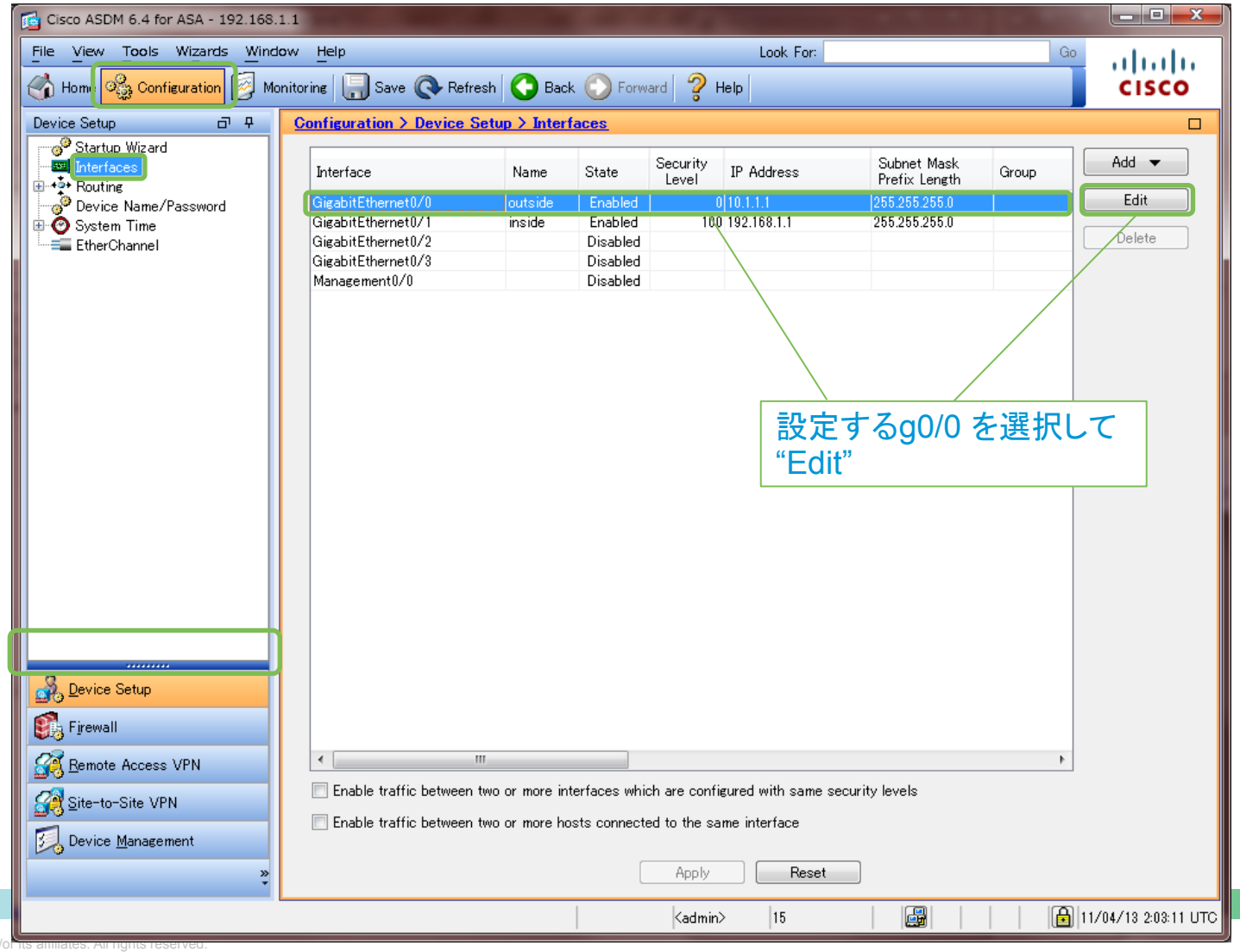
ASA のそれぞれのインターフェイスにはセキュリティレベルを設定する必要がある。
ASA を通過する通信は、通過するインターフェイスのセキュリティレベルの相対的な大小によって、以下のようなルールに従う。

セキュリティレベルが、
低いインターフェイス→高いインターフェイス
の通信:
原則として禁止される。(高いセキュリティレベルからのTCP/UDP の戻りパケットを除く)
通信を許可したい場合はACL を使用して明示的に許可する

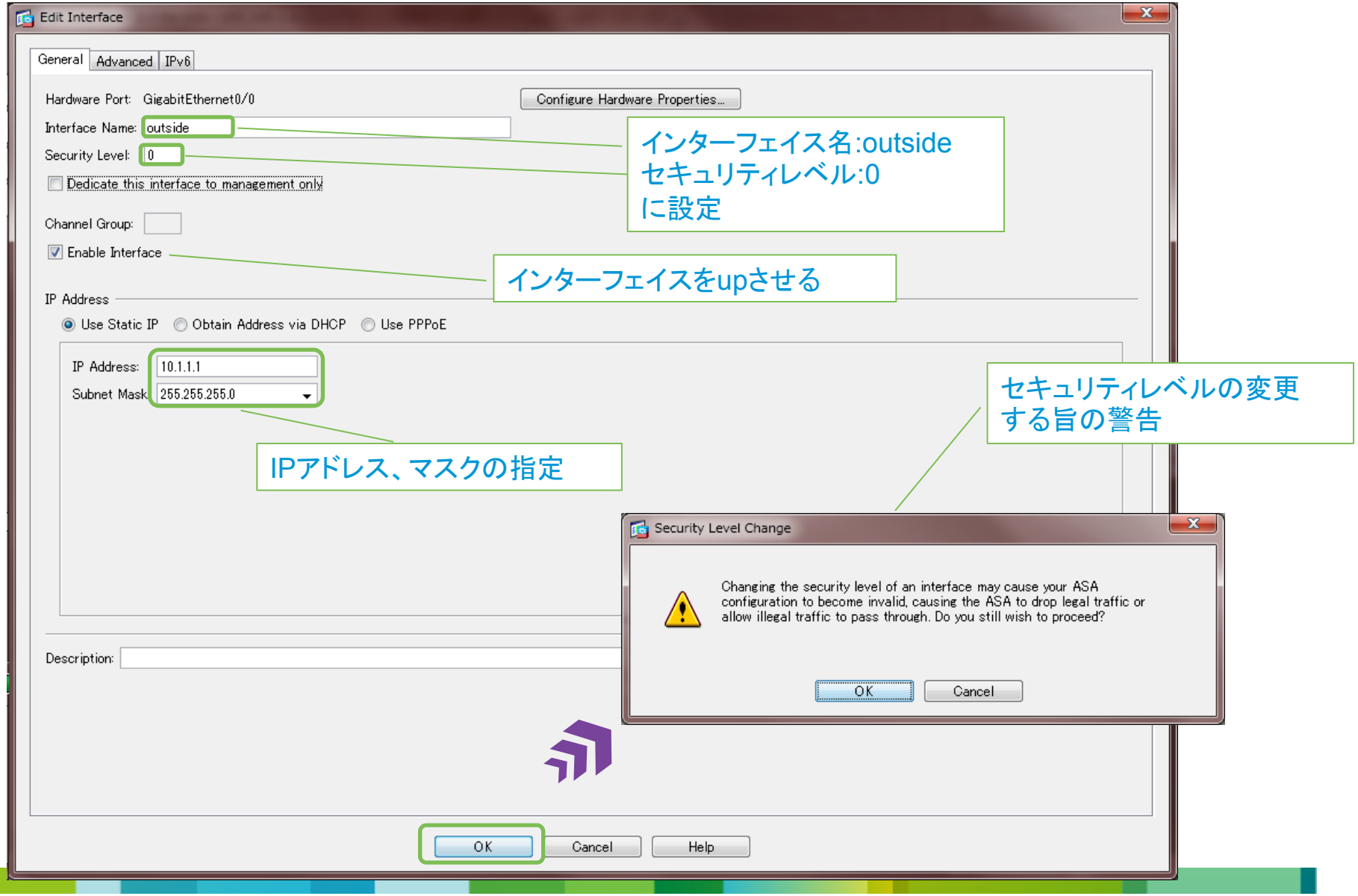
セキュリティレベルが、
高いインターフェイス→低いインターフェイス
の通信:
原則として許可される。
通信を禁止したい場合はACL を使用して明示的に禁止する
ACL の設定の際には"暗黙のDeny" に注意
詳細はフィルタリング設定の章参照

インターフェイスの設定1

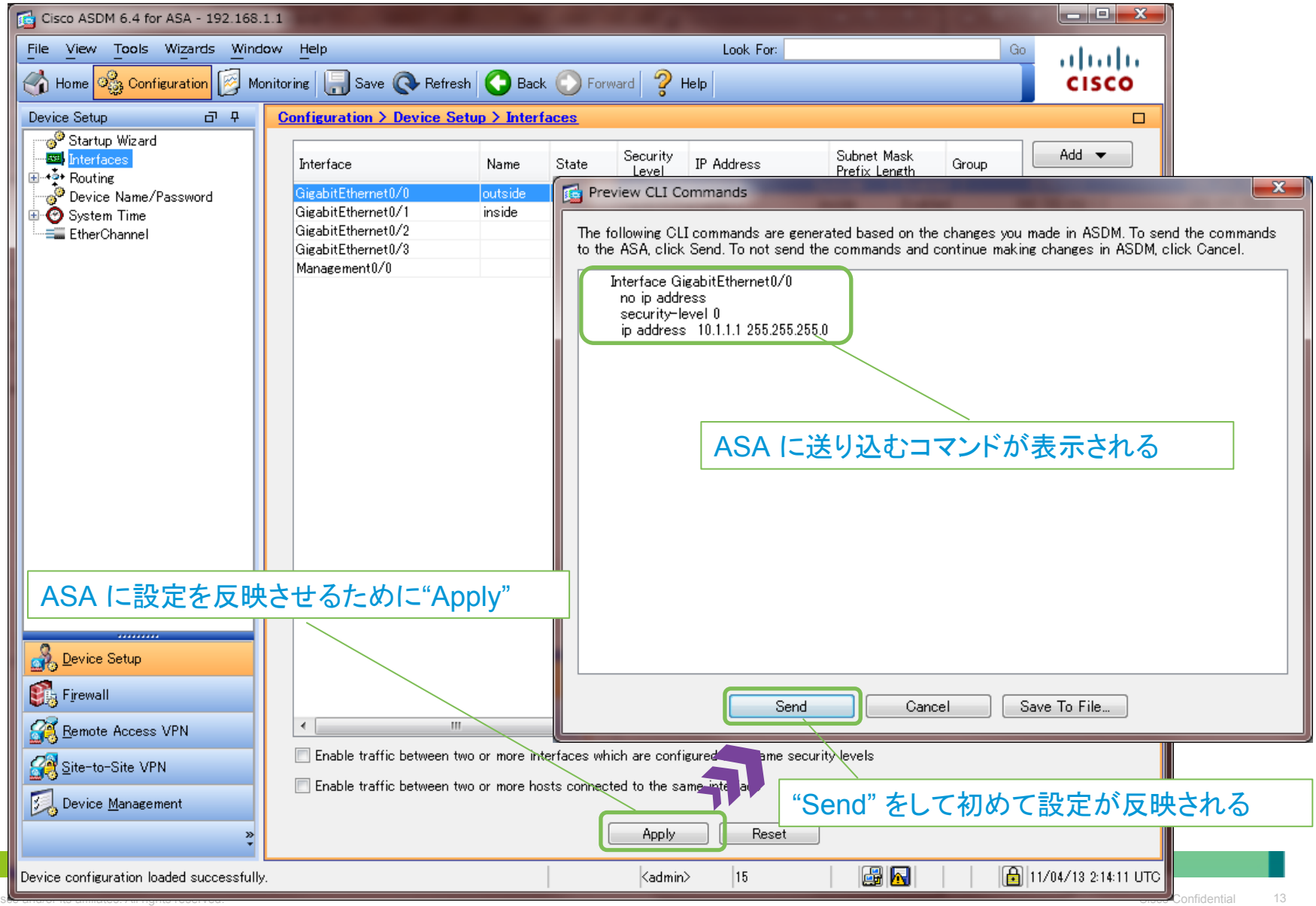
- inside は設定済みなので、ここではGi0/0 を “outside”, Security Level: 0, IPアドレス：10.1.1.1/24として設定する。



インターフェイスの設定2



インターフェイスの設定3 設定の反映

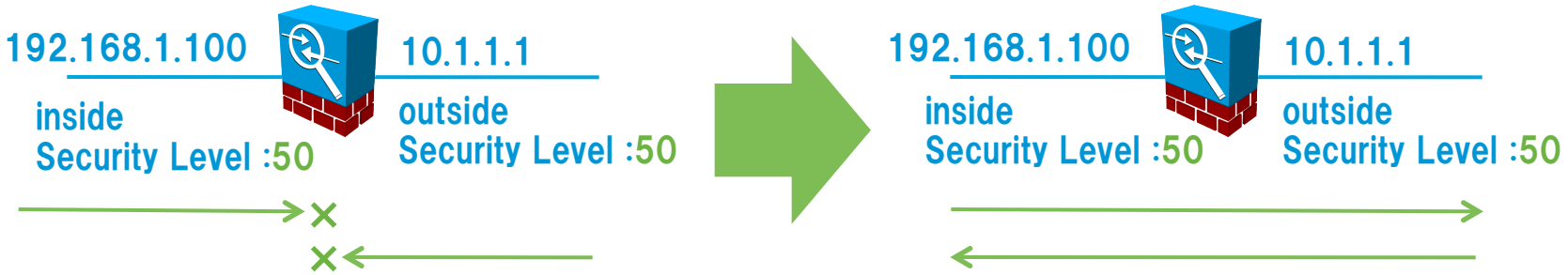


同一セキュリティレベルのインターフェイス間の通信

セキュリティレベルによる通信の制御は、設定ミス等によって生じる危険を低減させることができるが、状況によっては設定が煩雑になる場合がある。
そのような場合、以下の設定を行うことでセキュリティレベルによる通信制御を無効にすることが可能。

1. インターフェイスのセキュリティレベルに同一の値を設定
2. 同一セキュリティレベルのインターフェイス間の通信を許可

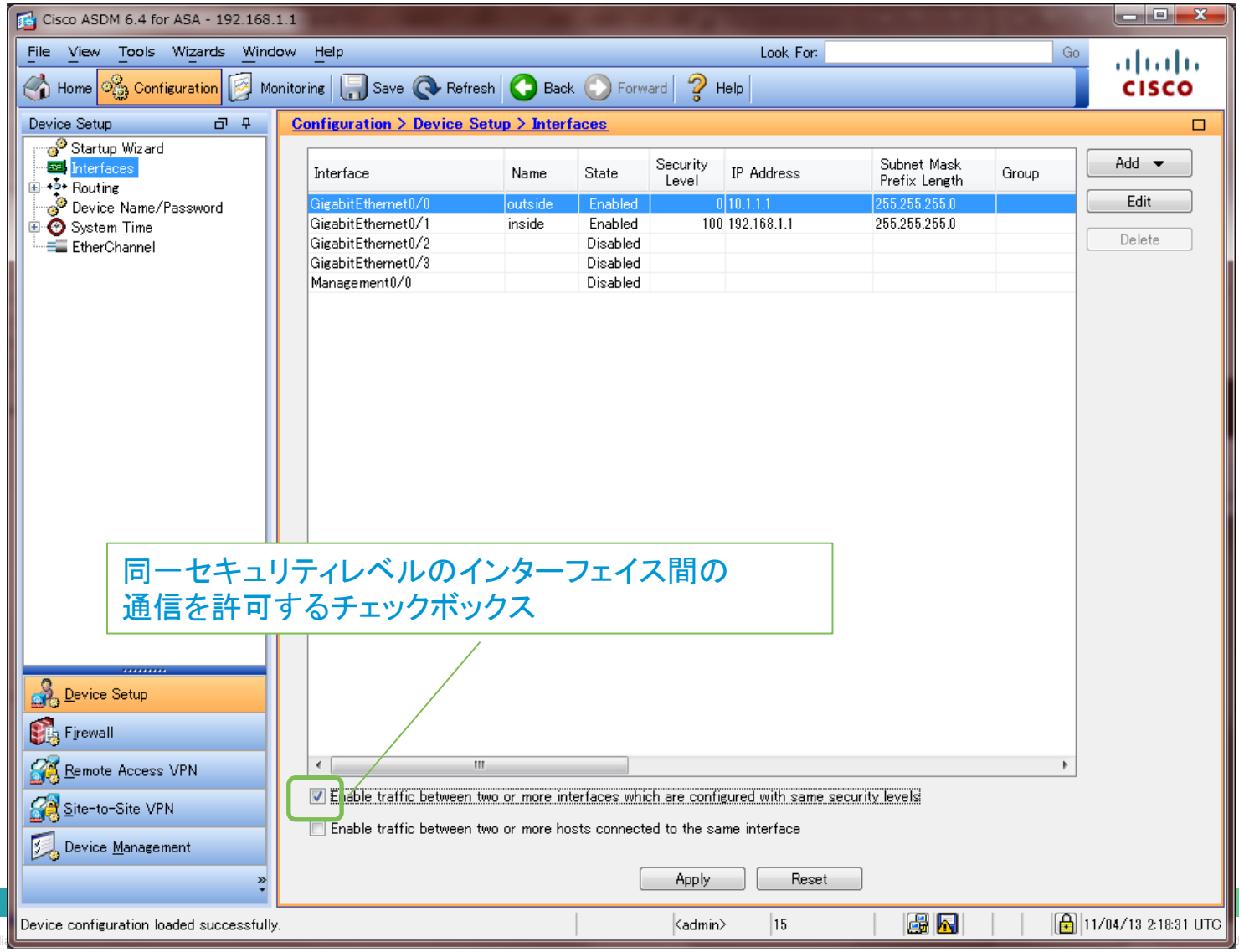
2つのインターフェイスに同一のセキュリティレベルを設定した場合、
デフォルトの設定では双方向の通信が原則禁止されるため、
同一セキュリティレベルのインターフェイス間の通信を許可する設定が必要



デフォルト状態

CLI: same-security-traffic permit

同一セキュリティレベルインターフェイス間の通信を許可する設定



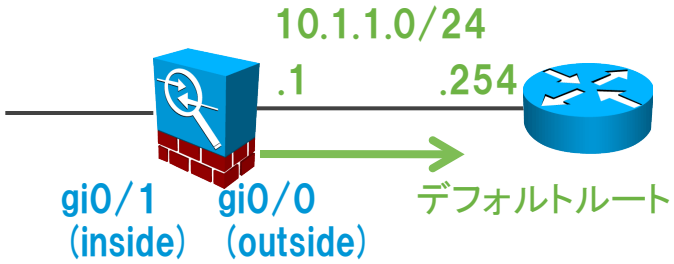
ルーティングの設定

ルーティングの設定概要

ASA はデフォルトではルータとして動作するRouted Mode となっているため、
必要に応じてルーティングの設定が必要
ASA 8.x では下記のルーティングプロトコルをサポート

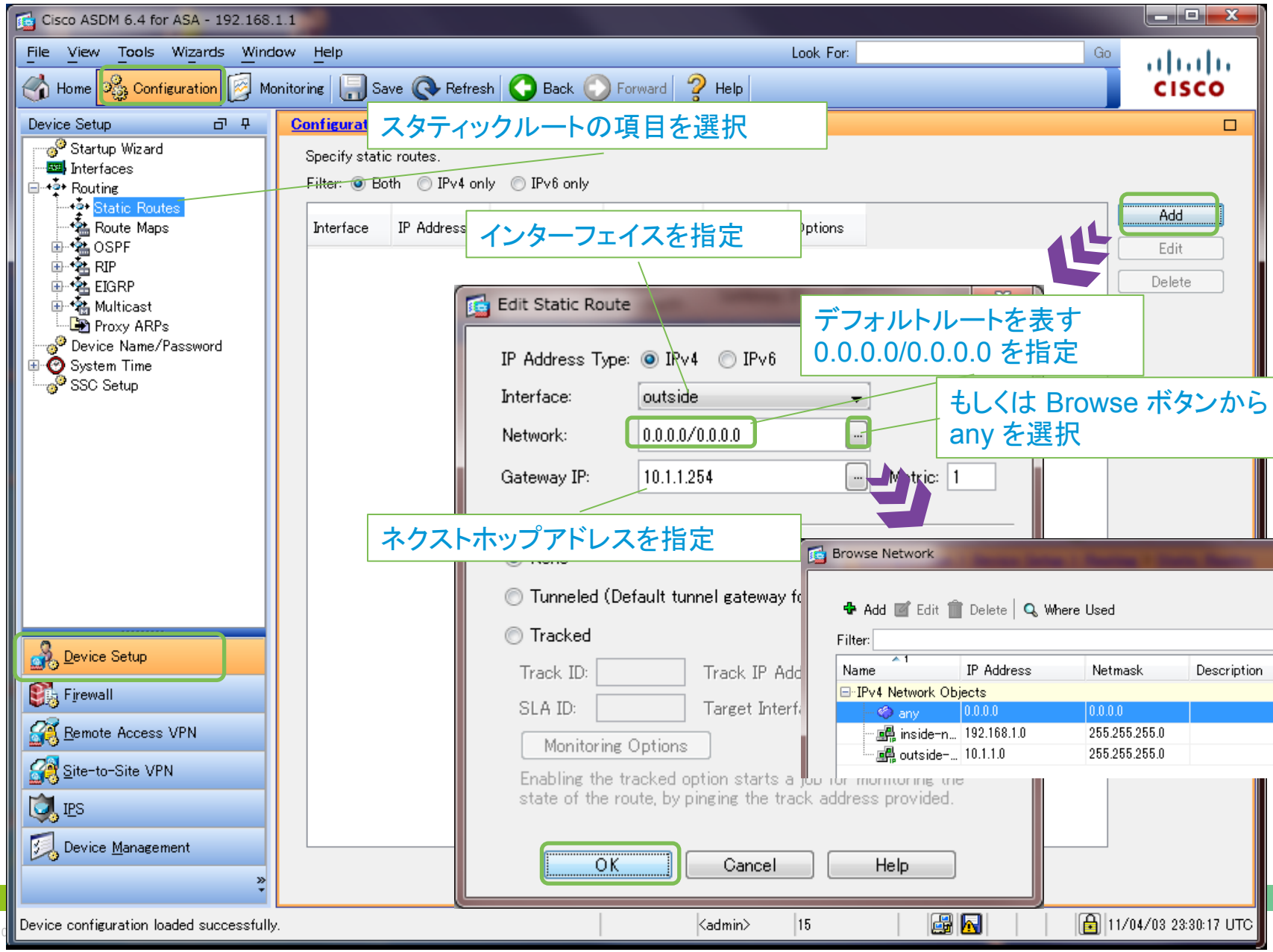
1. スタティックルーティング
   （デフォルトルートを含む）
2. RIP
3. OSPF
4. EIGRP

本資料では、outside インターフェイスの対向ルータをデフォルトルートとして設定

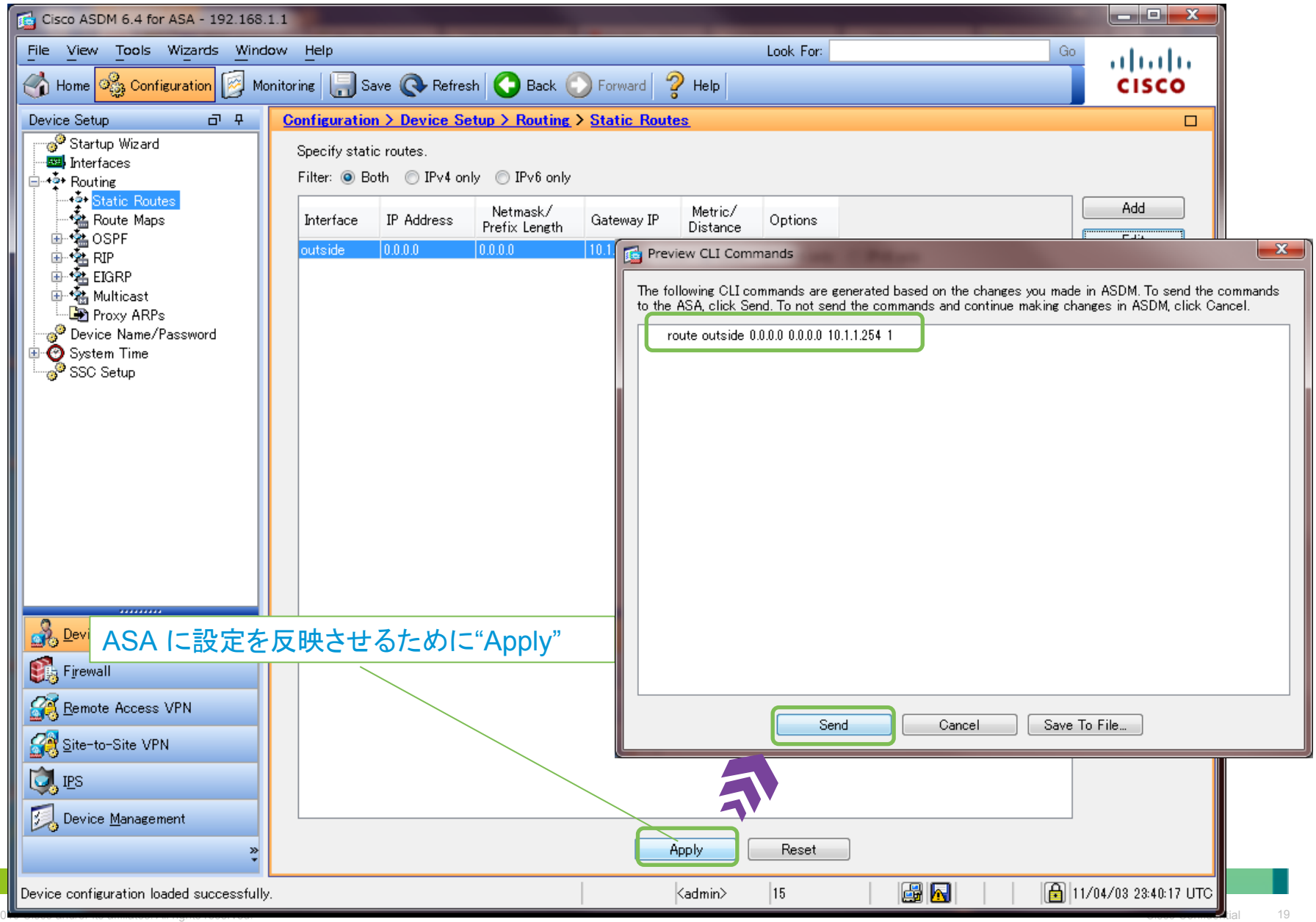


（注）Multiple Contextでは、スタティックルーティングのみ対応。

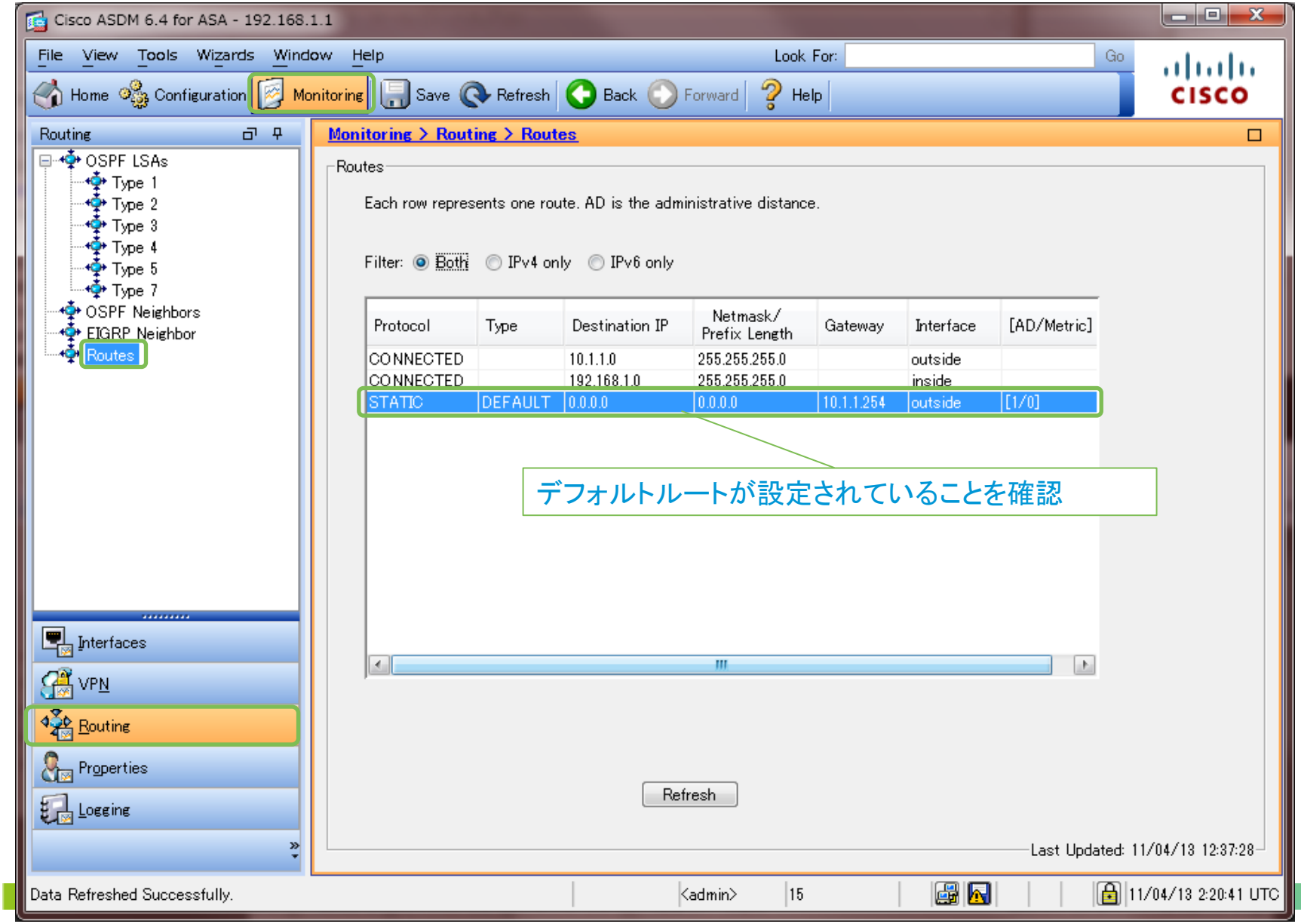
デフォルトルートの設定1



デフォルトルートの設定2 設定の反映



ルーティング設定の確認



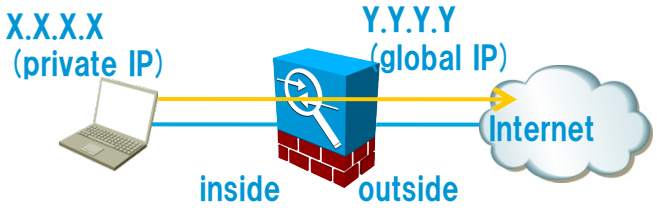
NATの設定

NAT の種類

static NAT

IP アドレスを1対1で静的にマッピング
ポート番号は変換されない

例）



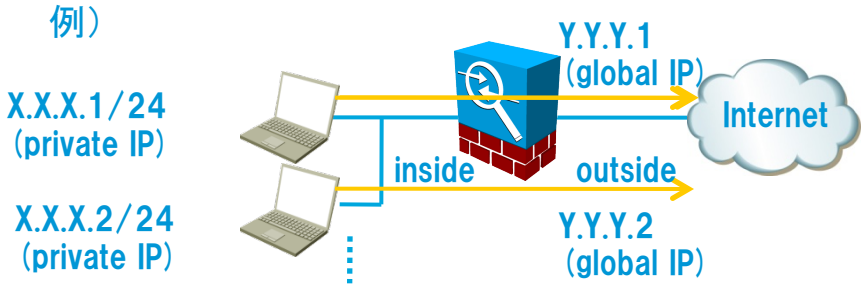
変換ルール

X.X.X.X (private IP) ⟷ Y.Y.Y.Y (global IP)

dynamic NAT

IP アドレスを1対1で動的にマッピング
ポート番号は変換されない
複数のホストに対して、複数のGlobal IP を動的にマッピングする場合等に使用

例）



変換ルール

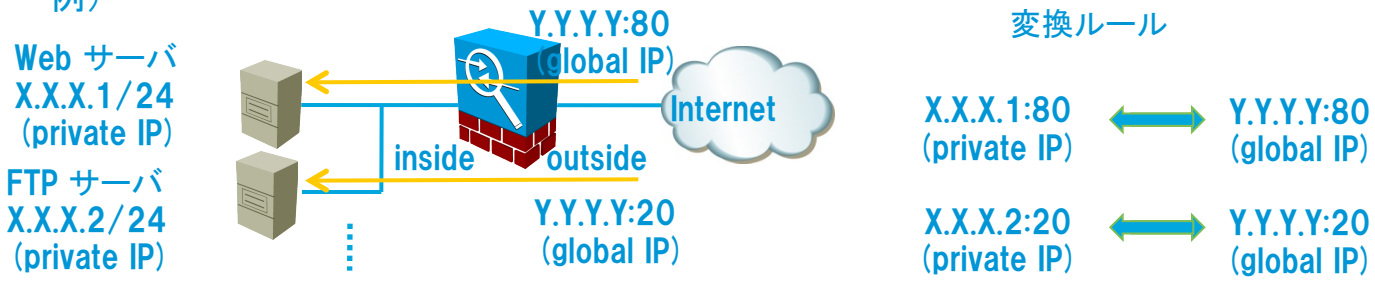
X.X.X.0/24 (private IP) ⟷ Y.Y.Y.1-10 (global IP)

NAT の種類 Cont.

static PAT

IPアドレス＋ポート番号を1対1でマッピング。
一つのglobal IP アドレスを複数台のサーバ に割り当てる場合等に使用

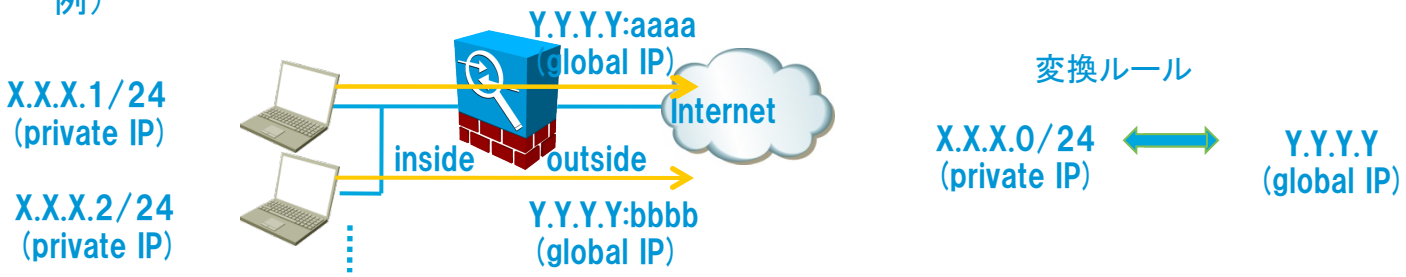
例）



dynamic PAT

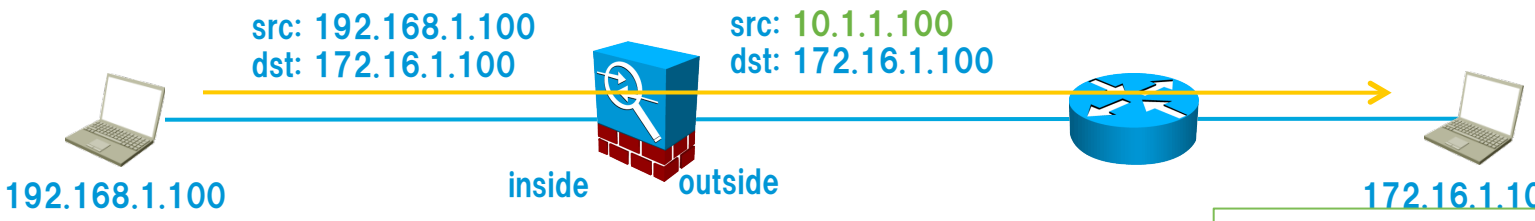
IPアドレス+ポート番号を動的にマッピング
複数のホストに対して、一つのGlobal IP を動的にマッピングする場合等に使用

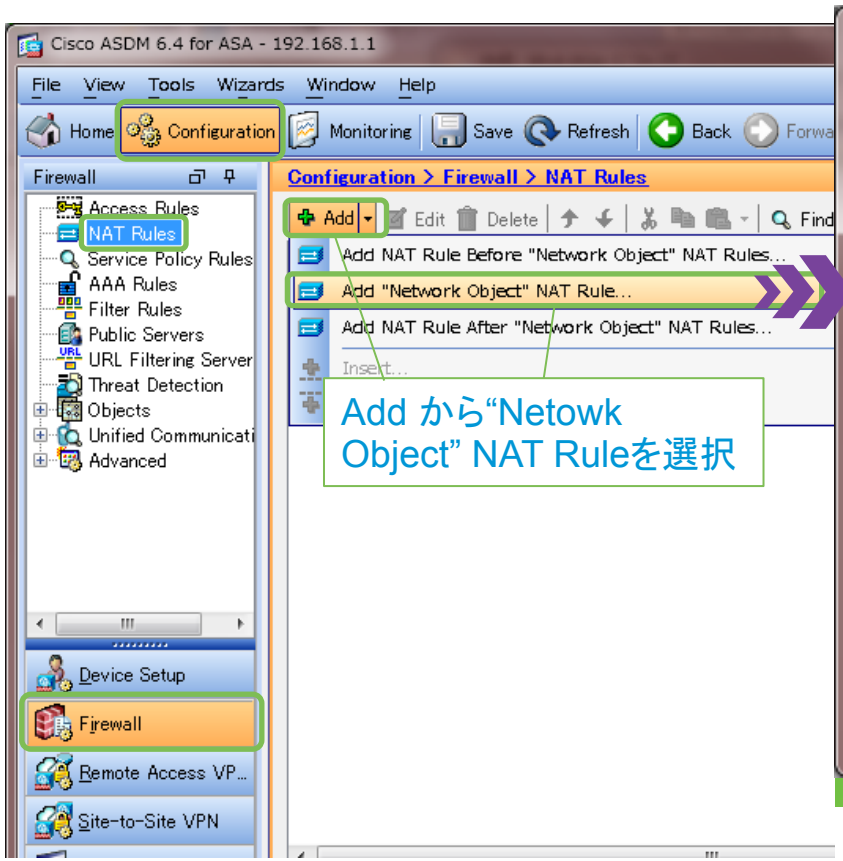
例）

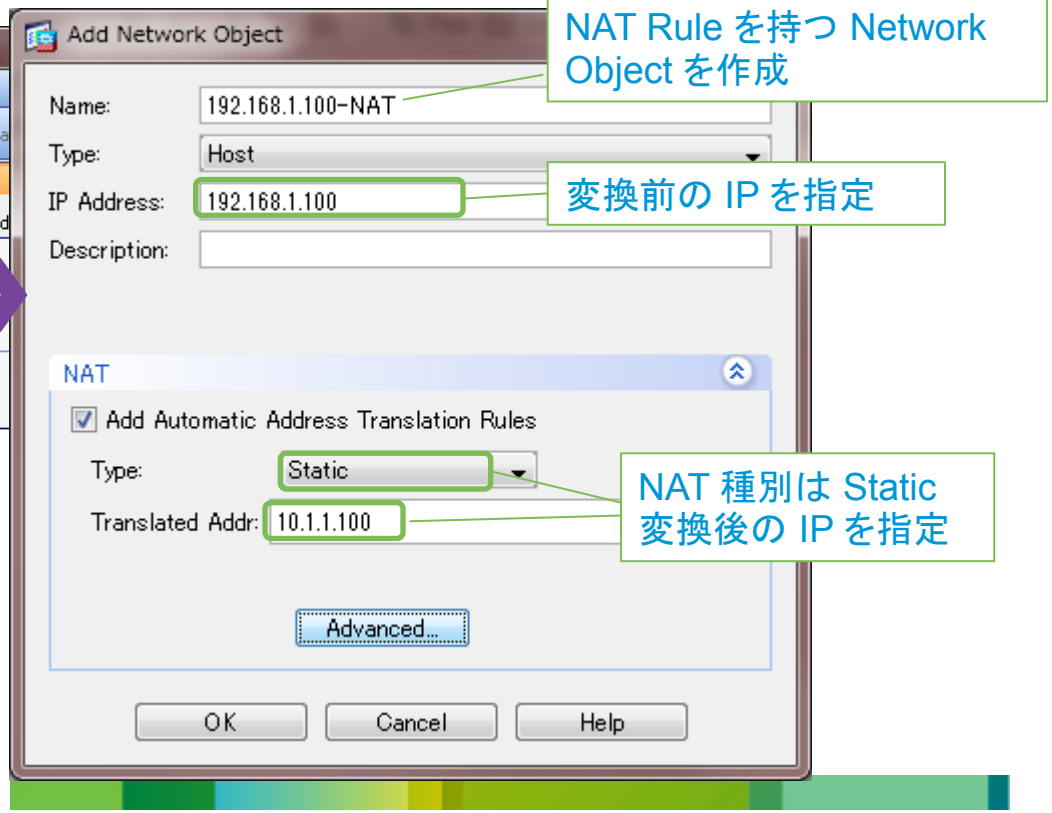


NAT 設定　Static NAT

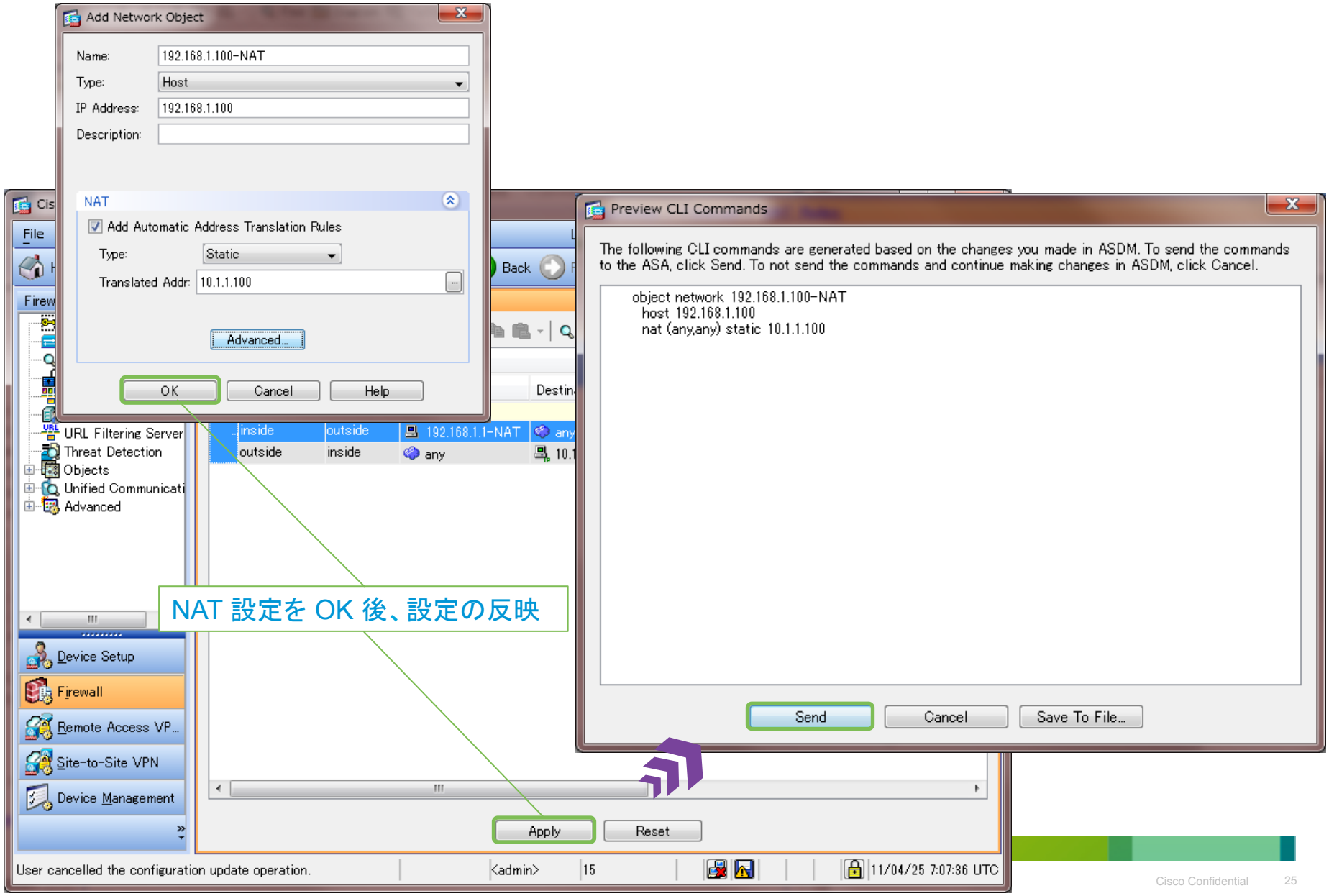
192.168.1.100 から来たトラフィックの送信元アドレスを 10.1.1.100 に変換するようなStatic NAT を設定する。





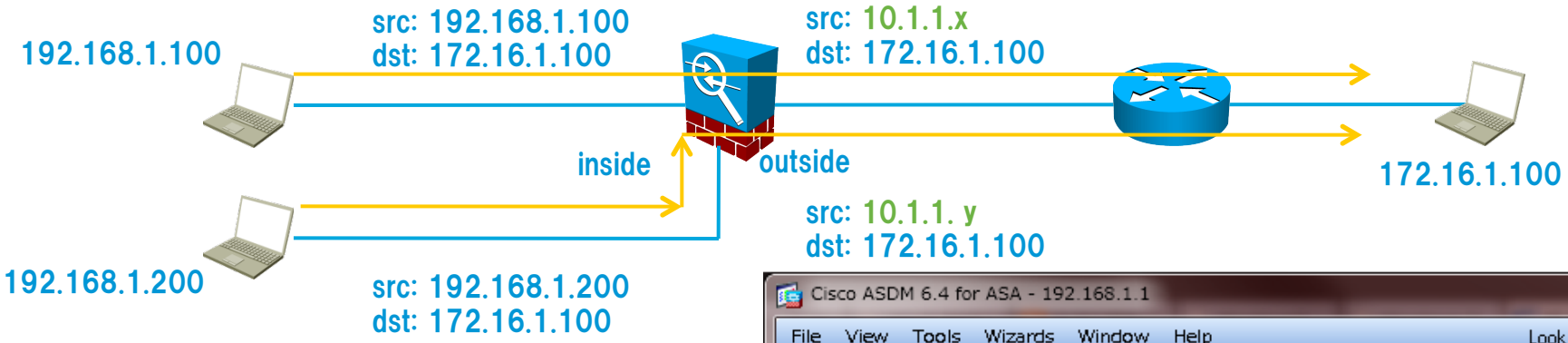


NAT 設定　Static NAT　設定の反映

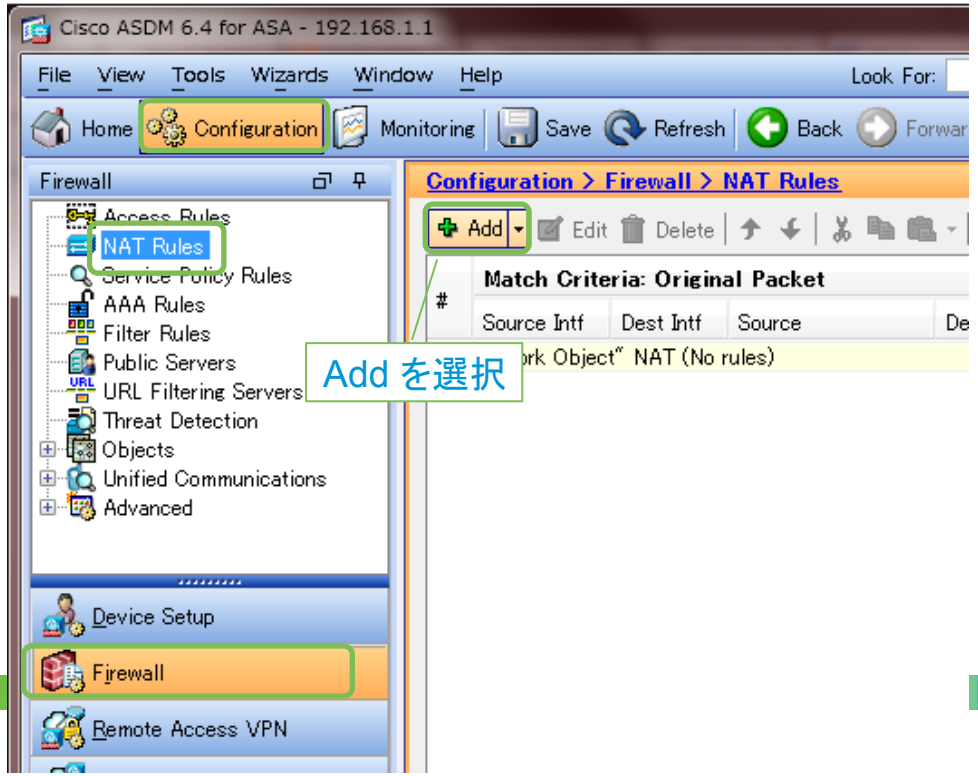


NAT 設定　Dynamic NAT

192.168.1.0/24 から来たトラフィックの送信元アドレスを 10.1.1.100-110 に変換するようなDynamic NAT を設定する。

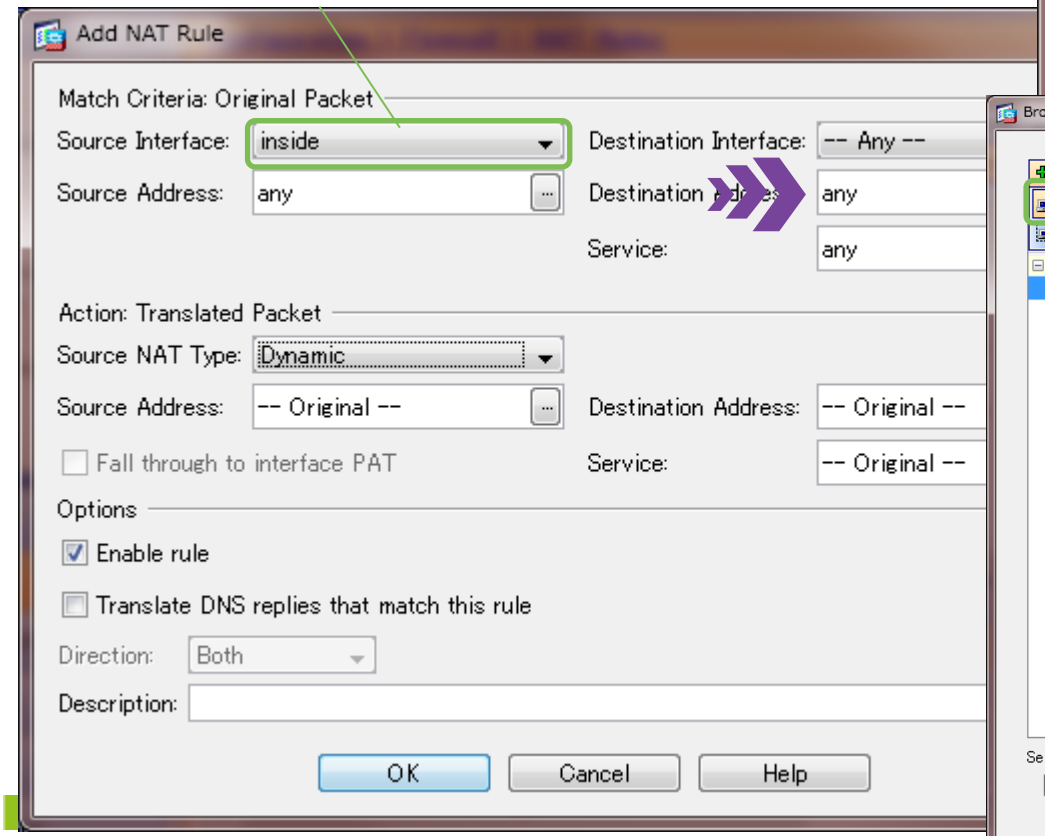


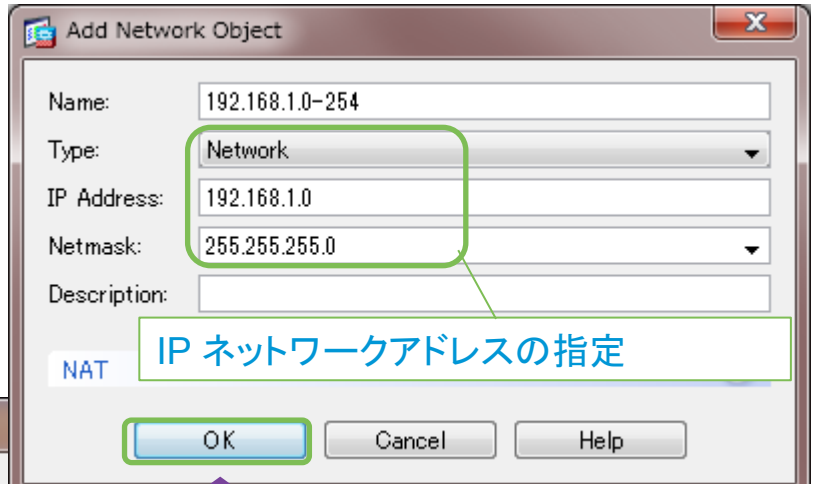
設定手順
1. NAT 対象のネットワークを指定
2. NAT 変換後のアドレスを指定
   2-1 変換後のアドレスプールを作成



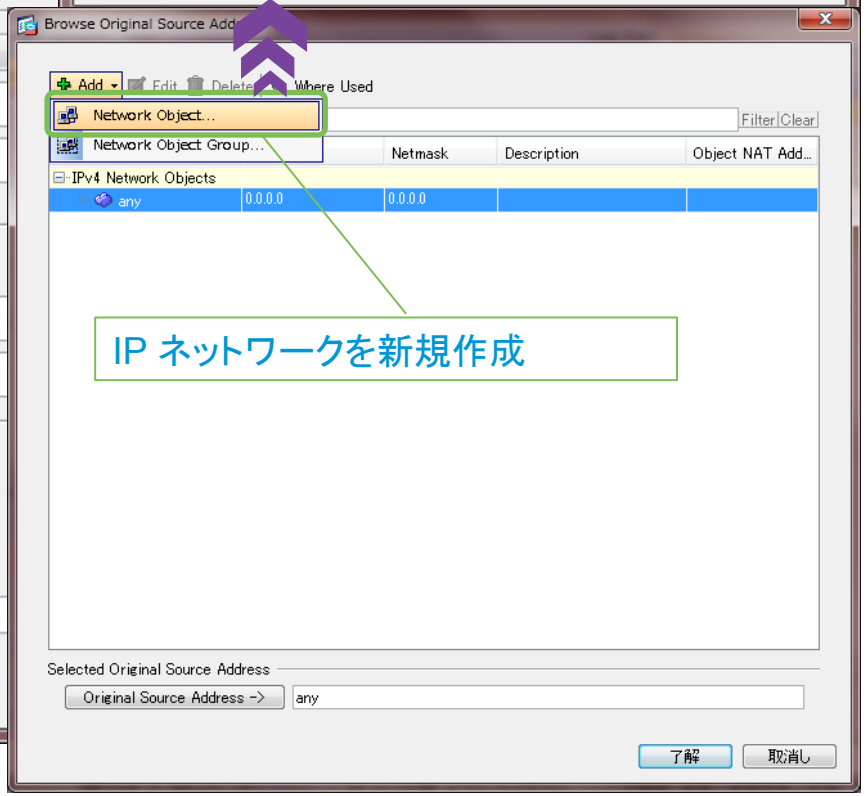
NAT 設定　Dynamic NAT2

NAT変換する対象のインターフェイスと
IPアドレス(ネットワーク)192.168.1.0/24
を指定



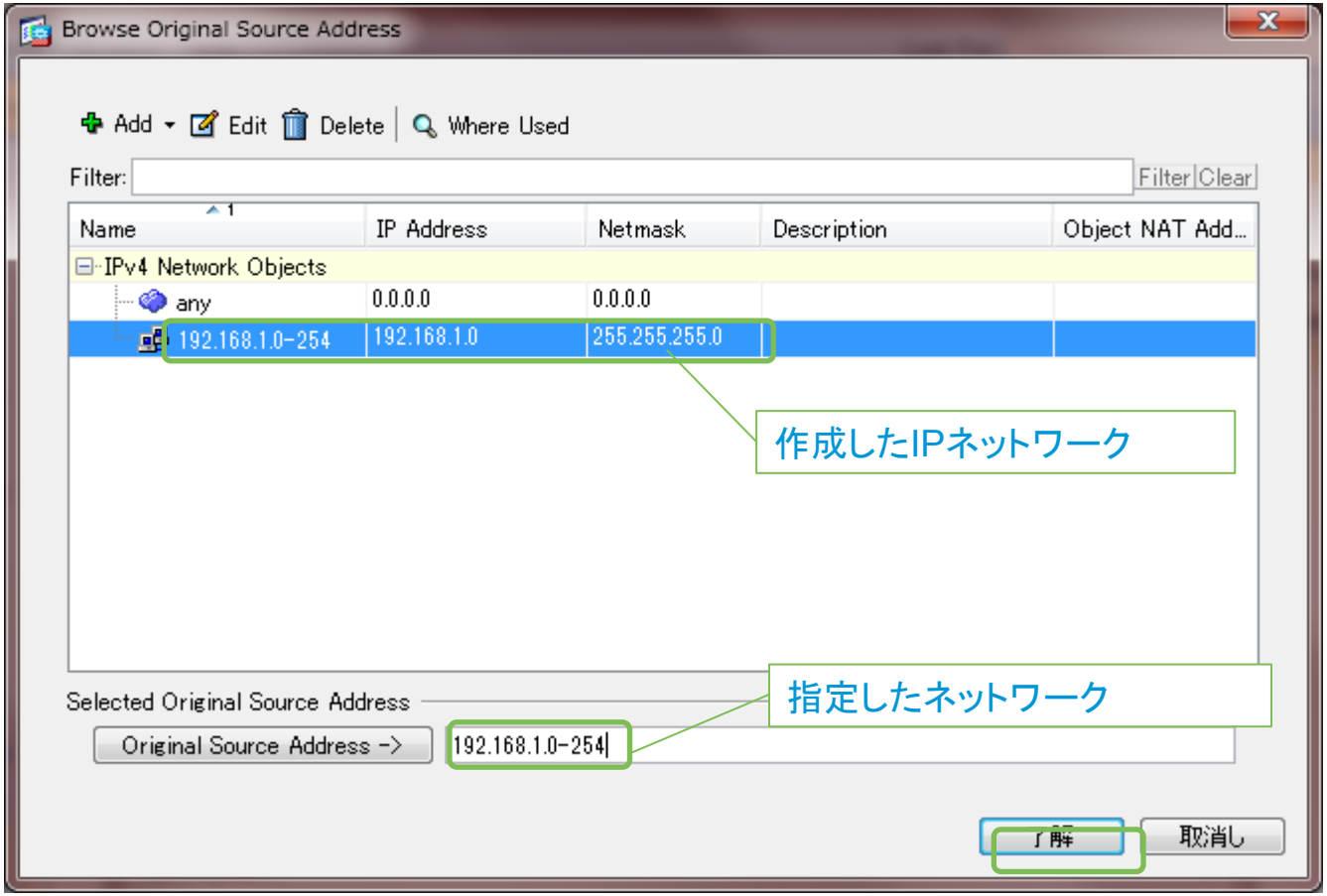


IP ネットワークアドレスの指定

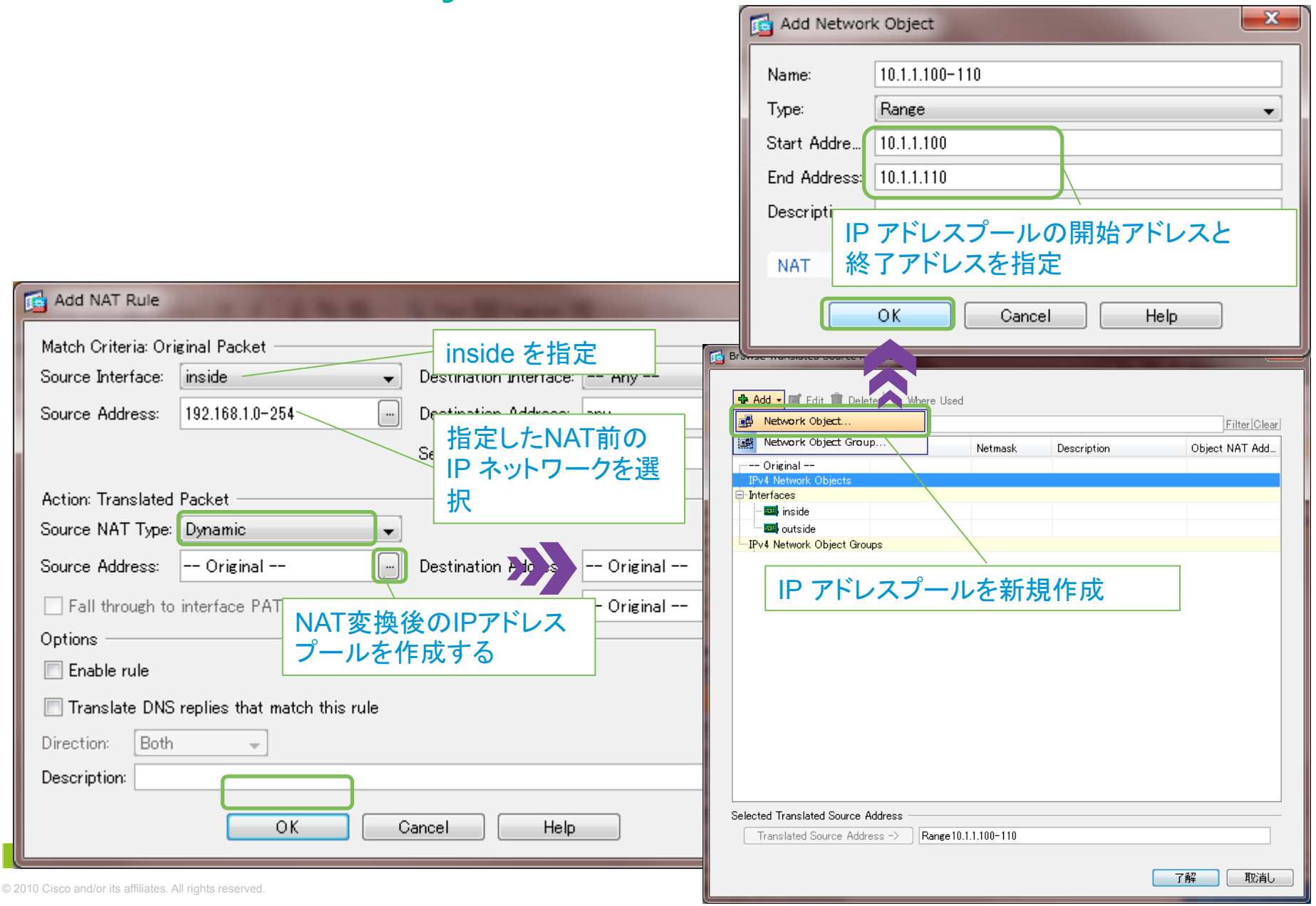


IP ネットワークを新規作成

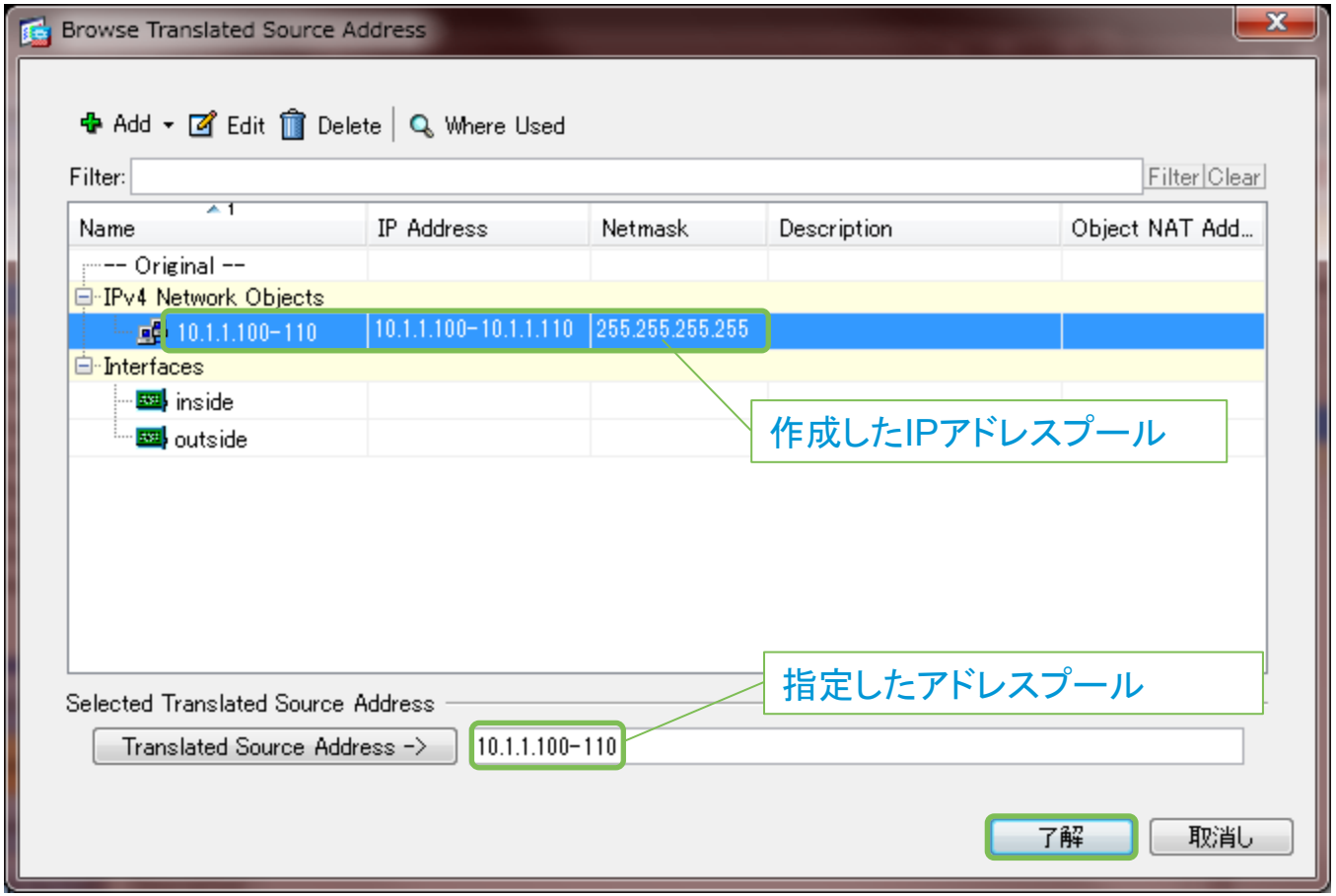
NAT 設定　Dynamic NAT ネットワーク指定



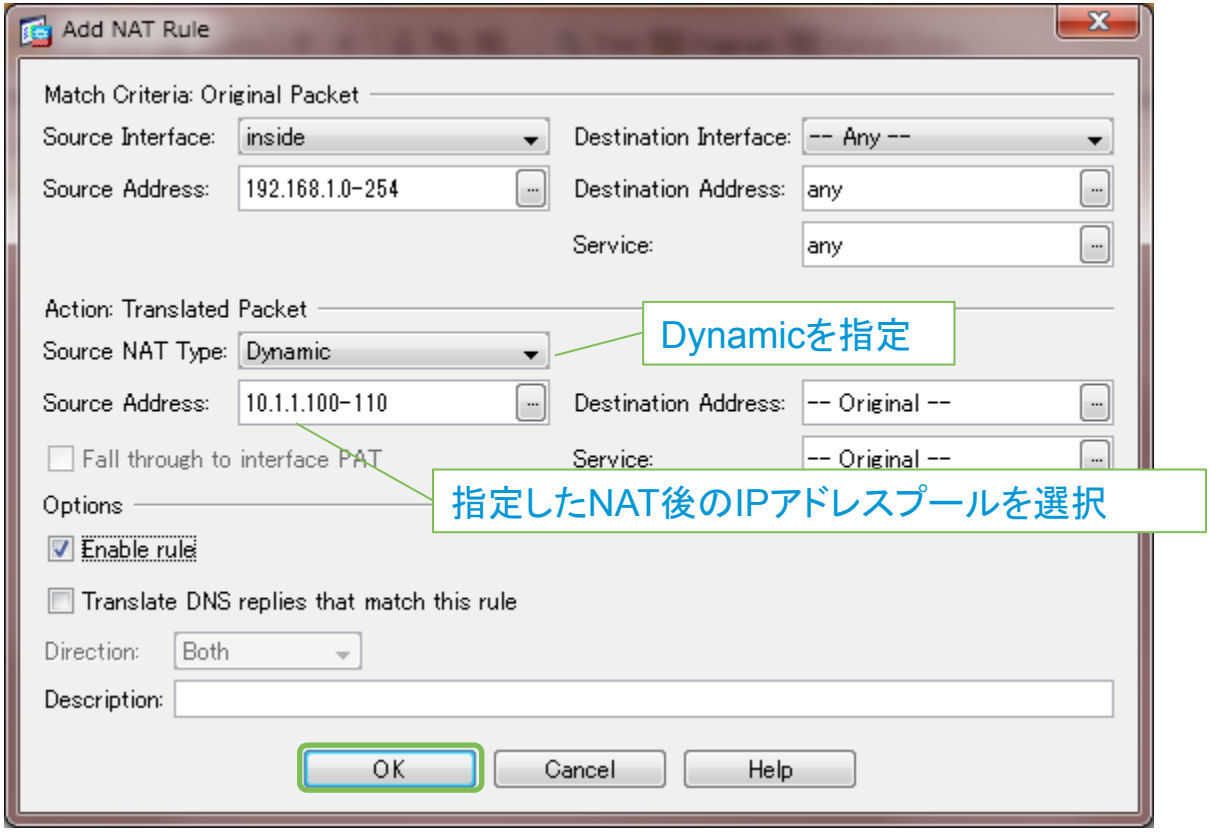
NAT 設定　Dynamic NAT3



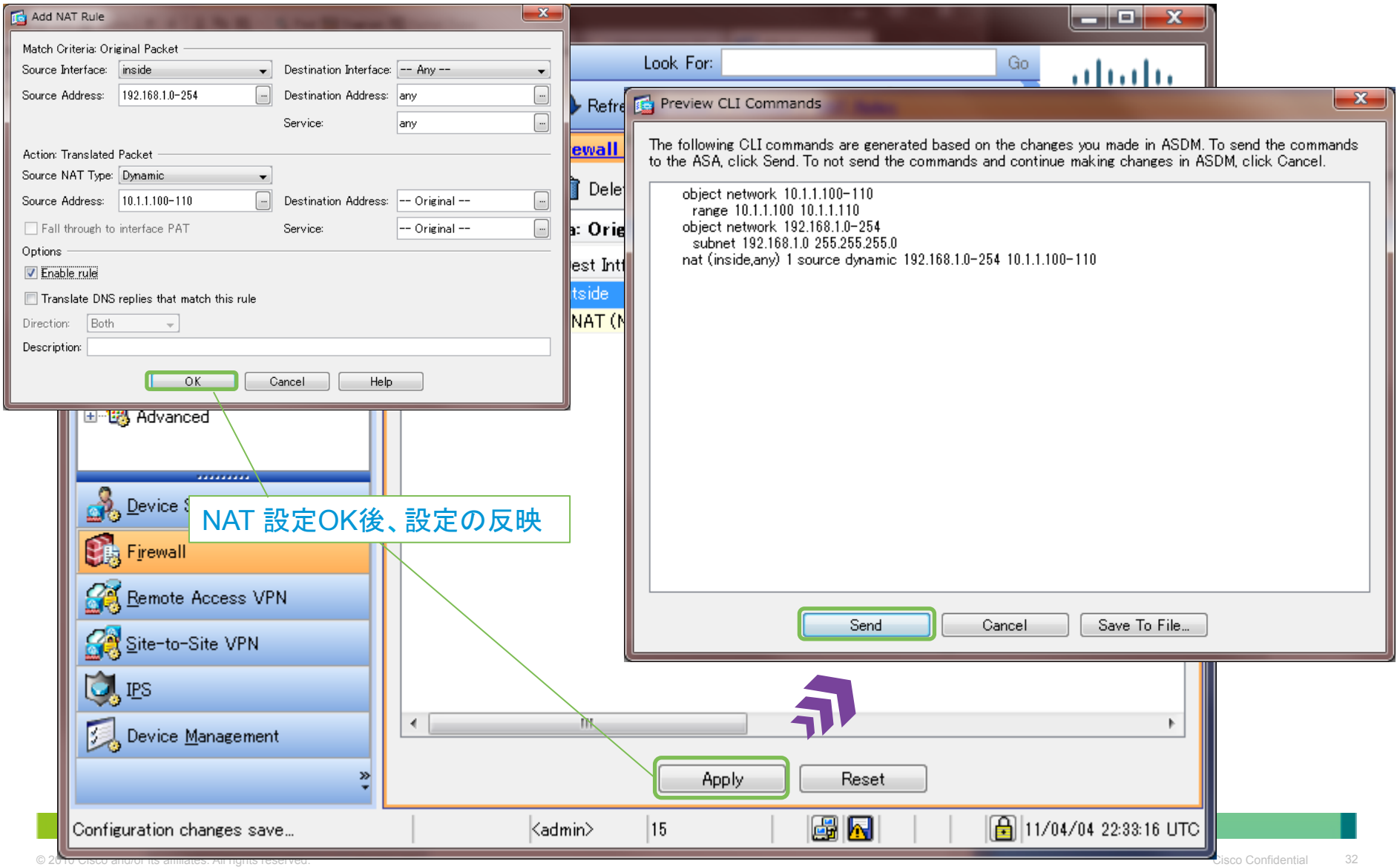
NAT 設定　Dynamic NAT アドレスプールの指定



NAT 設定　Dynamic NAT4

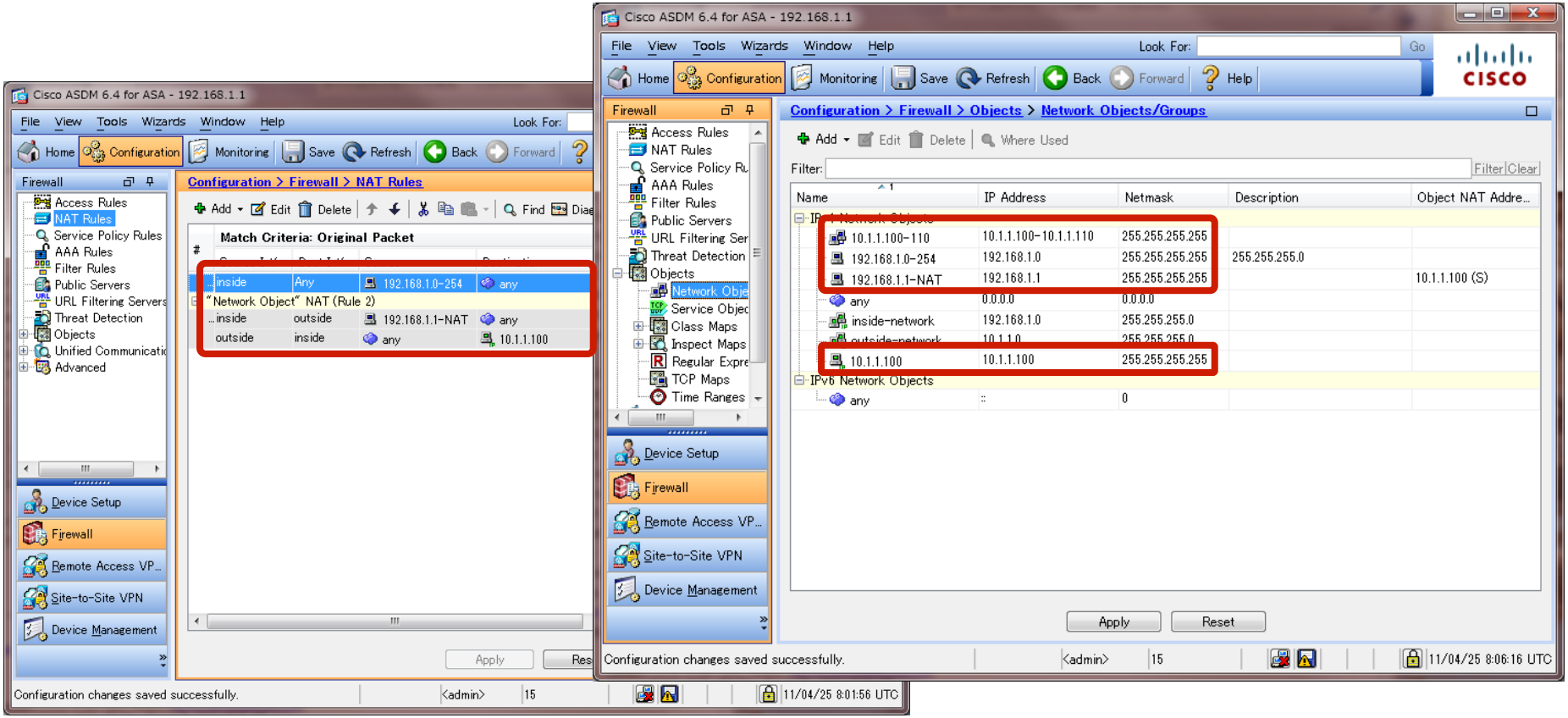


NAT 設定　Dynamic NAT 設定の反映



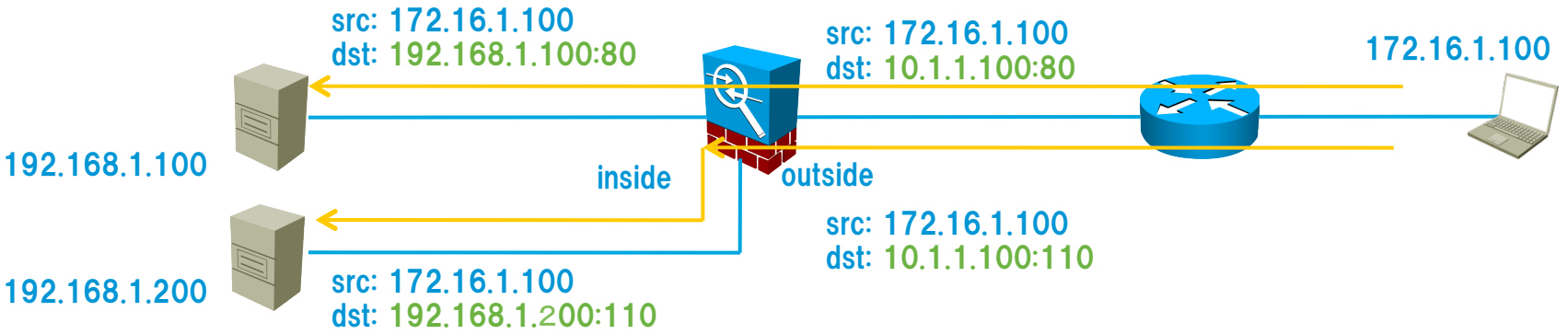
次の Exerciseの準備のために・・・

- 作成した NAT, Network Object を削除してください。



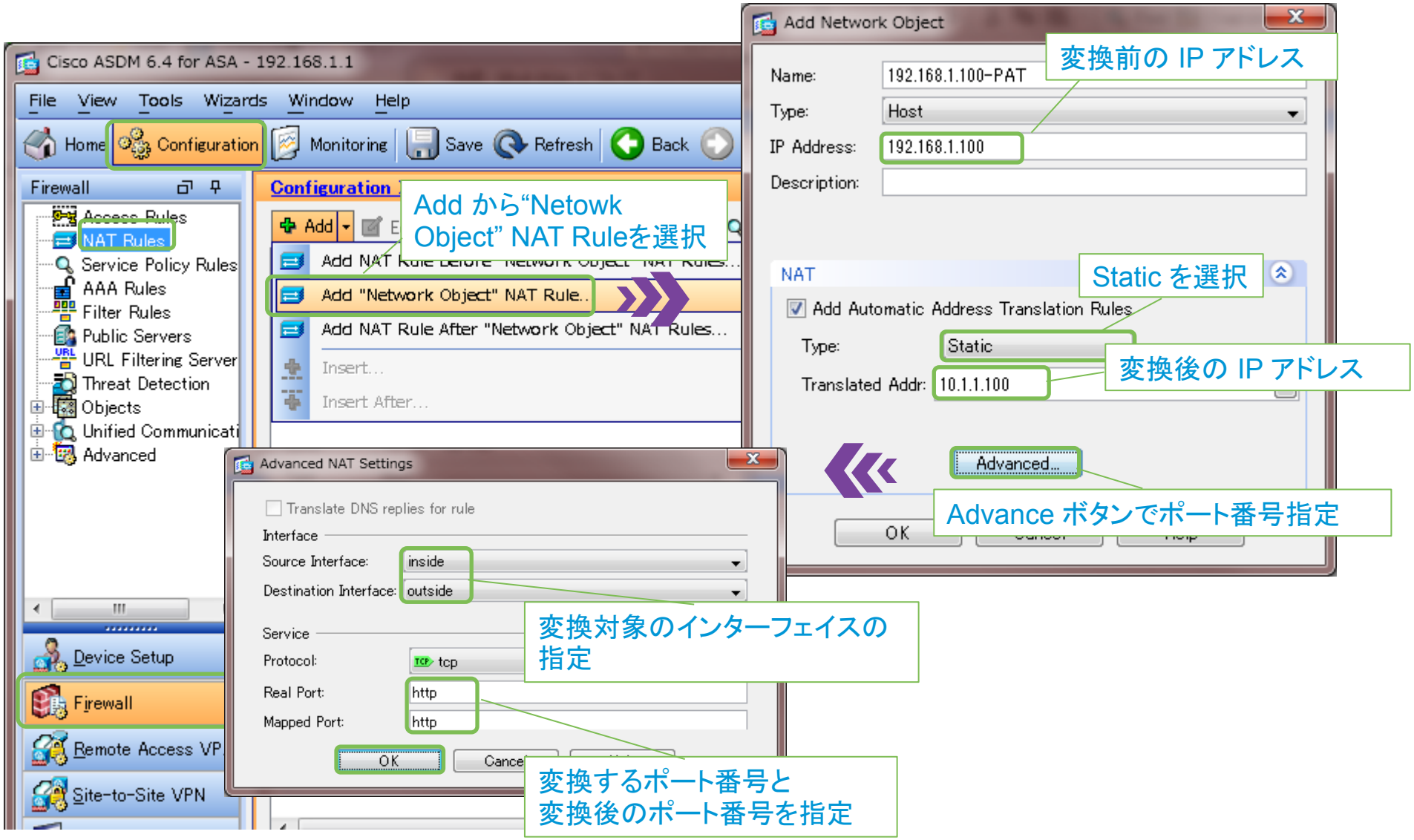
NAT 設定　Static PAT

10.1.1.100 へ来たWeb トラフィック (TCP 80番ポート) の宛先アドレスを
192.168.1.100 に変換し、
10.1.1.100 へ来たPOP3 トラフィック (TCP 110番ポート) の宛先アドレスを
192.168.1.100 に変換するようなStatic PAT を設定する。



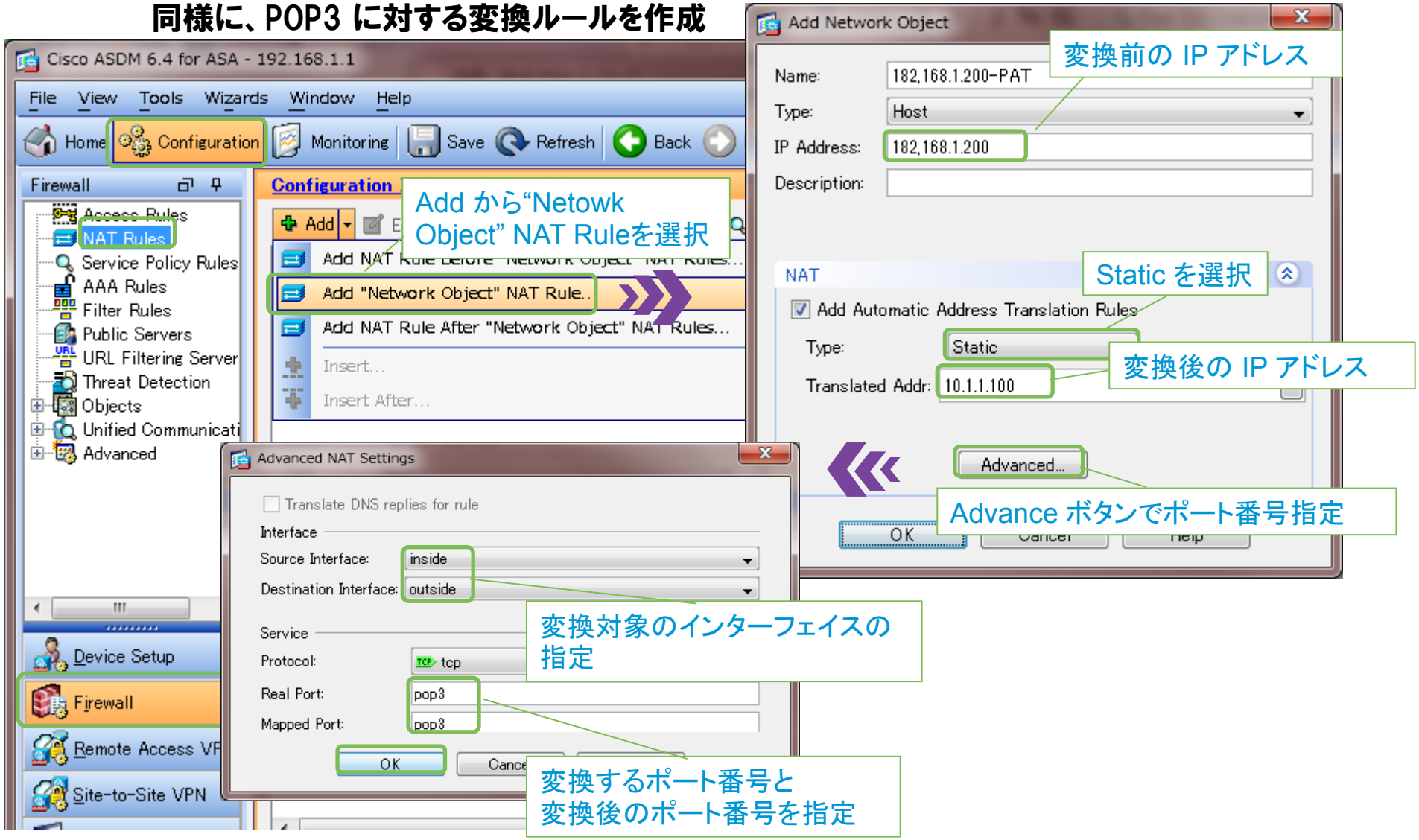
※実際にoutside からの通信を行うためには
ACL の設定が必要

NAT 設定 Static PAT(HTTP の変換ルール)

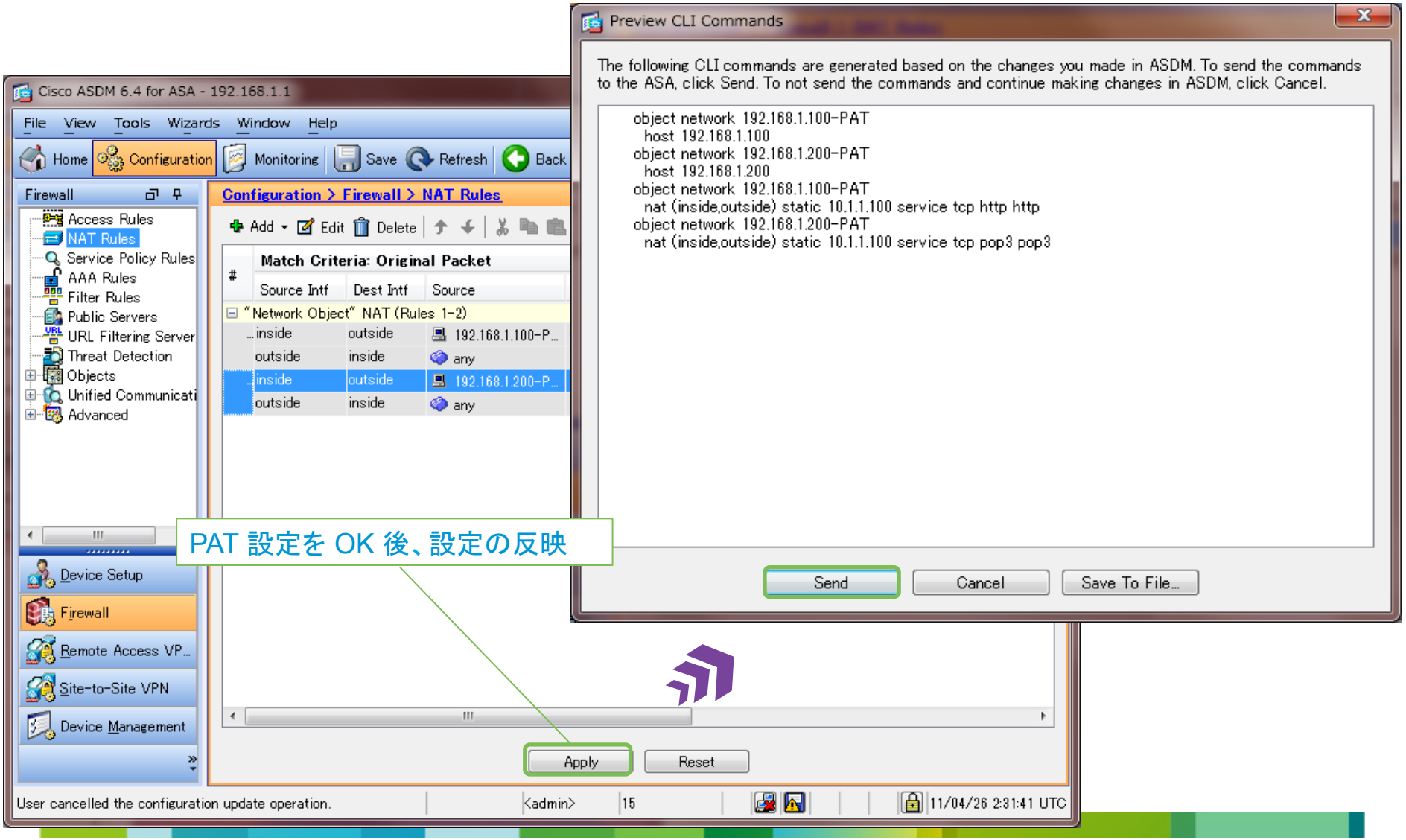


NAT 設定 Static PAT(POP3 の変換ルール)

同様に、POP3 に対する変換ルールを作成

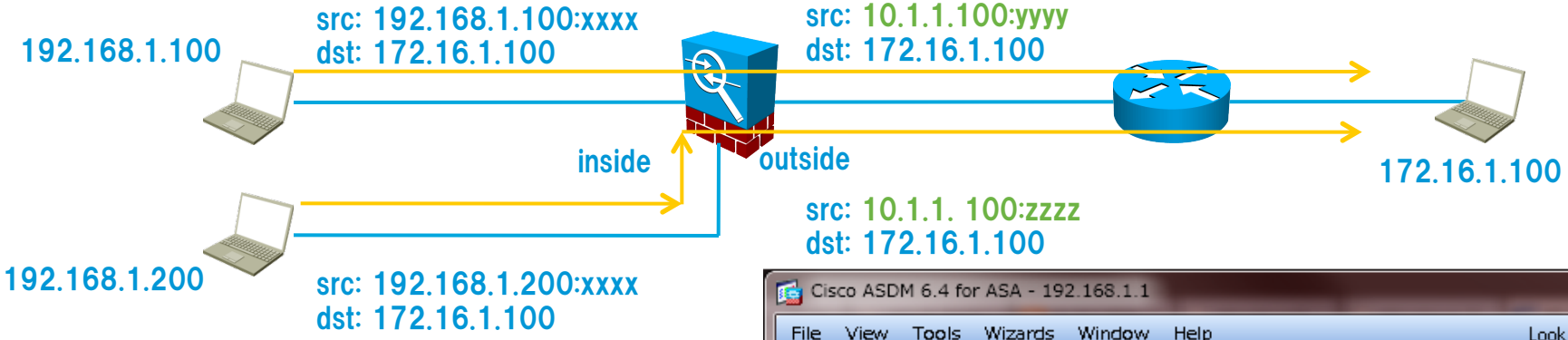


NAT 設定 Static PAT設定の反映

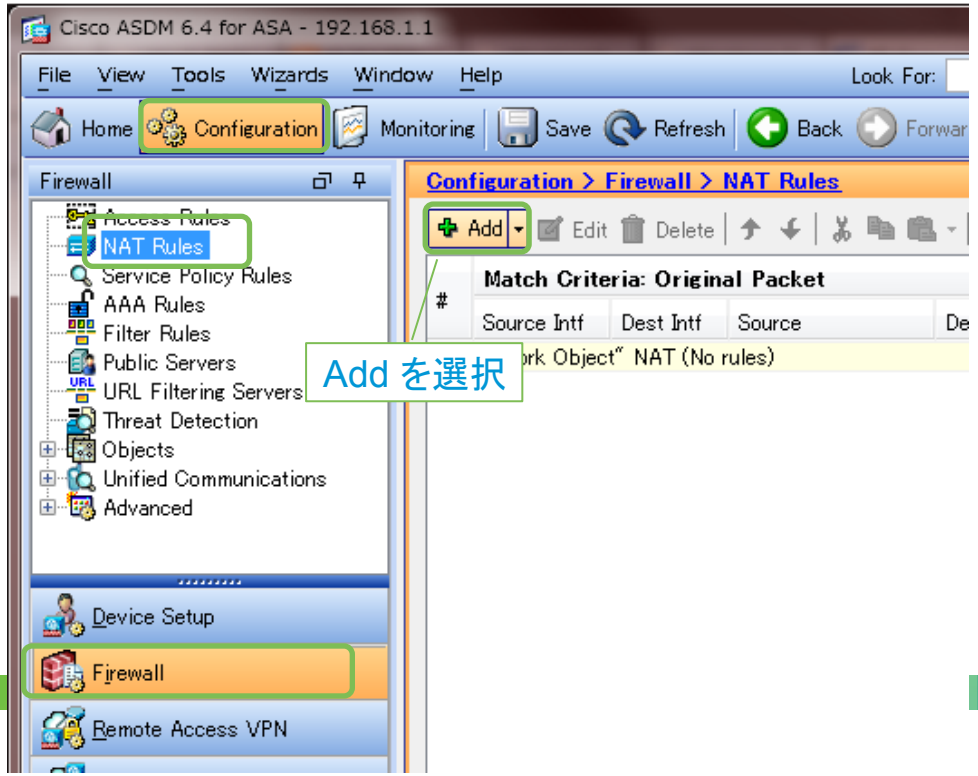


NAT 設定　Dynamic PAT

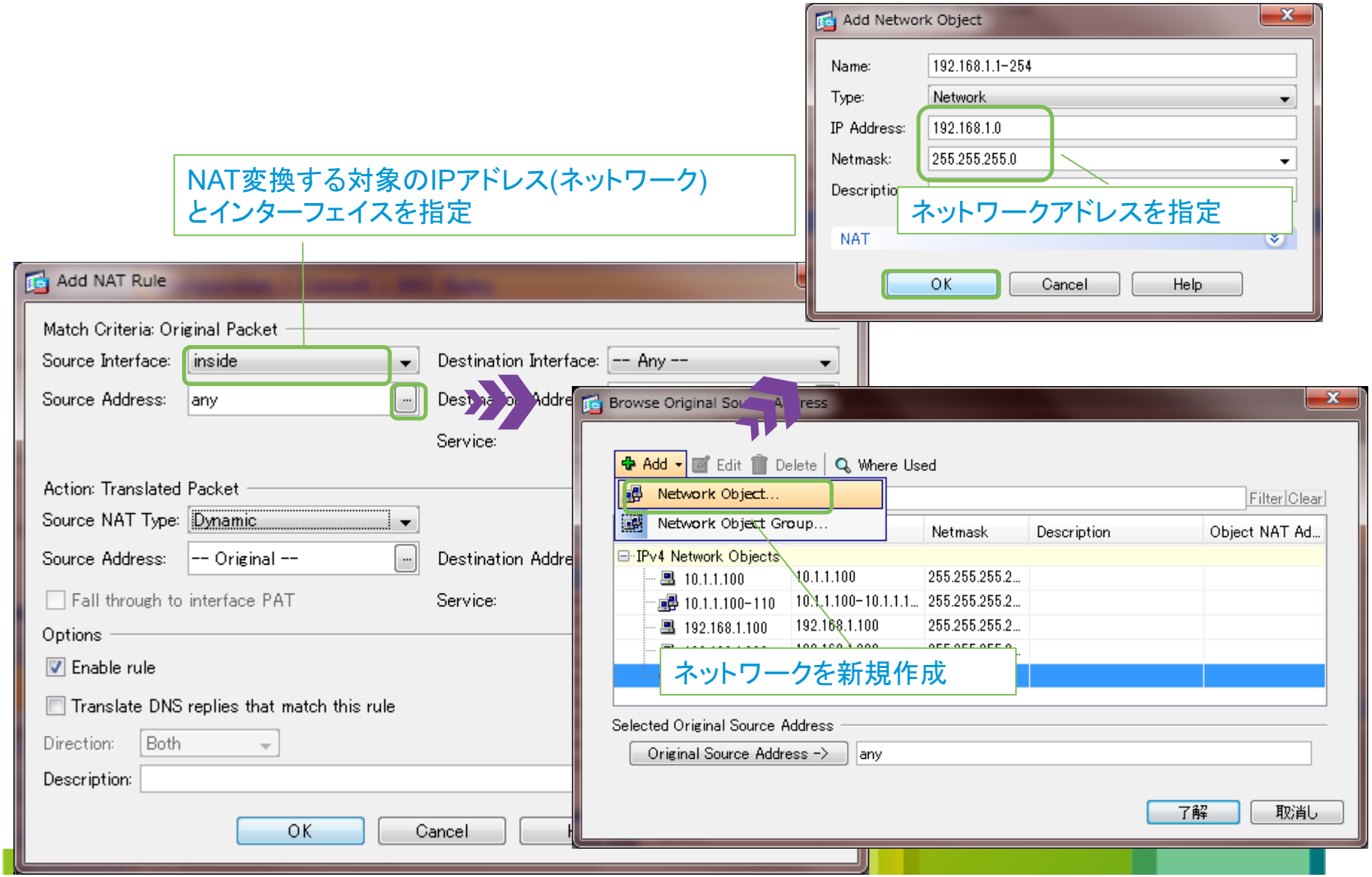
- 192.168.1.0/24 から来たトラフィックの送信元アドレスを10.1.1.100に変換するようなDynamic PAT を設定する。



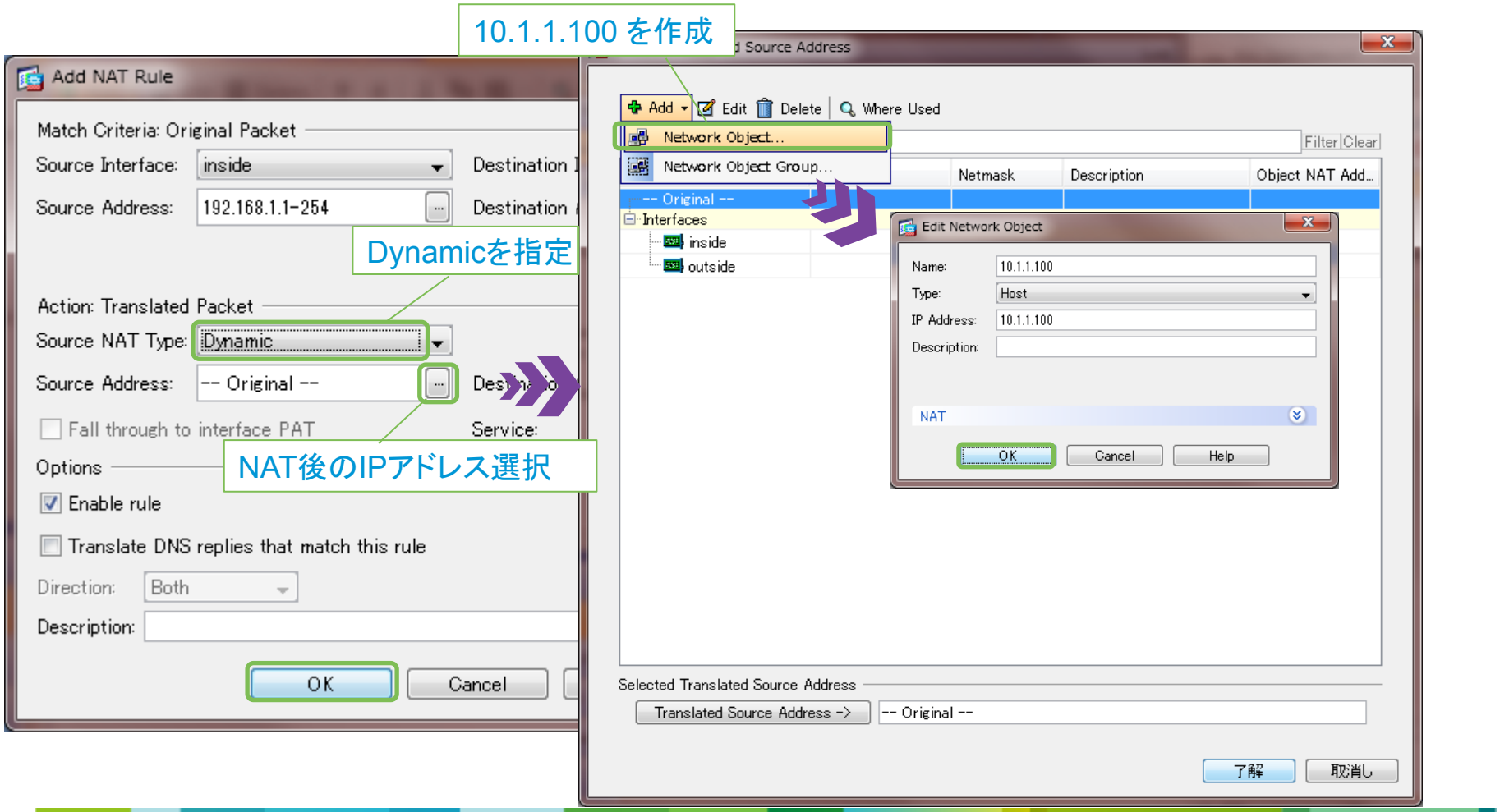
設定手順
1. NAT 対象のネットワークを指定
2. NAT 変換後のアドレスを指定
   2-1 変換後のIPアドレスを作成



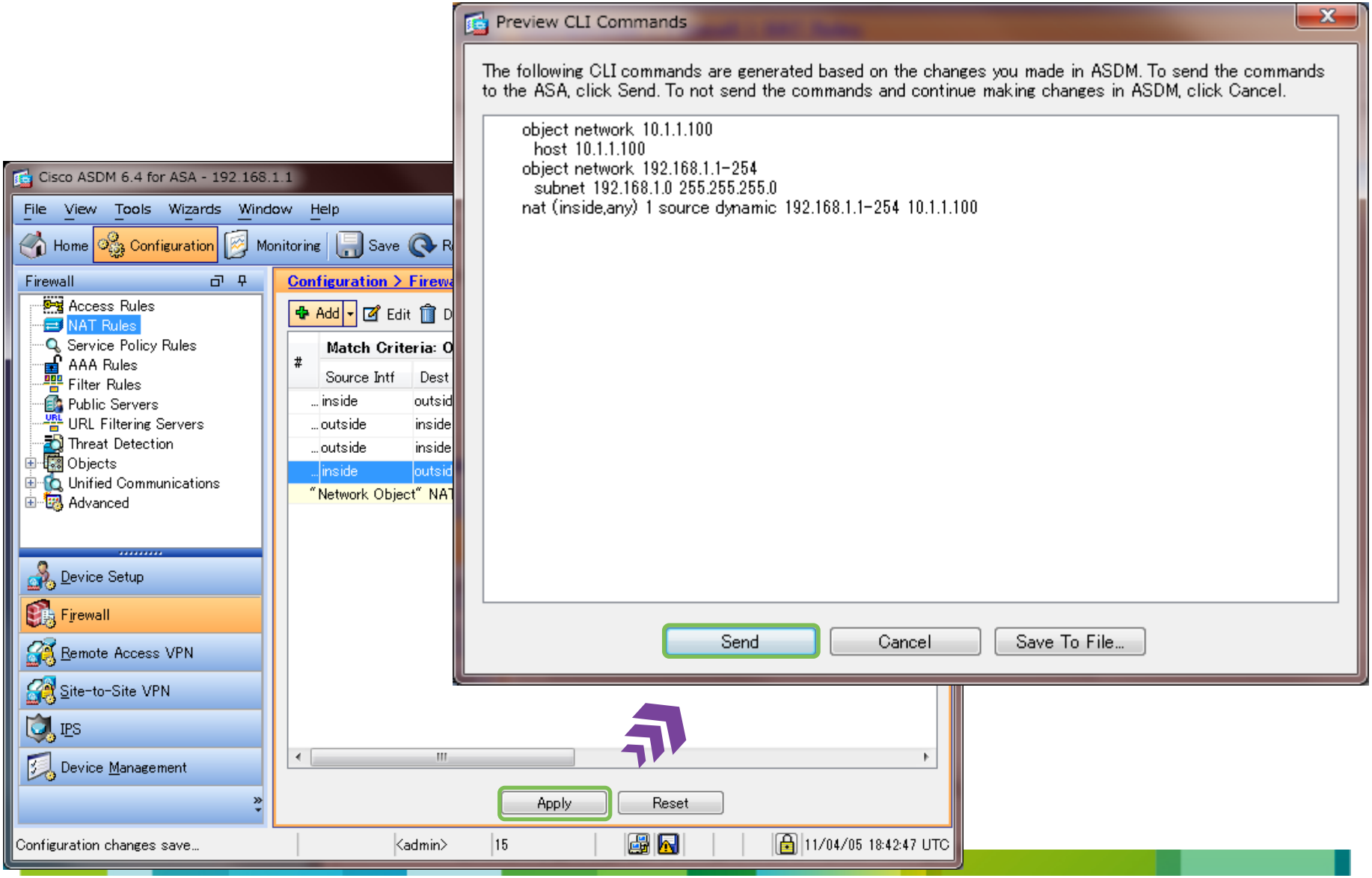
NAT 設定　Dynamic PAT



NAT 設定　Dynamic PAT

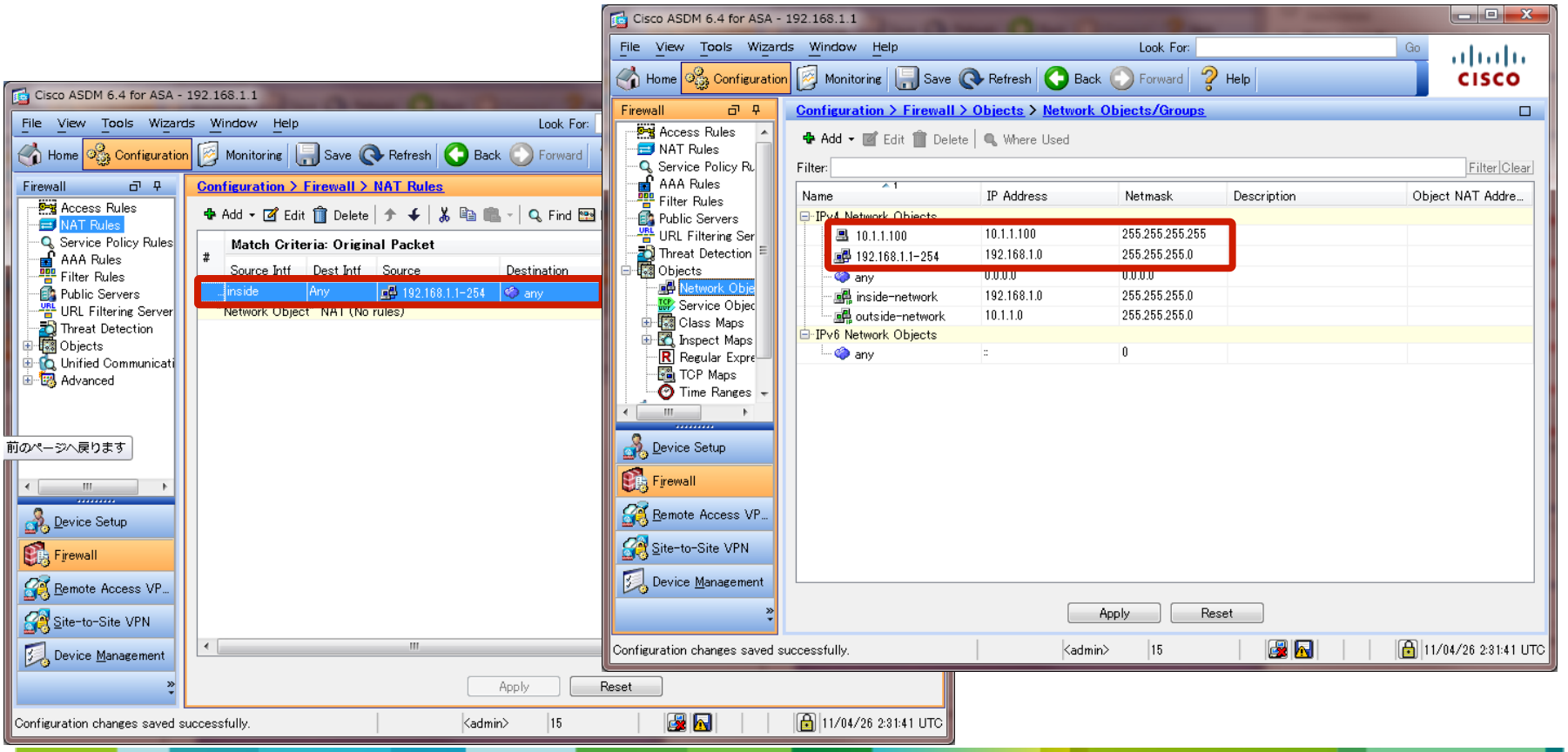


NAT 設定　Dynamic PAT 設定の反映



次の Exerciseの準備のために・・・

- 作成した NAT, Network Object を削除してください。



フィルタリングの設定

フィルタリング設定概要

- ACL (Access Control List) を各インターフェイスに設定し通信を許可/拒否する
- ACL は 複数のACE（Access Control Entry）から構成される。

ACE の主な構成要素

- permit/deny　:トラフィックを許可する場合はPermit、拒否する場合はDeny
- プロトコル　：ip、TCP、UDP、icmp、等を指定
- 送信元/宛先IP アドレス　：ホスト単位、ネットマスク単位、すべて(any)
- ポート番号　：TCP、UDP のトラフィックに対して、ポート番号の指定も可能

暗黙のDeny

ACL の最後にはすべてのIP パケットを拒否する”暗黙のDeny” が存在する
特定のトラフィックのみを拒否したい場合には特に注意が必要

特定のトラフィック以外を通したい場合、
拒否したいトラフィックを明示的に拒否(Deny)し、
最後に、すべてを許可するACE を加える

例）A→B のトラフィックのみ許可

1. permit A→B
2. deny any (暗黙のDeny)

A→B は1. のACE で許可され、
残りは2. の暗黙のdeny で拒否される

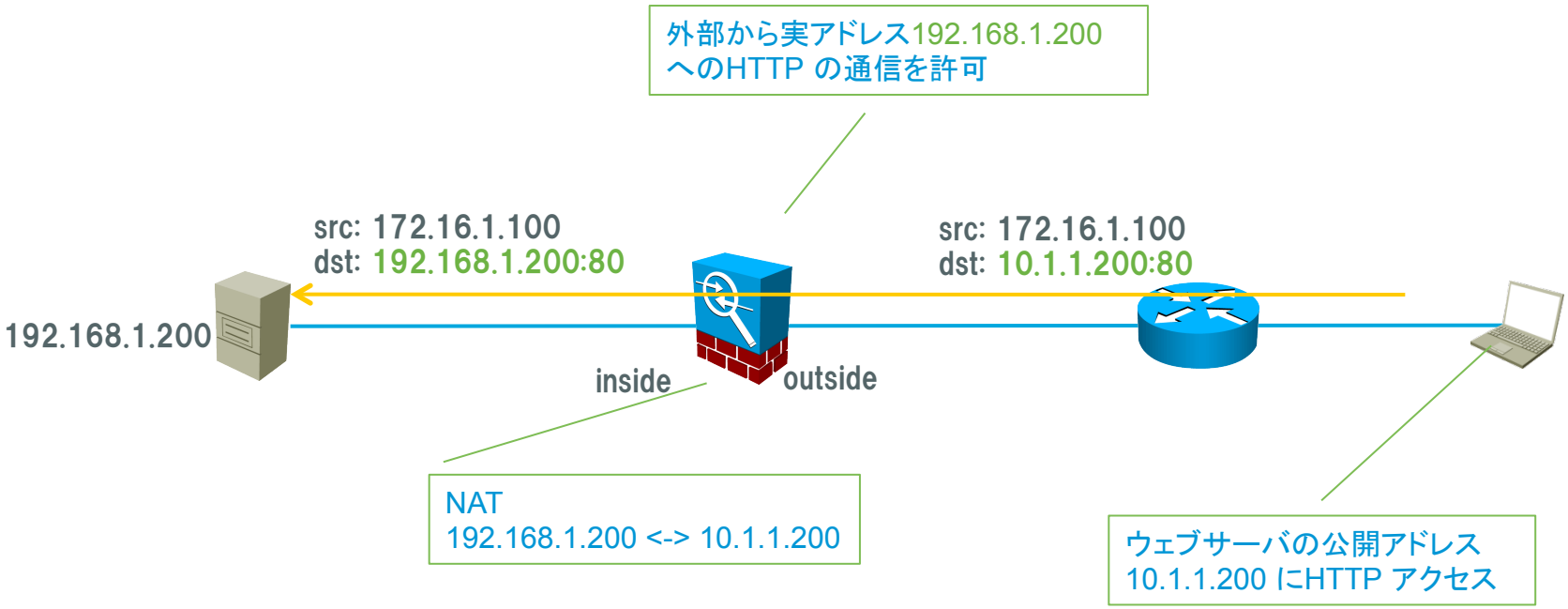
例）A→B のトラフィックのみ拒否

1. deny A→B
2. permit any ← 必要！
3. deny any (暗黙のDeny)

A→B は1. のACE で拒否され、
残りは2. のACEで許可される

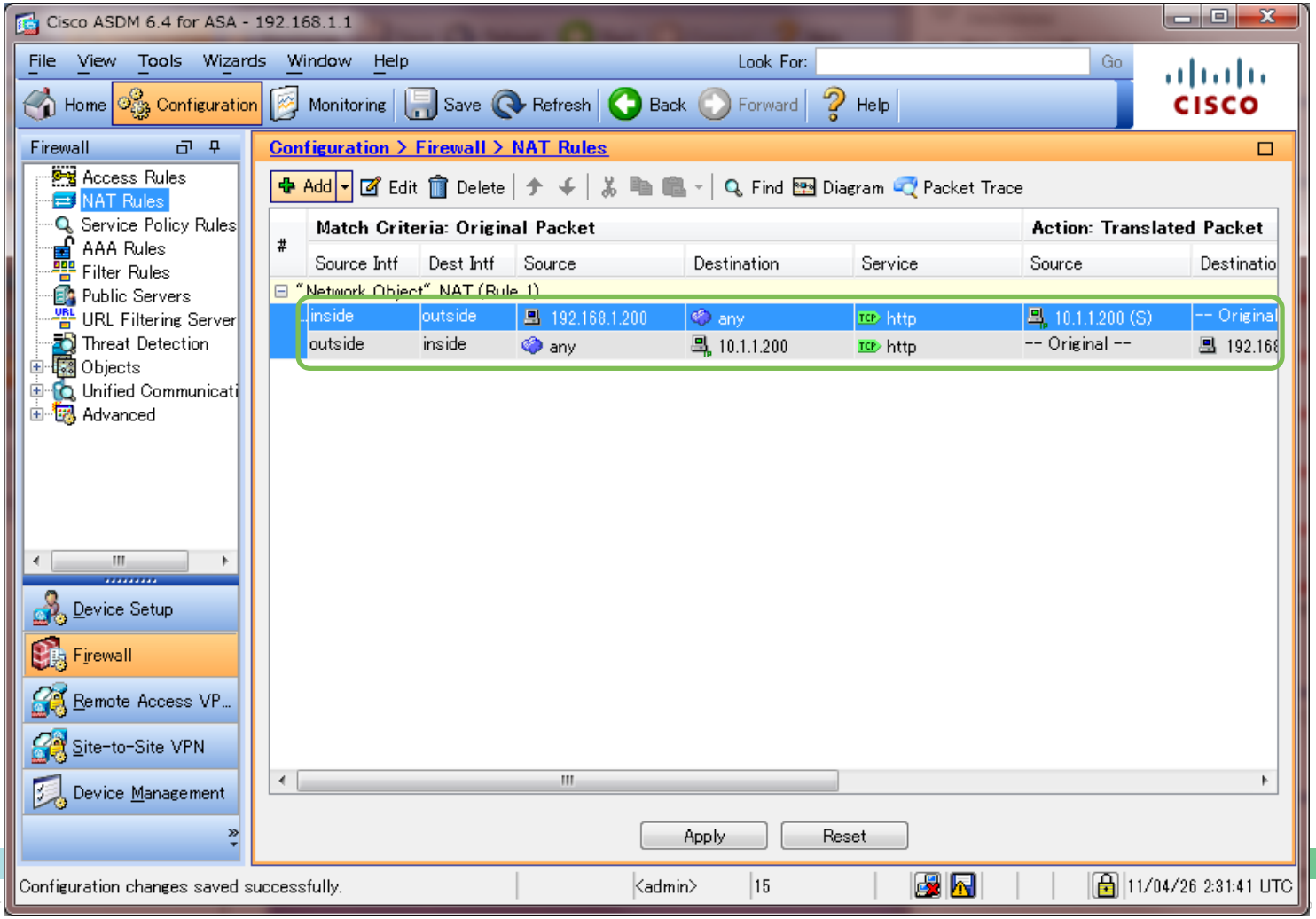
フィルタリング設定シナリオ

- 内部ネットワークにウェブサーバがあり、外部からのHTTP 通信を許可
- サーバのアドレスはStatic NAT をされて外部へ公開



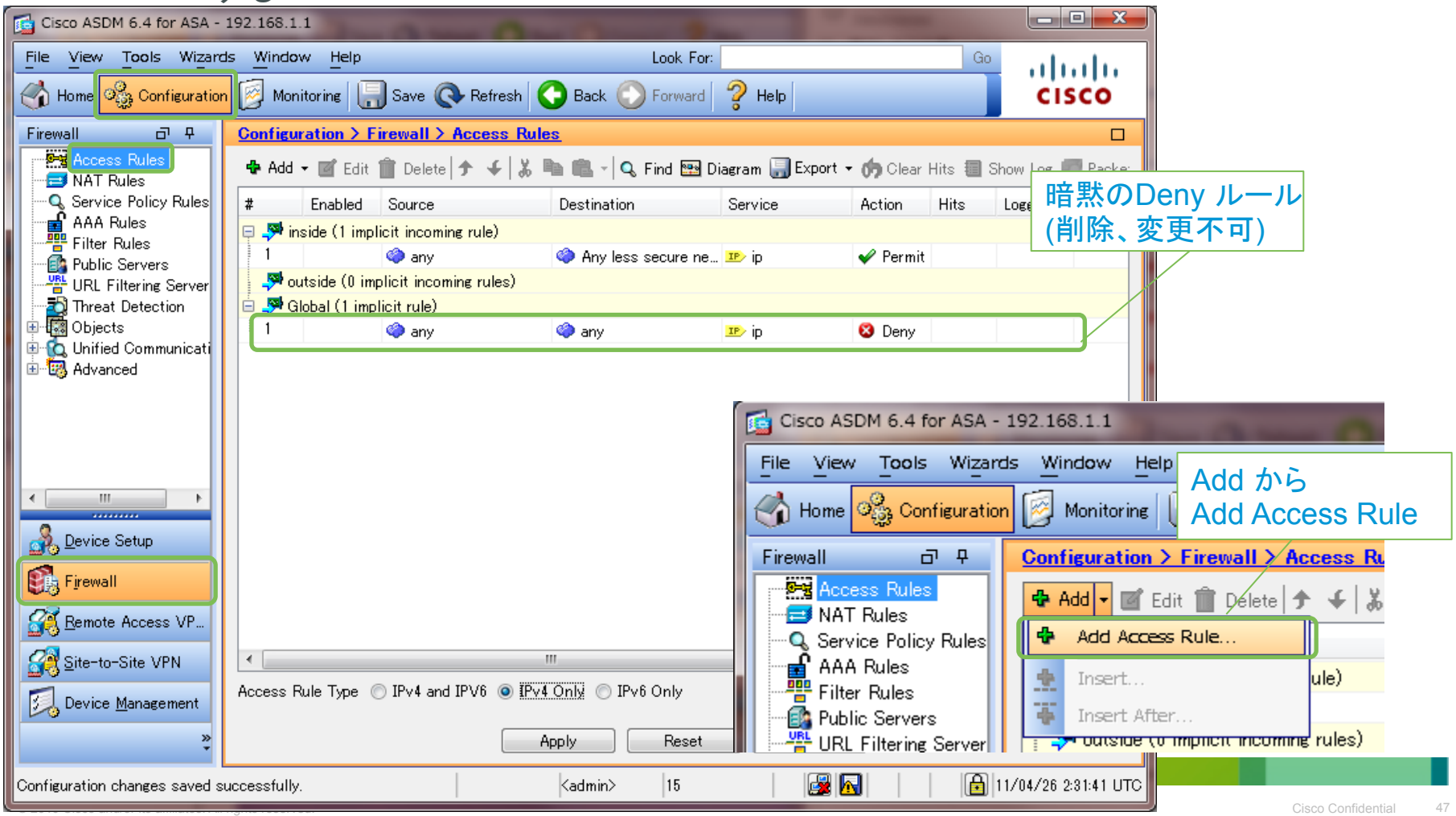
フィルタリング設定　NAT の設定

- ウェブサーバのIP アドレス192.168.1.200 を 公開アドレス10.1.1.200 に変換するNAT ルールを作成（作成方法 Static NAT の設定を参照）

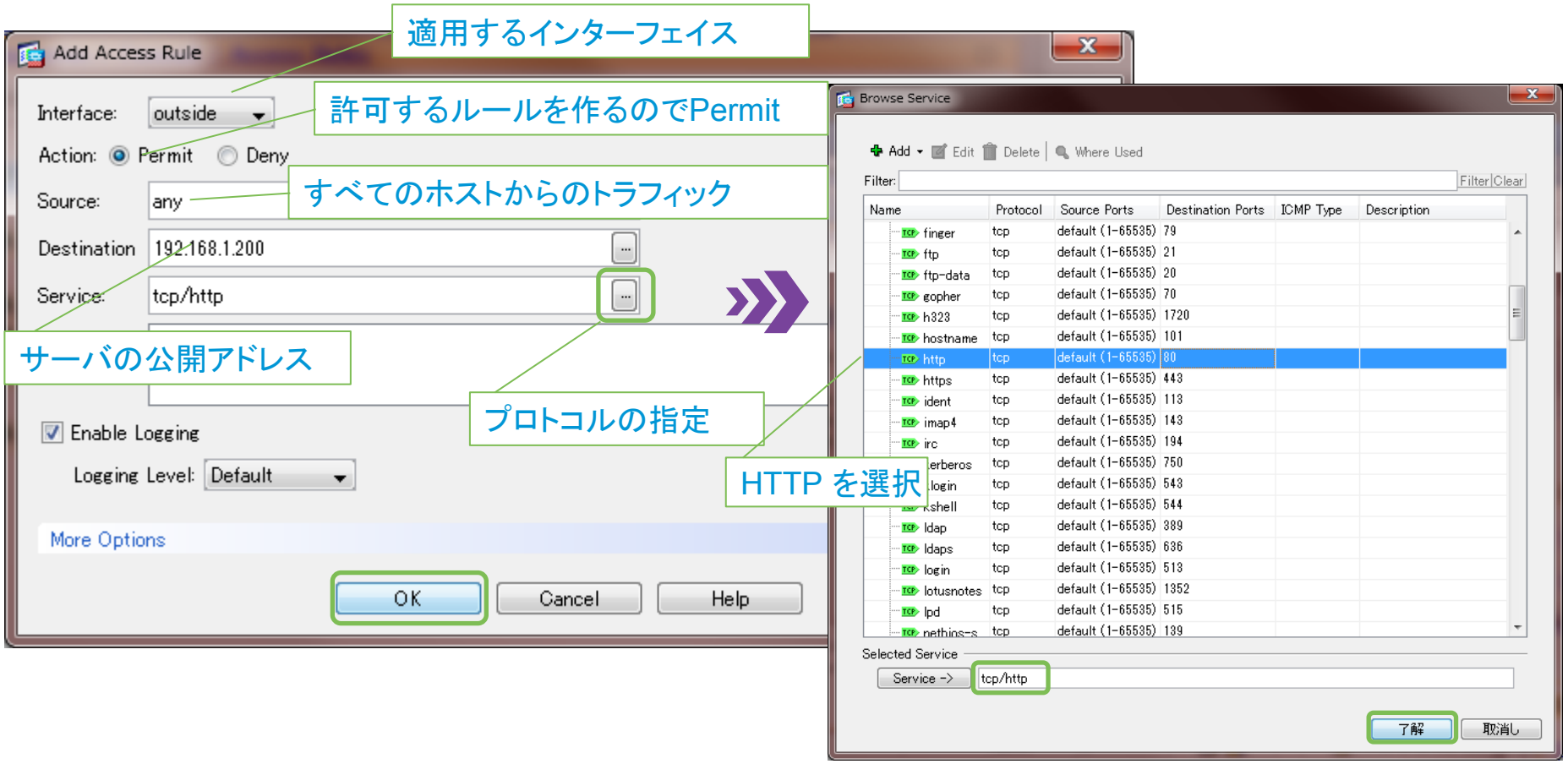


フィルタリング設定　アクセスルールの作成

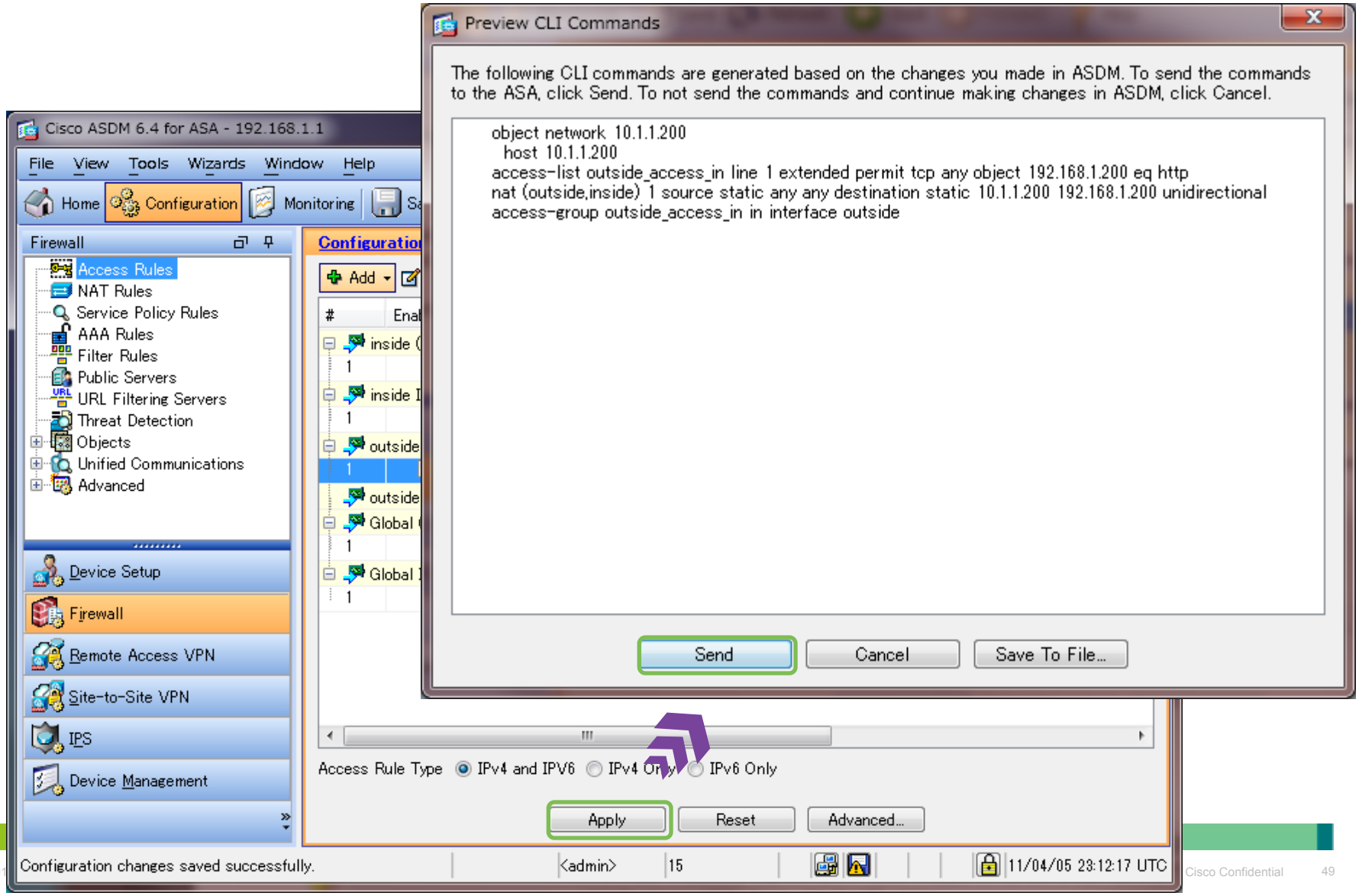
- 外部の任意のホストから実アドレス 192.168.1.200 へのTCP 80 番ポートへの通信を許可するためのアクセスルールを作成し、outside インターフェイスに設定する



フィルタリング設定　アクセスルールの作成 2



フィルタリング設定　設定の反映



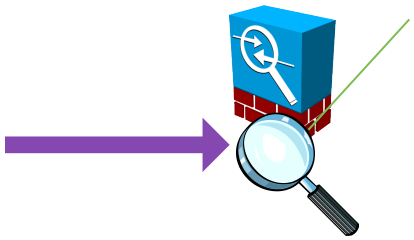
インスペクションの設定

インスペクションとMPF (Modular Policy Framework)

インスペクションにより、トラフィックのステート情報、アプリケーションレベルの情報を考慮したより高度な制御が可能

インスペクションはMPF (Modular Policy Framework) を用いて設定を行う

MPF (Modular Policy Framework)
特定のトラフィックに対してQoS、インスペクション等のアクションを柔軟に適用するための仕組み



1. ACL 等に従ってトラフィックをClass に分類
2. Class に応じたアクション(QoS、インスペクション等)を適用

この一連のルール（ポリシー）を特定のインターフェイス、もしくはすべてのインターフェイスに対して適用する

デフォルトのインスペクション設定
デフォルトでは次のトラフィックに対するインスペクションが有効

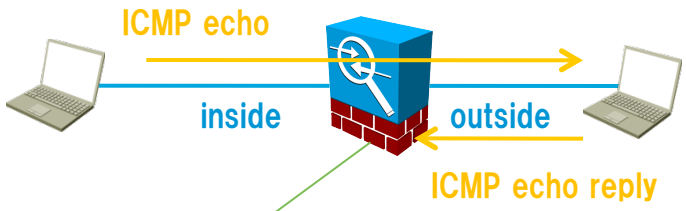
dns, ftp, h323 h225, h323 ras, ip options, netbios, rsh, rtsp, skinny, esmtp, sqlnet, sunrpc, tftp, sip, xdmcp

※ICMP はデフォルトでインスペクションが行われないことに注意

ICMP のインスペクション

デフォルトで無効になっているICMP のインスペクションを有効にすることで、
内部ネットワークから外部ネットワークに対する ping の戻りパケットを
自動的に許可することが可能

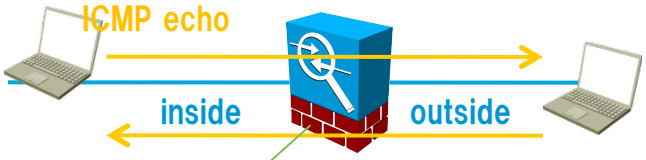
デフォルトの状態 (ICMP インスペクション：無効)



outside → inside の通信は原則拒否

inside からのping による疎通確認のために
outside にICMP を通すようなACL を
設定する必要がある

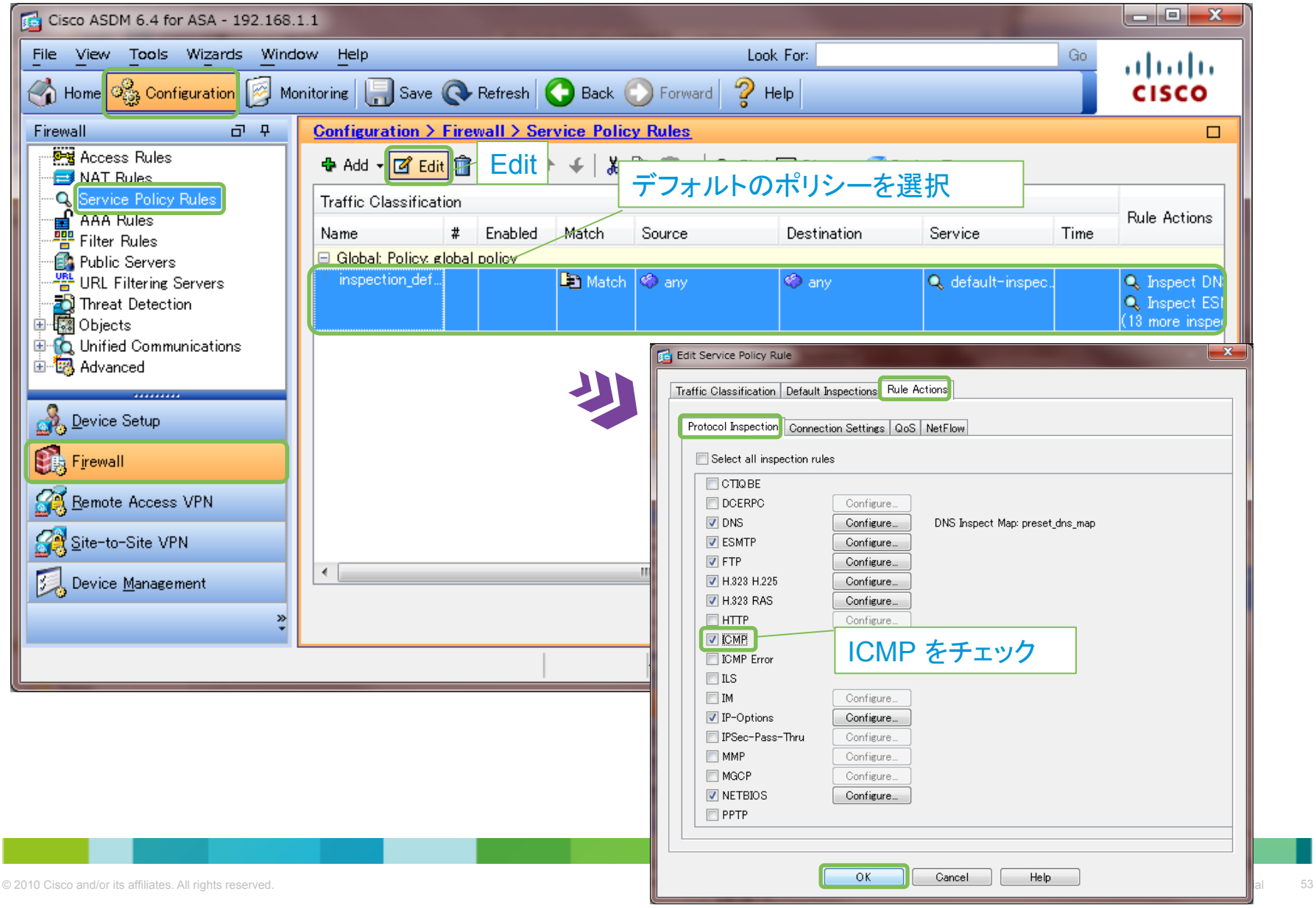
ICMP インスペクション：有効



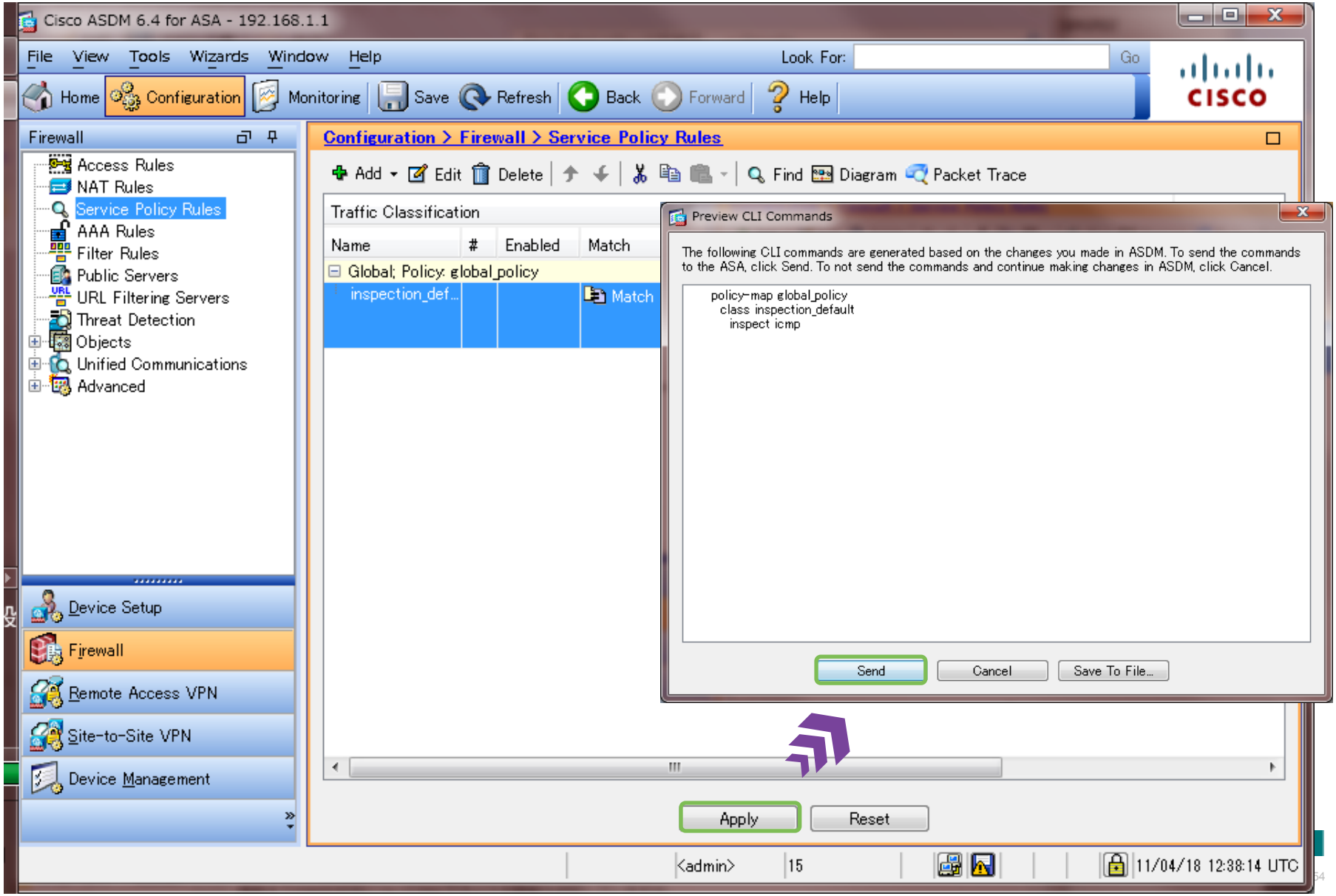
inside からの通信の戻りパケットは許可

inside からのping による疎通確認のために
outside にACL を設定する必要なし

ICMP インスペクション設定



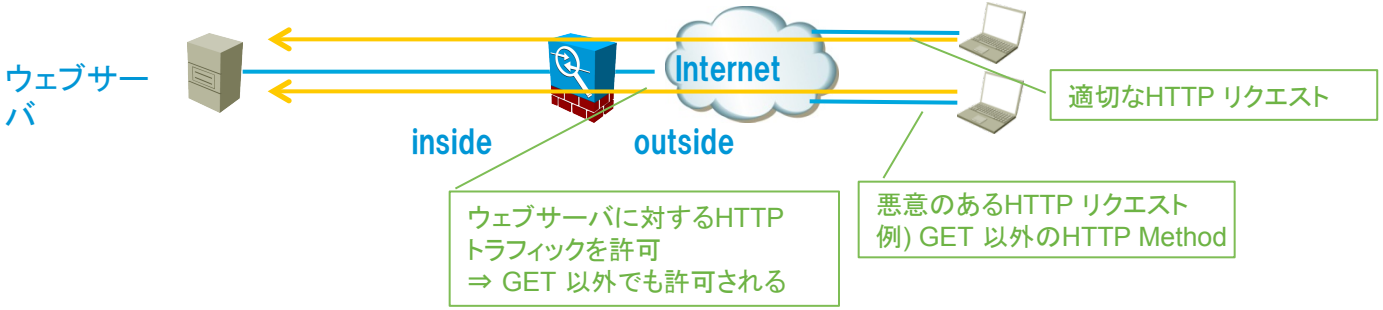
ICMP インスペクション設定 設定の反映



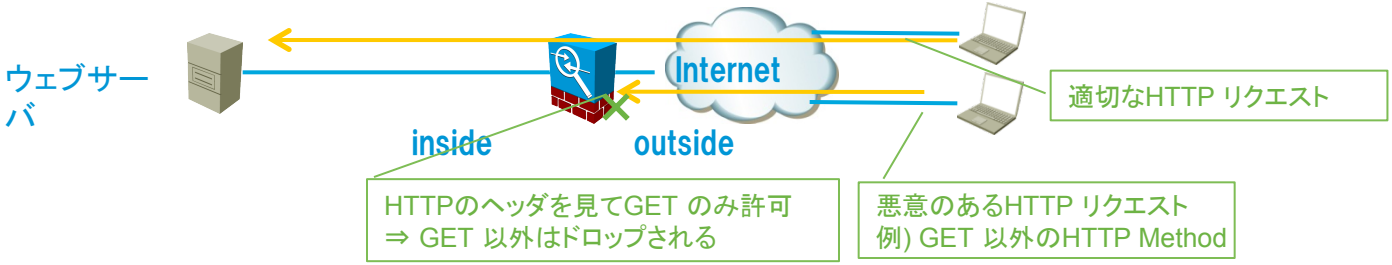
アプリケーションインスペクション概要

主要なアプリケーションのトラフィックに関しては、アプリケーションインスペクションを設定することで、L7（アプリケーション層）の情報に基づいてトラフィックの制御を行い、より高度なフィルタリングが可能

例）ACL によるフィルタリングのみの場合

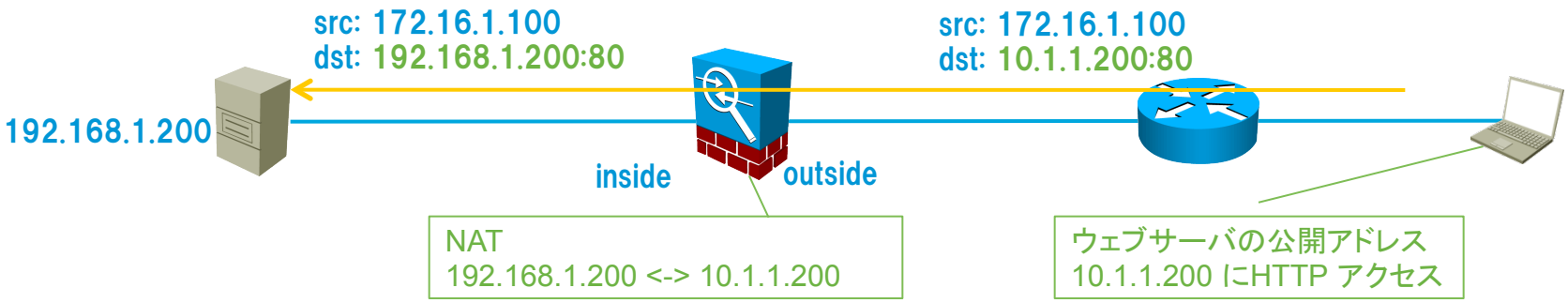


例）アプリケーションインスペクションによる制御



HTTP インスペクション設定概要

ここではアプリケーションインスペクションの例としてHTTP のインスペクションの設定を行う



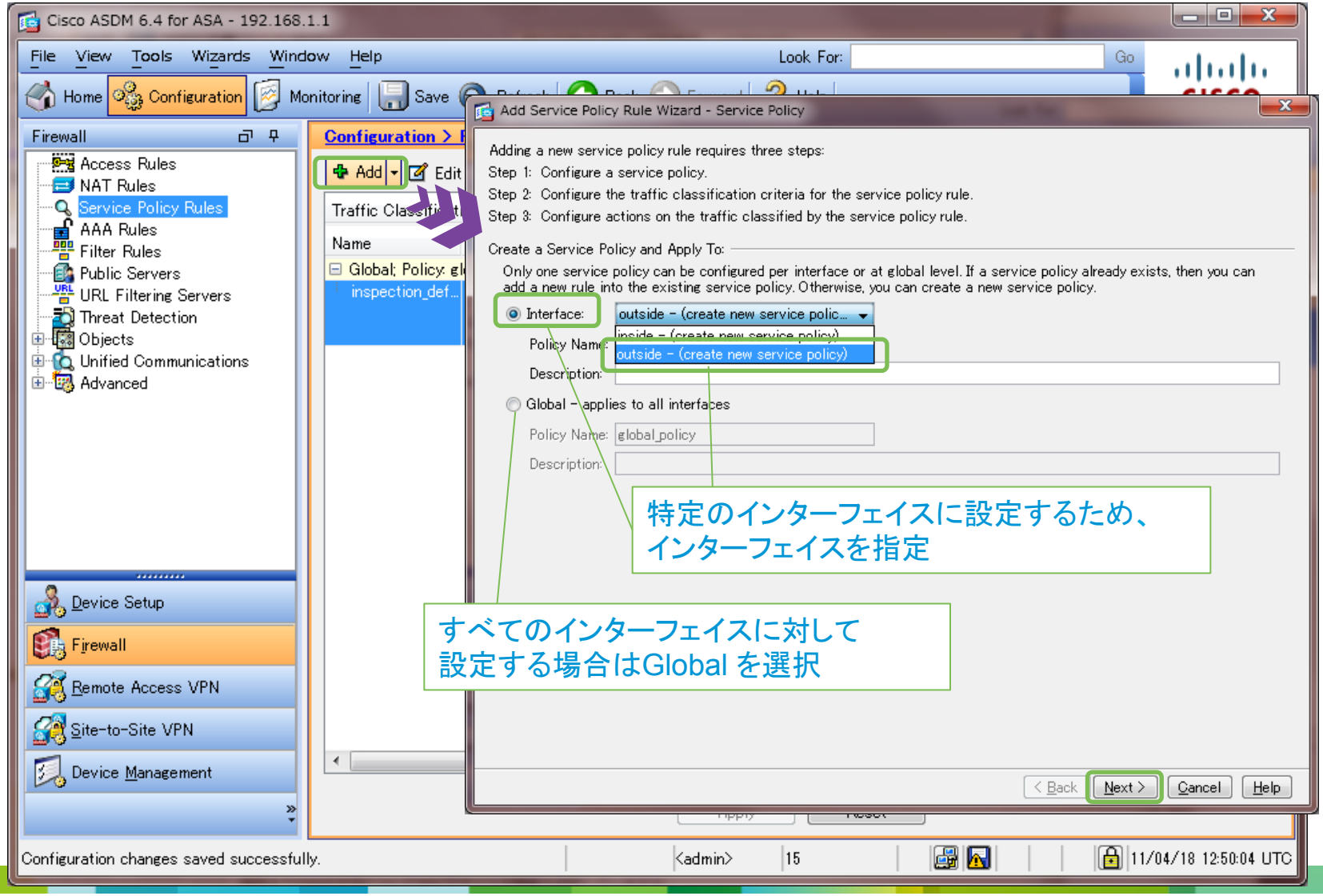
HTTP インスペクションの設定シナリオ

- HTTP Request のMethod は GET のみ許可
- 1024byte を超えるようなRequest は拒否
- ポリシーはoutside のインターフェイスに適用

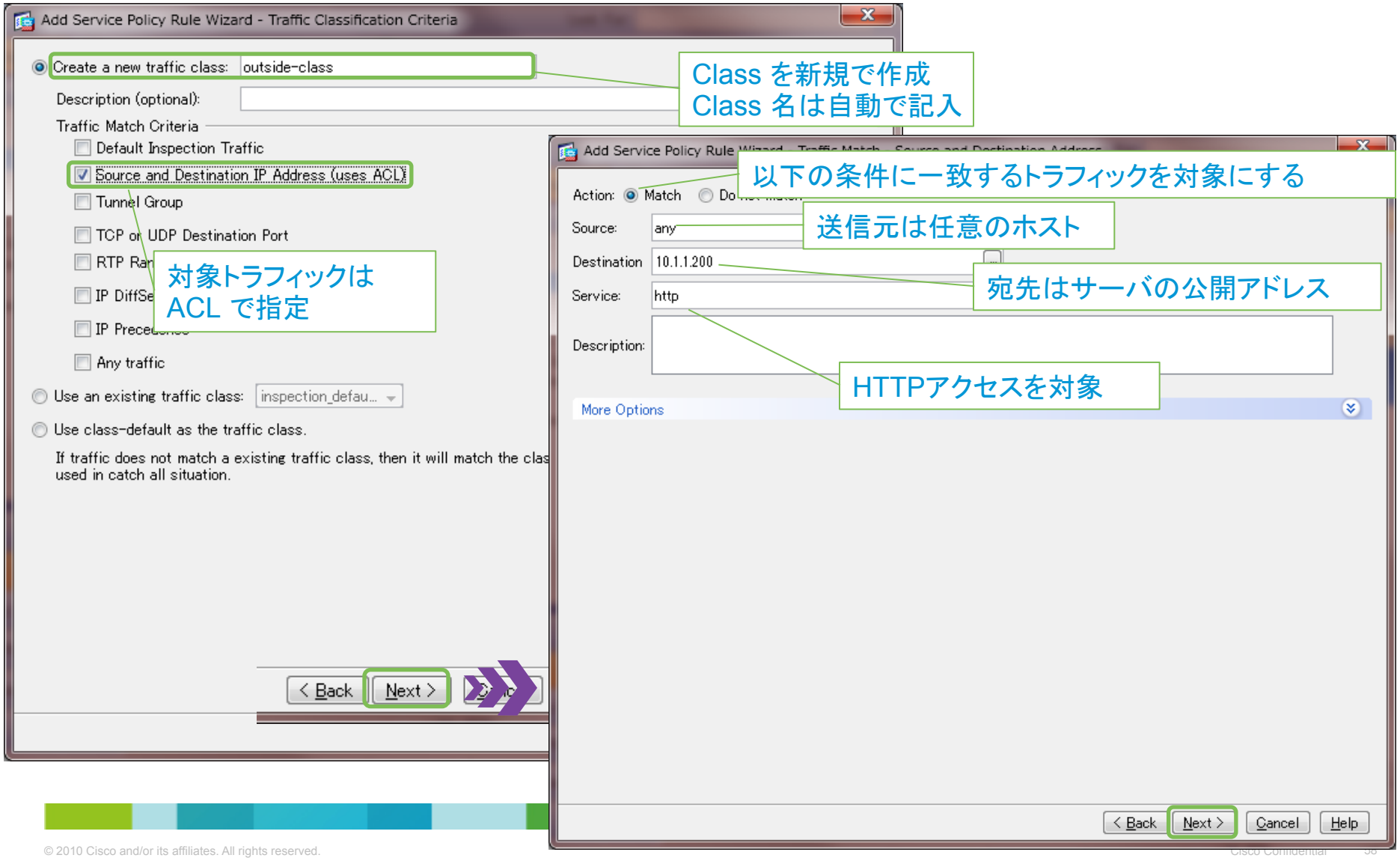
HTTP インスペクションの設定手順

- 適用インターフェイスの指定
- 対象トラフィックの指定
- インスペクションルールの作成

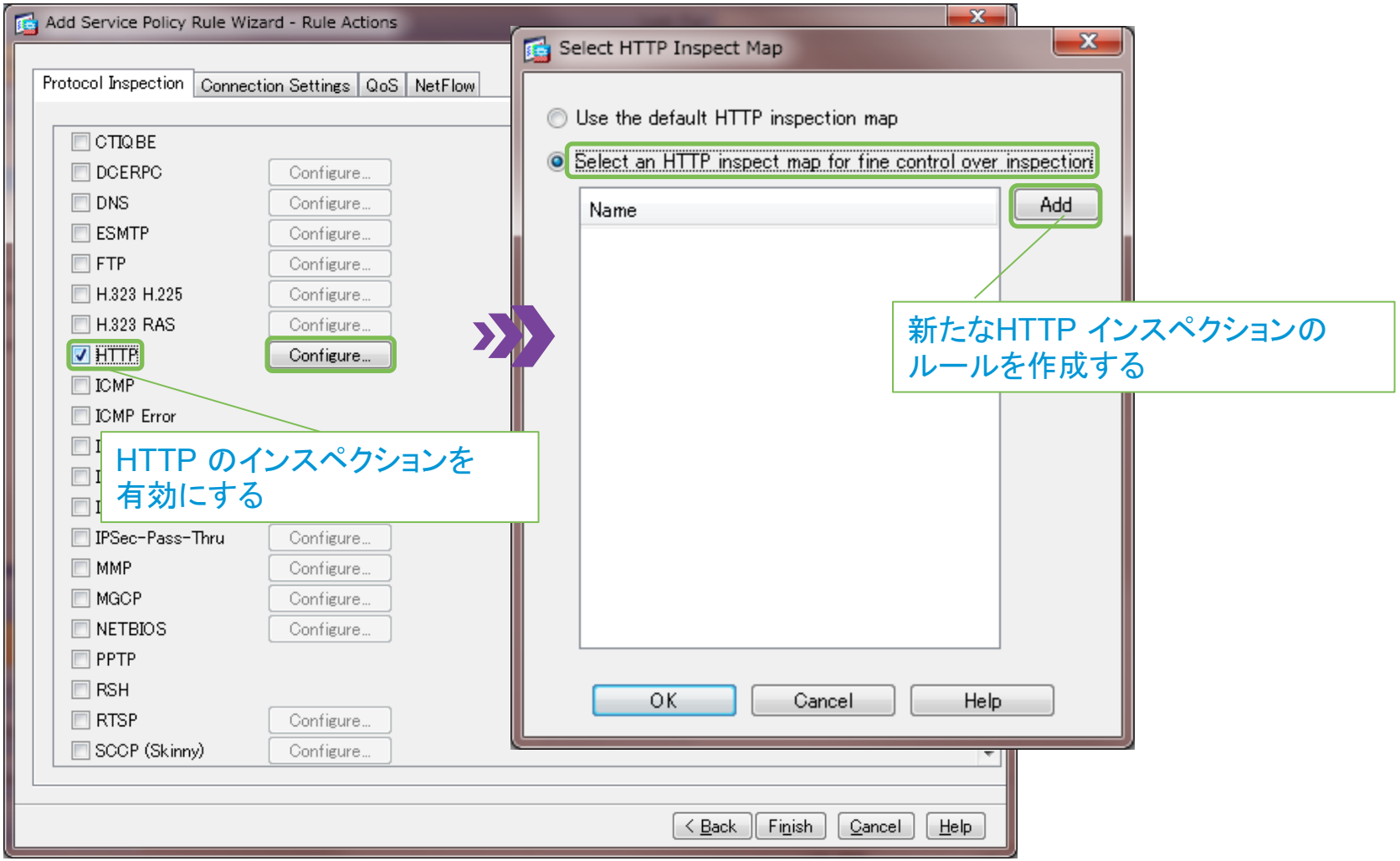
インスペクション設定 適用インターフェイスの指定



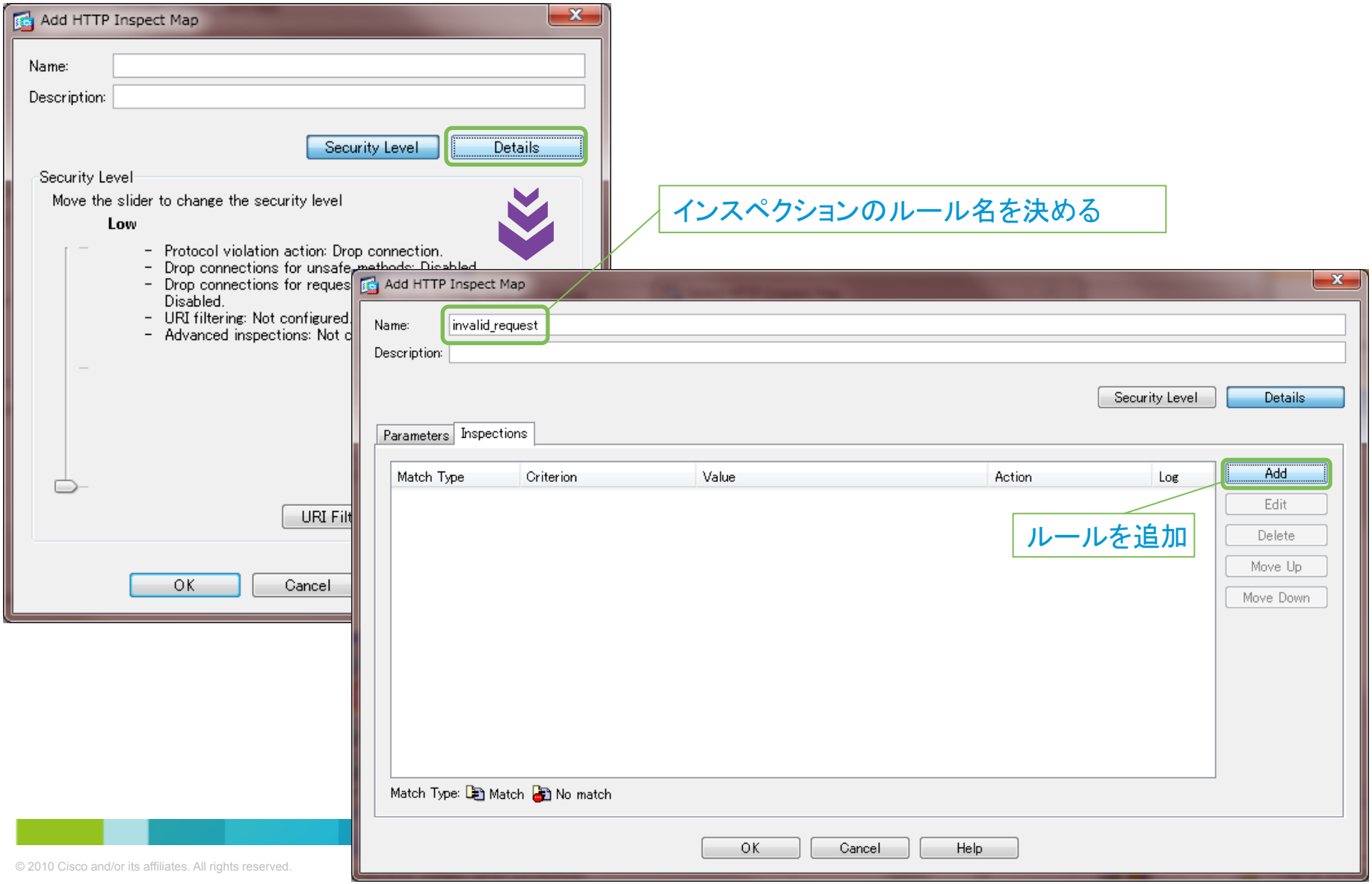
インスペクション設定 対象トラフィックの指定



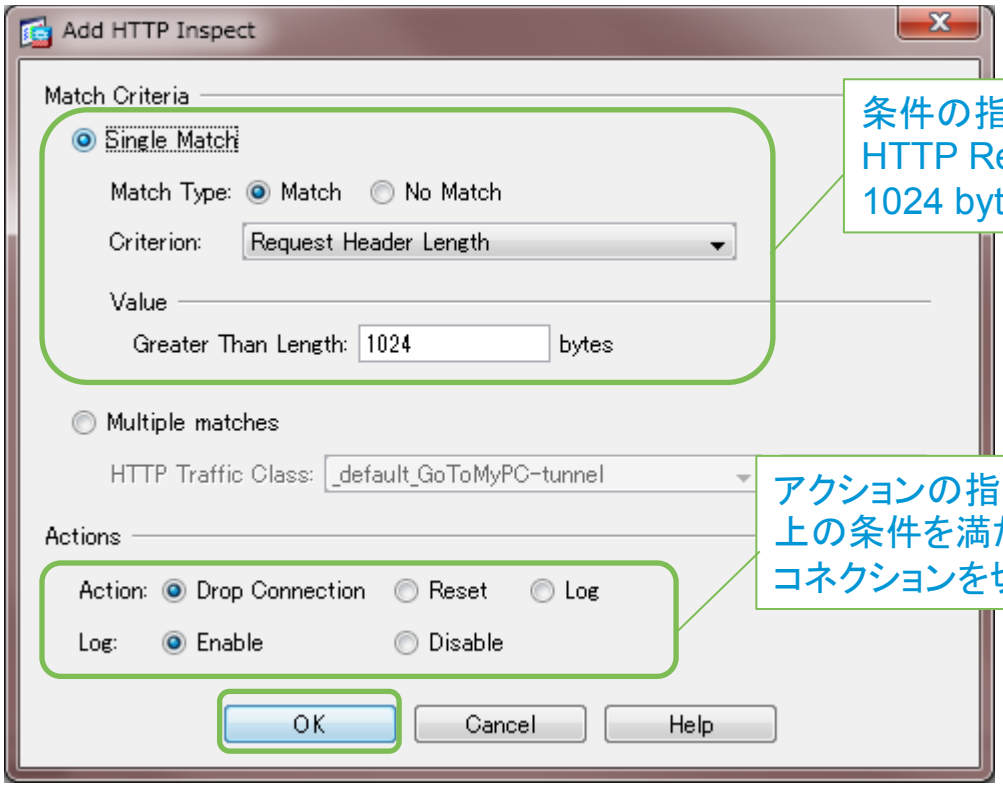
インスペクション設定 インスペクションルールの作成



インスペクション設定 インスペクションルールの作成2



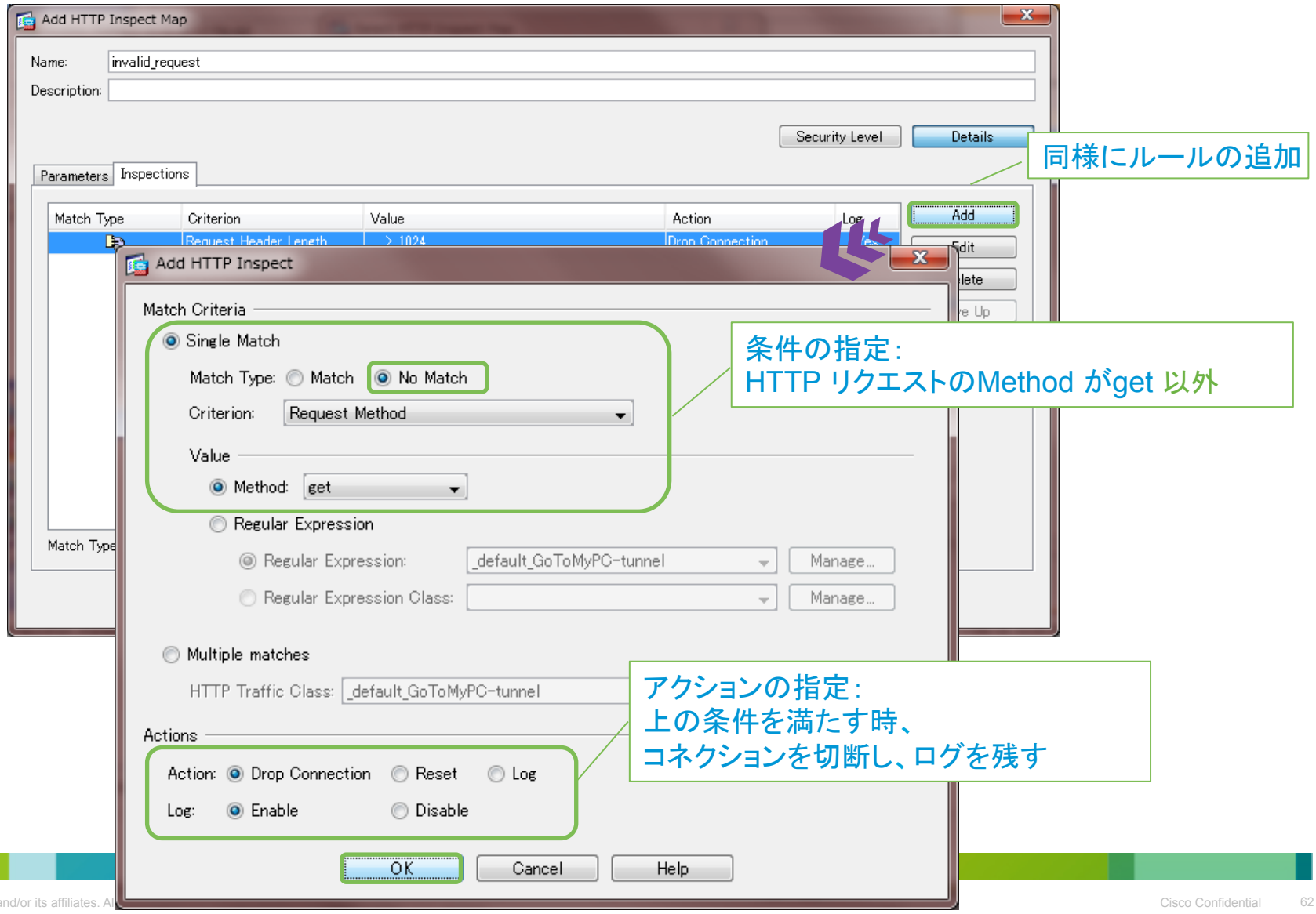
インスペクション設定 インスペクションルールの作成3



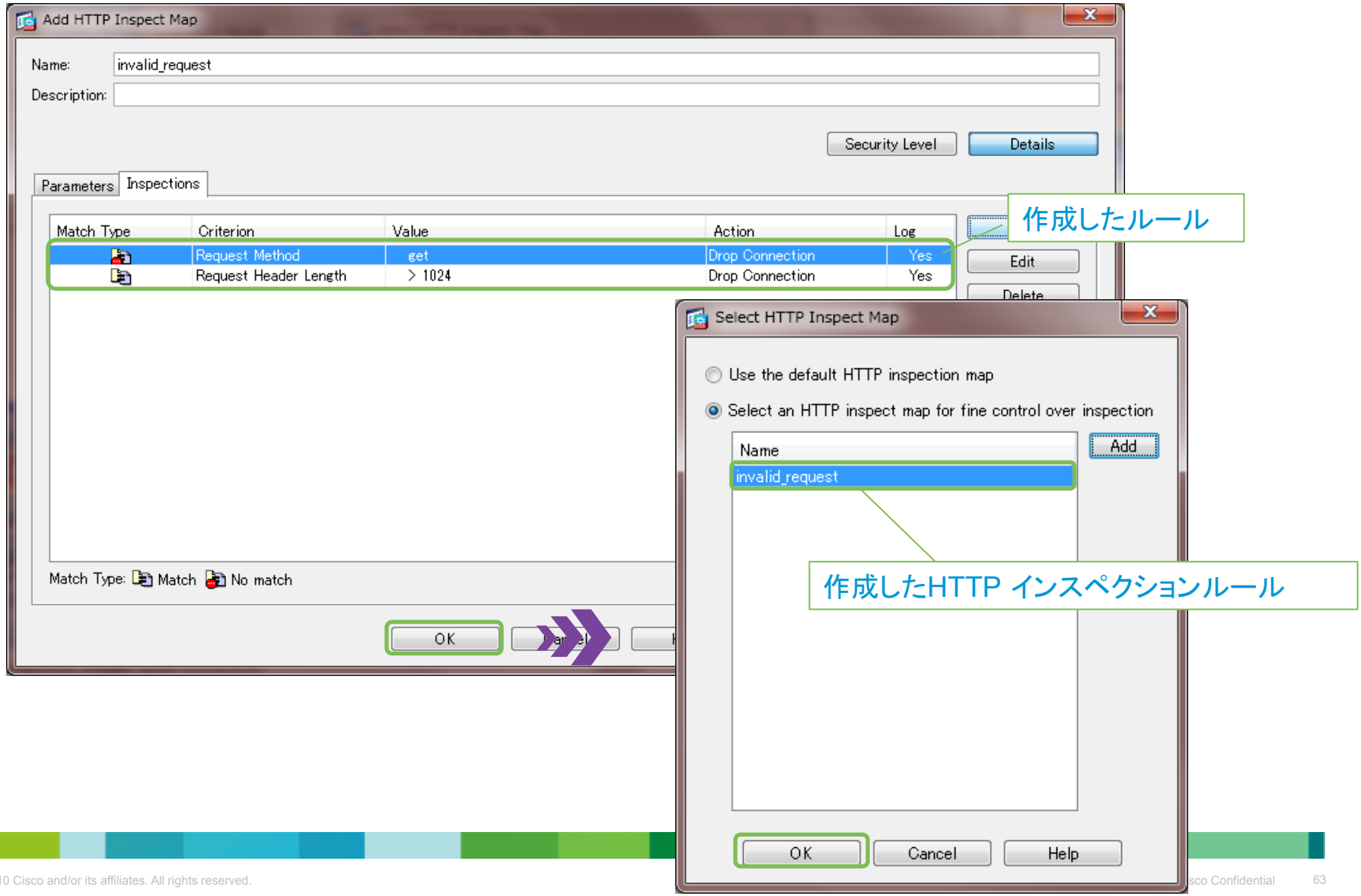
条件の指定:
HTTP Request のヘッダサイズが
1024 byte 以上

アクションの指定:
上の条件を満たす時、
コネクションを切断し、ログを残す

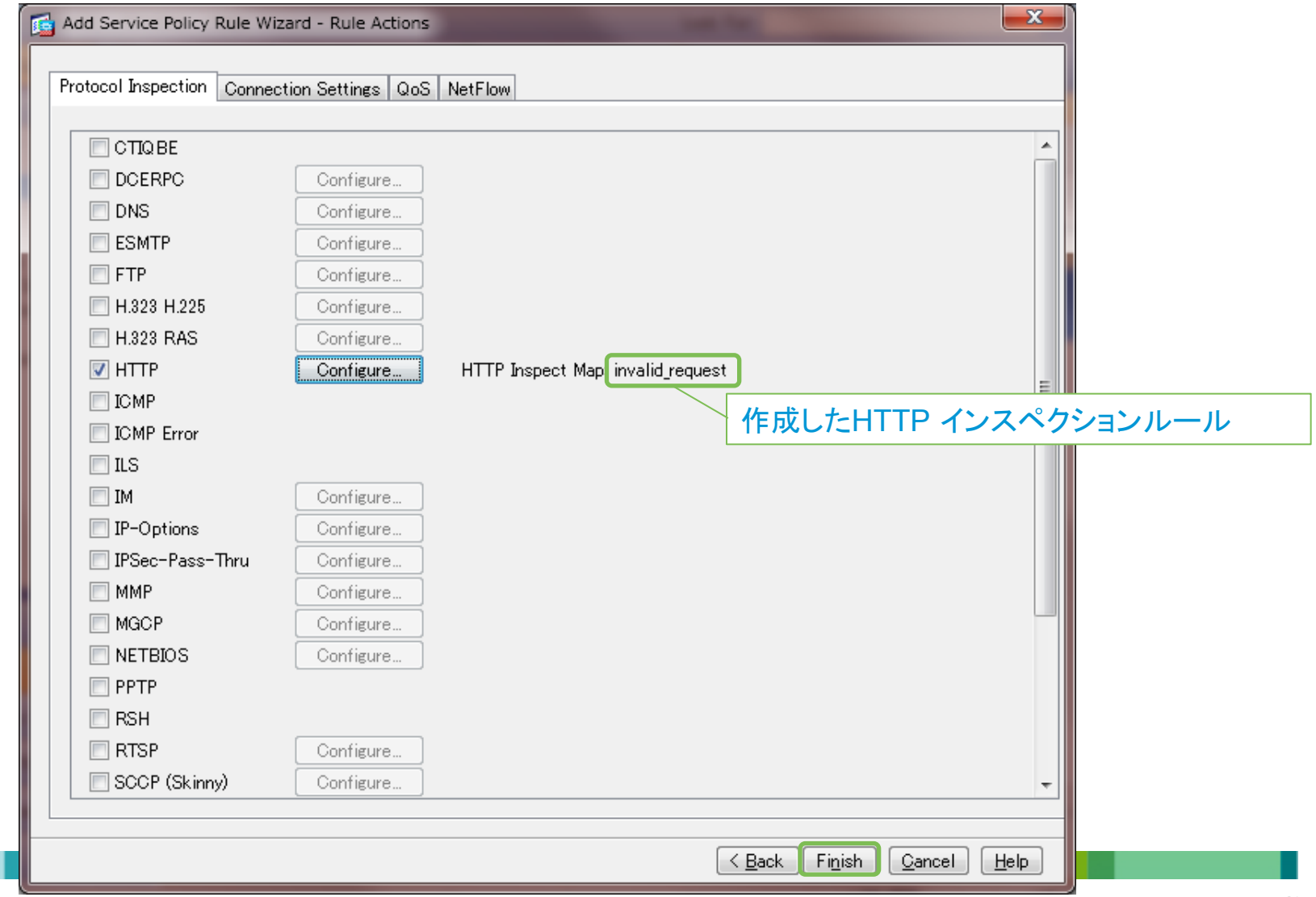
インスペクション設定 インスペクションルールの作成4



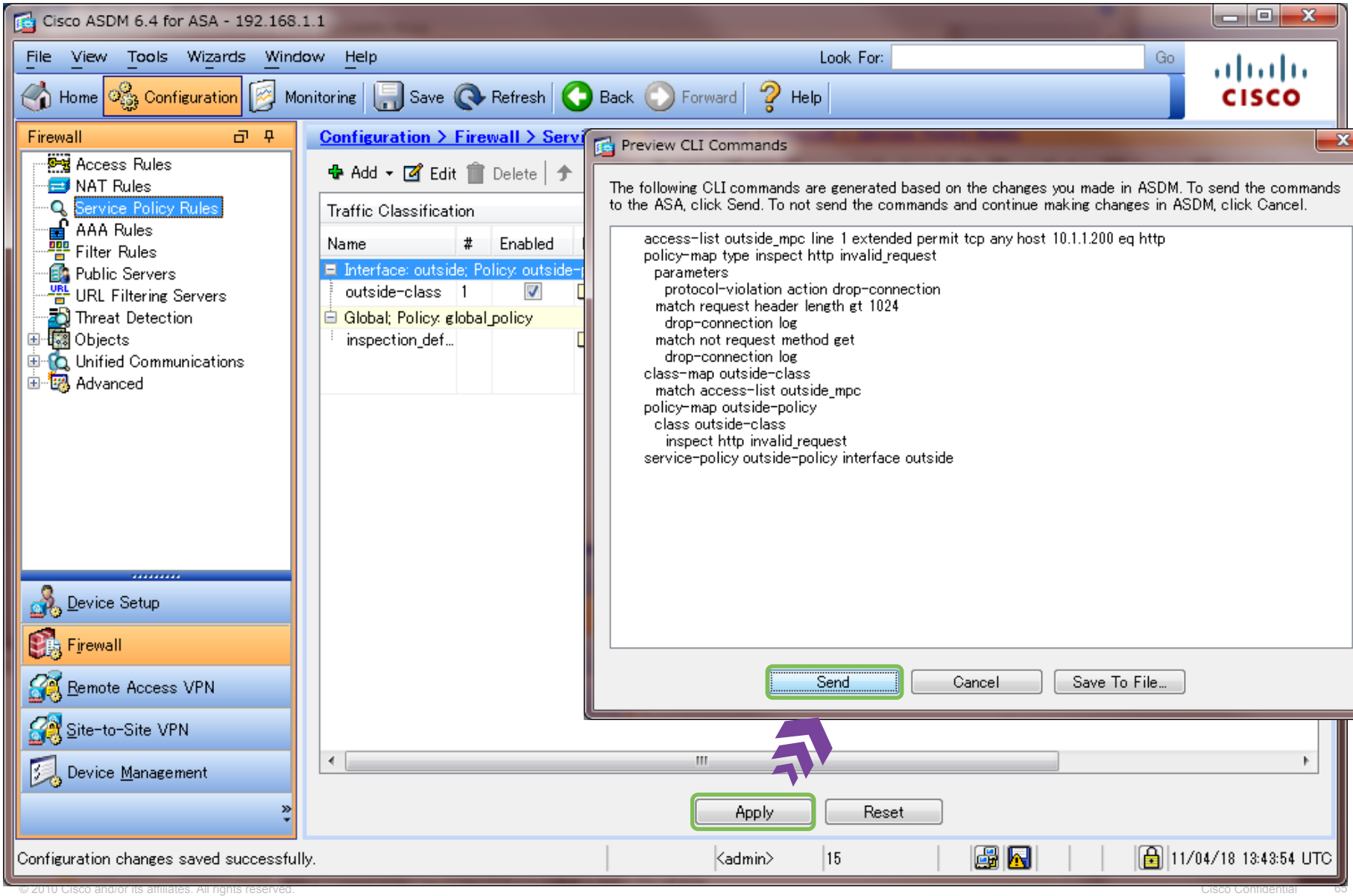
インスペクション設定 インスペクションルールの作成5



インスペクション設定 インスペクションルールの作成6

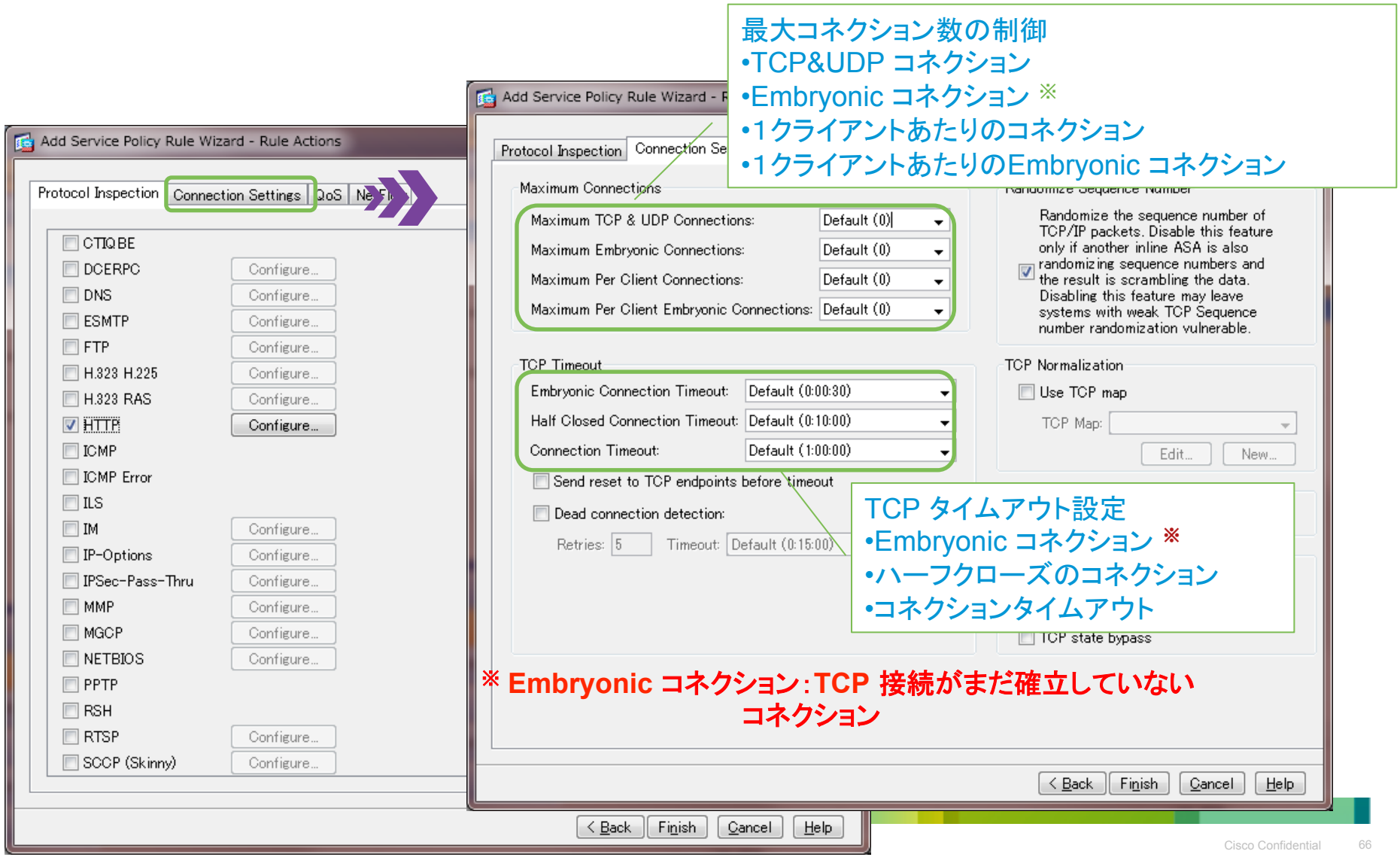


インスペクション設定 設定の反映



インスペクション設定　補足

インスペクションの設定の中で、コネクションに関連する制御も行うことが可能



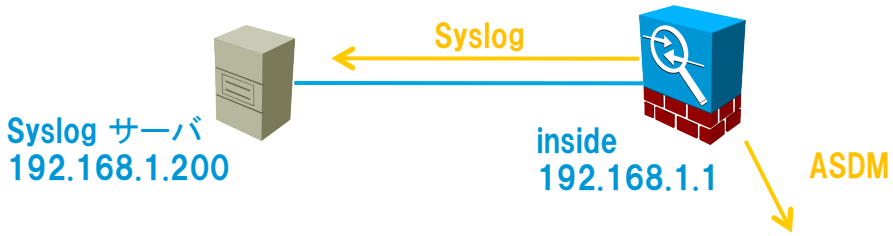
Loggingの設定

Logging 設定概要

ASA のログは次のような様々な方法で出力することが可能

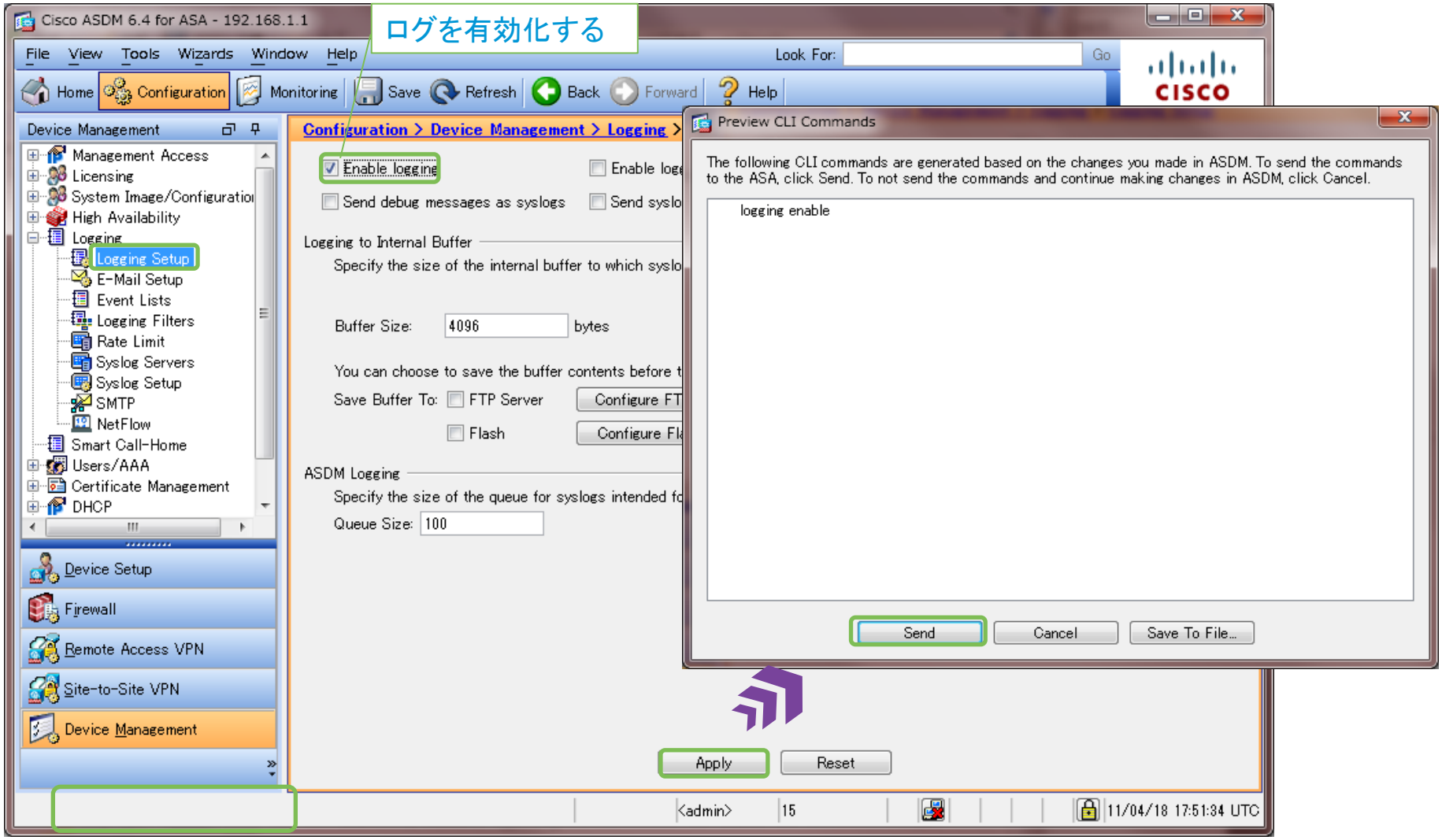
- ASA 内のバッファ
- SNMP Trap
- E-Mail
- コンソール
- ASDM
- Syslog サーバ

ここではASDM と Syslog サーバへのログ出力を設定する

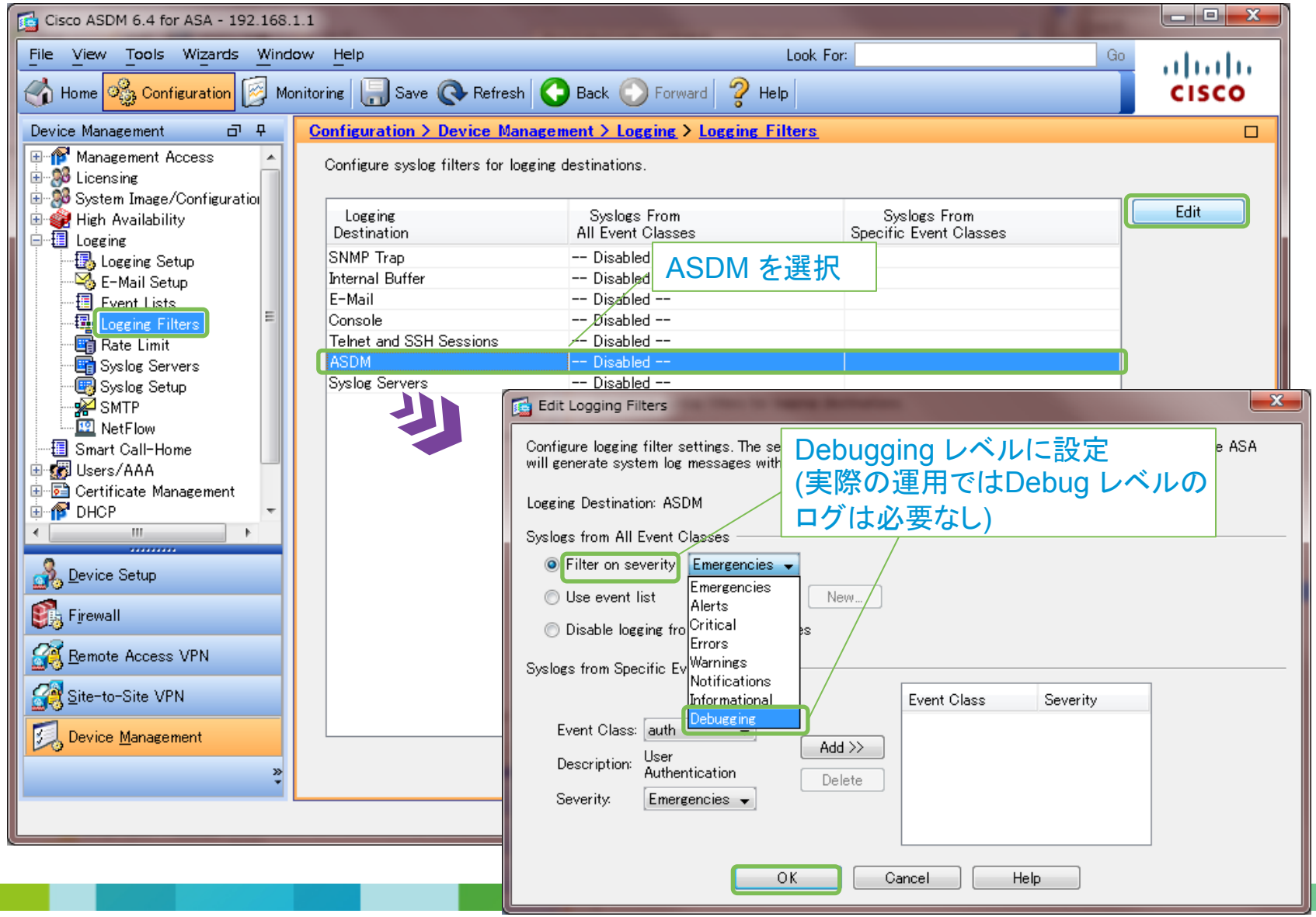


Severity	Date	Time	Syslog ID	Source IP	Source	Destination IP	Destina	Description
6	Apr 19 2011	04:31:55	302014	192.168.1.100	64249	192.168.1.1	443	Teardown TCP connection 598 for inside:192.168.1.100/64249 to identity:192.168.1.1
7	Apr 19 2011	04:31:55	710005	192.168.1.100	64249	192.168.1.1	443	TCP request discarded from 192.168.1.100/64249 to inside:192.168.1.1/443
6	Apr 19 2011	04:31:55	302014	192.168.1.100	64252	192.168.1.1	443	Teardown TCP connection 602 for inside:192.168.1.100/64252 to identity:192.168.1.1
6	Apr 19 2011	04:31:55	302014	192.168.1.100	64253	192.168.1.1	443	Teardown TCP connection 603 for inside:192.168.1.100/64253 to identity:192.168.1.1
7	Apr 19 2011	04:31:55	710005	192.168.1.100	64253	192.168.1.1	443	TCP request discarded from 192.168.1.100/64253 to inside:192.168.1.1/443
7	Apr 19 2011	04:31:55	710005	192.168.1.100	64251	192.168.1.1	443	TCP request discarded from 192.168.1.100/64251 to inside:192.168.1.1/443
6	Apr 19 2011	04:31:55	106015	192.168.1.100	64251	192.168.1.1	443	Deny TCP (no connection) from 192.168.1.100/64251 to 192.168.1.1/443 flags FIN A

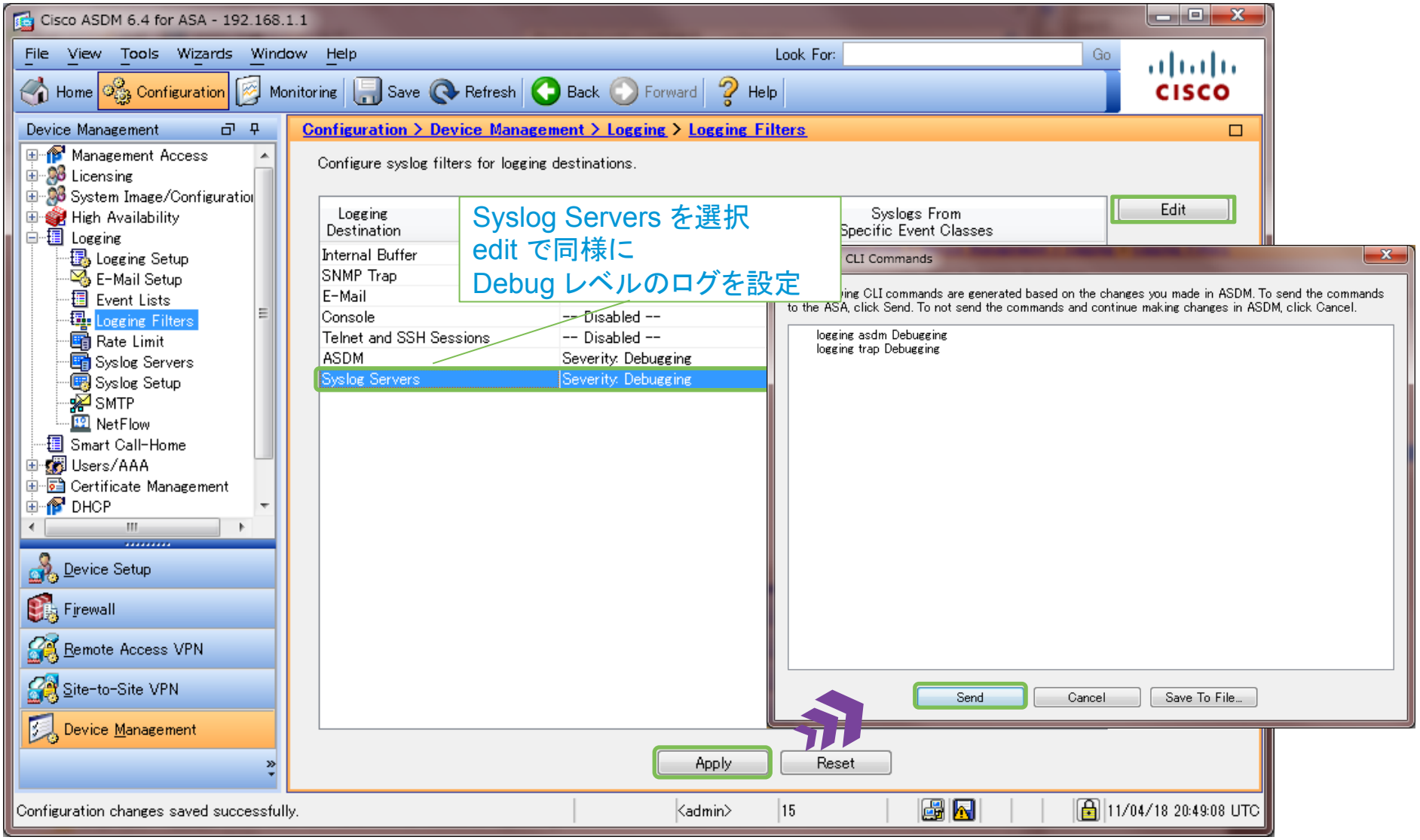
Logging 設定　ログの有効化



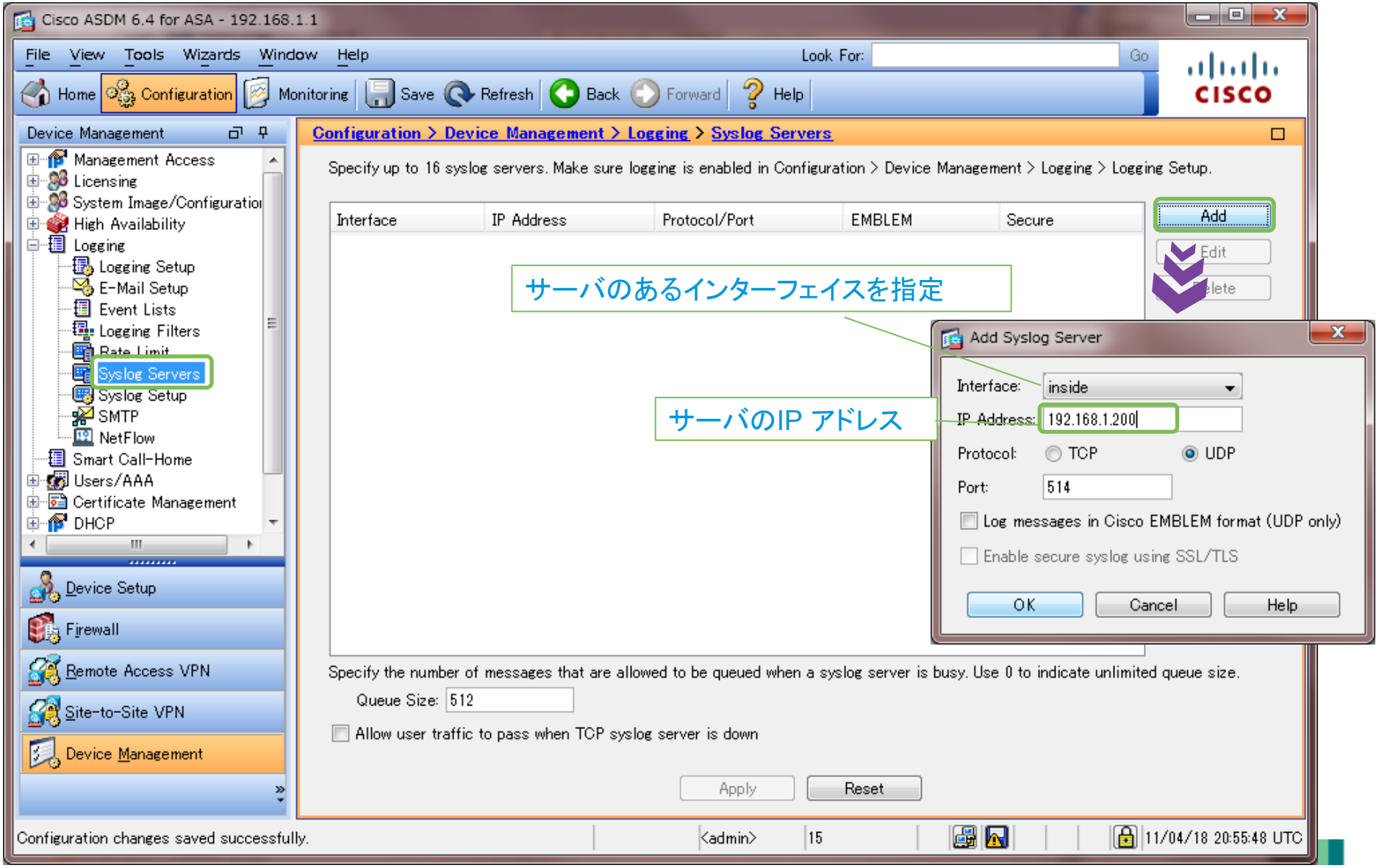
Logging 設定　ログの出力先の設定



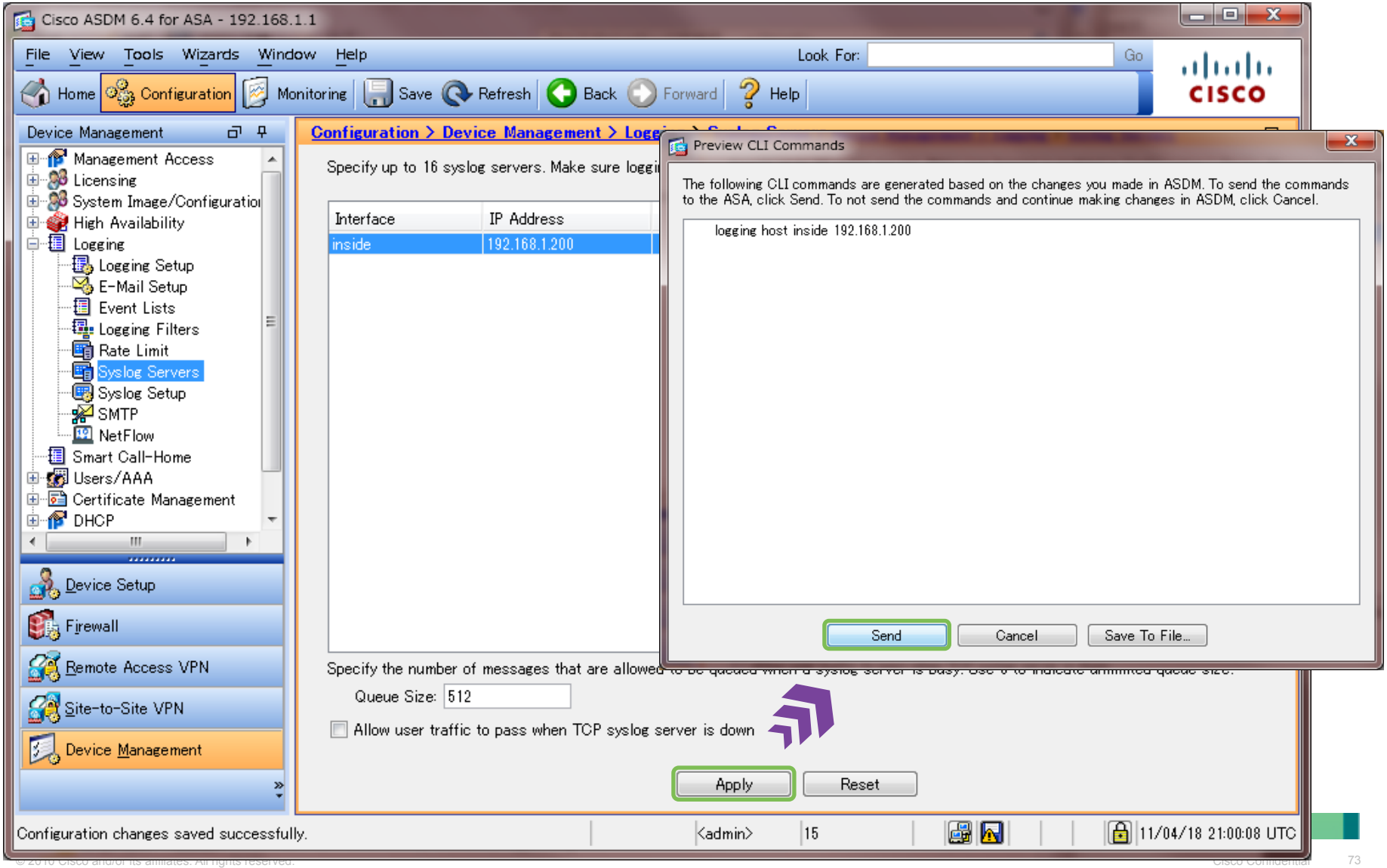
Logging 設定　ログの出力先の設定2



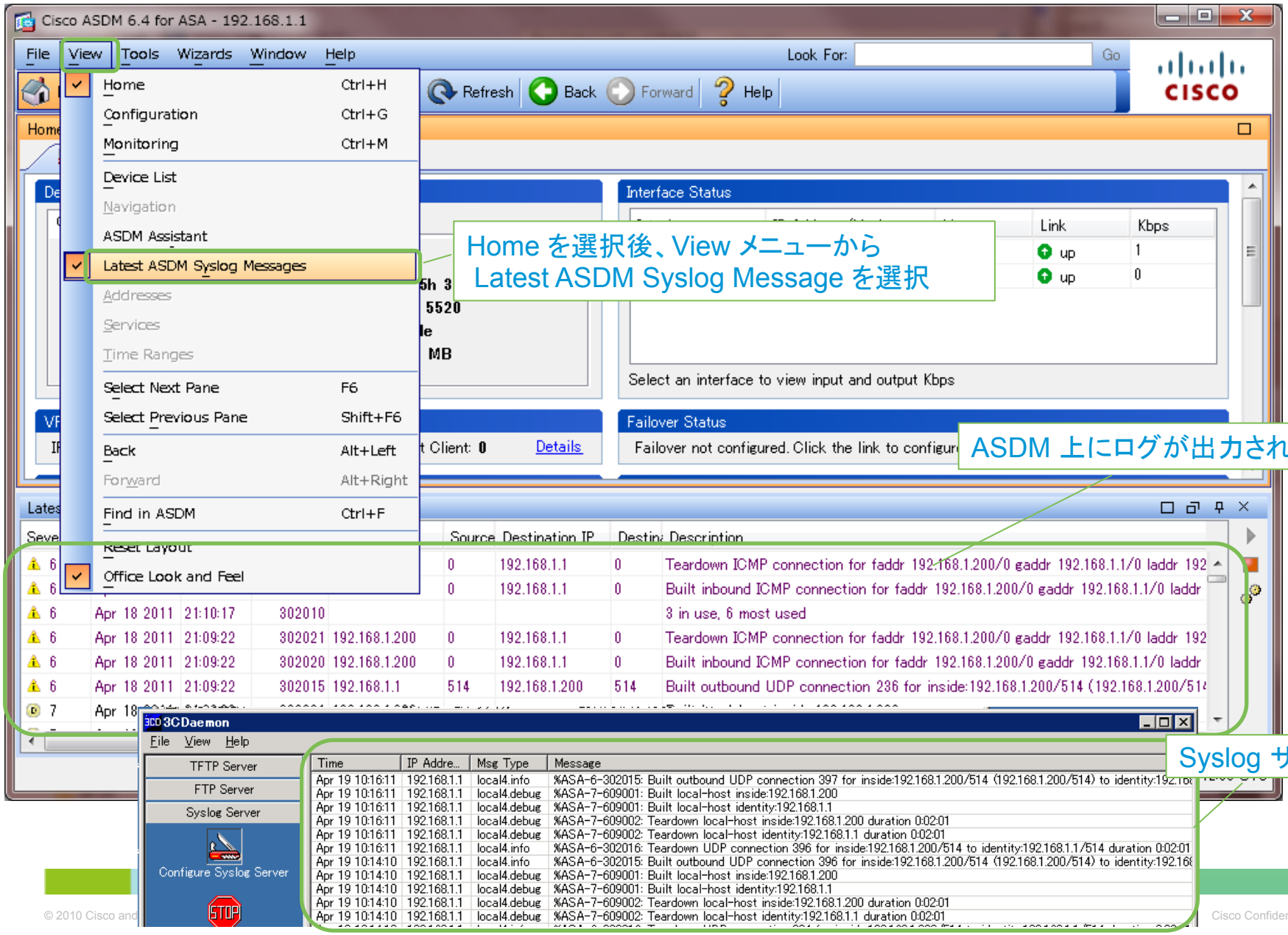
Logging 設定　Syslog サーバの設定



Logging 設定　Syslog サーバの設定　設定の反映



Logging 設定の確認

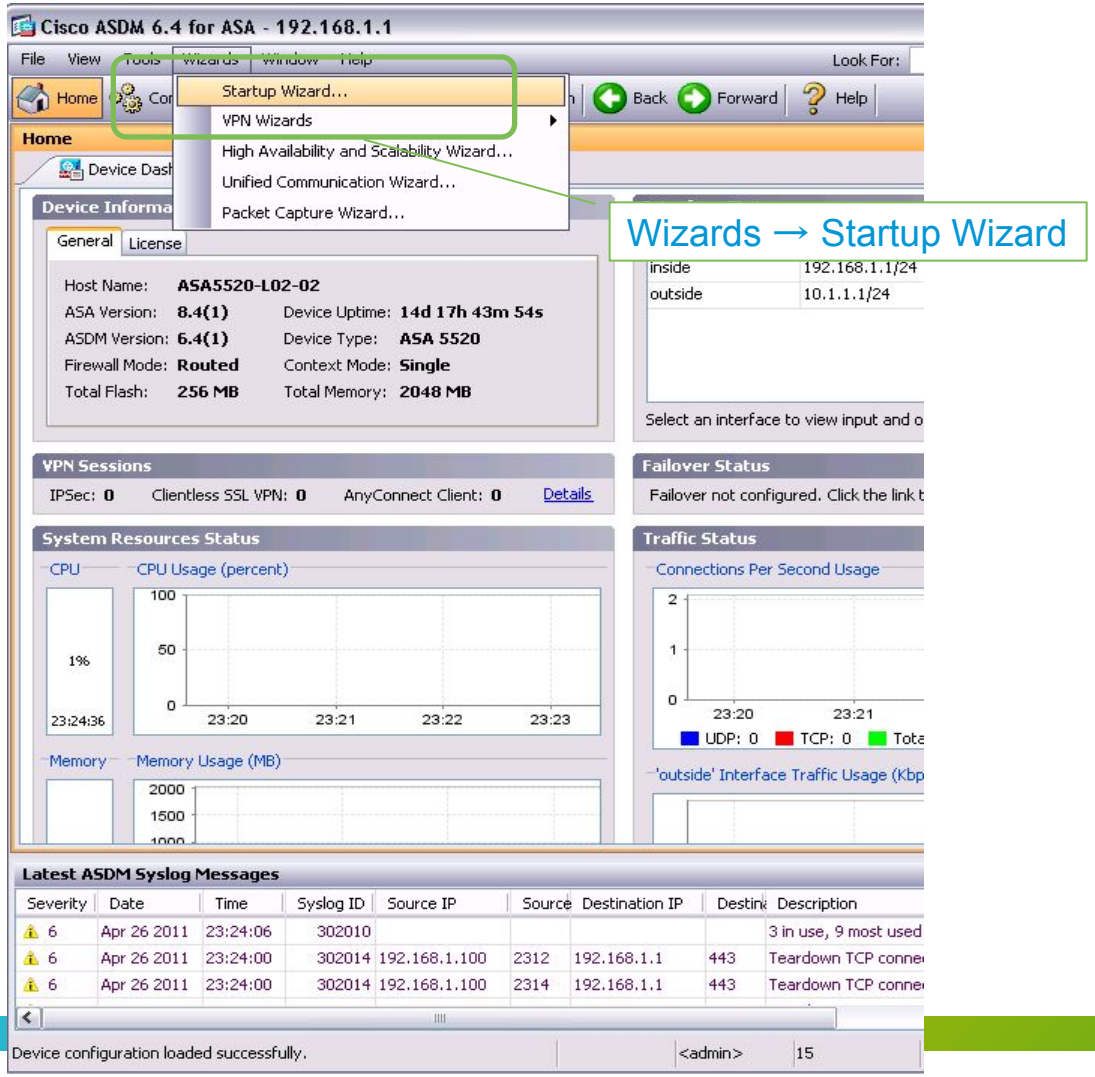


補足資料
ウィザードを使用した設定

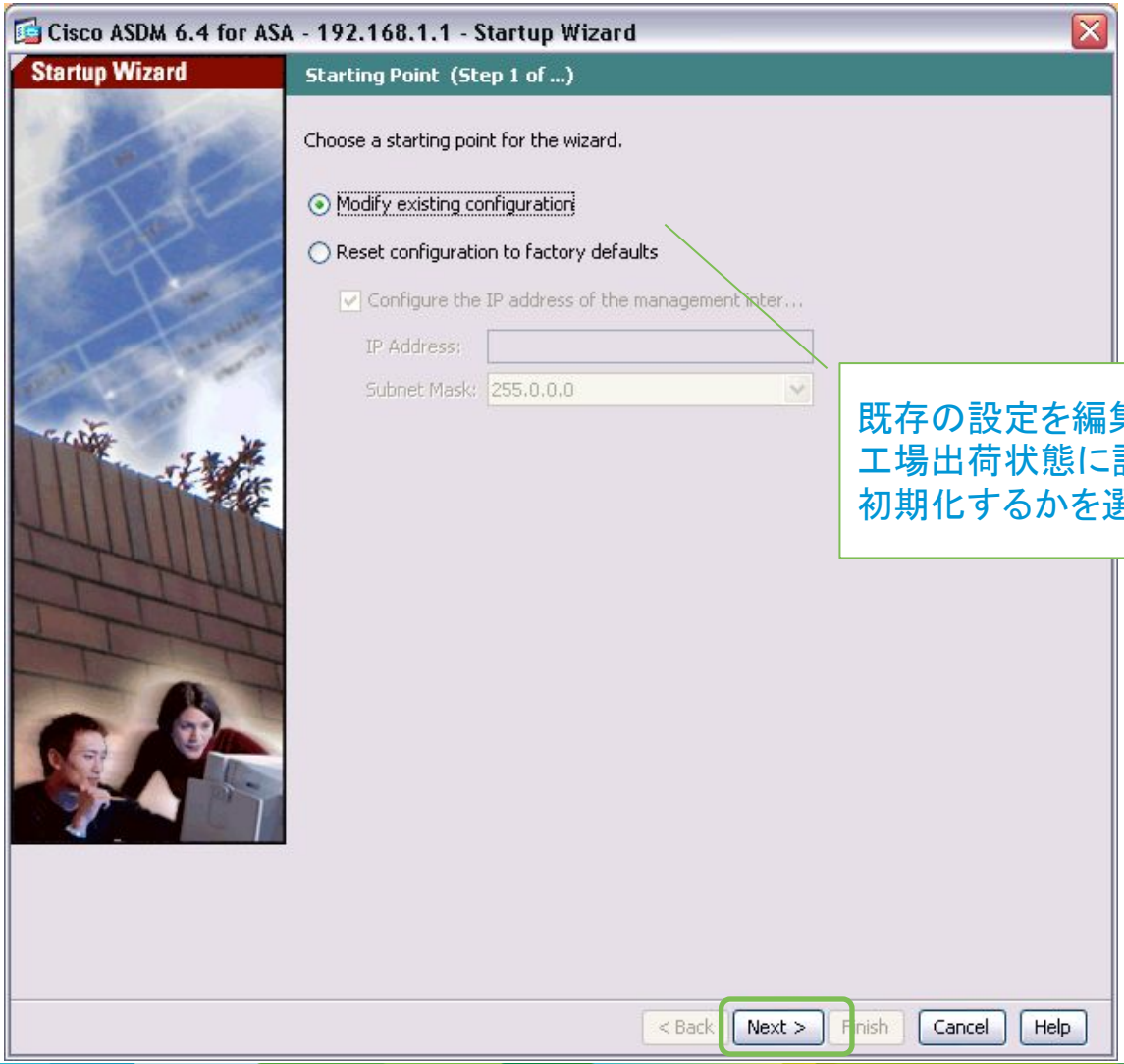
補足資料
ウィザードを使用した設定

ウィザードを使った設定

outside インターフェイスの設定、デフォルトルートの設定、NAT/PAT の設定は Startup Wizard を使用することでまとめて行うことが可能

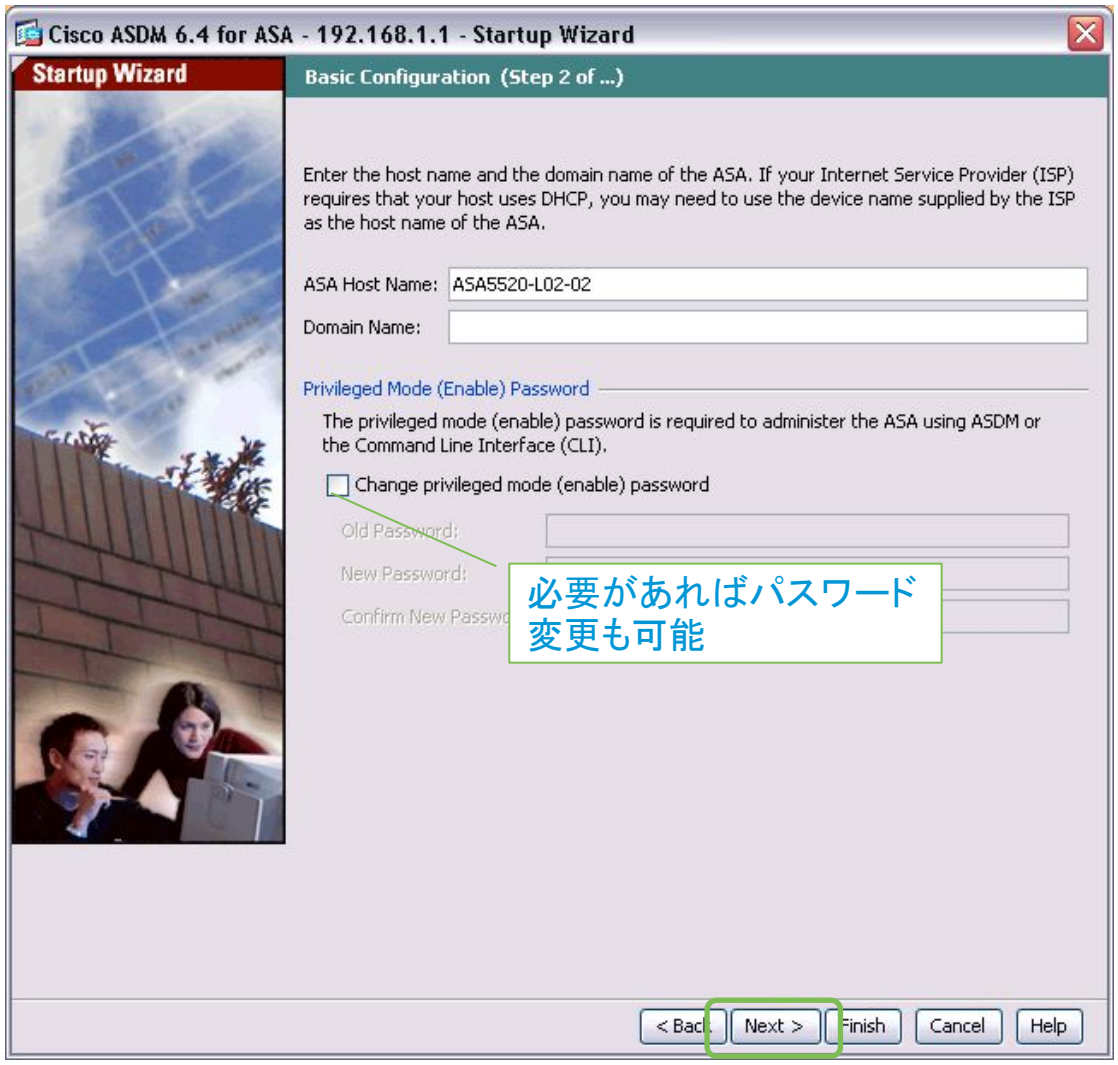


ウィザードを使った設定　ホスト名、ドメイン名

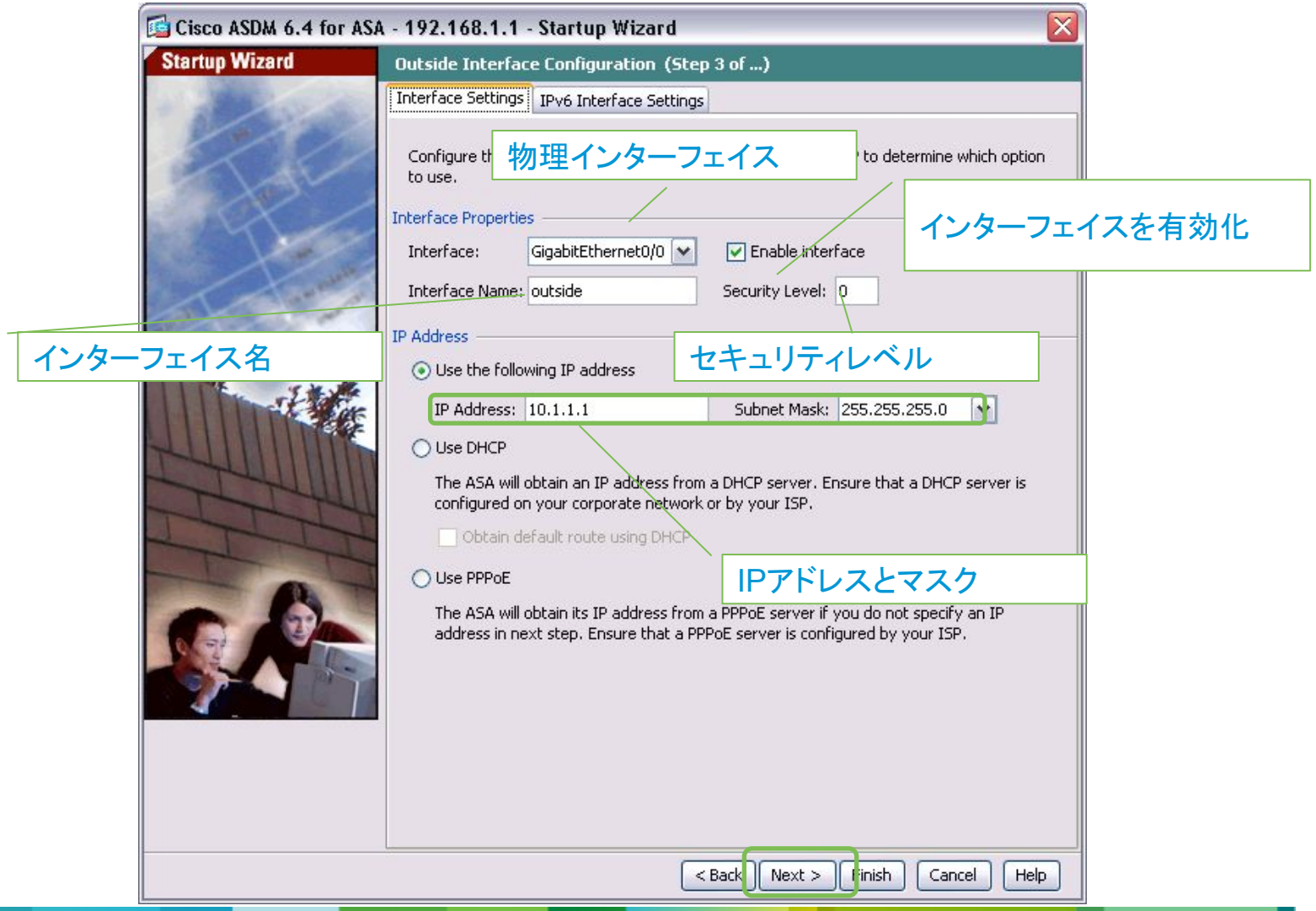


既存の設定を編集するか、
工場出荷状態に設定を
初期化するかを選択可能

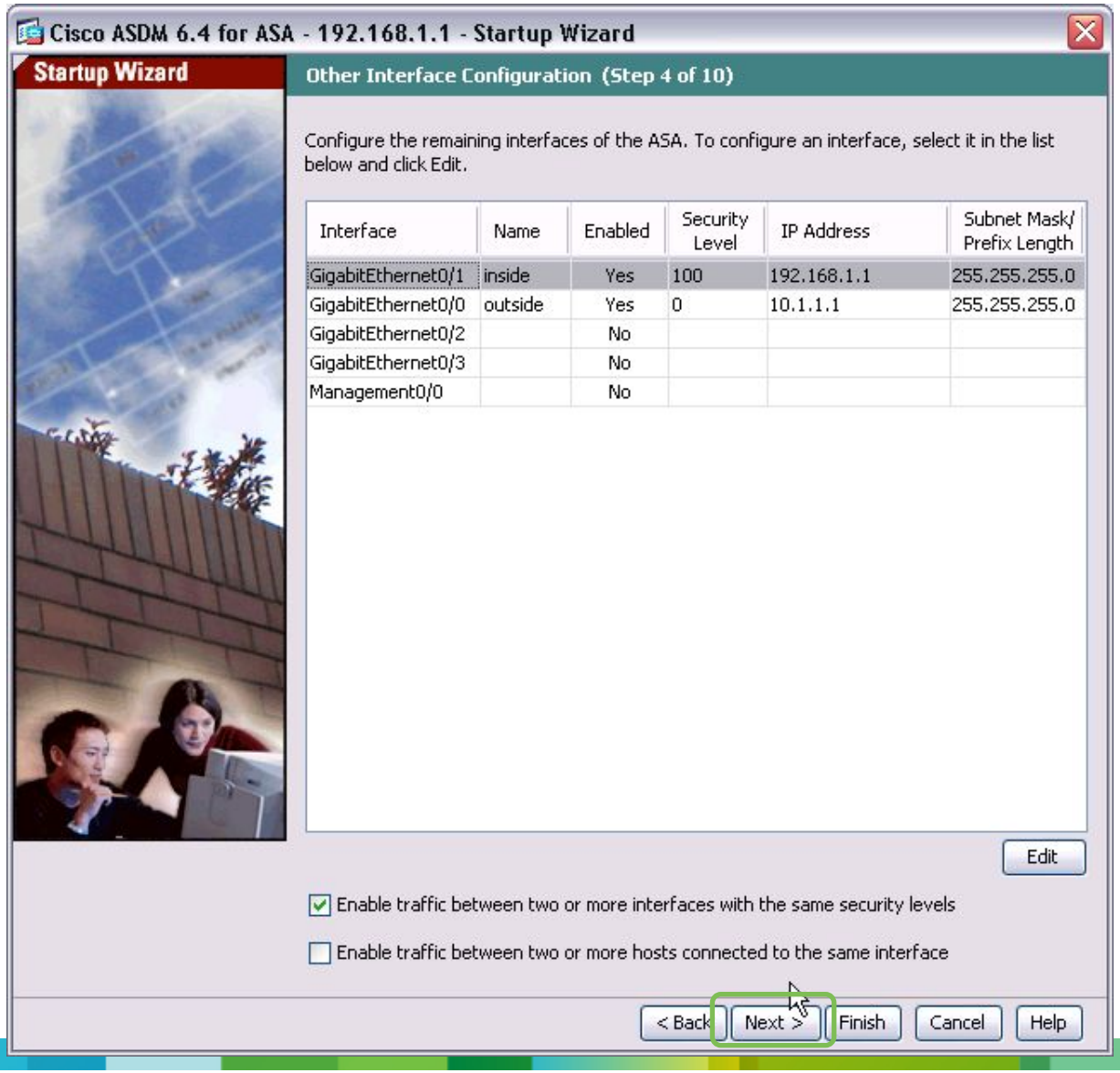
ウィザードを使った設定　ホスト名、ドメイン名



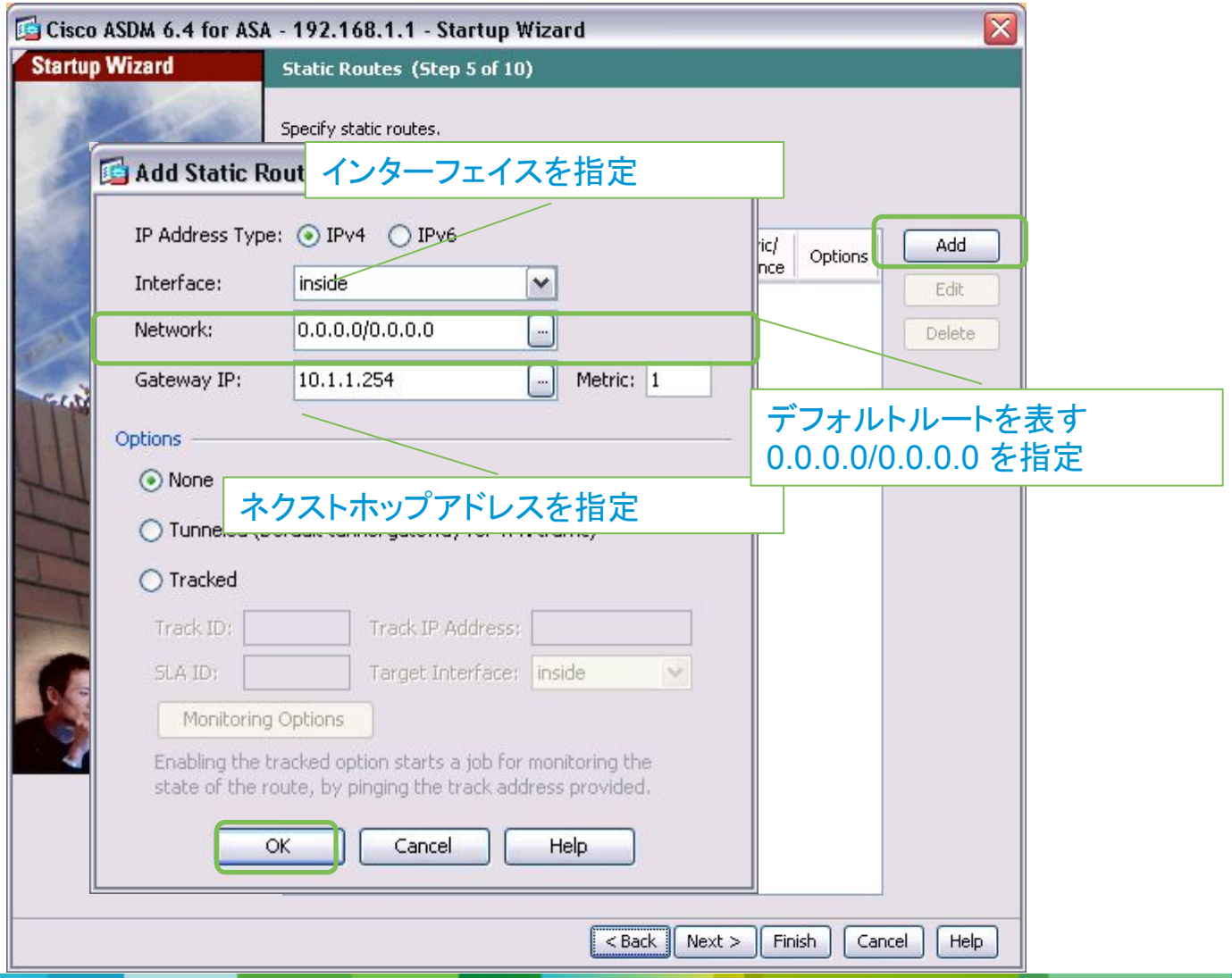
ウィザードを使った設定　自動アップデートの設定



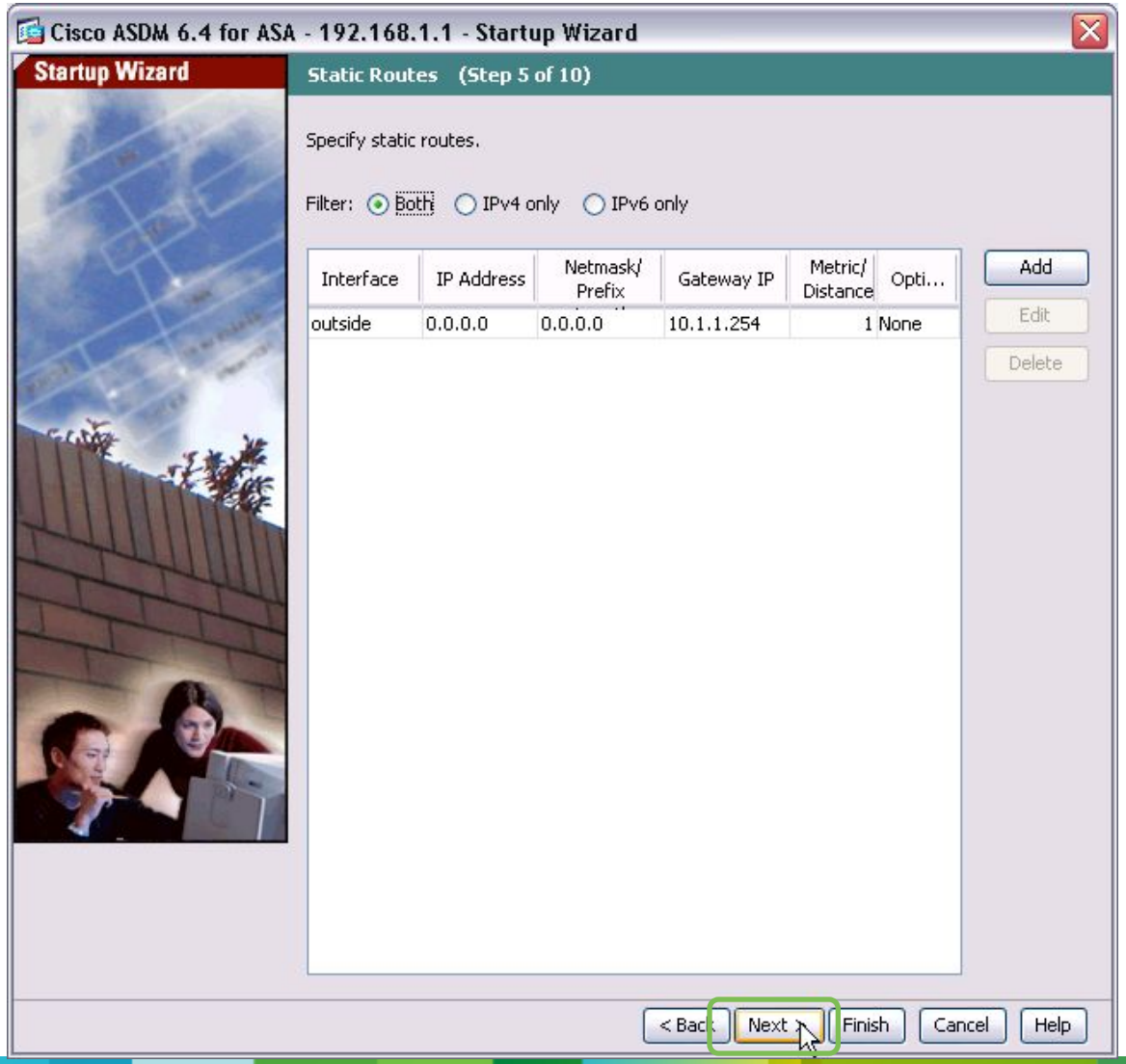
ウィザードを使った設定　その他のインターフェイス設定



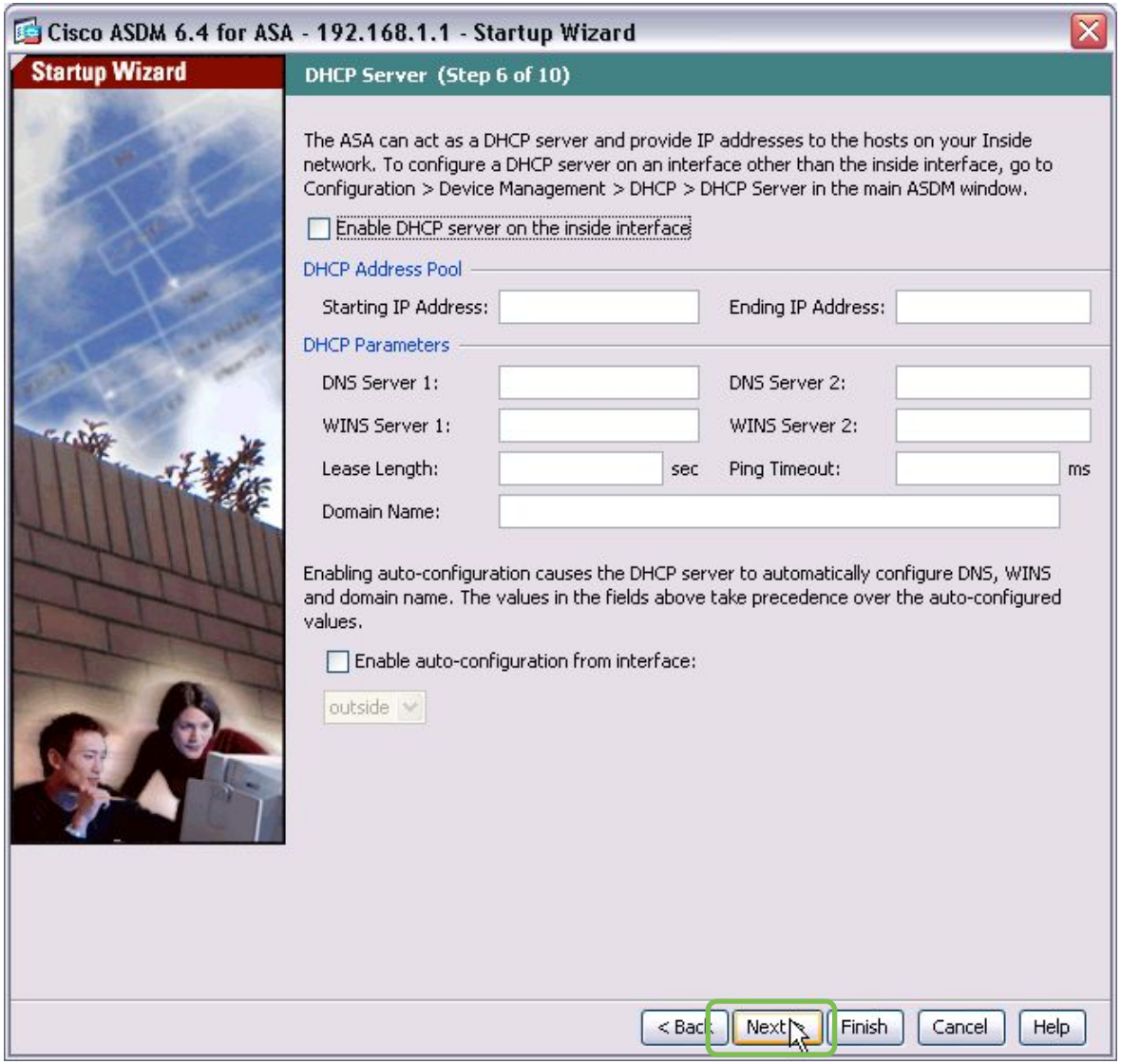
ウィザードを使った設定　スタティックルートの設定



ウィザードを使った設定　スタティックルートの設定

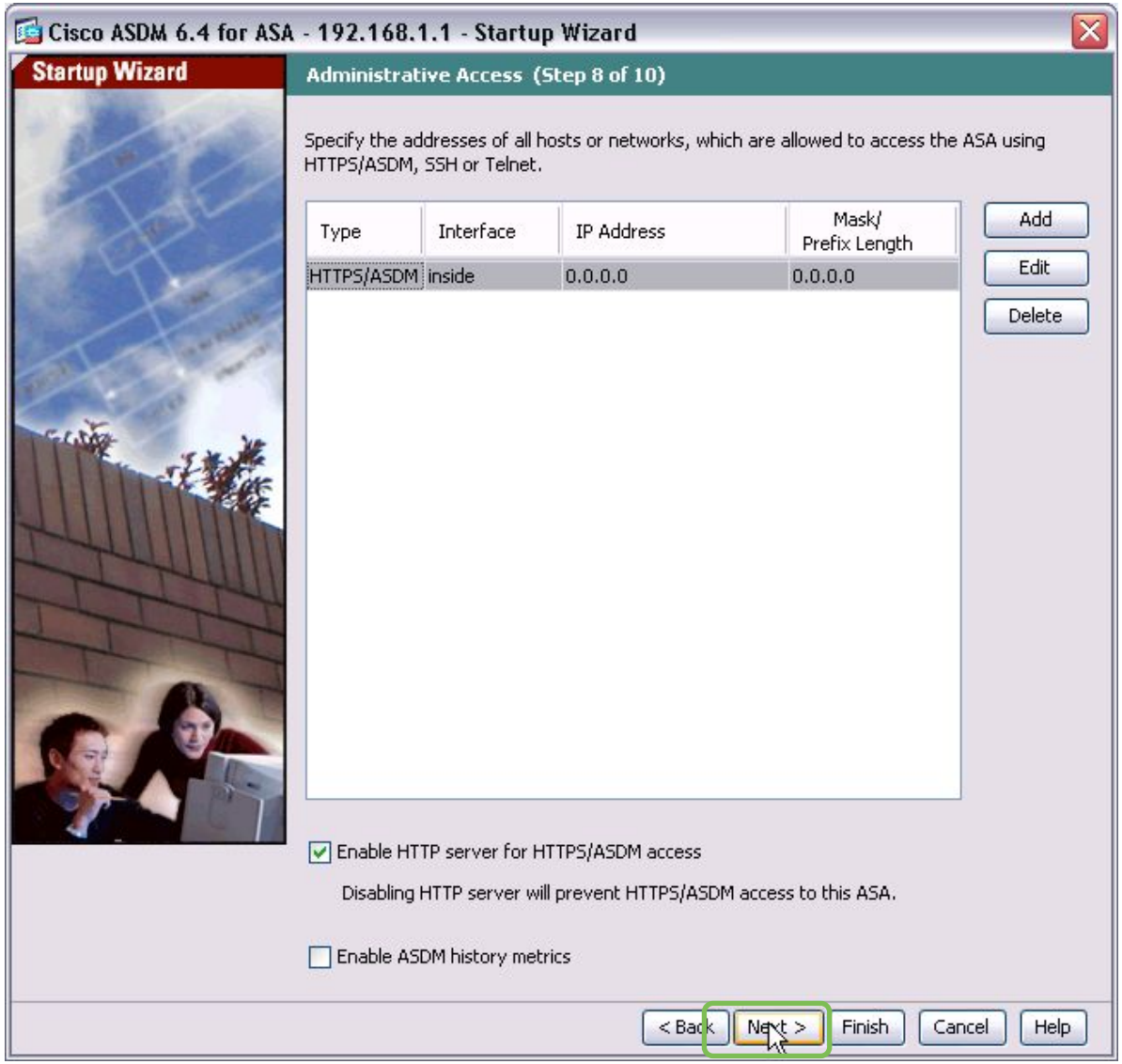


ウィザードを使った設定 DHCP サーバの設定

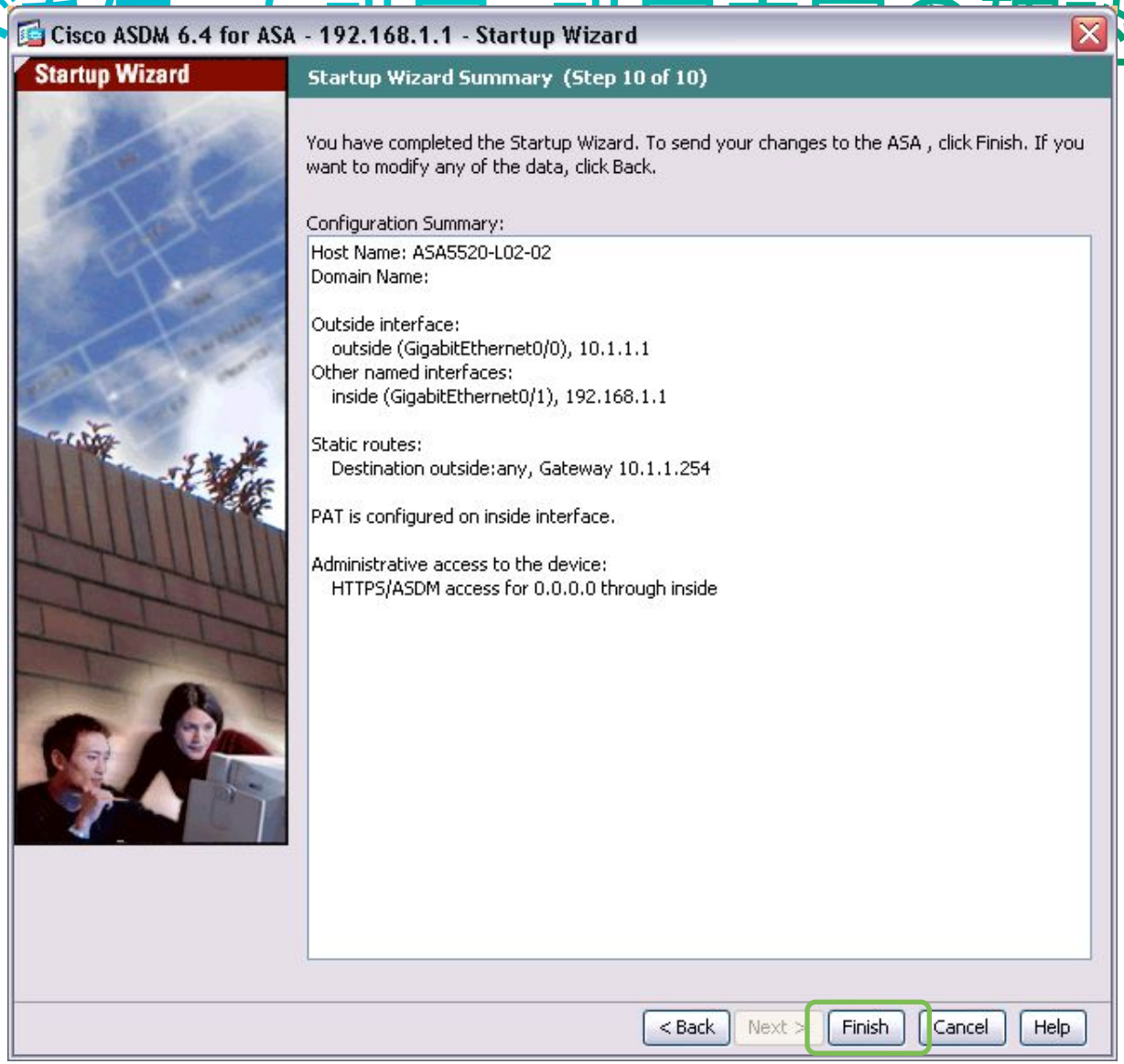


ウィザード

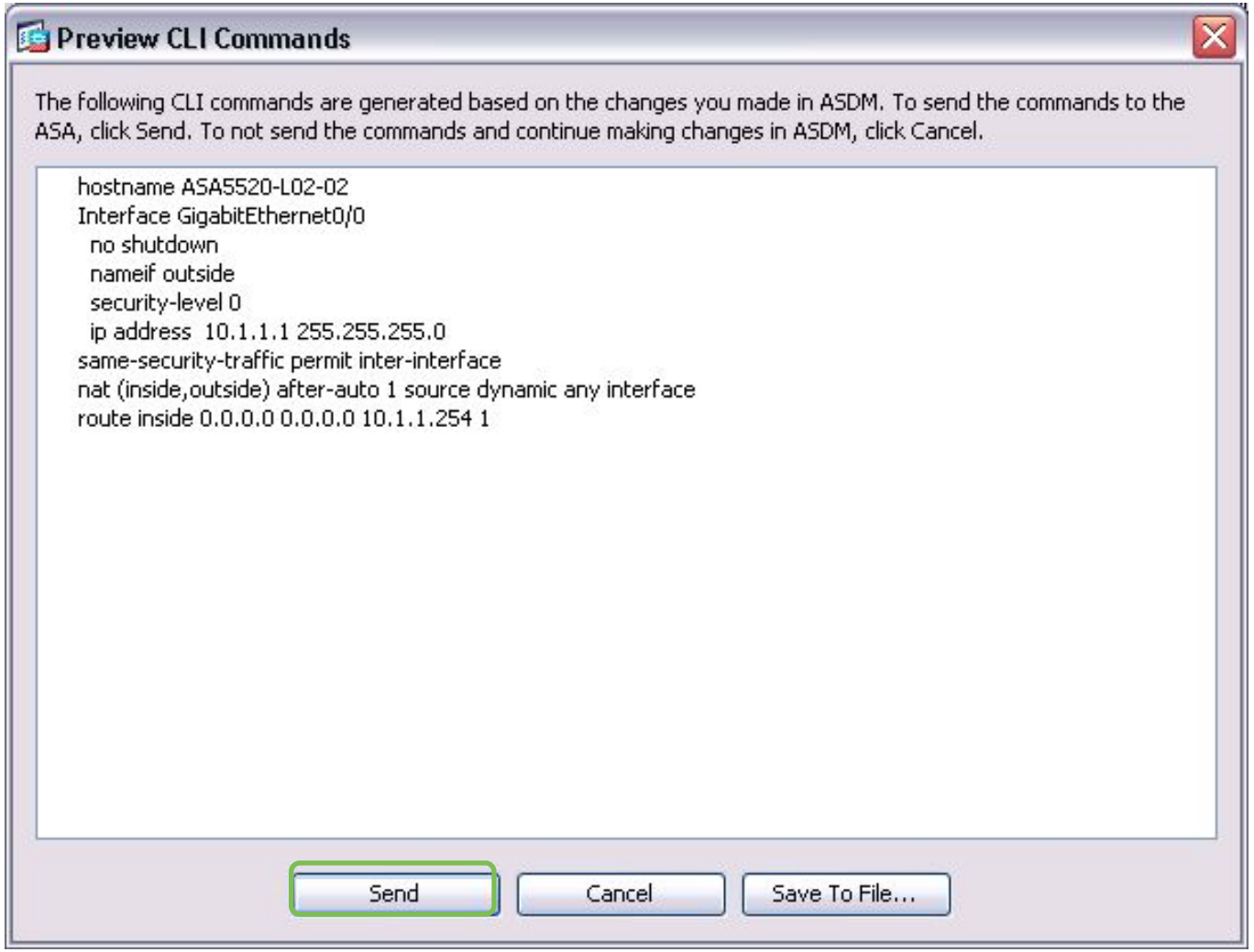
ウィザードを使った設定
ASDM へアクセスする端末の設定



ウィザードを使った設定：設定内容の確認



ウィザードを使った設定　CLI 表示



Thank you.