



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

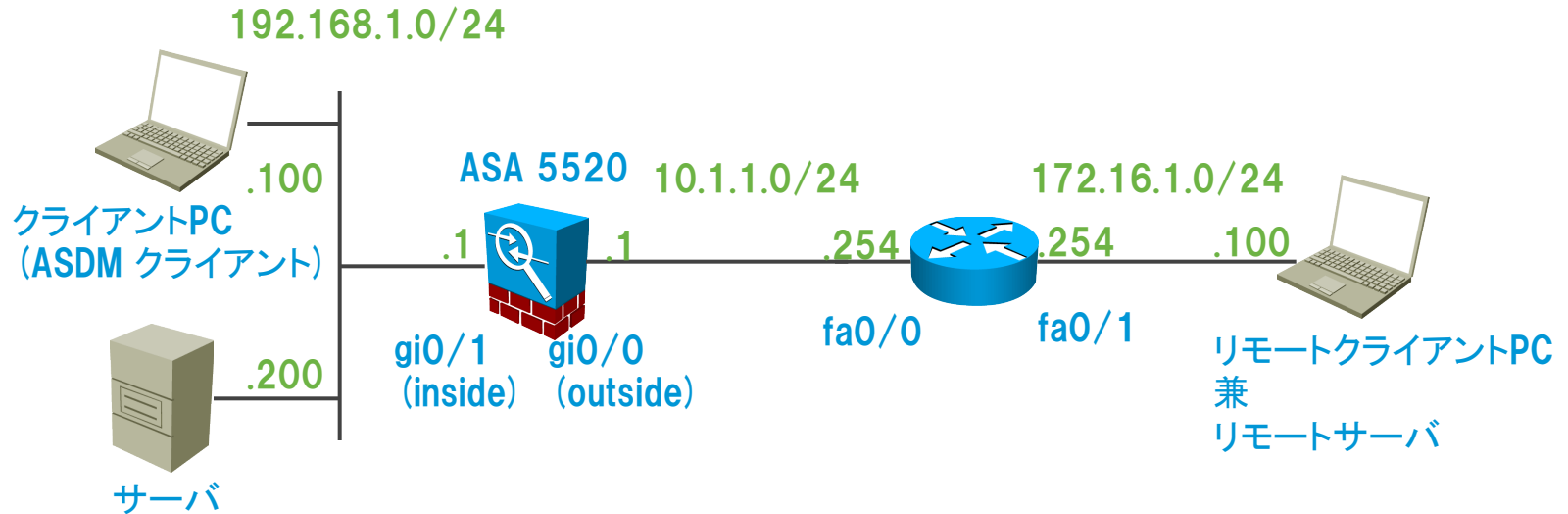
- 本資料ではASA 8.4 におけるファイアウォールの設定を紹介します。

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-if)# 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

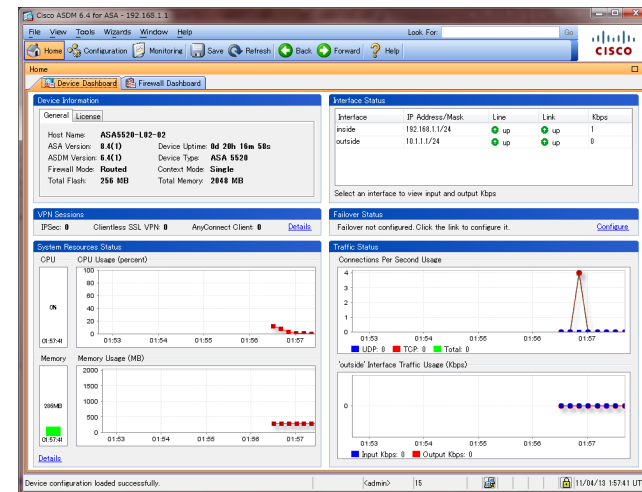
セットアップ
ウィザードを行
わない

ホスト名

192.168.1.1/24

利用する asdm イメージを指定

http/asdm アクセス端末指定



ASDM アクセス画面

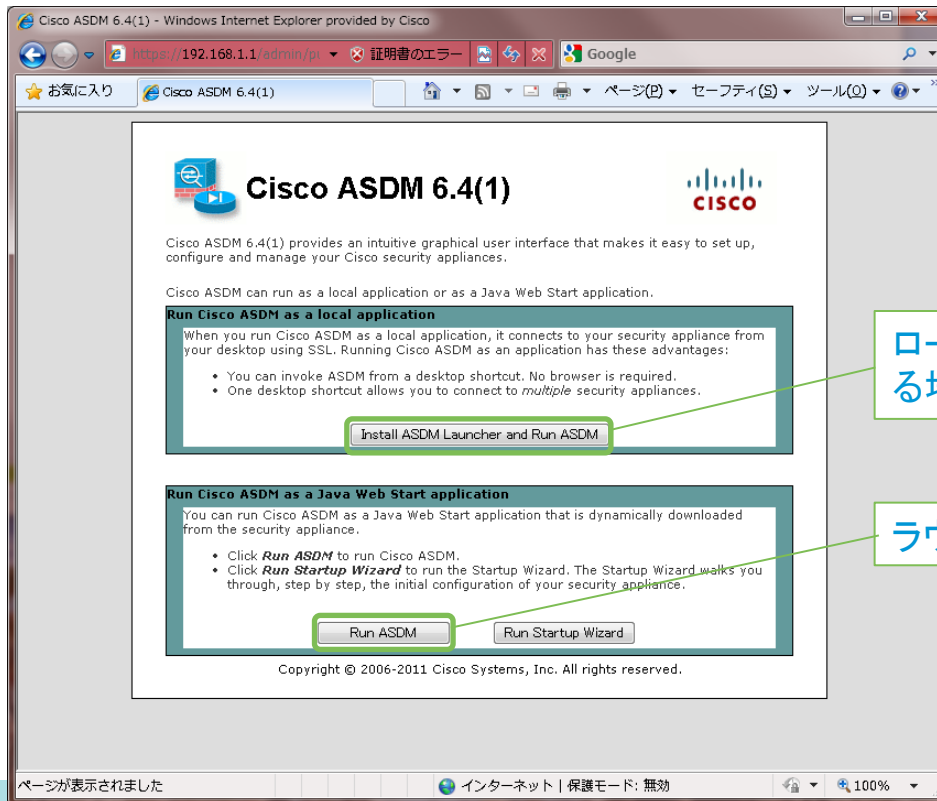
インターフェース g0/1 にinside を割当て

インターフェース有効

http サービス有効

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

The screenshot shows the Cisco ASDM 6.4 for ASA interface. The 'Tools' menu is open, and the 'Preferences...' option is highlighted. The 'Preferences' dialog box is displayed, showing the 'General' tab. The 'Preview commands before sending them to the device' checkbox is checked. A callout box points to this checkbox with the text '設定を送信する前にコマンドを表示させる'.

Interface Status

Interface: inside, outside

Select an interface

Failover Status

Failover not

Tran... Status

Tran... Status

CPU

10%

22:52:57

Memory

196MB

22:52:57

Memory Usage (MB)

500

400

300

200

100

0

22:48 22:49 22:50 22:51 22:52

UDP:

'outside' Inte

Input

Preferences

Indicate your preferences and click OK to activate them. To restore the default settings, click Default, then click OK to save them.

General Rule Tables Syslog

Warn that configuration in ASDM is out of sync with

Show configuration restriction message to read-only

Confirm before exiting ASDM

Warn that Easy VPN is enabled when visiting VPN Section

Enable screen reader support (requires ASDM restart)

Warn user everytime when ASDM loads of memory insufficiency

Communications

Preview commands before sending them to the device

Enable cumulative (batch) CLI delivery

Minimum Configuration Sending Timeout: 60 seconds (default 60)

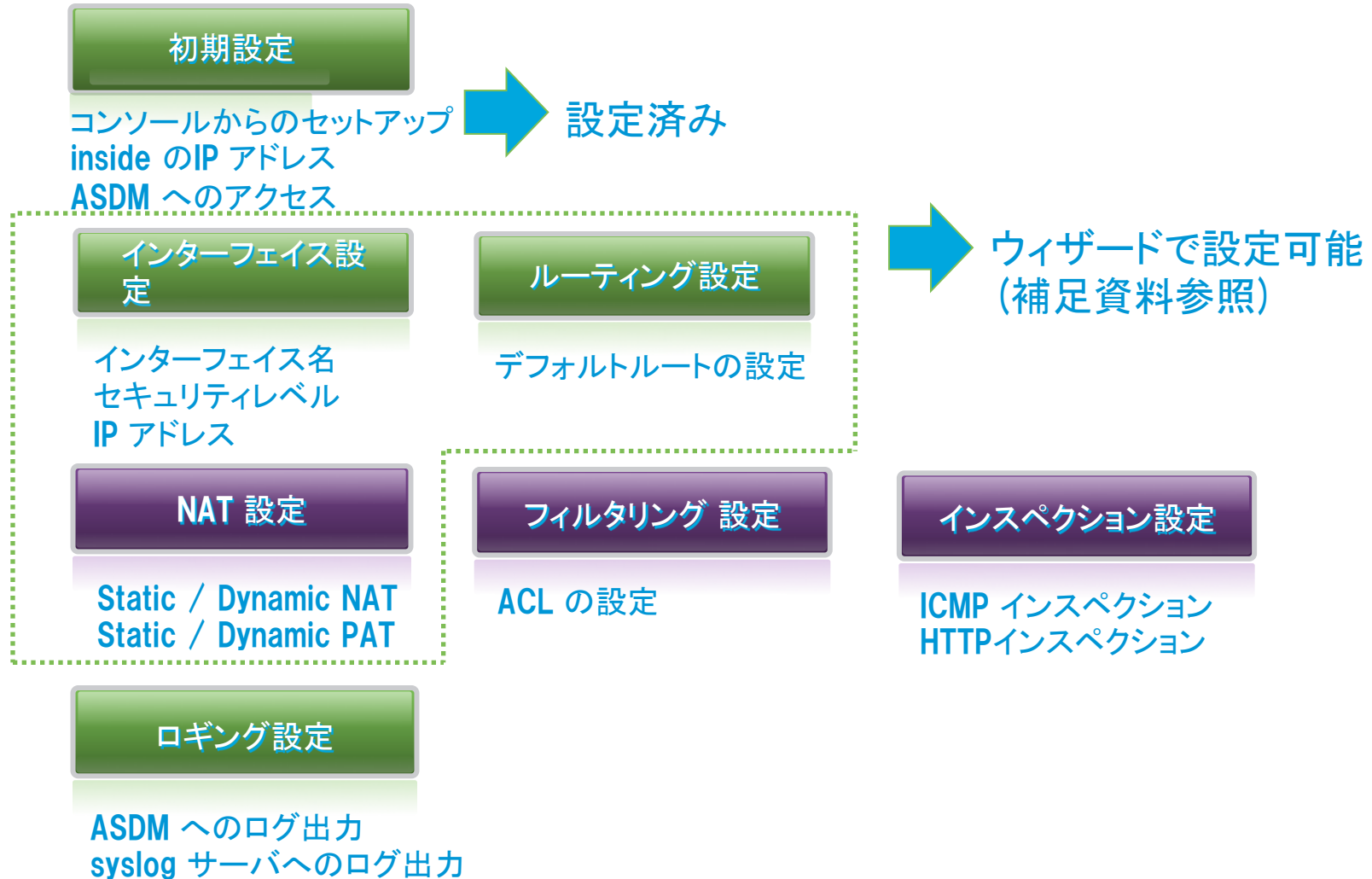
Packet Capture Wizard

Specify the path to your network sniffer application (such as Ethereal/Wireshark) which will be used by the Packet Capture Wizard to display the captured packets. If no path is specified, the default application for pcap files will be used.

Network Sniffer Application: Browse...

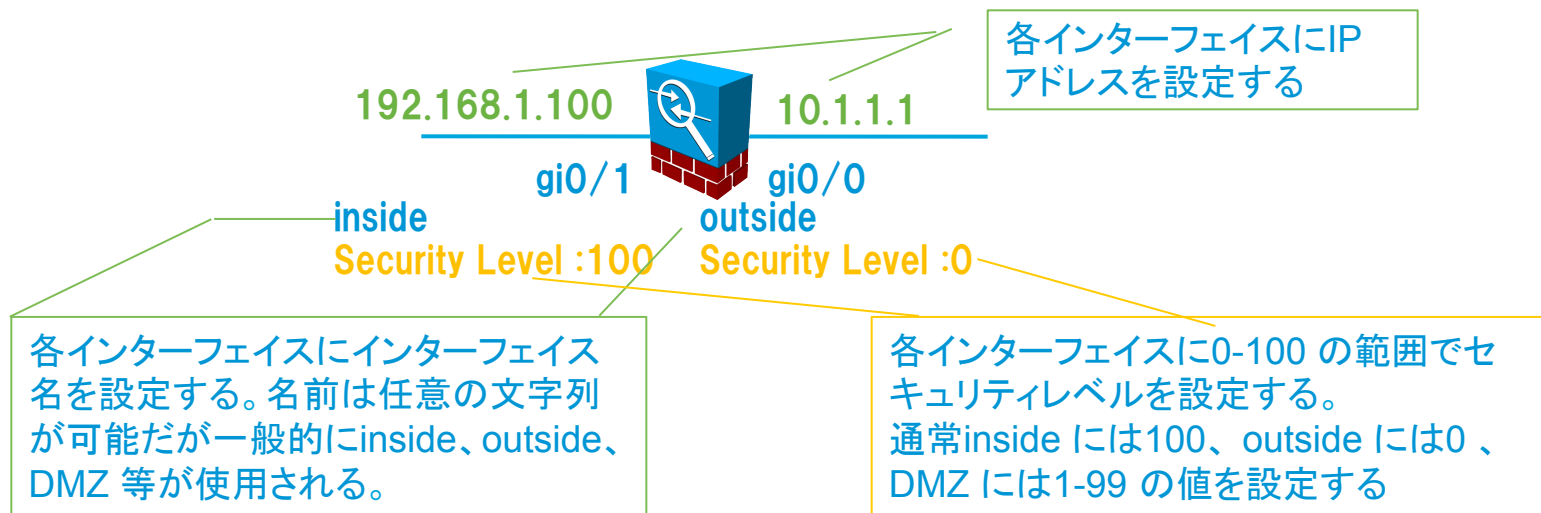
OK Cancel Restore Defaults Help

設定概要



インターフェイスの設定

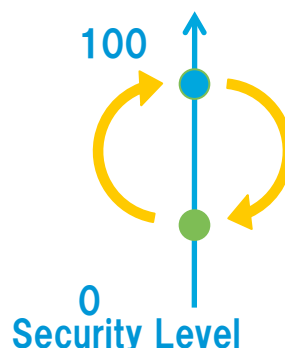
インターフェイス設定概要



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。

The screenshot shows the Cisco ASDM 6.4 for ASA configuration interface. The main window displays the configuration for the interfaces. The table below shows the current configuration:

Interface	Name	State	Security Level	IP Address	Subnet Mask Prefix Length	Group
GigabitEthernet0/0	outside	Enabled	0	10.1.1.1	255.255.255.0	
GigabitEthernet0/1	inside	Enabled	100	192.168.1.1	255.255.255.0	
GigabitEthernet0/2		Disabled				
GigabitEthernet0/3		Disabled				
Management0/0		Disabled				

A callout box with a green border points to the 'GigabitEthernet0/0' row and the 'Edit' button, containing the text: 設定するg0/0 を選択して “Edit”.

At the bottom of the interface configuration window, there are two checkboxes:

- Enable traffic between two or more interfaces which are configured with same security levels
- Enable traffic between two or more hosts connected to the same interface

Buttons for 'Apply' and 'Reset' are located at the bottom of the configuration window.

インターフェイスの設定2

The screenshot displays the 'Edit Interface' configuration window for the 'outside' interface. The 'General' tab is active, showing the following settings:

- Hardware Port: GigabitEthernet0/0
- Interface Name: outside
- Security Level: 0
- Dedicate this interface to management only
- Channel Group: (empty)
- Enable Interface
- IP Address: Use Static IP (selected), Obtain Address via DHCP, Use PPPoE
- IP Address: 10.1.1.1
- Subnet Mask: 255.255.255.0
- Description: (empty)

Callouts and annotations:

- インターフェイス名:outside
セキュリティレベル:0
に設定
- インターフェイスをupさせる
- IPアドレス、マスクの指定
- セキュリティレベルの変更
する旨の警告

A 'Security Level Change' warning dialog is displayed, stating: "Changing the security level of an interface may cause your ASA configuration to become invalid, causing the ASA to drop legal traffic or allow illegal traffic to pass through. Do you still wish to proceed?" with 'OK' and 'Cancel' buttons.

インターフェイスの設定3 設定の反映

The screenshot displays the Cisco ASDM 6.4 for ASA interface configuration page. The main window shows the configuration for interfaces, with a table listing GigabitEthernet0/0 (outside), GigabitEthernet0/1 (inside), GigabitEthernet0/2, GigabitEthernet0/3, and Management0/0. A 'Preview CLI Commands' dialog box is open, showing the generated CLI commands for the selected interface: 'Interface GigabitEthernet0/0', 'no ip address', 'security-level 0', and 'ip address 10.1.1.1 255.255.255.0'. The 'Send' button is highlighted, and a text box indicates that the commands are sent to the ASA. Another text box points to the 'Apply' button, stating that it is used to reflect settings on the ASA. A third text box points to the 'Send' button, stating that settings are reflected after clicking 'Send'.

Interface	Name	State	Security Level	IP Address	Subnet Mask Prefix Length	Group
GigabitEthernet0/0	outside					
GigabitEthernet0/1	inside					
GigabitEthernet0/2						
GigabitEthernet0/3						
Management0/0						

```
Interface GigabitEthernet0/0
no ip address
security-level 0
ip address 10.1.1.1 255.255.255.0
```

ASA に設定を反映させるために“Apply”

ASA に送り込むコマンドが表示される

“Send” をして初めて設定が反映される

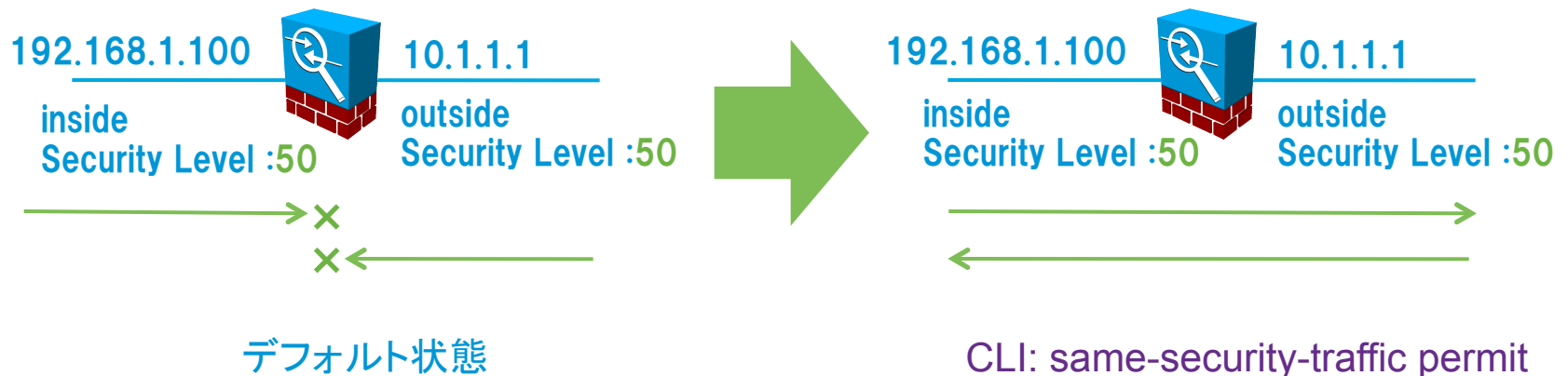
同一セキュリティレベルのインターフェイス間の通信

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



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

The screenshot shows the Cisco ASDM 6.4 for ASA interface configuration page. The left sidebar shows the navigation tree with 'Interfaces' selected. The main content area displays a table of interfaces and their configurations. Below the table, there are two checkboxes for enabling traffic between interfaces with the same security levels. A green box highlights the first checkbox, which is checked.

Interface	Name	State	Security Level	IP Address	Subnet Mask Prefix Length	Group
GigabitEthernet0/0	outside	Enabled	0	10.1.1.1	255.255.255.0	
GigabitEthernet0/1	inside	Enabled	100	192.168.1.1	255.255.255.0	
GigabitEthernet0/2		Disabled				
GigabitEthernet0/3		Disabled				
Management0/0		Disabled				

Configuration > Device Setup > Interfaces

Device Setup

- Startup Wizard
- Interfaces
- Routing
- Device Name/Password
- System Time
- EtherChannel

Device Setup

- Firewall
- Remote Access VPN
- Site-to-Site VPN
- Device Management

Enable traffic between two or more interfaces which are configured with same security levels

Enable traffic between two or more hosts connected to the same interface

Apply Reset

Device configuration loaded successfully.

<admin> 15 11/04/13 2:18:31 UTC

ルーティングの設定

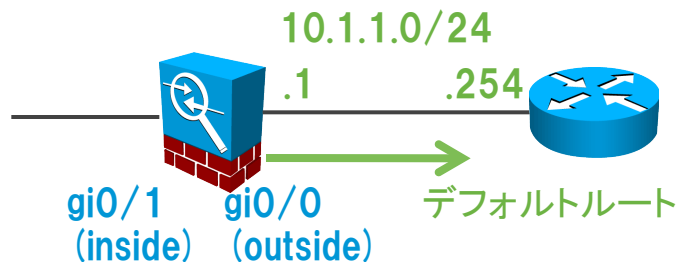
ルーティングの設定概要

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

The screenshot shows the Cisco ASDM 6.4 for ASA configuration interface. The main window displays the 'Configure' page for static routes. The left sidebar shows the 'Device Setup' tree with 'Static Routes' selected. The main area has a table for specifying static routes with columns for 'Interface', 'IP Address', and 'Options'. A callout box points to the 'Static Routes' item in the tree with the text 'スタティックルートの項目を選択'. Another callout points to the 'Interface' column with 'インターフェイスを指定'. A third callout points to the 'Network' field in the 'Edit Static Route' dialog, which is set to '0.0.0.0/0.0.0.0', with the text 'デフォルトルートを表す 0.0.0.0/0.0.0.0 を指定'. A fourth callout points to the 'Browse Network' dialog, which shows a list of network objects, with 'any' selected, and the text 'もしくは Browse ボタンから any を選択'. A fifth callout points to the 'Gateway IP' field in the dialog, which is set to '10.1.1.254', with the text 'ネクストホップアドレスを指定'. The 'Browse Network' dialog table is as follows:

Name	IP Address	Netmask	Description
IPv4 Network Objects			
any	0.0.0.0	0.0.0.0	
inside-n...	192.168.1.0	255.255.255.0	
outside-...	10.1.1.0	255.255.255.0	

At the bottom of the 'Edit Static Route' dialog, there are 'OK', 'Cancel', and 'Help' buttons. The status bar at the bottom of the window shows 'Device configuration loaded successfully.', the user 'admin', page number '15', and the date/time '11/04/03 23:30:17 UTC'.

デフォルトルートの設定2 設定の反映

The screenshot shows the Cisco ASDM 6.4 for ASA interface. The main window displays the configuration for a static route on the 'outside' interface. The table below shows the configuration details:

Interface	IP Address	Netmask/Prefix Length	Gateway IP	Metric/Distance	Options
outside	0.0.0.0	0.0.0.0	10.1.1.254	1	

A 'Preview CLI Commands' dialog box is open, showing the generated CLI command: `route outside 0.0.0.0 0.0.0.0 10.1.1.254 1`. The 'Send' button is highlighted with a green box. A blue callout box with the text 'ASA に設定を反映させるために“Apply”' points to the 'Apply' button in the main configuration window.

Device configuration loaded successfully. | <admin> | 15 | 11/04/03 23:40:17 UTC

ルーティング設定の確認

Monitoring > Routing > Routes

Each row represents one route. AD is the administrative distance.

Filter: Both IPv4 only IPv6 only

Protocol	Type	Destination IP	Netmask/ Prefix Length	Gateway	Interface	[AD/Metric]
CONNECTED		10.1.1.0	255.255.255.0		outside	
CONNECTED		192.168.1.0	255.255.255.0		inside	
STATIC	DEFAULT	0.0.0.0	0.0.0.0	10.1.1.254	outside	[1/0]

デフォルトルートが設定されていることを確認

Refresh

Last Updated: 11/04/13 12:37:28

Data Refreshed Successfully. <admin> 15 11/04/13 2:20:41 UTC

NATの設定

NATの種類

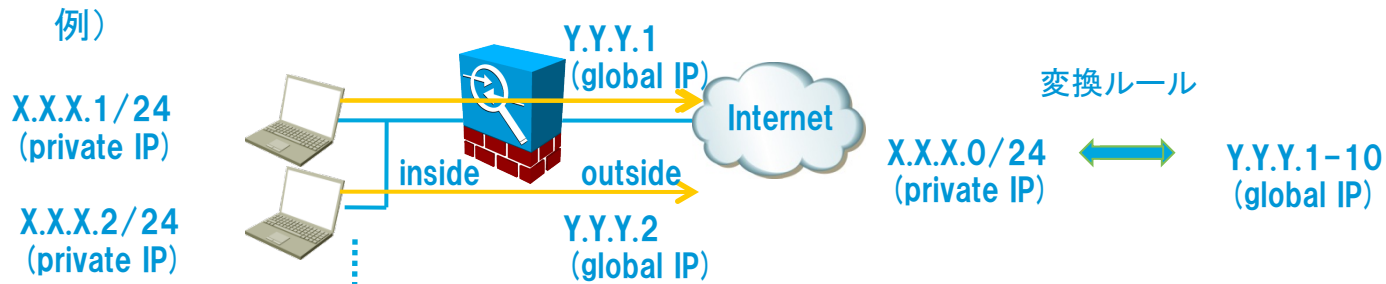
static NAT

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



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



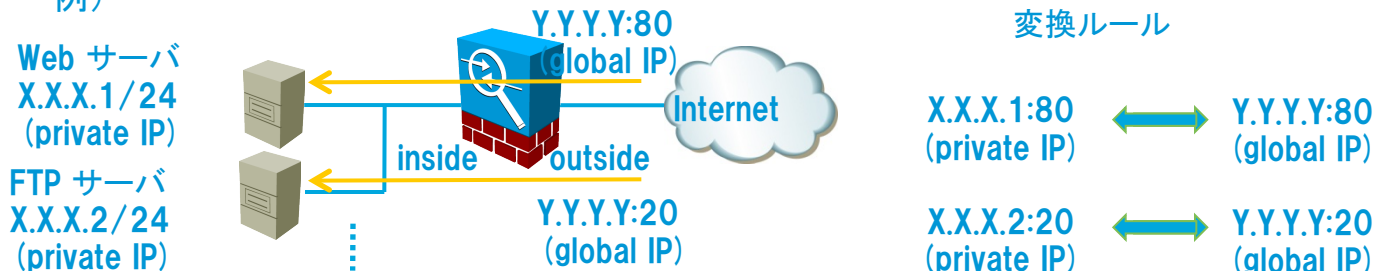
NATの種類 Cont.

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)

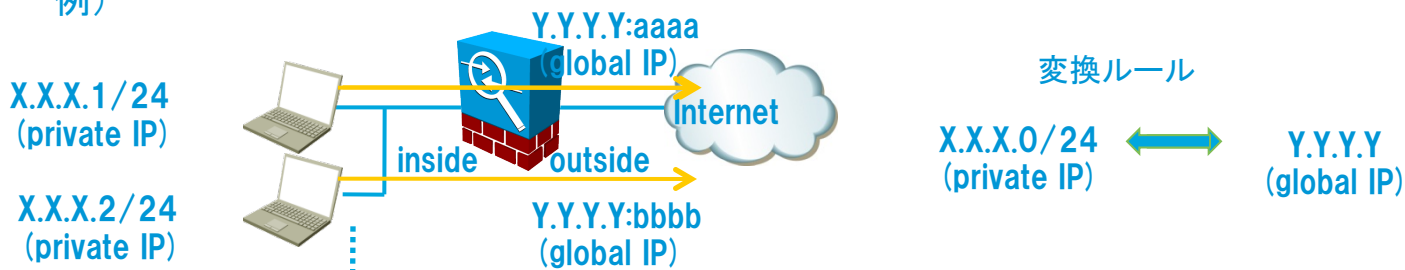


dynamic PAT

IPアドレス+ポート番号を動的にマッピング

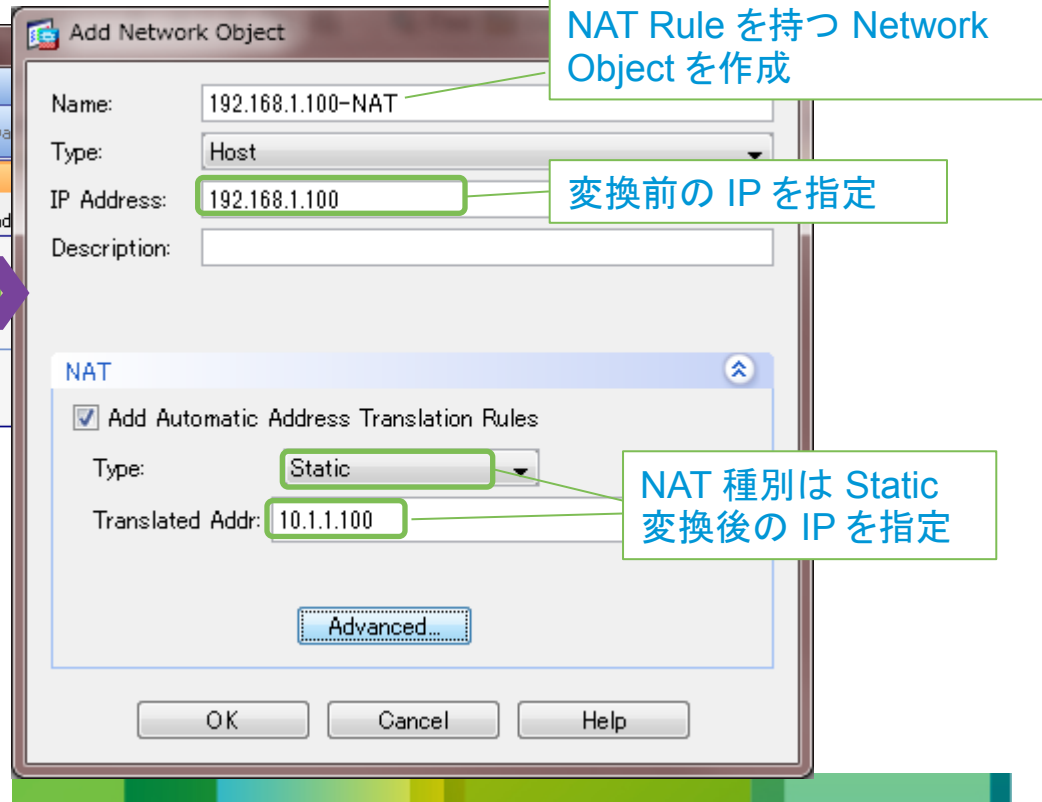
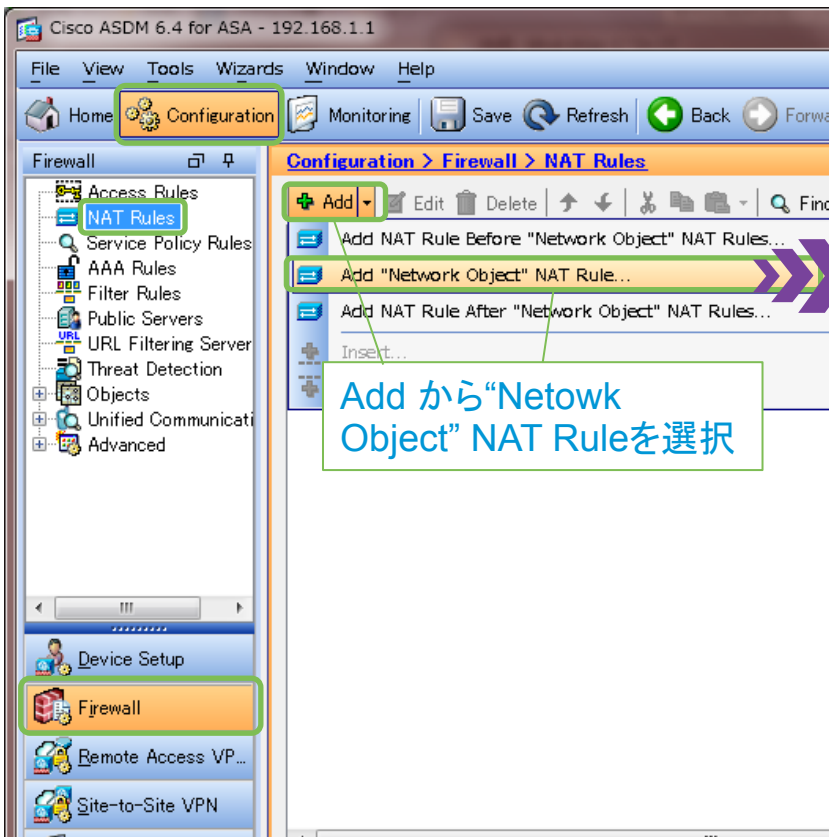
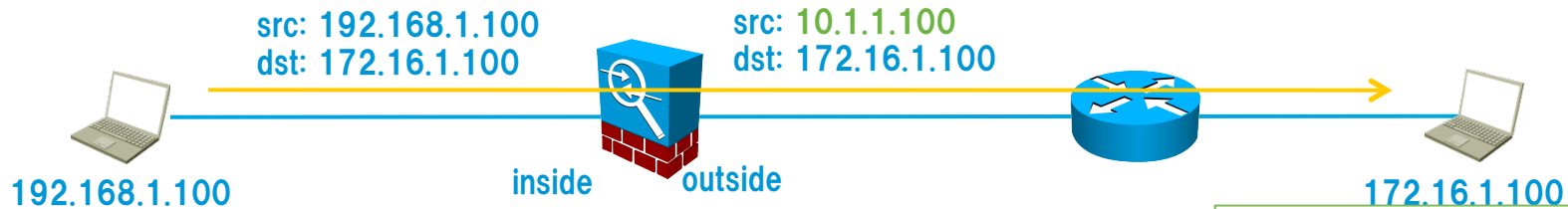
複数のホストに対して、一つのGlobal IP を動的にマッピングする場合等に使用

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

The screenshot illustrates the configuration of Static NAT in Cisco ASDM. It features three main dialog boxes:

- Add Network Object:** Name: 192.168.1.100-NAT, Type: Host, IP Address: 192.168.1.100.
- NAT:** Add Automatic Address Translation Rules: checked, Type: Static, Translated Addr: 10.1.1.100.
- Preview CLI Commands:** Shows the generated commands: `object network 192.168.1.100-NAT`, `host 192.168.1.100`, and `nat (any,any) static 10.1.1.100`.

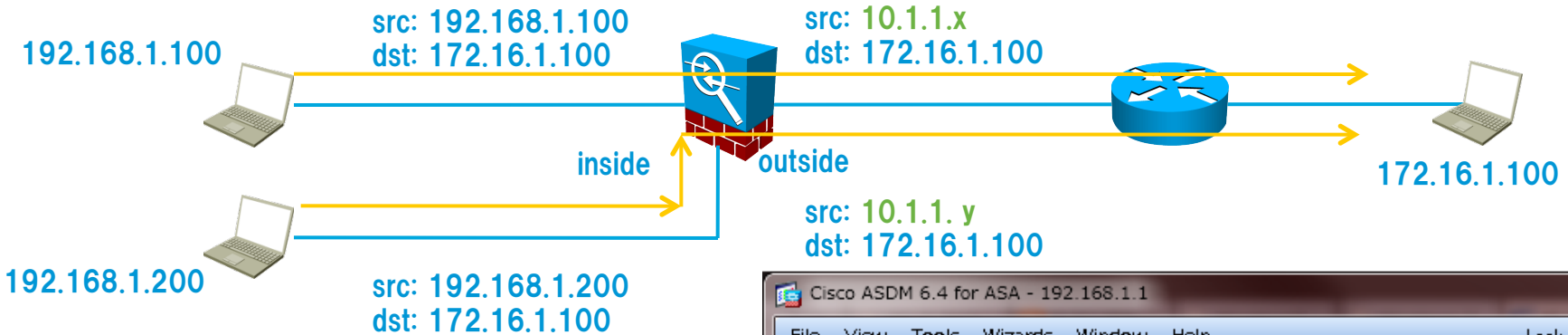
A callout box with the text "NAT 設定を OK 後、設定の反映" (Reflection of NAT settings after OK) points to the "Apply" button at the bottom of the main interface.

Direction	Source	Destination	Object
inside	outside	192.168.1.1-NAT	any
outside	inside	any	10.1.1.100

User cancelled the configuration update operation. | <admin> | 15 | 11/04/25 7:07:36 UTC

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

Add Network Object

Name: 192.168.1.0-254

Type: Network

IP Address: 192.168.1.0

Netmask: 255.255.255.0

Description:

NAT IP ネットワークアドレスの指定

OK Cancel Help

Add NAT Rule

Match Criteria: Original Packet

Source Interface: inside

Destination Interface: -- Any --

Source Address: any

Destination Address: any

Service: any

Action: Translated Packet

Source NAT Type: Dynamic

Source Address: -- Original --

Destination Address: -- Original --

Fall through to interface PAT

Service: -- Original --

Options

Enable rule

Translate DNS replies that match this rule

Direction: Both

Description:

OK Cancel Help

Browse Original Source Address

Network Object...

Network Object Group...	Netmask	Description	Object NAT Add...
IPv4 Network Objects			
any	0.0.0.0	0.0.0.0	

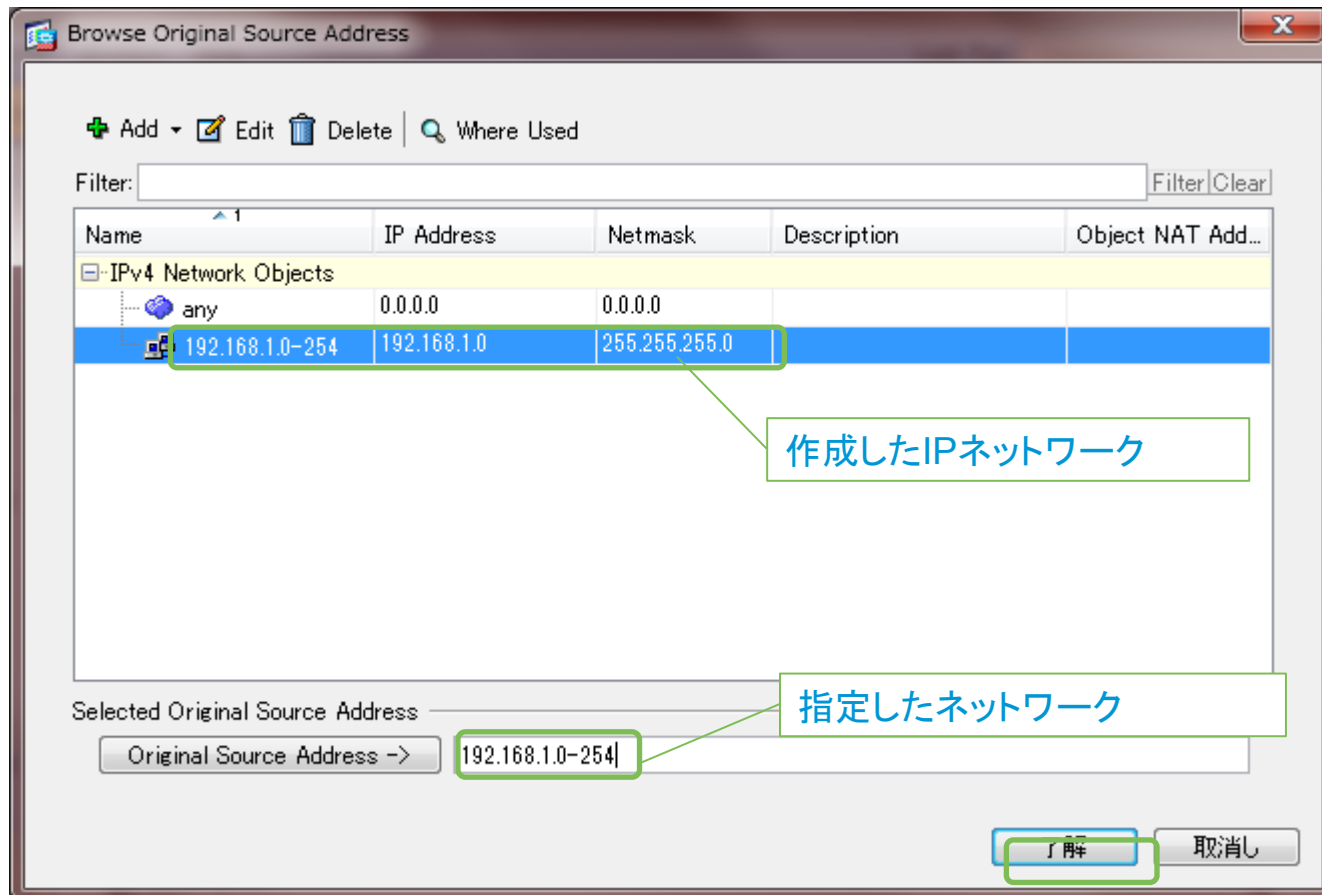
IP ネットワークを新規作成

Selected Original Source Address

Original Source Address -> any

了解 取消し

NAT 設定 Dynamic NAT ネットワーク指定



NAT 設定 Dynamic NAT3

Match Criteria: Original Packet

Source Interface: **inside** Destination Interface: -- Any --

Source Address: 192.168.1.0-254 Destination Address: -- Original --

Action: Translated Packet

Source NAT Type: **Dynamic**

Source Address: -- Original -- Destination Address: -- Original --

Fall through to interface PAT

Options

Enable rule

Translate DNS replies that match this rule

Direction: Both

Description:

OK Cancel Help

Add Network Object

Name: 10.1.1.100-110

Type: Range

Start Address: 10.1.1.100

End Address: 10.1.1.110

Description:

NAT

IP アドレスプールの開始アドレスと終了アドレスを指定

OK Cancel Help

Browse Translated Source

Network Object...

Network Object Group...

IP v4 Network Objects

Interfaces

inside

outside

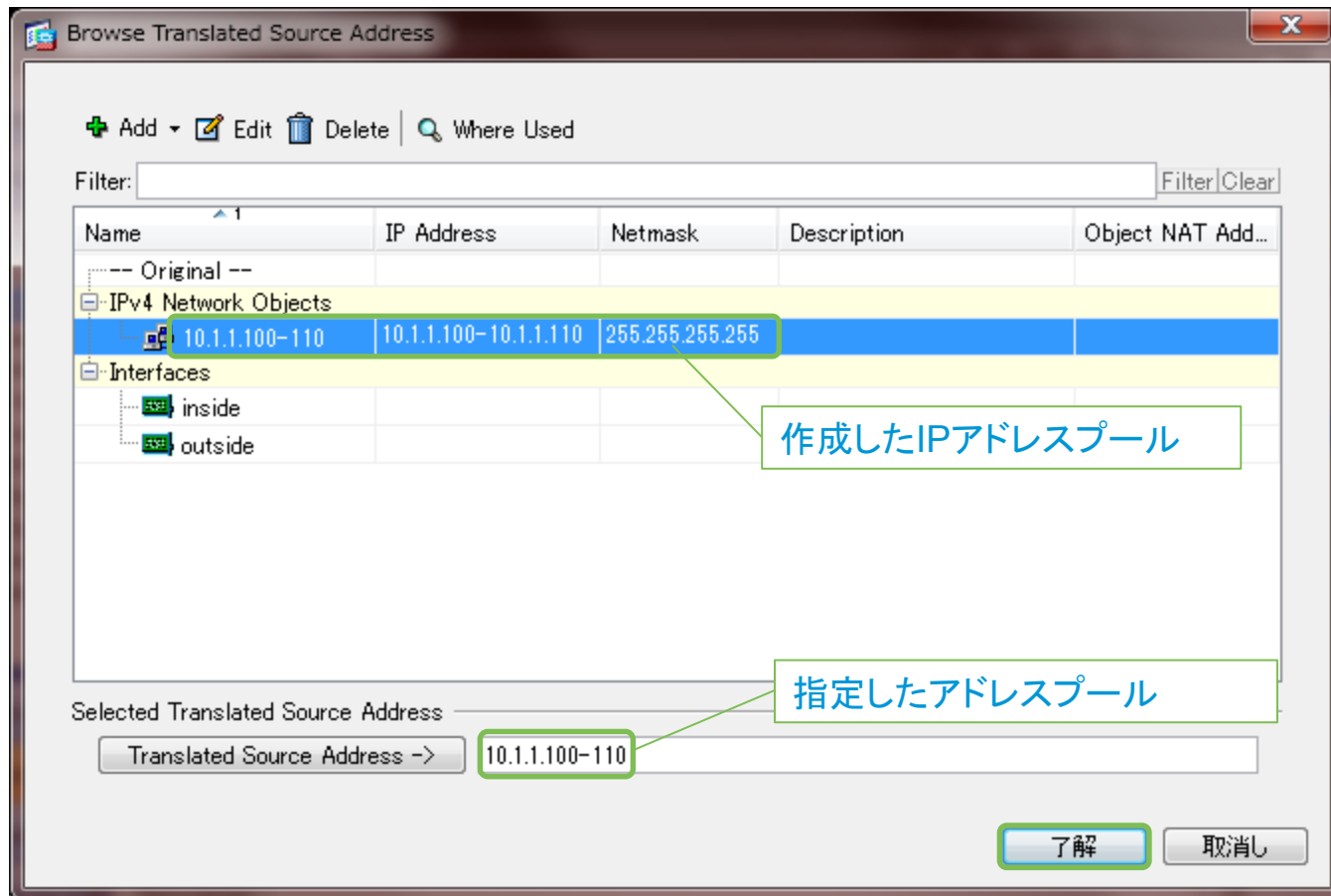
IP v4 Network Object Groups

Selected Translated Source Address

Translated Source Address -> Range 10.1.1.100-110

了解 取消し

NAT 設定 Dynamic NAT アドレスプールの指定



NAT 設定 Dynamic NAT4

Add NAT Rule

Match Criteria: Original Packet

Source Interface: inside Destination Interface: -- Any --

Source Address: 192.168.1.0-254 Destination Address: any

Service: any

Action: Translated Packet

Source NAT Type: **Dynamic** Destination Address: -- Original --

Source Address: 10.1.1.100-110 Service: -- Original --

Fall through to interface PAT

Options

Enable rule

Translate DNS replies that match this rule

Direction: Both

Description:

OK Cancel Help

NAT 設定 Dynamic NAT 設定の反映

The image displays the Cisco ASDM interface for configuring a Dynamic NAT rule. The 'Add NAT Rule' dialog box is open, showing the following configuration:

- Match Criteria: Original Packet**
 - Source Interface: inside
 - Destination Interface: -- Any --
 - Source Address: 192.168.1.0-254
 - Destination Address: any
 - Service: any
- Action: Translated Packet**
 - Source NAT Type: Dynamic
 - Source Address: 10.1.1.100-110
 - Destination Address: -- Original --
 - Service: -- Original --
- Fall through to interface PAT
- Enable rule
- Translate DNS replies that match this rule
- Direction: Both
- Description: (empty)

The 'Preview CLI Commands' dialog box shows the following commands generated from the configuration:

```
object network 10.1.1.100-110
  range 10.1.1.100 10.1.1.110
object network 192.168.1.0-254
  subnet 192.168.1.0 255.255.255.0
nat (inside,any) 1 source dynamic 192.168.1.0-254 10.1.1.100-110
```

A callout box with the text "NAT 設定OK後、設定の反映" (Reflection of NAT settings after OK) points to the 'Apply' button in the main ASDM window. The 'Apply' button is highlighted with a green box. The 'OK' button in the 'Add NAT Rule' dialog is also highlighted with a green box. The 'Send' button in the 'Preview CLI Commands' dialog is highlighted with a green box. The 'Apply' button in the main ASDM window is highlighted with a green box. The 'Send' button in the 'Preview CLI Commands' dialog is highlighted with a green box.

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。

The image displays three screenshots of the Cisco ASDM 6.4 for ASA interface, illustrating the configuration of NAT rules and network objects. The screenshots are arranged in a collage:

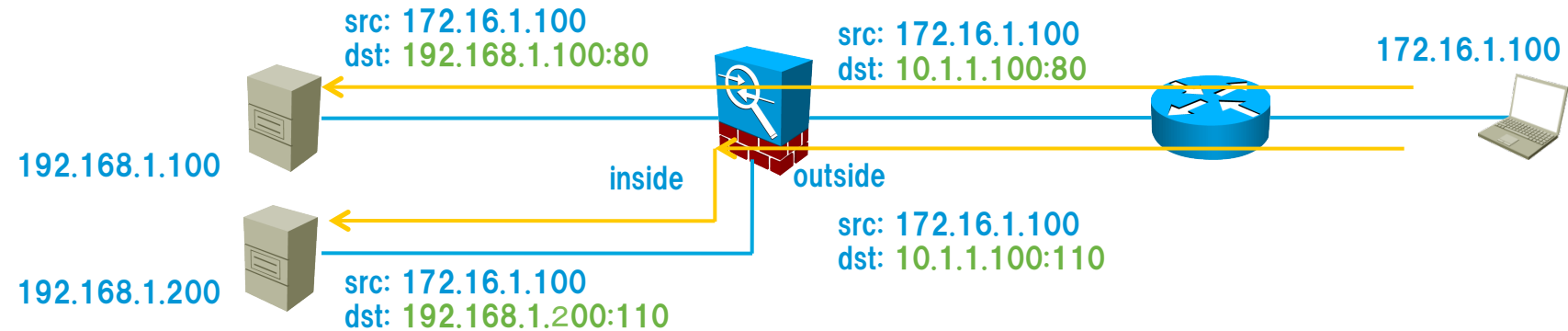
- Top Left:** Shows the 'NAT Rules' configuration page. A table of NAT rules is visible, with one rule highlighted in red. The rule is for '192.168.1.1-NAT'.
- Top Right:** Shows the 'Network Objects/Groups' configuration page. A table of network objects is visible, with two objects highlighted in red: '192.168.1.1-NAT' and '10.1.1.100'.
- Bottom:** Shows the status bar of the ASDM interface, indicating that configuration changes were saved successfully.

The table in the 'Network Objects/Groups' screenshot is as follows:

Name	IP Address	Netmask	Description	Object NAT Addr...
10.1.1.100-110	10.1.1.100-10.1.1.110	255.255.255.255		
192.168.1.0-254	192.168.1.0	255.255.255.255	255.255.255.0	
192.168.1.1-NAT	192.168.1.1	255.255.255.255		10.1.1.100 (S)
any	0.0.0.0	0.0.0.0		
inside-network	192.168.1.0	255.255.255.0		
outside-network	10.1.1.0	255.255.255.0		
10.1.1.100	10.1.1.100	255.255.255.255		
any	::	0		

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
192.168.1.200 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
は
ACL の設定が必要

NAT 設定 Static PAT(HTTP の変換ルール)

変換前の IP アドレス

変換後の IP アドレス

Static を選択

Advanced ボタンでポート番号指定

Add から“Netowk Object” NAT Ruleを選択

変換対象のインターフェイスの指定

変換するポート番号と変換後のポート番号を指定

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

変換前の IP アドレス

Add から“Netowk Object” NAT Ruleを選択

Static を選択

変換後の IP アドレス

Advanced ボタンでポート番号指定

変換対象のインターフェイスの指定

変換するポート番号と変換後のポート番号を指定

NAT 設定 Static PAT設定の反映

The screenshot displays the Cisco ASDM 6.4 for ASA interface. The main window shows the configuration for NAT Rules. A callout box points to the 'Apply' button with the text 'PAT 設定を OK 後、設定の反映'.

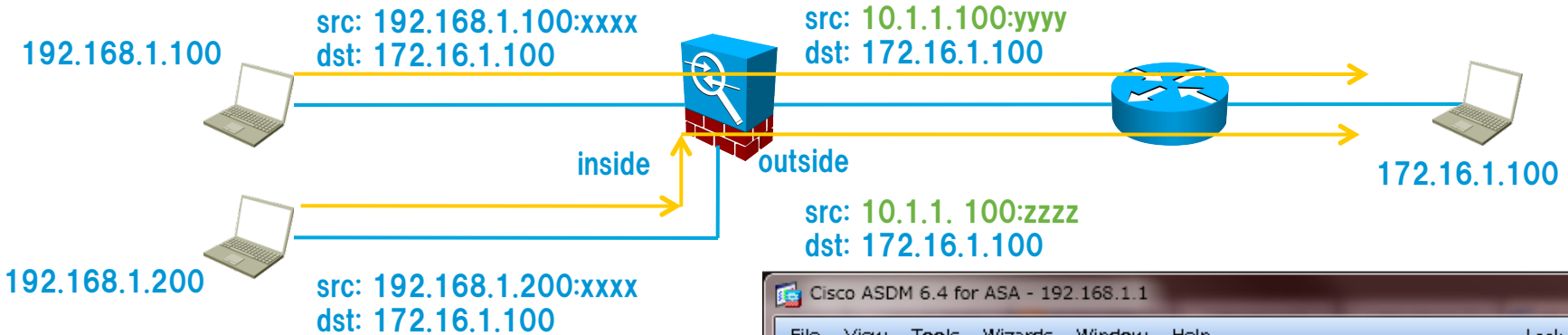
The 'Preview CLI Commands' window shows the following commands:

```
object network 192.168.1.100-PAT
 host 192.168.1.100
object network 192.168.1.200-PAT
 host 192.168.1.200
object network 192.168.1.100-PAT
 nat (inside,outside) static 10.1.1.100 service tcp http http
object network 192.168.1.200-PAT
 nat (inside,outside) static 10.1.1.100 service tcp pop3 pop3
```

The status bar at the bottom indicates: User cancelled the configuration update operation. | <admin> | 15 | 11/04/26 2:31:41 UTC

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変換する対象のIPアドレス(ネットワーク)とインターフェイスを指定

ネットワークアドレスを指定

Add NAT Rule

Match Criteria: Original Packet

Source Interface: **inside** Destination Interface: -- Any --

Source Address: **any** Destination Address: **any**

Service: **any**

Action: Translated Packet

Source NAT Type: **Dynamic**

Source Address: -- Original -- Destination Address: **any**

Fall through to interface PAT

Options

Enable rule

Translate DNS replies that match this rule

Direction: **Both**

Description:

OK Cancel

Add Network Object

Name: 192.168.1.1-254

Type: Network

IP Address: 192.168.1.0

Netmask: 255.255.255.0

Description:

NAT

OK Cancel Help

Browse Original Source Address

+ Add Edit Delete Where Used

Network Object... Network Object Group...

		Netmask	Description	Object NAT Ad...
IPv4 Network Objects				
10.1.1.100	10.1.1.100	255.255.255.2...		
10.1.1.100-110	10.1.1.100-10.1.1.1...	255.255.255.2...		
192.168.1.100	192.168.1.100	255.255.255.2...		
100.100.100.100	100.100.100.100	255.255.255.2...		

Selected Original Source Address

Original Source Address -> any

了解 取消し

ネットワークを新規作成

NAT 設定 Dynamic PAT

10.1.1.100 を作成

Dynamicを指定

NAT後のIPアドレス選択

Source Address

10.1.1.100

Host

10.1.1.100

OK Cancel Help

Selected Translated Source Address

Translated Source Address -> -- Original --

了解 取消し

NAT 設定 Dynamic PAT 設定の反映

The screenshot shows the Cisco ASDM 6.4 for ASA interface. The left sidebar contains a tree view with categories like Firewall, Objects, and Unified Communications. The main area displays the 'Configuration > Firewall' section with a table of NAT rules. A 'Preview CLI Commands' dialog box is overlaid on top, showing the generated CLI commands for the selected rule.

Configuration changes save... | <admin> | 15 | 11/04/05 18:42:47 UTC

Preview CLI Commands

The following CLI commands are generated based on the changes you made in ASDM. To send the commands to the ASA, click Send. To not send the commands and continue making changes in ASDM, click Cancel.

```
object network 10.1.1.100
 host 10.1.1.100
object network 192.168.1.1-254
 subnet 192.168.1.0 255.255.255.0
nat (inside,any) 1 source dynamic 192.168.1.1-254 10.1.1.100
```

Send Cancel Save To File...

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。

The left screenshot shows the 'NAT Rules' configuration page. The 'Match Criteria: Original Packet' table is as follows:

#	Source Intf	Dest Intf	Source	Destination
1	inside	Any	192.168.1.1-254	any

The right screenshot shows the 'Network Objects/Groups' configuration page. The table lists the following objects:

Name	IP Address	Netmask	Description	Object NAT Address
10.1.1.100	10.1.1.100	255.255.255.255		
192.168.1.1-254	192.168.1.0	255.255.255.0		
any	0.0.0.0	0.0.0.0		
inside-network	192.168.1.0	255.255.255.0		
outside-network	10.1.1.0	255.255.255.0		

フィルタリングの設定

フィルタリング設定概要

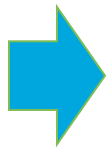
- ACL (Access Control List) を各インターフェイスに設定し通信を許可/拒否する
- ACL は 複数のACE (Access Control Entry) から構成される。

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

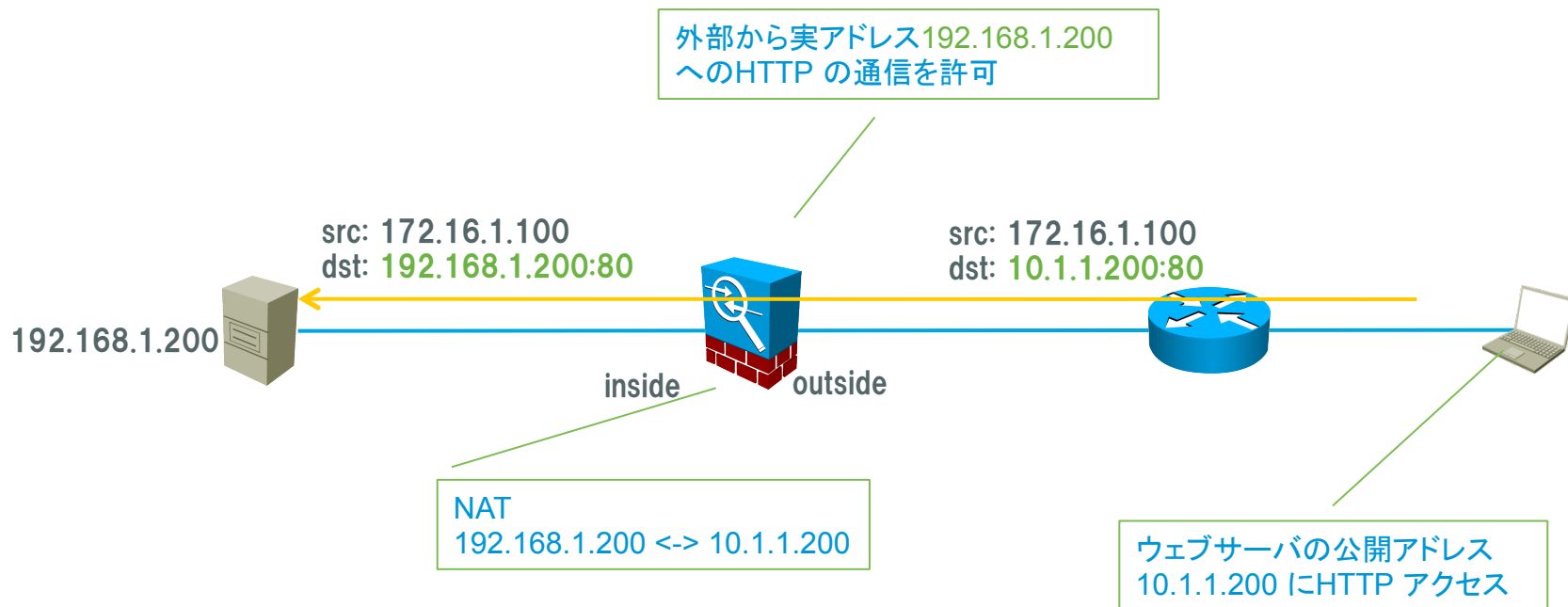
例) A→B のトラフィックのみ拒否

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)

The screenshot shows the Cisco ASDM 6.4 for ASA interface. The main window displays the configuration for a NAT rule under 'Configuration > Firewall > NAT Rules'. The rule is titled '"Network Object" NAT (Rule 1)'. The configuration table is as follows:

Match Criteria: Original Packet						Action: Translated Packet	
#	Source Intf	Dest Intf	Source	Destination	Service	Source	Destination
"Network Object" NAT (Rule 1)							
	inside	outside	192.168.1.200	any	tcp http	10.1.1.200 (S)	-- Original
	outside	inside	any	10.1.1.200	tcp http	-- Original --	192.168.1.200

At the bottom of the window, there are 'Apply' and 'Reset' buttons. A status bar at the very bottom indicates 'Configuration changes saved successfully.' and shows the user as '<admin>' with a session ID of '15'. The date and time are '11/04/26 2:31:41 UTC'.

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

Cisco ASDM 6.4 for ASA - 192.168.1.1

Configuration > Firewall > Access Rules

#	Enabled	Source	Destination	Service	Action	Hits	Log
inside (1 implicit incoming rule)							
1		any	Any less secure ne...	ip	Permit		
outside (0 implicit incoming rules)							
Global (1 implicit rule)							
1		any	any	ip	Deny		

Access Rule Type IPv4 and IPv6 IPv4 Only IPv6 Only

Apply Reset

Configuration changes saved successfully.

暗黙のDeny ルール
(削除、変更不可)

Cisco ASDM 6.4 for ASA - 192.168.1.1

Configuration > Firewall > Access Rules

Add から Add Access Rule

Add Access Rule...

Insert... (rule)

Insert After... (rule)

フィルタリング設定 アクセスルールの作成 2

The image shows two overlapping configuration windows from a Cisco ASA. The 'Add Access Rule' window is in the foreground, and the 'Browse Service' window is in the background.

Add Access Rule Window:

- Interface:** outside (Annotation: 適用するインターフェイス)
- Action:** Permit (Annotation: 許可するルールを作るのでPermit)
- Source:** any (Annotation: すべてのホストからのトラフィック)
- Destination:** 192.168.1.200 (Annotation: サーバの公開アドレス)
- Service:** tcp/http (Annotation: プロトコルの指定)
- Enable Logging
- Logging Level: Default
- Buttons: OK, Cancel, Help

Browse Service Window:

Name	Protocol	Source Ports	Destination Ports	ICMP Type	Description
finger	tcp	default (1-65535)	79		
ftp	tcp	default (1-65535)	21		
ftp-data	tcp	default (1-65535)	20		
gopher	tcp	default (1-65535)	70		
h323	tcp	default (1-65535)	1720		
hostname	tcp	default (1-65535)	101		
http	tcp	default (1-65535)	80		
https	tcp	default (1-65535)	443		
ident	tcp	default (1-65535)	113		
imap4	tcp	default (1-65535)	143		
irc	tcp	default (1-65535)	194		
kerberos	tcp	default (1-65535)	750		
login	tcp	default (1-65535)	543		
rsh	tcp	default (1-65535)	544		
ldap	tcp	default (1-65535)	389		
ldaps	tcp	default (1-65535)	636		
login	tcp	default (1-65535)	513		
lotusnotes	tcp	default (1-65535)	1352		
lpd	tcp	default (1-65535)	515		
nethins-s	tcp	default (1-65535)	139		

Selected Service: tcp/http (Annotation: HTTP を選択)

Buttons: 了解, 取消し

フィルタリング設定 設定の反映

The screenshot displays the Cisco ASDM 6.4 for ASA interface. The main window shows the 'Configuration' tab with a tree view on the left containing 'Access Rules', 'NAT Rules', 'Service Policy Rules', 'AAA Rules', 'Filter Rules', 'Public Servers', 'URL Filtering Servers', 'Threat Detection', 'Objects', 'Unified Communications', and 'Advanced'. The 'Firewall' section is expanded, showing a table of configuration items. A 'Preview CLI Commands' dialog box is overlaid on top, displaying the following commands:

```
object network 10.1.1.200
 host 10.1.1.200
access-list outside_access_in line 1 extended permit tcp any object 192.168.1.200 eq http
nat (outside,inside) 1 source static any any destination static 10.1.1.200 192.168.1.200 unidirectional
access-group outside_access_in in interface outside
```

The dialog box includes 'Send', 'Cancel', and 'Save To File...' buttons. Below the dialog, the 'Apply' button in the main configuration window is highlighted with a green box. A purple arrow points from the 'Apply' button to the 'Send' button in the dialog box. At the bottom of the main window, a status bar shows 'Configuration changes saved successfully.', a user prompt '<admin>', the number '15', and a timestamp '11/04/05 23:12:17 UTC'.

インスペクションの設定

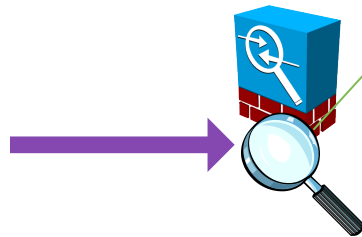
インスペクションとMPF (Modular Policy Framework)

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

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

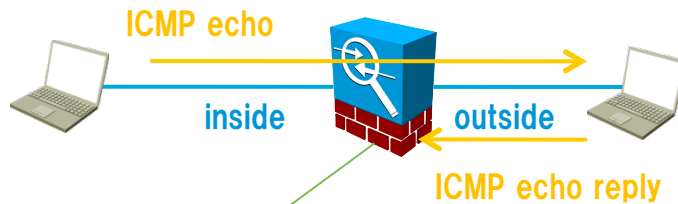
dns, ftp, h323 h225, h323 ras, ip options, netbios, rsh, rtsp, skinny, esmtp, sqlnet, sunrpc, tftp, sip, xdmcp

※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)

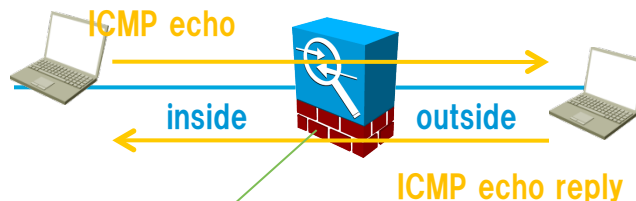


outside → inside の通信は原則拒否



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

The screenshot displays the Cisco ASDM 6.4 for ASA interface. The main window is titled "Configuration > Firewall > Service Policy Rules". A callout box with a green border and blue text says "デフォルトのポリシーを選択" (Select the default policy), pointing to the "inspection_def..." row in the table below.

Name	#	Enabled	Match	Source	Destination	Service	Time	Rule Actions
Global: Policy: global policy								
inspection_def...			Match	any	any	default-inspec...		Inspect DN Inspect ES (13 more insper

An "Edit Service Policy Rule" dialog box is open, showing the "Rule Actions" tab. A callout box with a green border and blue text says "ICMP をチェック" (Check ICMP), pointing to the checked checkbox for "ICMP" in the "Protocol Inspection" section.

Protocol Inspection

- Select all inspection rules
- CTIQBE
- DCERPC
- DNS
- ESMTTP
- FTP
- H.323 H.225
- H.323 RAS
- HTTP
- ICMP
- ICMP Error
- ILS
- IM
- IP-Options
- IPSec-Pass-Thru
- MMP
- MGCP
- NETBIOS
- PPTP

Buttons: OK, Cancel, Help

ICMP インспекション設定 設定の反映

The screenshot displays the Cisco ASDM 6.4 for ASA interface. The main window is titled "Configuration > Firewall > Service Policy Rules". The left sidebar shows the "Firewall" tree with "Service Policy Rules" selected. The main area shows a table for "Traffic Classification" with one entry: "inspection_def..." under the "Match" column. A "Preview CLI Commands" dialog box is open, showing the following commands:

```
policy-map global_policy
class inspection_default
inspect icmp
```

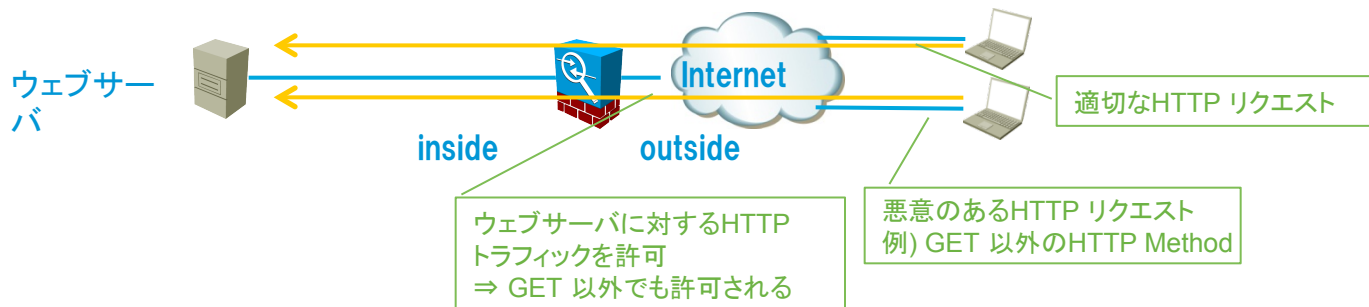
The dialog box has "Send", "Cancel", and "Save To File..." buttons. The "Send" button is highlighted with a green border. Below the dialog box, a purple arrow points to the "Apply" button in the main configuration window, which is also highlighted with a green border. The "Reset" button is also visible.

At the bottom of the window, the status bar shows "<admin> 15" and the date/time "11/04/18 12:38:14 UTC".

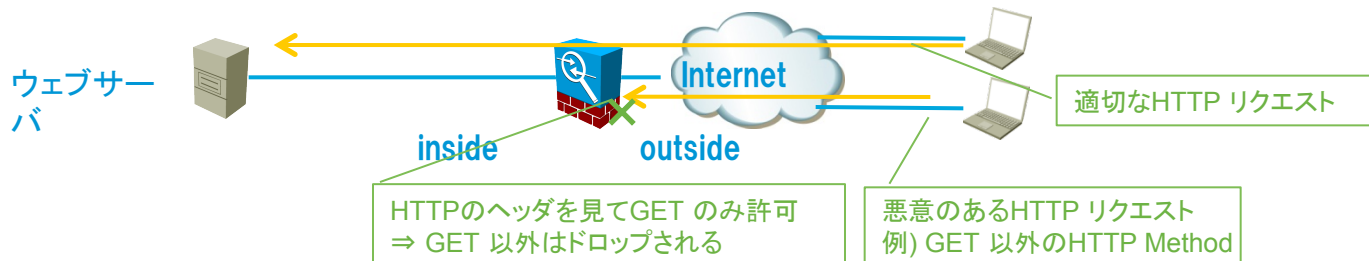
アプリケーションインスペクション概要

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

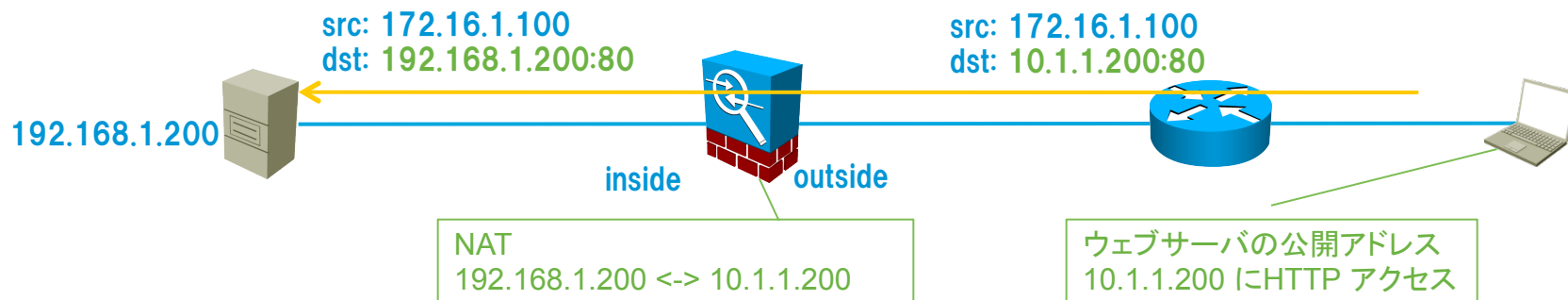


例) アプリケーションインスペクションによる制御



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

Adding a new service policy rule requires three steps:

- Step 1: Configure a service policy.
- Step 2: Configure the traffic classification criteria for the service policy rule.
- Step 3: Configure actions on the traffic classified by the service policy rule.

Create a Service Policy and Apply To:

Only one service policy can be configured per interface or at global level. If a service policy already exists, then you can add a new rule into the existing service policy. Otherwise, you can create a new service policy.

Interface: outside - (create new service polic...
inside - (create new service policy)

Policy Name: outside - (create new service policy)

Description:

Global - applies to all interfaces

Policy Name: global_policy

Description:

特定のインターフェイスに設定するため、インターフェイスを指定

すべてのインターフェイスに対して設定する場合はGlobal を選択

< Back **Next >** Cancel Help

インスペクション設定 対象トラフィックの指定

Add Service Policy Rule Wizard - Traffic Classification Criteria

Create a new traffic class:

Description (optional):

Traffic Match Criteria

- Default Inspection Traffic
- Source and Destination IP Address (uses ACL)
- Tunnel Group
- TCP or UDP Destination Port
- RTP Range
- IP DiffServ
- IP Precedence
- Any traffic

Use an existing traffic class:

Use class-default as the traffic class.

If traffic does not match a existing traffic class, then it will match the class used in catch all situation.

< Back **Next >** >>>

Class を新規で作成
Class 名は自動で記入

対象トラフィックは
ACL で指定

Add Service Policy Rule Wizard - Traffic Match - Source and Destination Address

以下の条件に一致するトラフィックを対象にする

Action: Match Do not match

Source: 送信元は任意のホスト

Destination: 宛先はサーバの公開アドレス

Service: HTTPアクセスを対象

Description:

More Options

< Back **Next >** Cancel Help

インスペクション設定 インスペクションルールの作成

Protocol Inspection Connection Settings QoS NetFlow

CTIQBE
 DCERPC Configure...
 DNS Configure...
 ESMTP Configure...
 FTP Configure...
 H.323 H.225 Configure...
 H.323 RAS Configure...
 HTTP Configure...
 ICMP
 ICMP Error
 IPsec-Pass-Thru Configure...
 MMP Configure...
 MGCP Configure...
 NETBIOS Configure...
 PPTP
 RSH
 RTSP Configure...
 SSCP (Skinny) Configure...

Select HTTP Inspect Map

Use the default HTTP inspection map
 Select an HTTP inspect map for fine control over inspection

Name Add

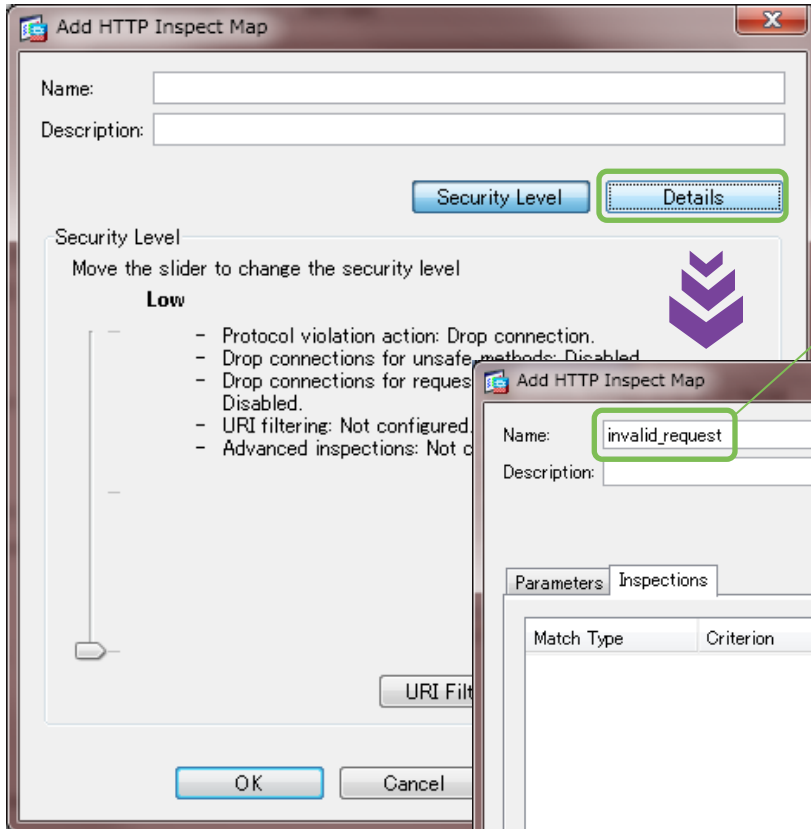
OK Cancel Help

< Back Finish Cancel Help

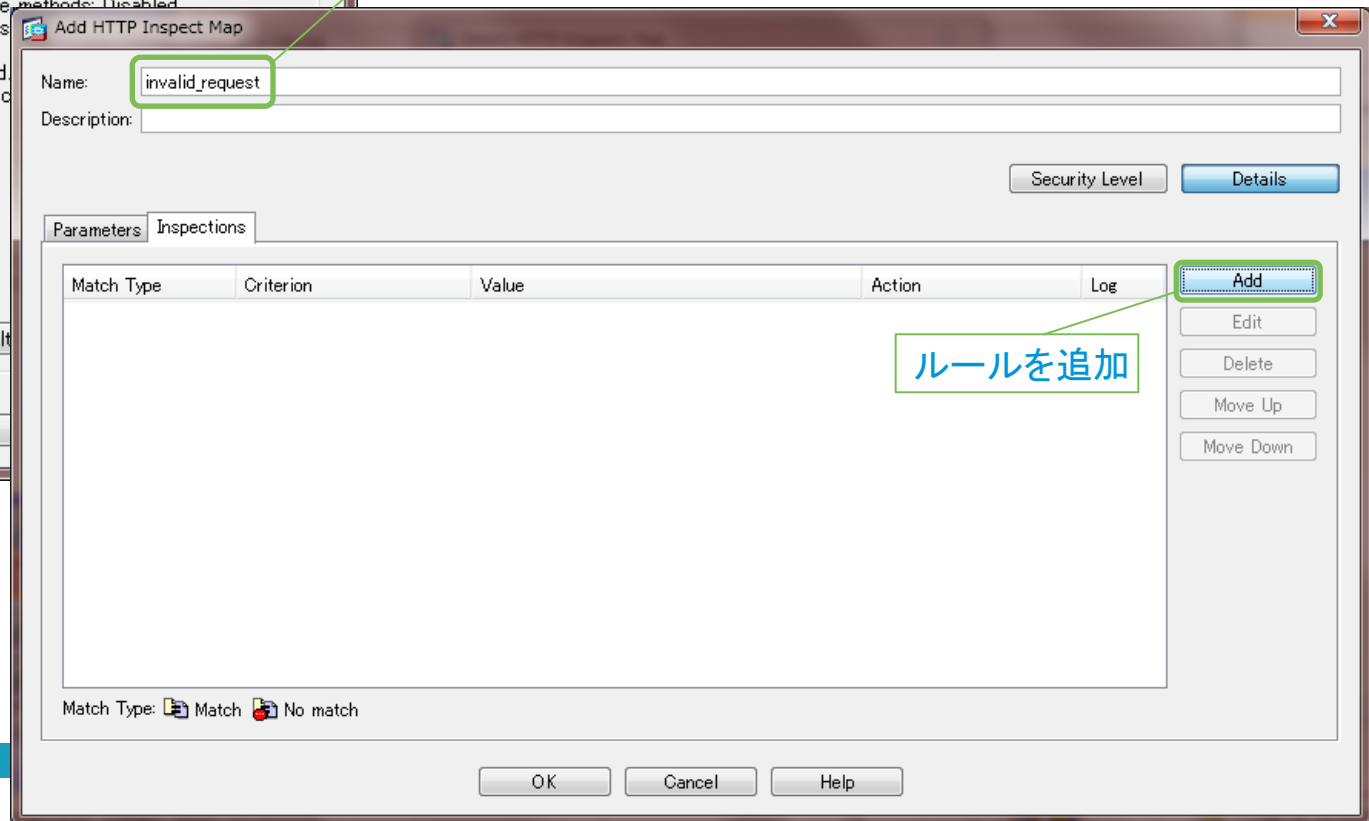
HTTP のインスペクションを有効にする

新たなHTTP インスペクションのルールを作成する

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



インスペクションのルール名を決める



ルールを追加

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

Match Criteria

Single Match

Match Type: Match No Match

Criterion: Request Header Length

Value

Greater Than Length: 1024 bytes

Multiple matches

HTTP Traffic Class: _default_GoToMyPC-tunnel

Actions

Action: Drop Connection Reset Log

Log: Enable Disable

OK Cancel Help

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

同様にルールの追加

条件の指定:
HTTP リクエストのMethod がget 以外

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

Match Type	Criterion	Value	Action	Log
	Request Header Length	> 1024	Drop Connection	

Match Criteria

Single Match

Match Type: Match No Match

Criterion: Request Method

Value

Method: get

Regular Expression

Regular Expression: _default_GoToMyPC-tunnel

Regular Expression Class:

Multiple matches

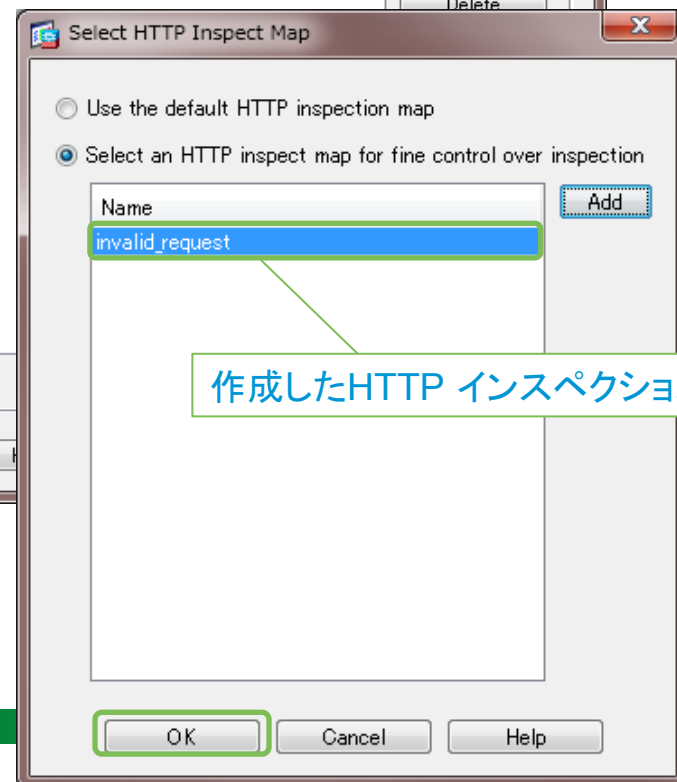
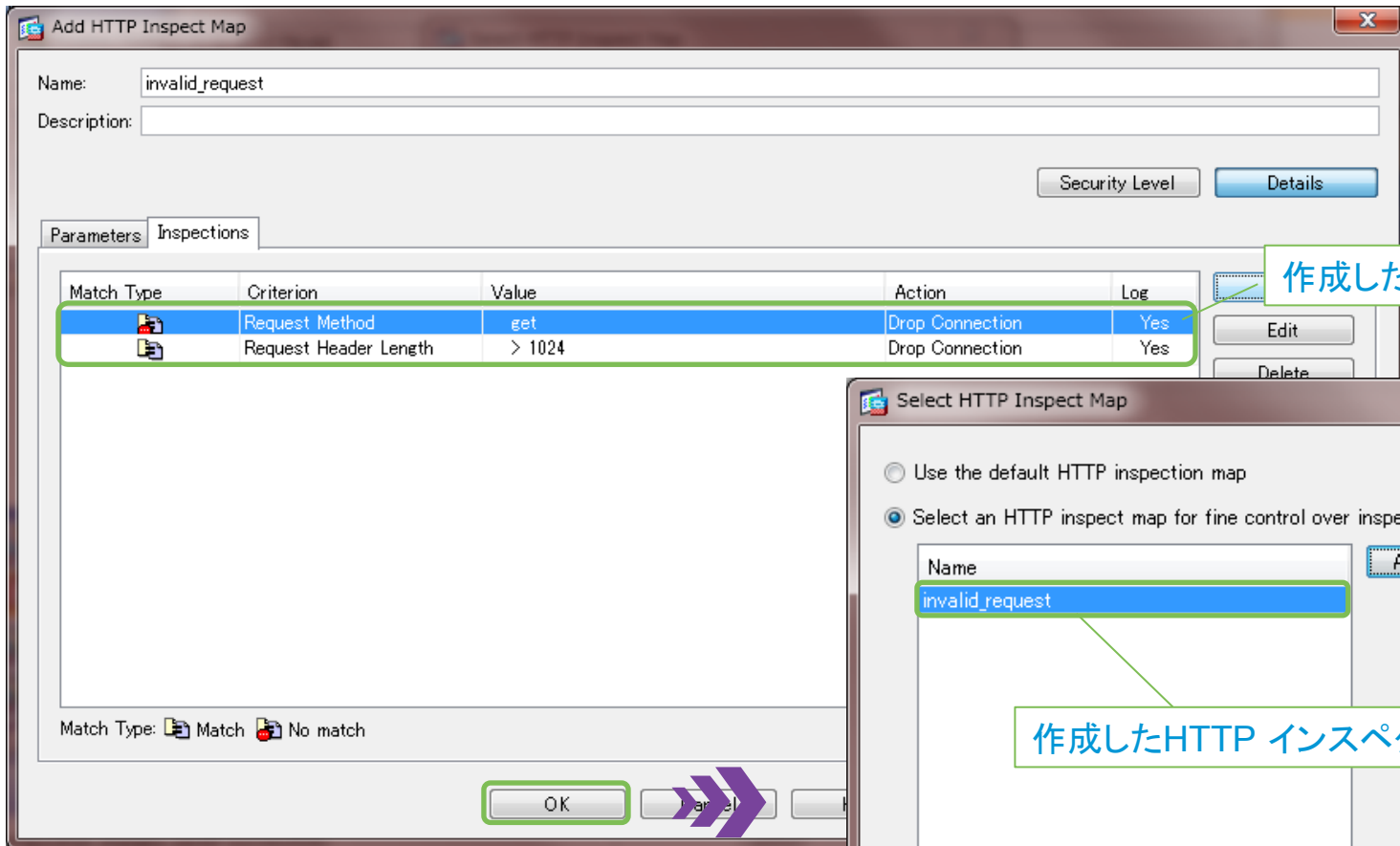
HTTP Traffic Class: _default_GoToMyPC-tunnel

Actions

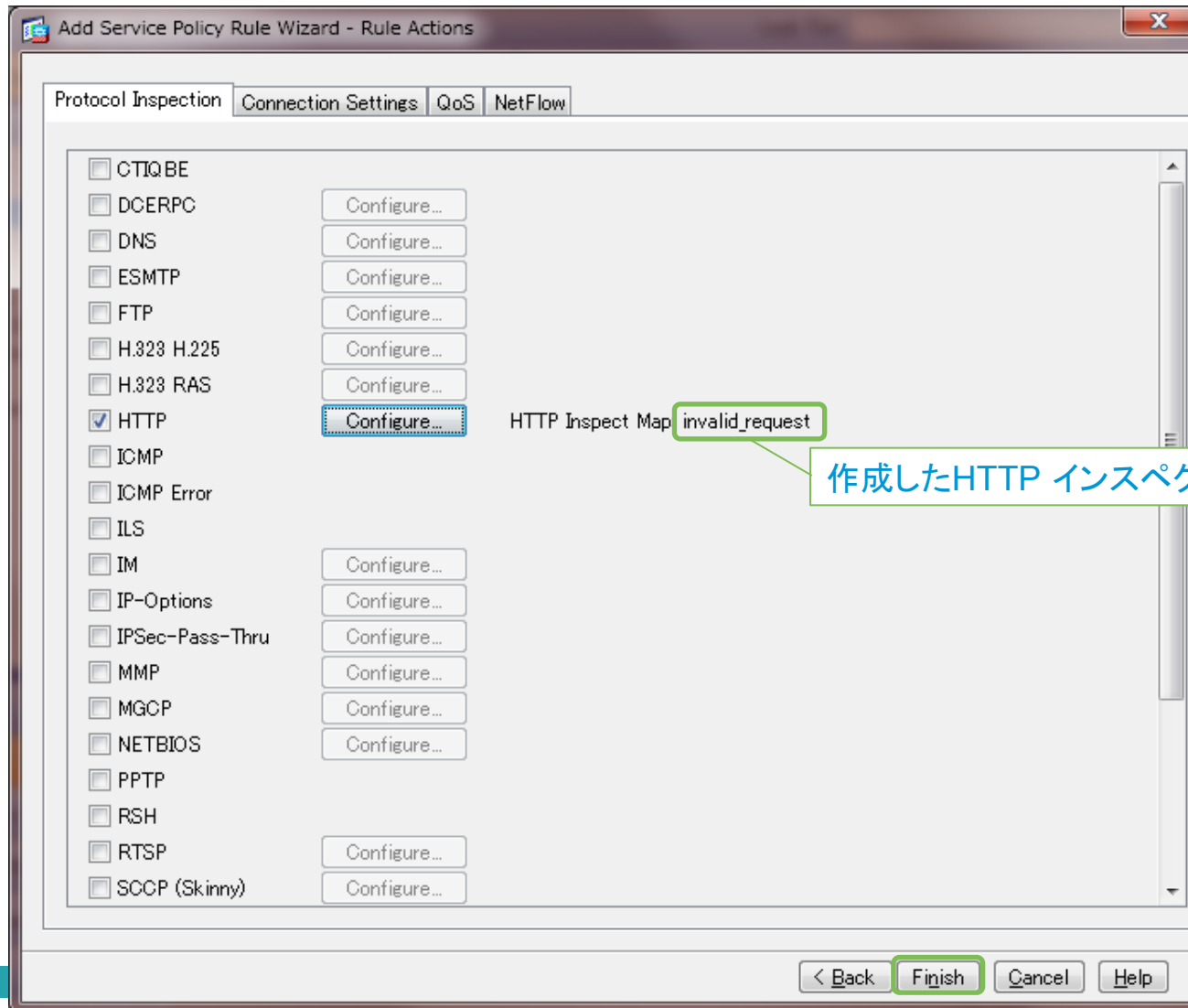
Action: Drop Connection Reset Log

Log: Enable Disable

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

The screenshot displays the Cisco ASDM 6.4 for ASA interface. The main window shows the configuration tree on the left, with 'Service Policy Rules' selected. The central pane shows the configuration for 'Interface: outside; Policy: outside-policy'. A 'Preview CLI Commands' dialog box is open, showing the generated CLI commands for the configuration changes. The 'Send' button in the dialog is highlighted with a green box, and a purple arrow points from it to the 'Apply' button in the main window, which is also highlighted with a green box. The status bar at the bottom indicates 'Configuration changes saved successfully.'

Configuration changes saved successfully.

```
access-list outside_mpc line 1 extended permit tcp any host 10.1.1.200 eq http
policy-map type inspect http invalid_request
  parameters
    protocol-violation action drop-connection
    match request header length gt 1024
    drop-connection log
    match not request method get
    drop-connection log
class-map outside-class
  match access-list outside_mpc
policy-map outside-policy
  class outside-class
    inspect http invalid_request
service-policy outside-policy interface outside
```

Apply Reset

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

最大コネクション数の制御

- TCP&UDP コネクション
- Embryonic コネクション ※
- 1クライアントあたりのコネクション
- 1クライアントあたりのEmbryonic コネクション

TCP タイムアウト設定

- Embryonic コネクション ※
- ハーフクローズのコネクション
- コネクションタイムアウト

※ Embryonic コネクション: TCP 接続がまだ確立していないコネクション

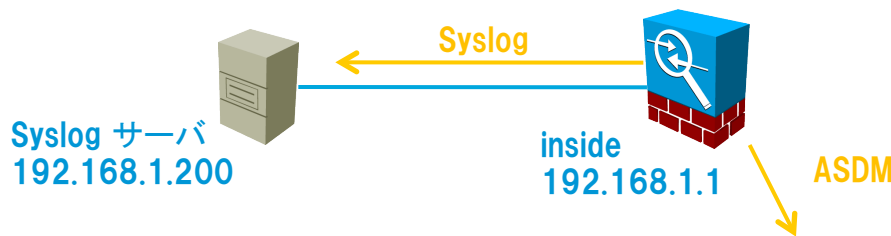
Loggingの設定

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	Destin	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...

Logging 設定 ログの有効化

The screenshot displays the Cisco ASDM 6.4 for ASA interface. The main window is titled "Cisco ASDM 6.4 for ASA - 192.168.1.1". The left sidebar shows the "Device Management" tree with "Logging Setup" selected. The main content area is titled "Configuration > Device Management > Logging" and contains the following settings:

- Enable logging
- Enable logging to external servers
- Send debug messages as syslog
- Send syslog to external servers

Logging to Internal Buffer

Specify the size of the internal buffer to which syslog messages are sent.

Buffer Size: bytes

You can choose to save the buffer contents before the buffer is full.

Save Buffer To: FTP Server Flash

ASDM Logging

Specify the size of the queue for syslog messages intended for ASDM.

Queue Size:

Buttons: Apply, Reset

Bottom status bar: <admin> | 15 | 11/04/18 17:51:34 UTC

A "Preview CLI Commands" dialog box is open in the foreground, showing the following text:

The following CLI commands are generated based on the changes you made in ASDM. To send the commands to the ASA, click Send. To not send the commands and continue making changes in ASDM, click Cancel.

```
logging enable
```

Buttons: Send, Cancel, Save To File...

A callout box with the text "ログを有効化する" (Enable logging) points to the "Enable logging" checkbox.

Logging 設定 ログの出力先の設定

The screenshot displays the Cisco ASDM 6.4 for ASA interface. The main window is titled "Configuration > Device Management > Logging > Logging Filters". It contains a table for configuring syslog filters for logging destinations. The "ASDM" row is highlighted, and a callout box points to it with the text "ASDM を選択".

Logging Destination	Syslogs From All Event Classes	Syslogs From Specific Event Classes
SNMP Trap	-- Disabled	
Internal Buffer	-- Disabled	
E-Mail	-- Disabled --	
Console	-- Disabled --	
Telnet and SSH Sessions	-- Disabled --	
ASDM	-- Disabled --	
Syslog Servers	-- Disabled --	

The "Edit Logging Filters" dialog box is open, showing the configuration for the selected "ASDM" destination. The "Logging Destination" is "ASDM". Under "Syslogs from All Event Classes", the "Filter on severity" option is selected. The severity dropdown menu is open, showing "Debugging" selected. A callout box points to this selection with the text "Debugging レベルに設定 (実際の運用ではDebug レベルのログは必要なし)".

Event Class: auth
Description: User Authentication
Severity: Emergency

Logging 設定 ログの出力先の設定2

Configuration > Device Management > Logging > Logging Filters

Configure syslog filters for logging destinations.

Logging Destination	Severity
Internal Buffer	-- Disabled --
SNMP Trap	-- Disabled --
E-Mail	-- Disabled --
Console	-- Disabled --
Telnet and SSH Sessions	-- Disabled --
ASDM	Severity: Debugging
Syslog Servers	Severity: Debugging

Syslog Servers を選択
edit で同様に
Debug レベルのログを設定

CLI Commands

```
logging asdm Debugging
logging trap Debugging
```

Configuration changes saved successfully.

<admin> | 15 | 11/04/18 20:49:08 UTC

Logging 設定 Syslog サーバの設定

Configuration > Device Management > Logging > Syslog Servers

Specify up to 16 syslog servers. Make sure logging is enabled in Configuration > Device Management > Logging > Logging Setup.

Interface	IP Address	Protocol/Port	EMBLEM	Secure
-----------	------------	---------------	--------	--------

サーバのあるインターフェイスを指定

サーバのIP アドレス

Add Syslog Server

Interface: inside

IP Address: 192.168.1.200

Protocol: TCP UDP

Port: 514

Log messages in Cisco EMBLEM format (UDP only)

Enable secure syslog using SSL/TLS

OK Cancel Help

Specify the number of messages that are allowed to be queued when a syslog server is busy. Use 0 to indicate unlimited queue size.

Queue Size: 512

Allow user traffic to pass when TCP syslog server is down

Apply Reset

Configuration changes saved successfully.

<admin> | 15 | 11/04/18 20:55:48 UTC

Logging 設定 Syslog サーバの設定 設定の反映

The screenshot shows the Cisco ASDM 6.4 for ASA interface. The left sidebar displays the configuration tree with 'Syslog Servers' selected. The main pane shows the 'Syslog Servers' configuration page with a table of servers. A 'Preview CLI Commands' dialog box is open, showing the generated CLI command for the selected server.

Interface	IP Address
inside	192.168.1.200

Specify up to 16 syslog servers. Make sure logging is enabled on the interface.

Specify the number of messages that are allowed to be queued when a syslog server is busy. Use 0 to indicate unlimited queue size.

Queue Size:

Allow user traffic to pass when TCP syslog server is down

Buttons: Send, Cancel, Save To File..., Apply, Reset

Configuration changes saved successfully.

© 2010 Cisco and/or its affiliates. All rights reserved. Cisco Confidential

Logging 設定の確認

The screenshot shows the Cisco ASDM 6.4 for ASA interface. The 'View' menu is open, and 'Latest ASDM Syslog Messages' is selected. A callout box points to this menu item with the text: 'Home を選択後、View メニューから Latest ASDM Syslog Message を選択'.

Below the menu, a table displays the latest Syslog messages. A callout box points to this table with the text: 'ASDM 上にログが出力される'.

Time	IP Address	Msg Type	Message
Apr 19 10:16:11	192.168.1.1	local4.info	%ASA-6-302015: Built outbound UDP connection 397 for inside:192.168.1.200/514 (192.168.1.200/514) to identity:192.168.1.1
Apr 19 10:16:11	192.168.1.1	local4.debug	%ASA-7-609001: Built local-host inside:192.168.1.200
Apr 19 10:16:11	192.168.1.1	local4.debug	%ASA-7-609001: Built local-host identity:192.168.1.1
Apr 19 10:16:11	192.168.1.1	local4.debug	%ASA-7-609002: Teardown local-host inside:192.168.1.200 duration 0:02:01
Apr 19 10:16:11	192.168.1.1	local4.debug	%ASA-7-609002: Teardown local-host identity:192.168.1.1 duration 0:02:01
Apr 19 10:16:11	192.168.1.1	local4.info	%ASA-6-302016: Teardown UDP connection 396 for inside:192.168.1.200/514 to identity:192.168.1.1/514 duration 0:02:01
Apr 19 10:14:10	192.168.1.1	local4.info	%ASA-6-302015: Built outbound UDP connection 396 for inside:192.168.1.200/514 (192.168.1.200/514) to identity:192.168.1.1
Apr 19 10:14:10	192.168.1.1	local4.debug	%ASA-7-609001: Built local-host inside:192.168.1.200
Apr 19 10:14:10	192.168.1.1	local4.debug	%ASA-7-609001: Built local-host identity:192.168.1.1
Apr 19 10:14:10	192.168.1.1	local4.debug	%ASA-7-609002: Teardown local-host inside:192.168.1.200 duration 0:02:01
Apr 19 10:14:10	192.168.1.1	local4.debug	%ASA-7-609002: Teardown local-host identity:192.168.1.1 duration 0:02:01

At the bottom, a 'Syslog Server' configuration window is visible, with a callout box pointing to it: 'Syslog サーバ'.

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

The screenshot shows the Cisco ASDM 6.4 for ASA interface. The 'Wizards' menu is open, and 'Startup Wizard...' is highlighted. A green box highlights the 'Wizards' menu and the 'Startup Wizard...' option. A callout box points to the 'Startup Wizard...' option with the text 'Wizards → Startup Wizard'. The main interface displays device information for ASA 5520-L02-02, including ASA Version 8.4(1), ASDM Version 6.4(1), and Firewall Mode Routed. The 'Device Information' section shows the following details:

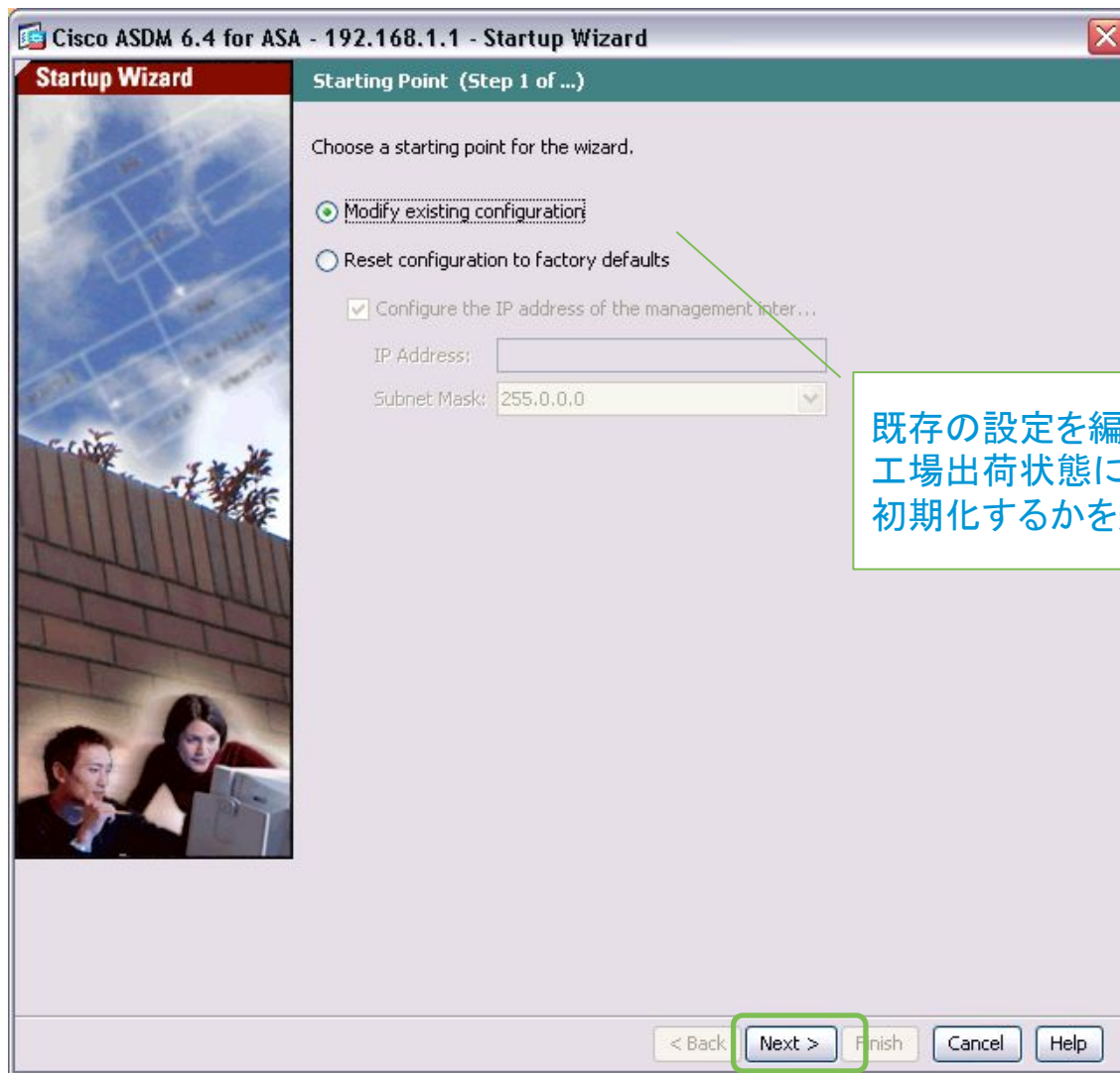
Field	Value
Host Name	ASA5520-L02-02
ASA Version	8.4(1)
ASDM Version	6.4(1)
Firewall Mode	Routed
Total Flash	256 MB
Device Uptime	14d 17h 43m 54s
Device Type	ASA 5520
Context Mode	Single
Total Memory	2048 MB

The 'VPN Sessions' section shows 0 IPsec, 0 Clientless SSL VPN, and 0 AnyConnect Client. The 'System Resources Status' section shows CPU usage at 1% and Memory usage at 1000 MB. The 'Latest ASDM Syslog Messages' section shows the following messages:

Severity	Date	Time	Syslog ID	Source IP	Source	Destination IP	Destin	Description
6	Apr 26 2011	23:24:06	302010					3 in use, 9 most used
6	Apr 26 2011	23:24:00	302014	192.168.1.100	2312	192.168.1.1	443	Teardown TCP connec
6	Apr 26 2011	23:24:00	302014	192.168.1.100	2314	192.168.1.1	443	Teardown TCP connec

The status bar at the bottom indicates 'Device configuration loaded successfully.' and shows the user as '<admin>' with 15 sessions.

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

Cisco ASDM 6.4 for ASA - 192.168.1.1 - Startup Wizard

Startup Wizard

Basic Configuration (Step 2 of ...)

Enter the host name and the domain name of the ASA. If your Internet Service Provider (ISP) requires that your host uses DHCP, you may need to use the device name supplied by the ISP as the host name of the ASA.

ASA Host Name:

Domain Name:

Privileged Mode (Enable) Password

The privileged mode (enable) password is required to administer the ASA using ASDM or the Command Line Interface (CLI).

Change privileged mode (enable) password

Old Password:

New Password:

Confirm New Password:

必要があればパスワード変更も可能

< Back Next > Finish Cancel Help

ウィザードを使った設定 自動アップデートの設定

Cisco ASDM 6.4 for ASA - 192.168.1.1 - Startup Wizard

Startup Wizard

Outside Interface Configuration (Step 3 of ...)

Interface Settings: IPv6 Interface Settings

Configure the **物理インターフェイス** to determine which option to use.

Interface Properties

Interface: GigabitEthernet0/0 Enable interface

Interface Name: outside Security Level: 0

IP Address

Use the following IP address **セキュリティレベル**

IP Address: 10.1.1.1 Subnet Mask: 255.255.255.0

Use DHCP

The ASA will obtain an IP address from a DHCP server. Ensure that a DHCP server is configured on your corporate network or by your ISP.

Obtain default route using DHCP

Use PPPoE **IPアドレスとマスク**

The ASA will obtain its IP address from a PPPoE server if you do not specify an IP address in next step. Ensure that a PPPoE server is configured by your ISP.

< Back Next > Finish Cancel Help

インターフェイス名

物理インターフェイス

インターフェイスを有効化

セキュリティレベル

IPアドレスとマスク

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

Startup Wizard

Other Interface Configuration (Step 4 of 10)

Configure the remaining interfaces of the ASA. To configure an interface, select it in the list below and click Edit.

Interface	Name	Enabled	Security Level	IP Address	Subnet Mask/Prefix Length
GigabitEthernet0/1	inside	Yes	100	192.168.1.1	255.255.255.0
GigabitEthernet0/0	outside	Yes	0	10.1.1.1	255.255.255.0
GigabitEthernet0/2		No			
GigabitEthernet0/3		No			
Management0/0		No			

Edit

Enable traffic between two or more interfaces with the same security levels

Enable traffic between two or more hosts connected to the same interface

< Back Next > Finish Cancel Help

ウィザードを使った設定 スタティックルートの設定

Cisco ASDM 6.4 for ASA - 192.168.1.1 - Startup Wizard

Startup Wizard Static Routes (Step 5 of 10)

Specify static routes.

Add Static Route インターフェイスを指定

IP Address Type: IPv4 IPv6

Interface: inside

Network: 0.0.0.0/0.0.0.0

Gateway IP: 10.1.1.254 Metric: 1

Options

None

Tunnel

Tracked

Track ID: Track IP Address:

SLA ID: Target Interface: inside

Monitoring Options

Enabling the tracked option starts a job for monitoring the state of the route, by pinging the track address provided.

デフォルトルートを表す 0.0.0.0/0.0.0.0 を指定

ネクストホップアドレスを指定

OK Cancel Help

< Back Next > Finish Cancel Help

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

The screenshot shows the 'Startup Wizard' window for configuring a DHCP server on a Cisco ASA. The window title is 'Cisco ASDM 6.4 for ASA - 192.168.1.1 - Startup Wizard'. The current step is 'DHCP Server (Step 6 of 10)'. The left sidebar shows a network diagram and a photo of two people working at a computer. The main content area contains the following text and fields:

The ASA can act as a DHCP server and provide IP addresses to the hosts on your Inside network. To configure a DHCP server on an interface other than the inside interface, go to Configuration > Device Management > DHCP > DHCP Server in the main ASDM window.

Enable DHCP server on the inside interface

DHCP Address Pool

Starting IP Address: Ending IP Address:

DHCP Parameters

DNS Server 1: DNS Server 2:

WINS Server 1: WINS Server 2:

Lease Length: sec Ping Timeout: ms

Domain Name:

Enabling auto-configuration causes the DHCP server to automatically configure DNS, WINS and domain name. The values in the fields above take precedence over the auto-configured values.

Enable auto-configuration from interface:

outside ▾

At the bottom, there are five buttons: '< Back', 'Next', 'Finish', 'Cancel', and 'Help'. The 'Next' button is highlighted with a green box and a mouse cursor is pointing at it.

ウィザード

Startup Wizard Cisco ASDM 6.4 for ASA - 192.168.1.1 - Startup Wizard

Address Translation (NAT/PAT) (Step 7 of 10)

Select Port Address Translation (PAT) to share a single external IP address for devices on the inside interface. Select Network Address Translation (NAT) to share several external IP addresses for devices on the inside interface. Select the first option, if no address translation is desired between the inside and outside interfaces.

This NAT configuration applies to all the traffic from the inside interface to the outside interface.

- No Address Translation
- Use Port Address Translation (PAT)
 - Use the IP address on the outside interface
 - Specify an IP address
- Use Network Address Translation (NAT)

IP Address: []

IP Address Range: []

Buttons: < Back, Next >, Finish, Cancel, Help

インターフェイスのIP アドレスを使用して PAT 変換を行う

ウィザードを使った設定 ASDM へアクセスする端末の設定

Cisco ASDM 6.4 for ASA - 192.168.1.1 - Startup Wizard

Startup Wizard

Administrative Access (Step 8 of 10)

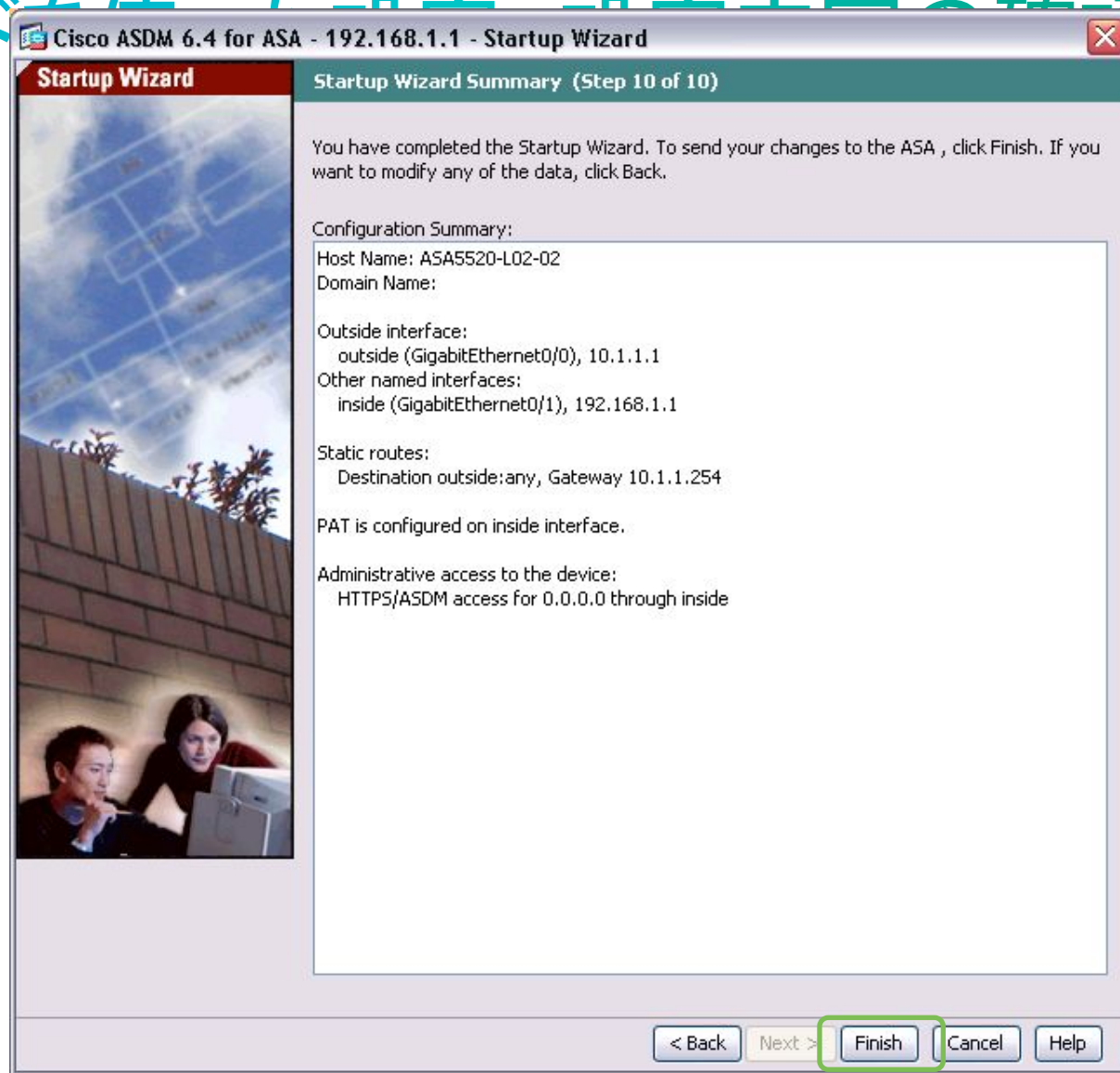
Specify the addresses of all hosts or networks, which are allowed to access the ASA using HTTPS/ASDM, SSH or Telnet.

Type	Interface	IP Address	Mask/ Prefix Length
HTTPS/ASDM	inside	0.0.0.0	0.0.0.0

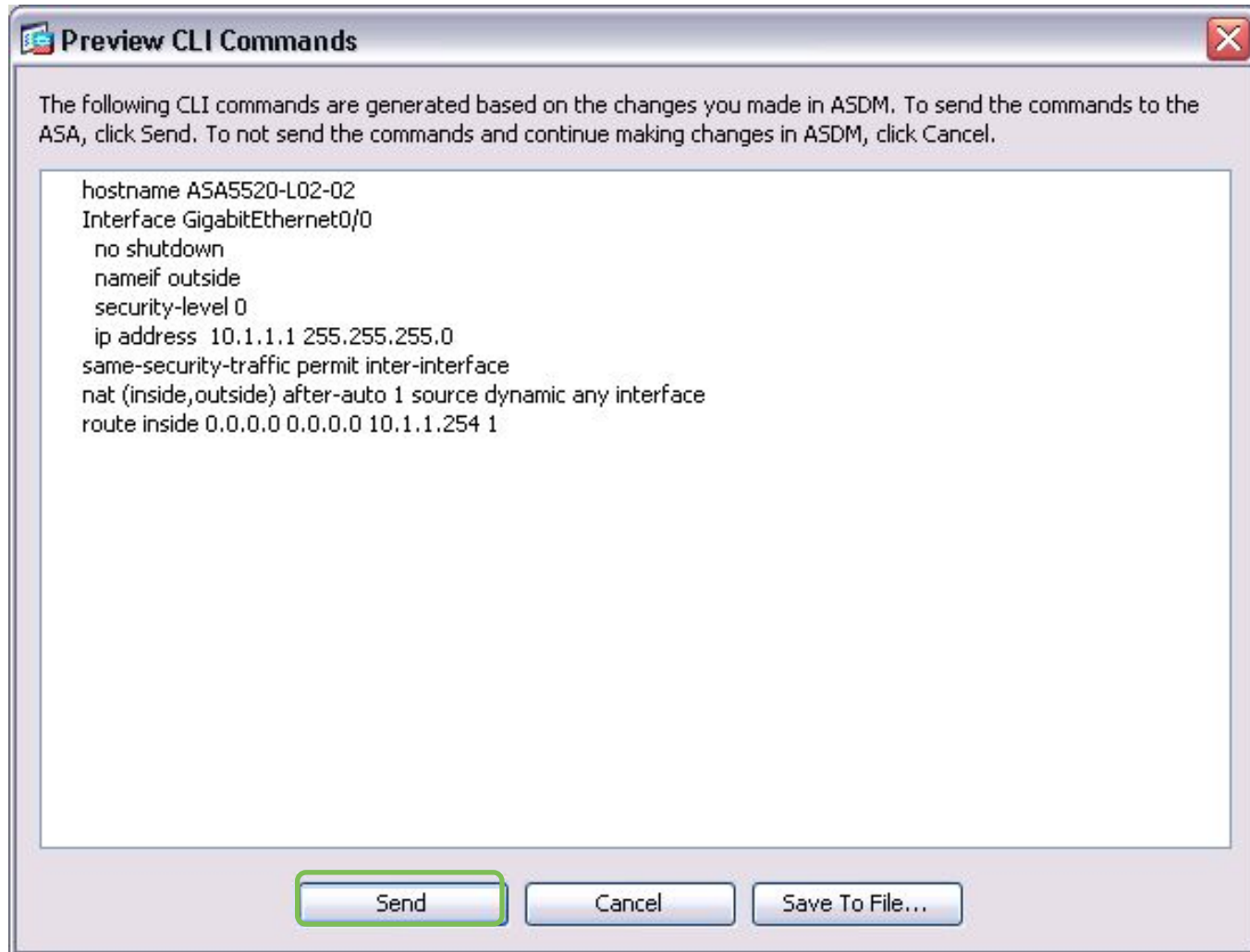
Enable HTTP server for HTTPS/ASDM access
Disabling HTTP server will prevent HTTPS/ASDM access to this ASA.

Enable ASDM history metrics

ウィザード



ウィザードを使った設定 CLI 表示



Thank you.

