

パケットトレーサで学ぶNW構築 (基礎編その2)

Firewallで必要な通信を許可しよう！



お 品 書 き

1 Firewallの基礎

- (1) Firewallとは？
- (2) Firewallによるフィルタリング方式
- (3) ステートフルインスペクションの動作

2 Cisco ASAの概要

- (1) CiscoASAとは？
- (2) ASAにおけるインタフェース設定について
- (3) ASAでの設定例
 - ア パケットフィルタリング方式の例
 - イ ステートフルインスペクション方式の例

3 Firewall設定と確認

- (1) 構成条件
- (2) 今回の設定要領
 - ア パケットフィルタリング方式
 - イ ステートフルインスペクション方式

4 参考資料

Firewall(ASA)での基本的な通信制御～その1

<https://hetare-nw.net/archives/1426>

Firewall(ASA)での基本的な通信制御～その2

<https://hetare-nw.net/archives/1436>

Firewall(ASA)での基本的な通信制御～その3

<https://hetare-nw.net/archives/1445>

今回使用するパケットトレーサファイルは以下の3つになります。

ASA-Base-drop.pkt

(ASAのインタフェース特性を確認する)

ASA-Packet-Filtering.pkt

(ASAでのパケットフィルタリング設定済)

ASA-Statefull-FW.pkt

(ASAでのステートフルインスペクション設定済)

Sougo-1-Mihon-FW.pkt

(総合実習でのNWにASAを追加)

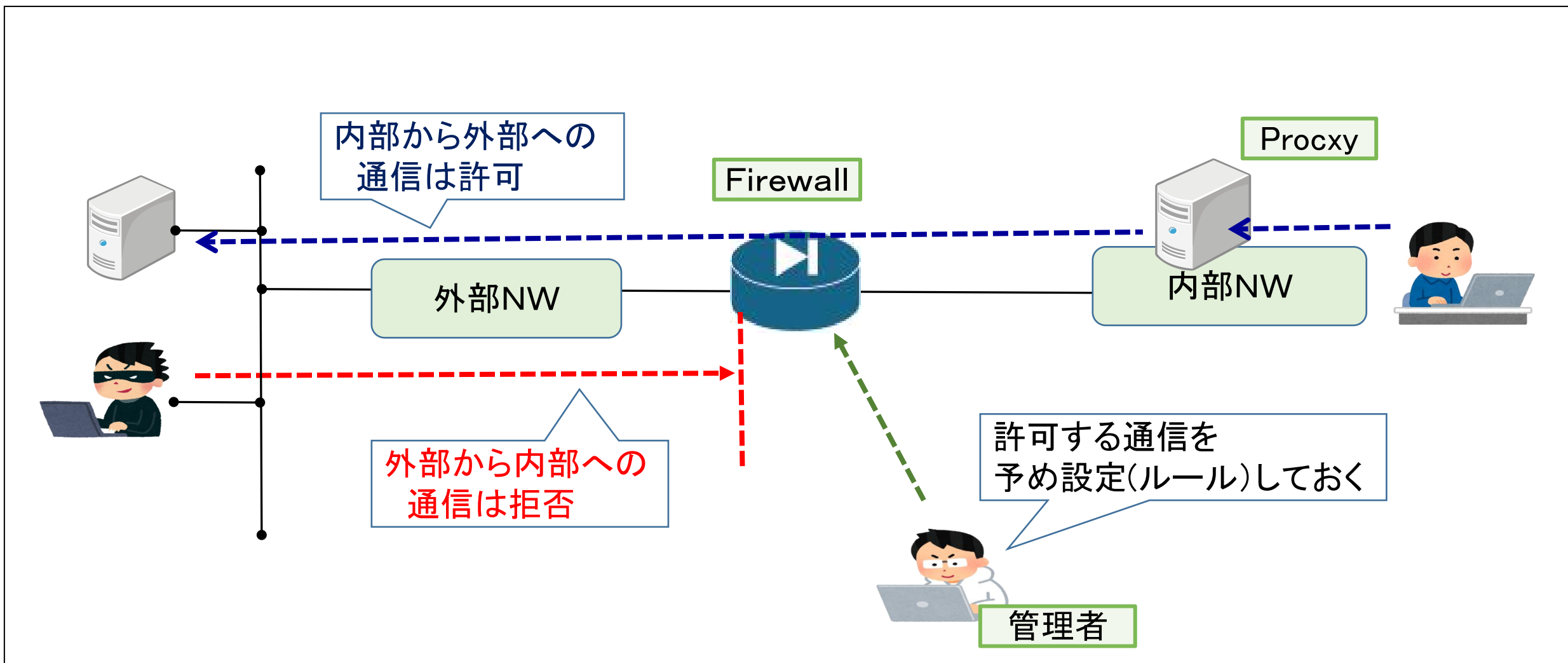
1

Firewallの基礎

1 Firewallの基礎

Firewallとは？

内部のコンピュータネットワークと外部との通信を、内部のコンピュータネットワークの安全を維持することを目的とした物（ソフトウェアもしくはハードウェア）



1 Firewallの基礎

(2) Firewallによるフィルタリング方式

1 Firewallの基礎

(2) ファイアウォールによるフィルタリング方式

フィルタリングの方式は以下の3つになります。

① パケットフィルタリング型(ステートレス)

パケットのヘッダ情報に含まれるIPアドレス、ポート番号に基づいて
フィルタリングを行う

② アプリケーションレベルゲートウェイ型

プロトコルごとにプロキシ(中継専用プログラム)をもち、パケットのアプリケーション層も含めた情報に基づいてフィルタリングを行う

現在、主流

③ ステートフルインスペクション型(ステートフル)

セッション(通信の開始から終了まで管理する単位)の状態を管理して、
常にその情報に基づいてフィルタリングを行う。

今回は① パケットフィルタリング型 と ③ ステートフルインスペクション型 の実習を行います！！

1 Firewallの基礎

(2) ファイアウォールによるフィルタリング方式

ステートフルインスペクション型FWの動作

フィルタリングルールとコネクションテーブル双方が連携して動作

【フィルタリングルール】: 管理者が設定

どんな通信を許可し、どんな通信を拒否するかを定義している設定です。

設定項目:

送信元IPアドレス、宛先IPアドレス、プロトコル、送信元ポート番号、
通信制御 などがあります。

【コネクションテーブル】: 通過する通信により動的に作成

自身を経由するコネクションの情報を管理しているテーブル

管理項目:

送信元IPアドレス、宛先IPアドレス、プロトコル、送信元IPポート番号、
宛先ポート番号、コネクションの状態、アイドルタイムアウト
などがあります。

1 Firewallの基礎

(2) ファイアウォールによるフィルタリング方式

ステートフルインスペクション型FWの動作

フィルタリングルールとコネクションテーブル双方が連携して動作

動作イメージ

FW管理者



【フィルタリングルール】
あらかじめ設定を定義

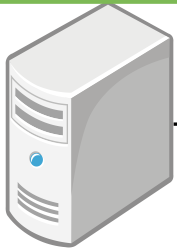
動的に作成！



【コネクションテーブル】

自身を経由する通信を
フィルタリングルールに
より許可しかつ変更

サーバ



Firewall



クライアント



フィルタリングルールにより通過を許可
コネクションテーブルにより通過を許可

2 Cisco ASAの概要

(1) Cisco ASAとは？？

2 Cisco ASAの概要

(1) Cisco ASAとは？

Cisco ASA シリーズは、豊富な実績を持つ複数のセキュリティテクノロジーを単一のプラットフォーム内に統合した適応型セキュリティアプライアンスです

今回についてはパケットレーサーで利用できる以下の装置を使用します。

CISCO ASA 5506



今回はCLIモードで基本的な設定を実施し、Firewall機能を体験します！



パケットレーサーで利用できるASAの機能は残念ながら限定されています。。
が一般的なFirewallの機能を理解するのには十分です！

2 Cisco ASAの概要

(2) ASAにおけるインタフェース設定について

2 Cisco ASAの概要

(2) ASAにおけるインタフェース設定について

CISCOルータと大きく違うのは「nameif」および「security-level」が存在します。

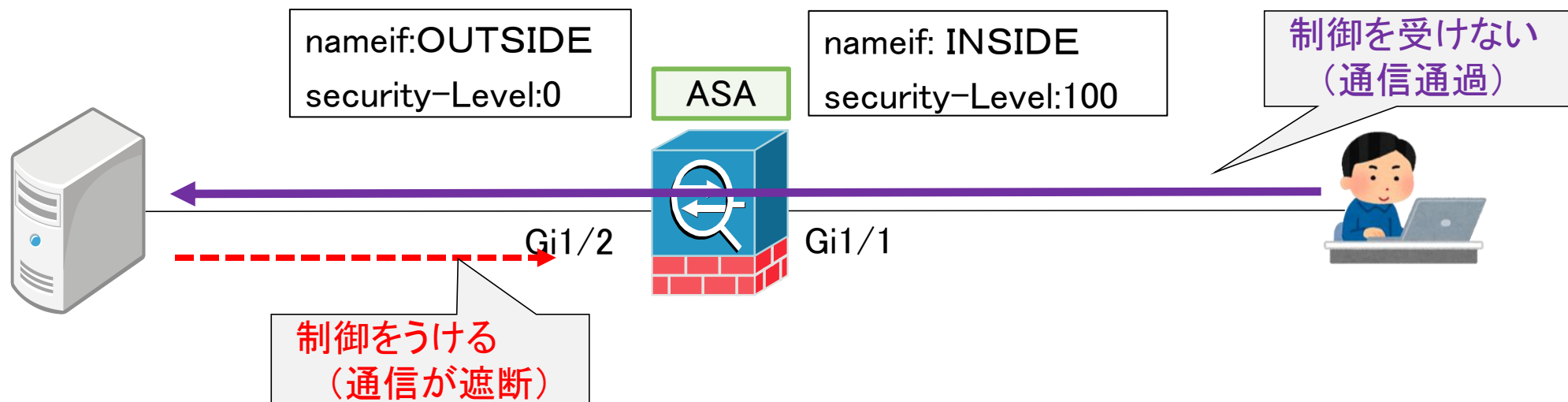
「nameif」: インタフェースの名前(任意の名前を設定できます)

「security-level」: nameifに関連づく、セキュリティの強さです。

セキュリティレベルの高いnameifから低いnameifに通信するときは、基本的には素通りします。

セキュリティレベルの低いnameif から高いnameifに通信するときは、制御がかかります。

例



上記の例で説明すると

nameif: INSIDE (Gi1/1) → nameif: OUTSIDE (Gi1/2) に出っていく通信は制御無しで通りますがその戻り通信は制御を受けることになります。

2 Cisco ASAの概要

(2) ASAにおけるインタフェース設定について

インタフェース設定における通信の状態を確認しましょう！

次の図に示すNW構成を実施します
(構成)

① ASAのインターフェースに対して以下の条件で設定を実施します

- ・Gi1/3を「UCHI」、セキュリティレベル50
- ・Gi1/4を「SOTO」、セキュリティレベル20

② OSPFの設定を実施します。

(確認)

③ L3-SW⇔ASA R ⇔ ASA間で経路情報を交換できることを確認します

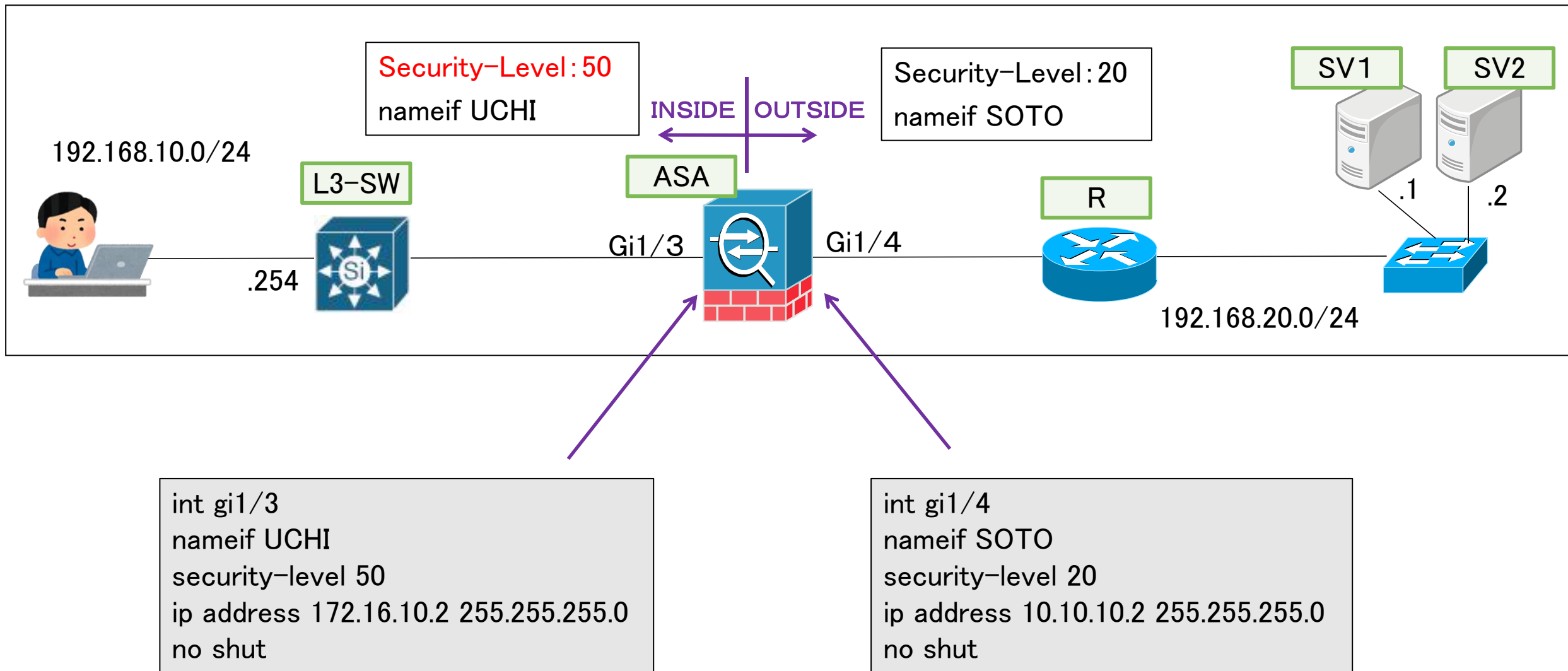
④ PC⇔サーバ間のPingを実施し、失敗することを確認してください。

サンプルパケットキャプチャファイルは”ASA-Base-Drop.pkt”になります

2 Cisco ASAの概要

(2) ASAにおけるインタフェース設定について

① ASAのインターフェースに対して以下の条件で設定を実施します



2 Cisco ASAの概要

(2) ASAにおけるインタフェース設定について

① ASAのインターフェースに対して以下の条件で設定を実施します

○設定後、ASAのインタフェースの情報を確認します。

ASA5506

Physical Config CLI Attributes

IOS Command Line Interface

```
ciscoasa(config)#
ciscoasa(config)#
ciscoasa(config)#
ciscoasa(config)#
ciscoasa(config)#
ciscoasa(config)#
ciscoasa(config)#do show inter
ciscoasa(config)#exit
ciscoasa#
ciscoasa#
ciscoasa#show inter
ciscoasa#show interface ip br
ciscoasa#show interface ip brief
```

Interface	IP-Address	OK?	Method	Status
Virtual0	127.1.0.1	YES	unset	up
GigabitEthernet1/1	unassigned	YES	unset	administratively down
GigabitEthernet1/2	unassigned	YES	unset	administratively down
GigabitEthernet1/3	172.16.10.2	YES	manual	up
GigabitEthernet1/4	10.10.10.2	YES	manual	up
GigabitEthernet1/5	unassigned	YES	unset	administratively down
GigabitEthernet1/6	unassigned	YES	unset	administratively down
GigabitEthernet1/7	unassigned	YES	unset	administratively down
GigabitEthernet1/8	unassigned	YES	unset	administratively down
Management1/1	unassigned	YES	unset	administratively down
Internal-Controll1/1	127.0.1.1	YES	unset	up
Internal-Datal1/1	unassigned	YES	unset	up
Internal-Datal2	unassigned	YES	unset	up
Internal-Datal3	unassigned	YES	unset	up

ciscoasa#

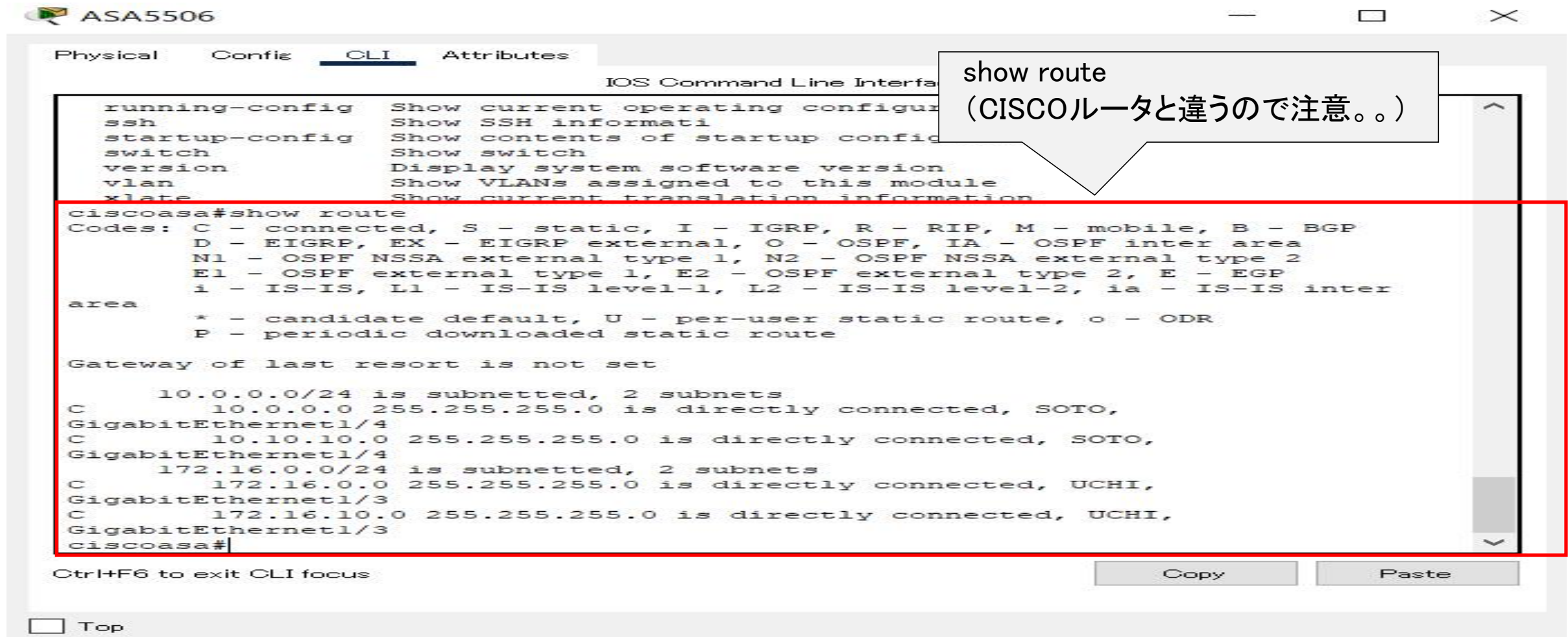
show interface ip brief
(CISCOルータと違うので注意。。)

2 Cisco ASAの概要

(2) ASAにおけるインタフェース設定について

① ASAのインターフェースに対して以下の条件で設定を実施します

○設定後、ASAの経路情報を確認します。



The screenshot shows the Cisco ASA CLI interface with the 'show route' command executed. The output displays the routing table, including connected interfaces and static routes. A red box highlights the output text, and a callout bubble points to the command name.

show route
(CISCOルータと違うので注意。。)

```
ciscoasa#show route
Codes: C - connected, S - static, I - IGRP, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2, E - EGP
       i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter
       area
       * - candidate default, U - per-user static route, o - ODR
       P - periodic downloaded static route

Gateway of last resort is not set

 10.0.0.0/24 is subnetted, 2 subnets
C    10.0.0.0 255.255.255.0 is directly connected, SOTO,
GigabitEthernet1/4
C    10.10.10.0 255.255.255.0 is directly connected, SOTO,
GigabitEthernet1/4
 172.16.0.0/24 is subnetted, 2 subnets
C    172.16.0.0 255.255.255.0 is directly connected, UCHI,
GigabitEthernet1/3
C    172.16.10.0 255.255.255.0 is directly connected, UCHI,
GigabitEthernet1/3
ciscoasa#
```

Ctrl+H6 to exit CLI focus

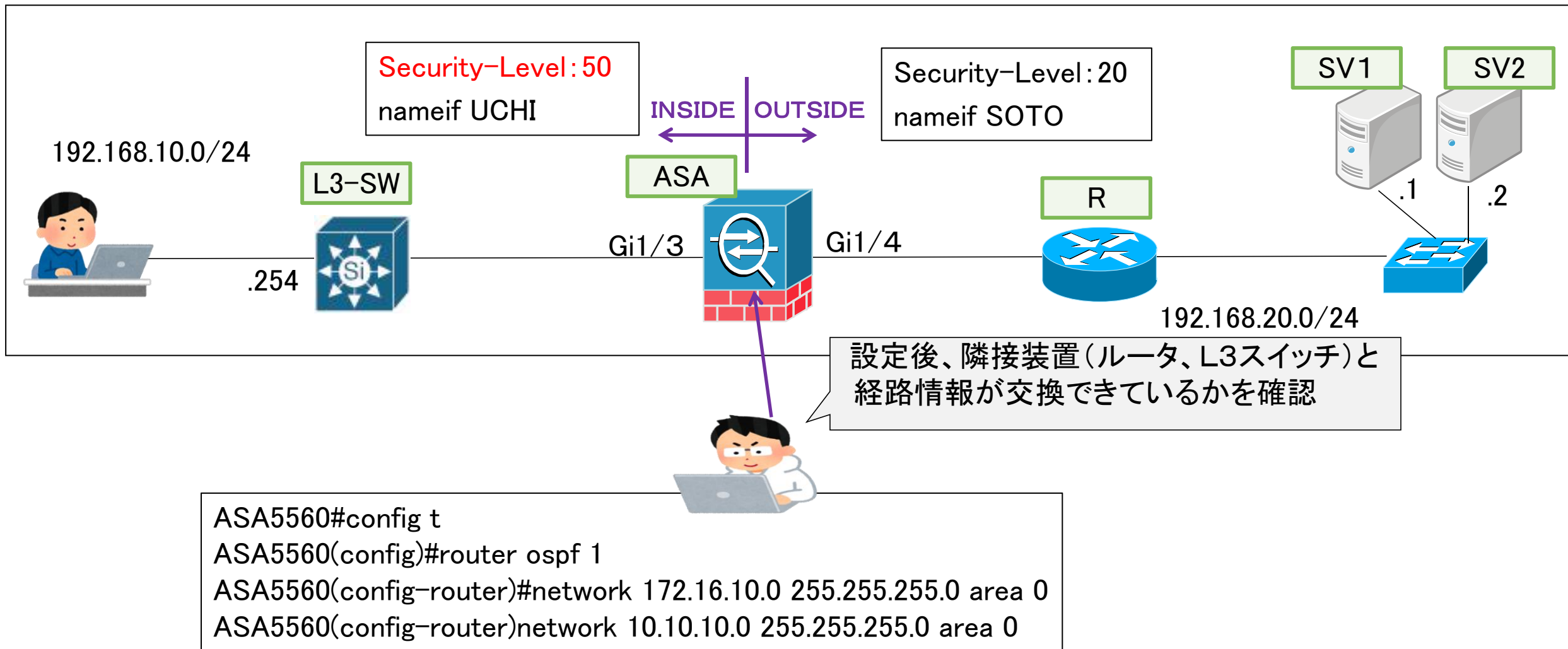
Copy Paste

Top

2 Cisco ASAの概要

(2) ASAにおけるインタフェース設定について

② OSPFの設定を実施します



2 Cisco ASAの概要

(2) ASAにおけるインタフェース設定について

③ L3-SW⇔ASA R ⇔ ASA間で経路情報を交換できることを確認します

ASA5506

Physical

Config

CLI

Attributes

IOS Command Line Interface

```
ciscoasa#
ciscoasa#
ciscoasa#
ciscoasa#show route
Codes: C - connected, S - static, I - IGRP, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2, E - EGP
       i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter
       area
       * - candidate default, U - per-user static route, o - ODR
       P - periodic downloaded static route

Gateway of last resort is not set

  10.0.0.0/24 is subnetted, 2 subnets
C      10.0.0.0 255.255.255.0 is directly connected, SOTO,
GigabitEthernet1/4
C      10.10.10.0 255.255.255.0 is directly connected, SOTO,
GigabitEthernet1/4
  172.16.0.0/24 is subnetted, 2 subnets
C      172.16.0.0 255.255.255.0 is directly connected, UCHI,
GigabitEthernet1/3
C      172.16.10.0 255.255.255.0 is directly connected, UCHI,
GigabitEthernet1/3
O      192.168.10.0 255.255.255.0 [110/2] via 172.16.10.1, UCHI, 00:00:23,
GigabitEthernet1/3
O      192.168.20.0 255.255.255.0 [110/2] via 10.10.10.1, SOTO, 00:00:01,
GigabitEthernet1/4
ciscoasa#
```

Ctrl+F6 to exit CLI focus

Copy

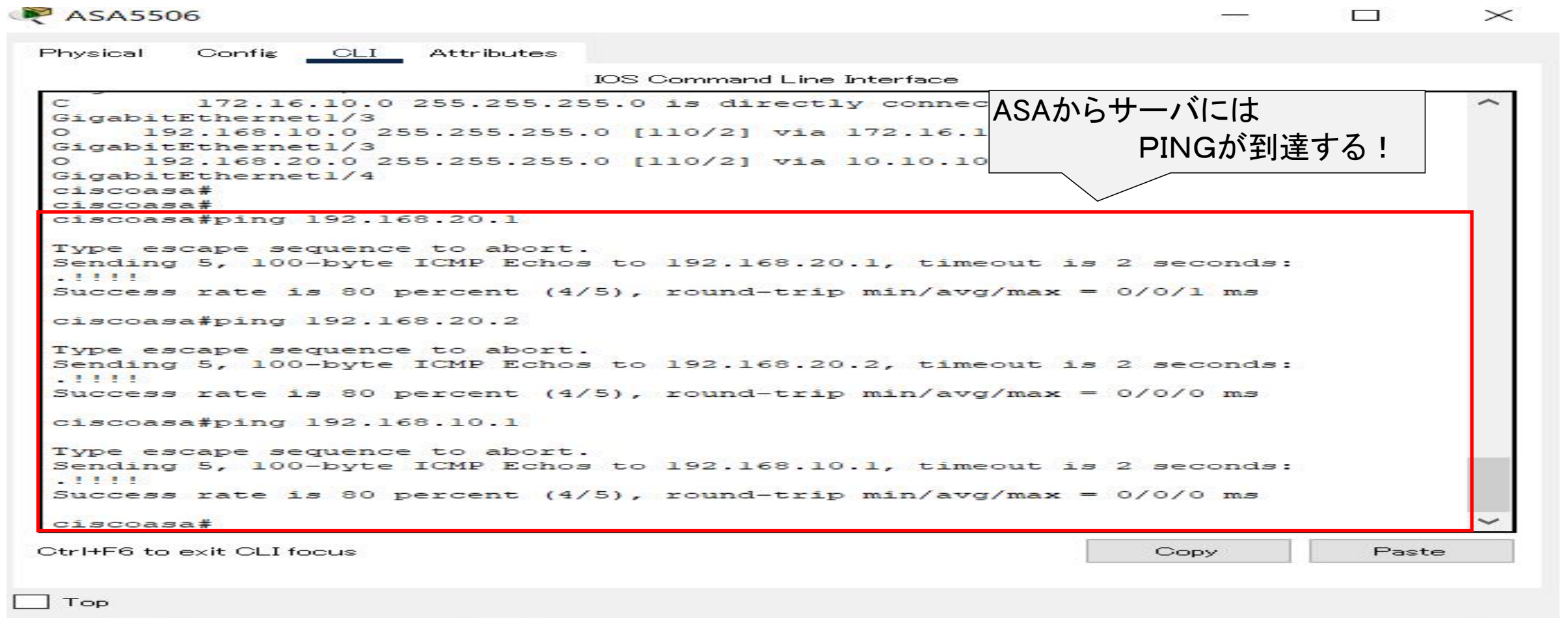
Paste

2 Cisco ASAの概要

(2) ASAにおけるインタフェース設定について

② OSPFの設定を実施します

- PINGにより疎通確認を実施します



The screenshot shows the Cisco ASA CLI interface with the following content:

```
ASA5506
Physical Config CLI Attributes
IOS Command Line Interface
C 172.16.10.0 255.255.255.0 is directly connected to GigabitEthernet1/3
O 192.168.10.0 255.255.255.0 [110/2] via 172.16.10.1 GigabitEthernet1/3
O 192.168.20.0 255.255.255.0 [110/2] via 10.10.10.1 GigabitEthernet1/4
ciscoasa#
ciscoasa#
ciscoasa#ping 192.168.20.1
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.20.1, timeout is 2 seconds:
.!!!!
Success rate is 80 percent (4/5), round-trip min/avg/max = 0/0/1 ms
ciscoasa#ping 192.168.20.2
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.20.2, timeout is 2 seconds:
.!!!!
Success rate is 80 percent (4/5), round-trip min/avg/max = 0/0/0 ms
ciscoasa#ping 192.168.10.1
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.10.1, timeout is 2 seconds:
.!!!!
Success rate is 80 percent (4/5), round-trip min/avg/max = 0/0/0 ms
ciscoasa#
```

A callout box points to the ping results, stating: "ASAからサーバには PINGが到達する！"

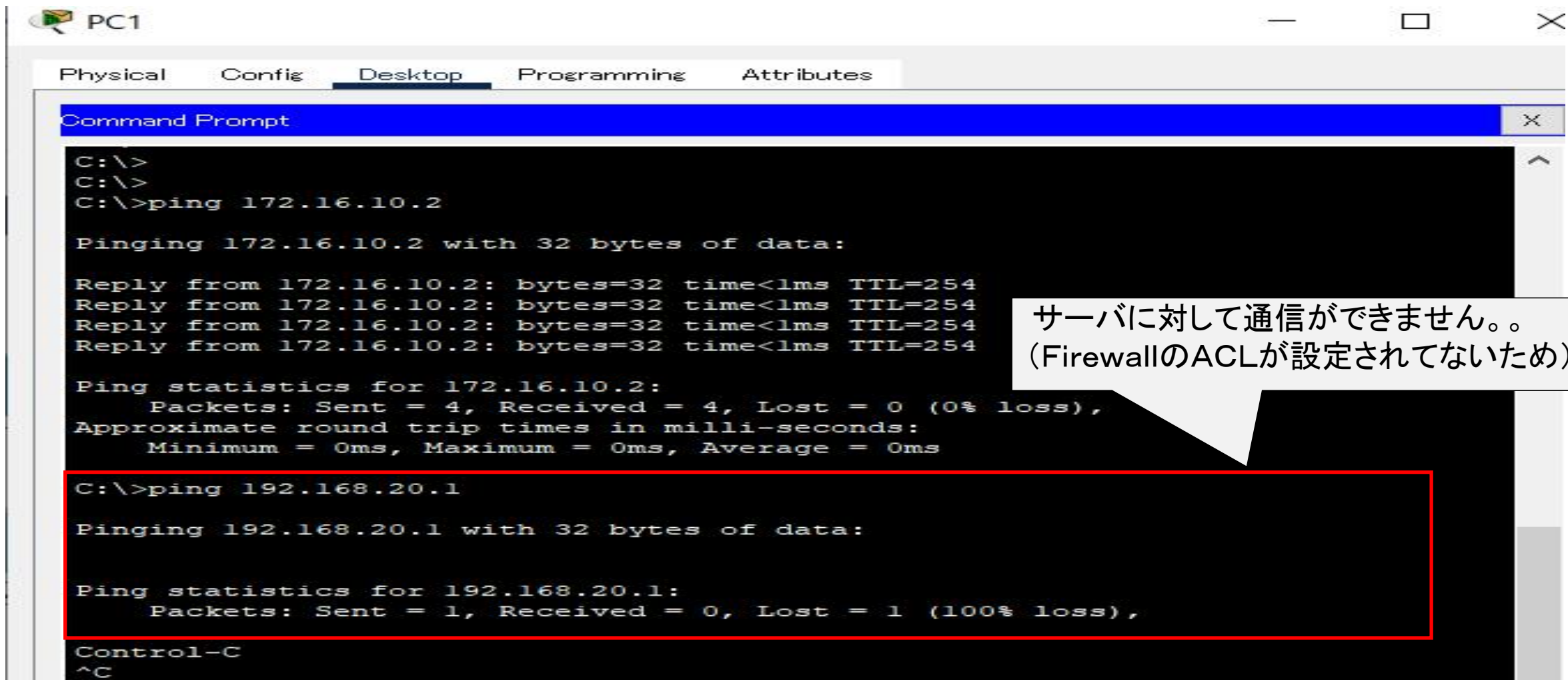
At the bottom of the window, there are buttons for "Copy" and "Paste", and a "Top" link.

2 Cisco ASAの概要

(2) ASAにおけるインタフェース設定について

④ PC⇔サーバ間のPingを実施し、失敗することを確認してください。

○ PC1からのPING結果



```
C:\>
C:\>
C:\>ping 172.16.10.2

Pinging 172.16.10.2 with 32 bytes of data:

Reply from 172.16.10.2: bytes=32 time<1ms TTL=254
Reply from 172.16.10.2: bytes=32 time<1ms TTL=254
Reply from 172.16.10.2: bytes=32 time<1ms TTL=254
Reply from 172.16.10.2: bytes=32 time<1ms TTL=254

Ping statistics for 172.16.10.2:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 0ms, Average = 0ms

C:\>ping 192.168.20.1

Pinging 192.168.20.1 with 32 bytes of data:

Ping statistics for 192.168.20.1:
    Packets: Sent = 1, Received = 0, Lost = 1 (100% loss),

Control-C
^C
```

サーバに対して通信ができません。
(FirewallのACLが設定されていないため)

2 Cisco ASAの概要

(2) ASAにおけるインタフェース設定について

○ シミュレーションモードを使って通信がどこまで確立していたかを見てみましょう！

○ シミュレーションモードとは？

Packet Tracerには、パケットレベルでのやり取りを視覚的に確認することができるモードです。

Cisco Packet Tracer - C:\Users\ユーザー\Desktop\勉強関連\cisco\ASAでの基本的な通信制御_初期.pkt

File Edit Options View Tools Extensions Window Help

Logical Physical x: 441, y: 147

パケットのやり取りが視覚的に確認可能！

Event Listを確認することにより段階的にパケットのやり取りを確認可能

Simulation Panel

Vis.	Time(sec)	Last Device	At Device	Type
	0.002	L3SW	ASA5506	ICMP
	0.003	ASA5506	RT	ICMP
	0.004	RT	L2SW	ICMP
	0.005	L2SW	SV1	ICMP
	0.006	SV1	L2SW	ICMP
	0.007	L2SW	RT	ICMP
<input checked="" type="checkbox"/>	0.008	RT	ASA5506	ICMP

Reset Simulation ☒ Constant Delay Captured to: 0.008 s

Play Controls

Simulationボタンを押す

Event List Filters - Visible Events
ICMP, OSPF

Edit Filters Show All/None

Time: 00:38:41.321 PLAY CONTROLS: [Previous] [Play] [Next]

Scenario 0

New Delete

Toggle PDU List Window

Fire Last Status Source Destination Type Color

2 Cisco ASAの概要

(2) ASAにおけるインタフェース設定について

- シミュレーションモードを使って通信がどこまで確立していたかを見てみましょう！

シミュレーションモードによる確認要領

サンプルパケットキャプチャファイルは”ASA-Base-Drop.pkt”を起動します

右下の”シミュレーション”ボタンを押します

PC-PT PC1からサーバ 192.168.20.1に対してPINGを送信します。

Play Controlsの右ボタンをクリックしながら右上のEventlistの動作を確認します

サーバ 192.168.20.1からの応答パケットがASAで廃棄されているのを確認します

つまり

SecurityLevelが高いインタフェースから送信されたPINGはASAを通過しますが。。

SecuirtyLevelが低いインタフェースから入力されたPING応答パケットは通過できずASAで破棄されていることが確認できます。。

2 Cisco ASAの概要

(2) ASAにおけるインタフェース設定について

シュミレーションモードによる確認要領

右下の”シュミレーション”ボタンを押します

The screenshot displays the Cisco Packet Tracer interface. The main workspace shows a network topology with the following components and connections:

- PC-PT PC1** (IP: 192.168.10.1) connected to **3560-24PS L3SW** (Fa0/1, IP: 192.168.10.254) via VLAN192.
- 3560-24PS L3SW** connected to **5506-X ASA5506** (Gi0/1, IP: 172.16.10.1) via VLAN172.
- 5506-X ASA5506** connected to **1941 RT** (Gi0/1, IP: 192.168.20.1) via a 10.10.10.0/24 network.
- 1941 RT** connected to **2960-24 L2SW** (G0/0, IP: 192.168.20.254) via a 192.168.20.0/24 network.
- 2960-24 L2SW** connected to **Server-PT SV1** (IP: 192.168.20.1) and **Server-PT SV2** (IP: 192.168.20.2) via a 192.168.20.0/24 network.

The ASA is configured with OSPF1. The simulation panel on the right shows the Event List and Play Controls. A red box highlights the 'Simulation' button in the bottom right corner.

Simulation

2 Cisco ASAの概要

(2) ASAにおけるインタフェース設定について

PC-PT PC1からサーバ 192.168.20.1に対してPINGを送信します。

The diagram illustrates a network topology in Cisco Packet Tracer. A PC (PC1) is connected to a switch (3560-24PS L3SW) via Fa0/1. The switch is connected to a router (1941 RT) via Gi0/1. The router is connected to a firewall (ASA5506) via Gi1/3. The firewall is connected to a switch (2960-24T L2SW) via Gi1/4. The switch is connected to two servers (Server-PT SV1 and Server-PT SV2) via G0/0. The firewall has two interfaces: inside (10.10.10.0/24) and outside (192.168.20.0/24). A callout points to the firewall with the text: "ASAでパケットが破棄されていることを確認。" (Confirm that packets are being dropped by ASA).

A command prompt window on PC1 shows the following output:

```
Cisco Packet Tracer PC Command Line 1.0
C:\>ping 192.168.20.1

Pinging 192.168.20.1 with 32 bytes of data:

Request timed out.
```

A callout points to the command prompt with the text: "PINGがTimeoutしている。。" (PING is timing out...).

The Simulation Panel on the right shows the Event List:

Vis.	Time(sec)	Last Device
	0.000	--
	0.002	--
	0.003	PC1
	0.004	L3SW
	0.005	ASA5506
	6.005	--
	6.006	PC1
	6.007	L3SW
	6.008	ASA5506
	6.009	RT
	6.010	L2SW
	6.011	SV1
	6.012	L2SW
	6.013	RT

A callout points to the Play Controls in the Simulation Panel with the text: "Play Controlsをクリック → 通信の流れ確認" (Click Play Controls → Confirm the flow of communication).

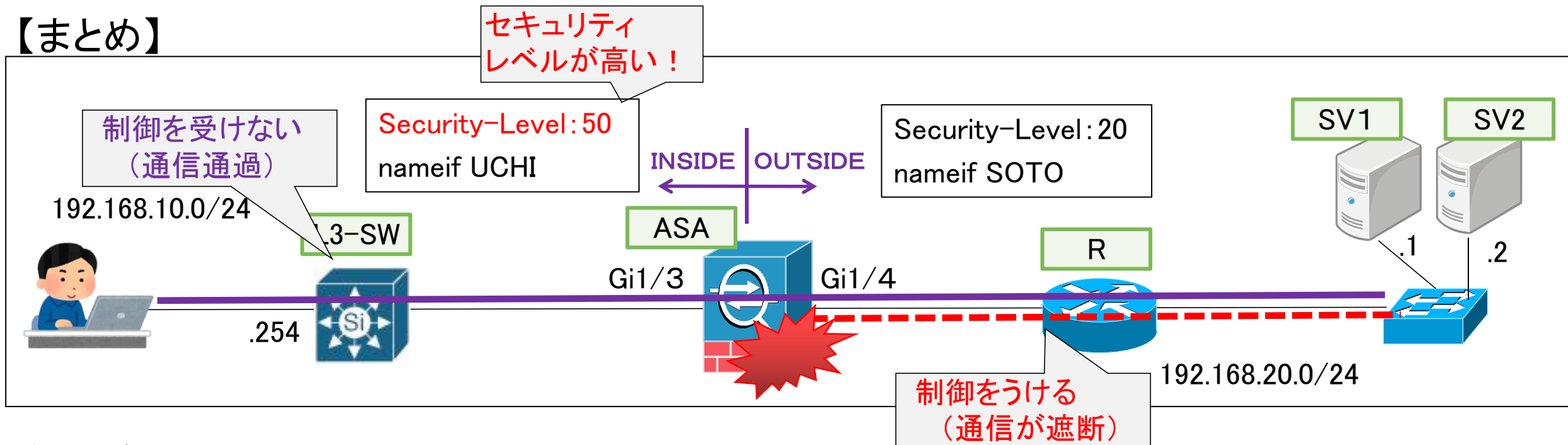
The Simulation Panel also shows the Event List Filters - Visible Events: ICMP, OSPF. The bottom of the panel has buttons for Event List, Realtime, and Simulation.

Simulation

2 Cisco ASAの概要

(2) ASAにおけるインタフェース設定について

【まとめ】



今回の例では

nameif:INSIDE (Gi1/3) → nameif:OUTSIDE (Gi1/4) に出ていく通信は制御無しで通りますがその戻り通信は制御を受けることになります。

そのため、次ページで紹介する2つの方法のどちらかを設定する必要があります！

- 1 パケットフィルタリング方式
- 2 ステートフルインスペクション方式



2 Cisco ASAの概要

(3) ASAでの設定例

パケットフィルタリング方式

2 Cisco ASAの概要

(3) ASAでの設定例

パケットフィルタリング方式

【実習内容】

① 設定したFirewallに対して以下のフィルタリング設定を実施

ア フィルタリングするためのaccess-listを設定します

- ・ PC1からSV1に対してはHTTPのみ許可
- ・ PC1からSV2に対してはICMPのみ許可
- ・ OSPF通信を許可

イ アで作成したaccess-listをインタフェースに適用します（適用インタフェース "SOTO"）

② PC1 ⇒ SV1に対してHTTP通信が可能か確認します

PC1 ⇒ SV2に対してICMP通信が可能かを確認します。

ASA-Packet-Filtering.pkt

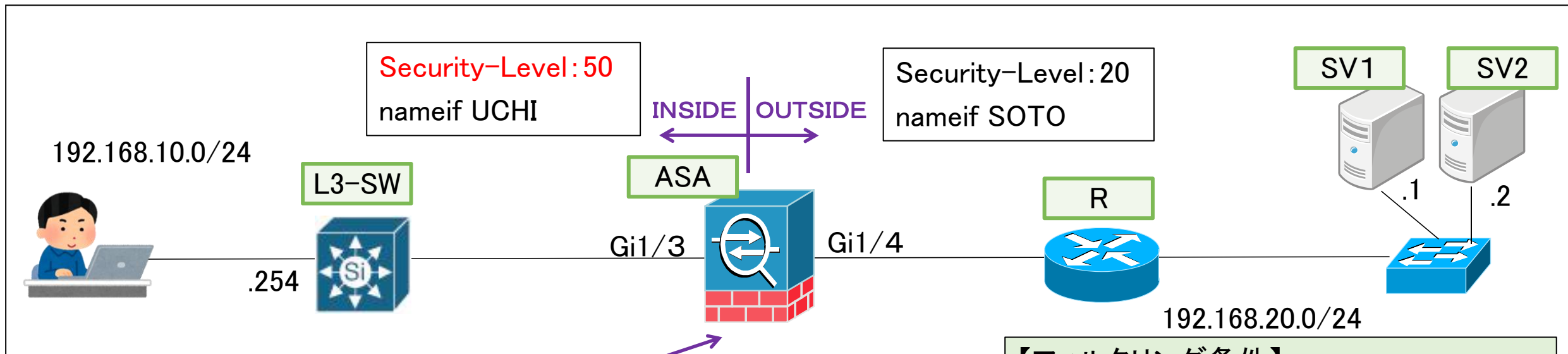
（ASAでのパケットフィルタリング設定済）

2 Cisco ASAの概要

(3) ASAでの設定例

パケットフィルタリング方式

① 設定したFirewallに対して以下のフィルタリング設定を実施



【フィルタリング条件】
PC1からSV1に対してはHTTPのみ許可
PC1からSV2に対してはICMPのみ許可
OSPF通信を許可

```
# conf t
(config)# access-list SOTO-to-UCHI extended permit tcp host 192.168.20.1 host 192.168.10.1
(config)# access-list SOTO-to-UCHI extended permit icmp host 192.168.20.2 host 192.168.10.1
(config)# access-list SOTO-to-UCHI extended permit ip host 10.10.10.1 host 10.10.10.2
(config)# access-list SOTO-to-UCHI extended permit ip host 10.10.10.1 host 224.0.0.5
(config)# access-group SOTO-to-UCHI in interface SOTO
```

/イ) アを インタフェース "SOTO"に適用

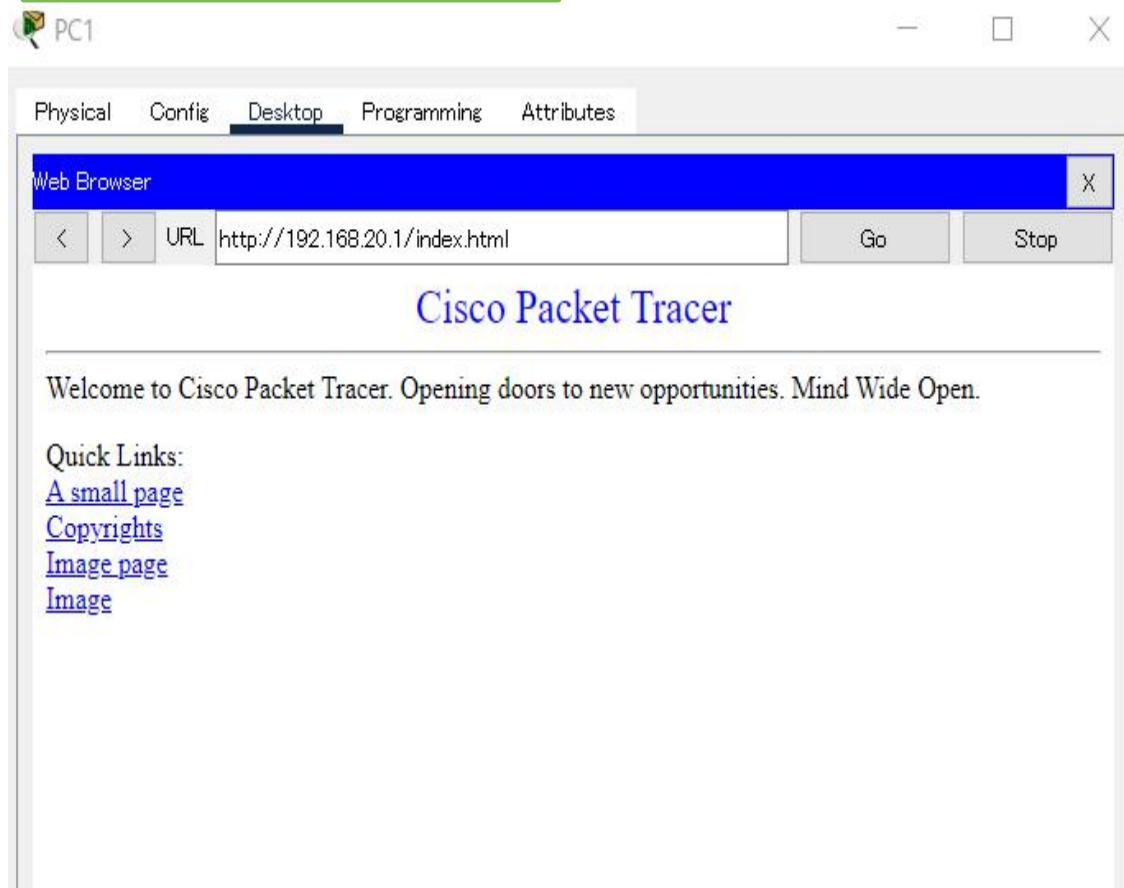
2 Cisco ASAの概要

(3) ASAでの設定例

パケットフィルタリング方式

- ② PC1 ⇒ SV1に対してHTTP通信が可能か確認します
PC1 ⇒ SV2に対してICMP通信が可能かを確認します。

PC⇒SV1へHTTP



PC⇒SV2へPING

```
C:\>ping 192.168.20.2

Pinging 192.168.20.2 with 32 bytes of data:

Reply from 192.168.20.2: bytes=32 time<1ms TTL=125
Reply from 192.168.20.2: bytes=32 time<1ms TTL=125
Reply from 192.168.20.2: bytes=32 time<1ms TTL=125
Reply from 192.168.20.2: bytes=32 time<1ms TTL=125

Ping statistics for 192.168.20.2:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 0ms, Average = 0ms

C:\>
```

2 Cisco ASAの概要

(3) ASAでの設定例

ステートフルインスペクション例

2 Cisco ASAの概要

(3) ASAでの設定例

ステートフルインスペクション方式

【実習内容】

① ～その2～で設定したACL設定を削除します

② ステートフルインスペクション設定を実施します

<1> クラスマップでインスペクションする
プロトコルを指定

<2> クラスマップをポリシーマップに適用し
サービスポリシーに適用

③ 設定後、通信確認を実施します

ア PC → SV1、SV2にICMP、SV1にHTTP通信ができることを確認

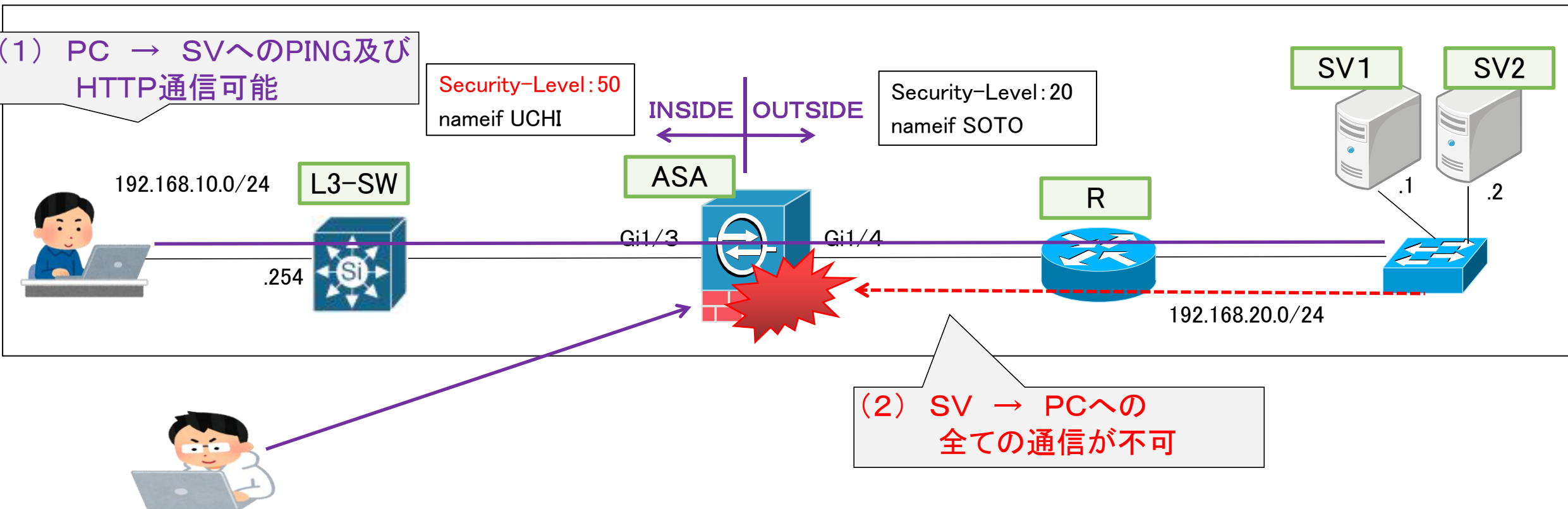
イ SV1, 2 → PCにICMP通信ができないことを確認

2 Cisco ASAの概要

(3) ASAでの設定例

ステートフルインスペクション方式

② ステートフルインスペクション設定を実施します



② ステートフルインスペクション設定を実施します

- <1> クラスマップでインスペクションする
プロトコルを指定
- <2> クラスマップをポリシーマップに適用し
サービスポリシーに適用

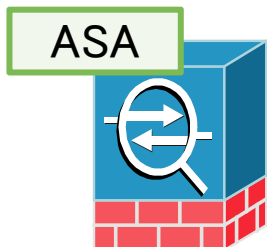
2 Cisco ASAの概要

(3) ASAでの設定例

② ステートフルインスペクション設定を実施します

ステートフルインスペクション方式

- <1> クラスマップでインスペクションするプロトコルを指定
- <2> クラスマップをポリシーマップに適用しサービスポリシーに適用



```
# conf t
(config)# class-map CMAP          / CMAPというクラスマップを設定
(config-cmap)# match default-inspection-traffic
(config-cmap)# exit
(config)# policy-map PMAP         / PMAPというポリシーマップを設定
(config-pmap)# class CMAP        / クラスマップCMAPと紐付けする
(config-pmap-c)# inspect icmp    / ICMPを許可
(config-pmap-c)# inspect http    / HTTPを許可
(config-pmap-c)# exit
(config)#
(config)# service-policy PMAP global / PMAPを適用
(config)# end
```

2 Cisco ASAの概要

(3) ASAでの設定例

ステートフルインスペクション方式

② ステートフルインスペクション設定を実施します

```
ciscoasa#configure terminal
ciscoasa(config)#class-map CMAP
ciscoasa(config-cmap)#match default-inspection-traffic
ciscoasa(config-cmap)#exit
ciscoasa(config)#policy-map PMAP
ciscoasa(config-pmap)#class CMAP
ciscoasa(config-pmap-c)#inspect icmp
ciscoasa(config-pmap-c)#inspect http
ciscoasa(config-pmap-c)#exit
ciscoasa(config)#
ciscoasa(config)#service-policy PMAP global
ciscoasa(config)#
ciscoasa(config)#exit
ciscoasa#
ciscoasa#copy running-config startup-config
Source filename [running-config]?
Cryptochecksum: 11e63ab2 4c1533c5 39526ecd 32d13356

1363 bytes copied in 2.786 secs (489 bytes/sec)
```

2 Cisco ASAの概要

(3) ASAでの設定例

ステートフルインスペクション方式

③ 設定後、通信確認を実施します

ア PC → SV1、SV2にICMP、SV1にHTTP通信ができることを確認

イ SV1, 2 → PCにICMP通信ができないことを確認

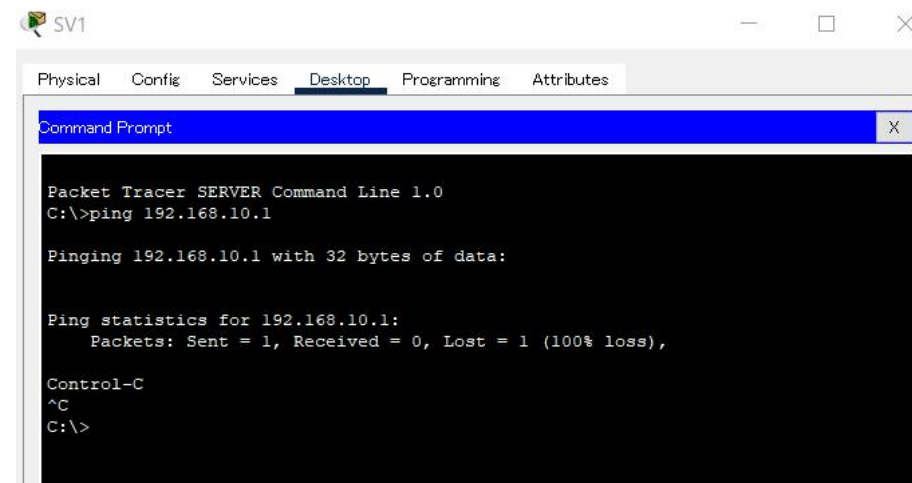
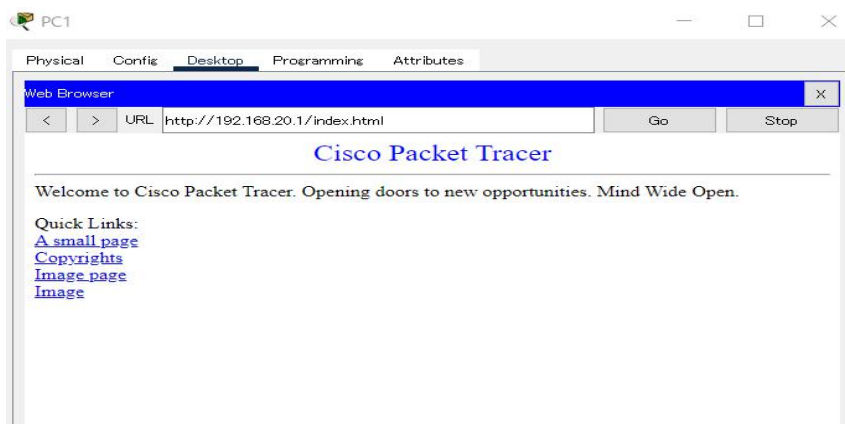
```
C:\>ping 192.168.20.2

Pinging 192.168.20.2 with 32 bytes of data:

Reply from 192.168.20.2: bytes=32 time<1ms TTL=125
Reply from 192.168.20.2: bytes=32 time<1ms TTL=125
Reply from 192.168.20.2: bytes=32 time<1ms TTL=125
Reply from 192.168.20.2: bytes=32 time<1ms TTL=125

Ping statistics for 192.168.20.2:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 0ms, Average = 0ms

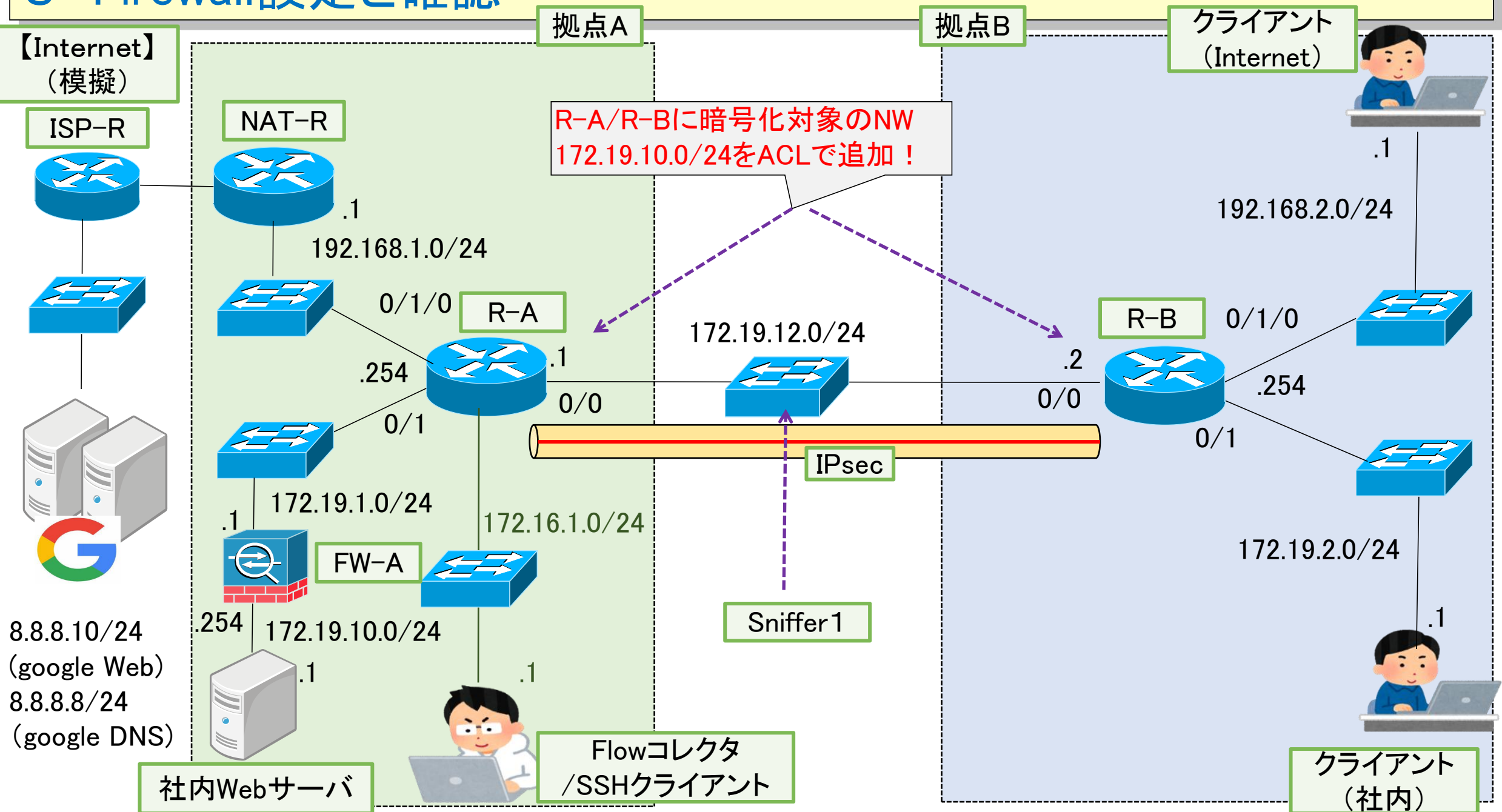
C:\>
```



3

Firewall設定と確認

3 Firewall設定と確認



3 Firewall設定と確認

拠点Aの詳細図

拠点A

社内Webサーバ

HTTPのみ許可

nameif: INSIDE
security-Level:100

FW-A

nameif: OUTSIDE
security-Level:20

R-A

IPsec

.1

Gi1/4
.254

Gi1/3
.1

0/1
.254

172.19.10.0/24

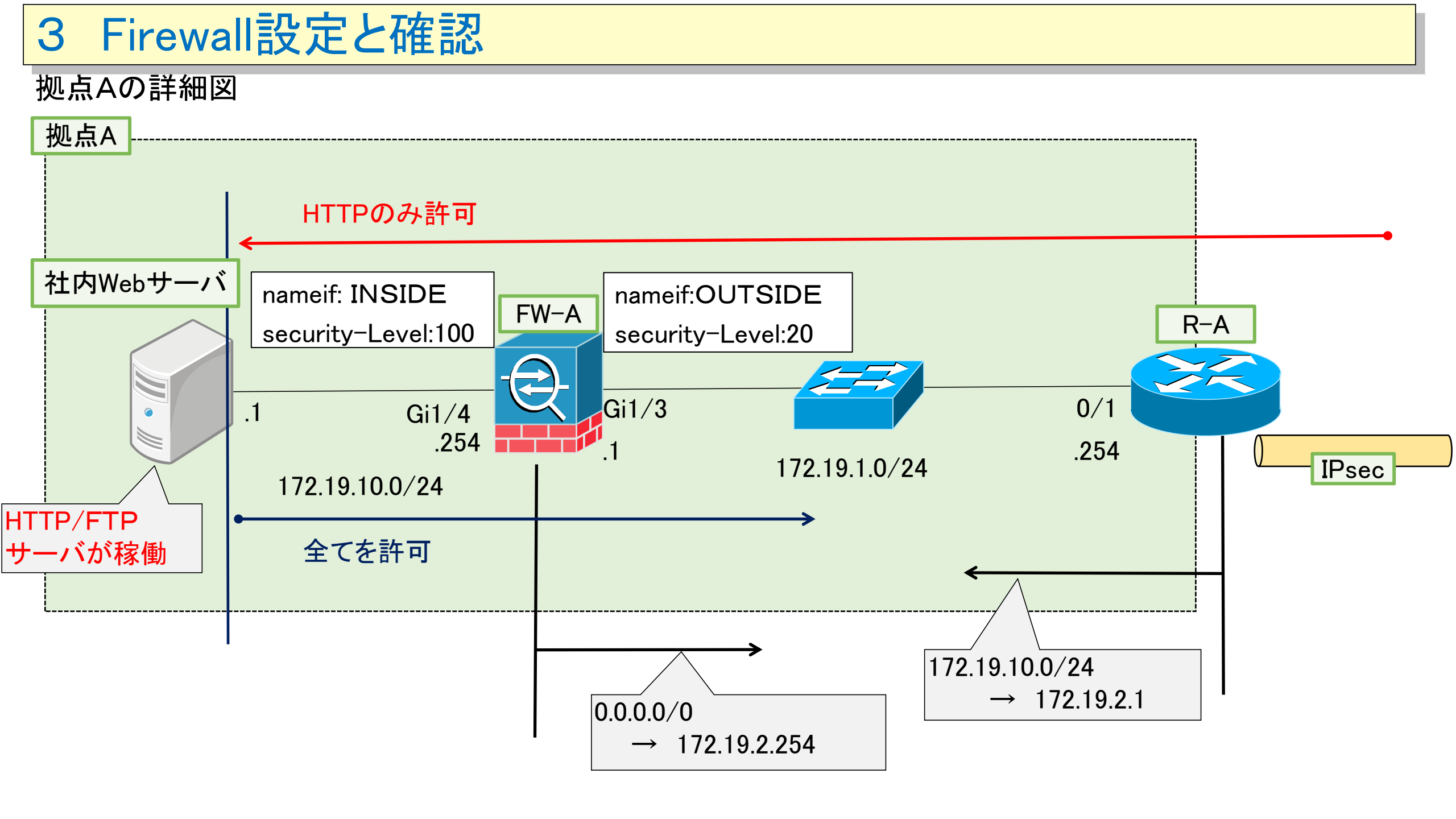
172.19.1.0/24

HTTP/FTP
サーバが稼働

全てを許可

0.0.0.0/0
→ 172.19.2.254

172.19.10.0/24
→ 172.19.2.1



3 Firewall設定と確認

以下の要領で設定します

(事前確認)

拠点AにFirewall(ASA5506)を接続します。

拠点Aのルータ向けにデフォルトルートを設定

インタフェースのセキュリティレベル

nameif: INSIDE security-Level:100

nameif:OUTSIDE security-Level:20

全ての通信を通過させるためのAccess-Listを設定 → ①

拠点Bの端末から拠点AのサーバにPING/HTTP/FTPアクセスできるかを確認します

(セキュリティ設定)

インタフェースのセキュリティレベル

nameif: INSIDE security-Level:100

nameif:OUTSIDE security-Level:20

Access-Listを変更して以下の条件で設定変更

OUTSIDE→INSIDE:HTTPのみ許可 OUTSIDE→INSIDE:全ての通信を許可 → ②

拠点Bの端末から拠点AのサーバにHTTPアクセスできるかを確認します

拠点Bの端末から拠点AのサーバにFTPアクセスできないことを確認します

3 Firewall設定と確認

ASAに適用するAccess-List

① 双方向の通信を許可

```
ciscoasa(config)#access-list OUTSIDE-to-INSIDE extended permit ip any any
ciscoasa(config)#access-group OUTSIDE-to-INSIDE in interface OUTSIDE
ciscoasa(config)#
ciscoasa(config)#exit
ciscoasa#
```

② OUTSIDE→INSIDE: HTTPのみ許可 OUTSIDE→INSIDE: 全ての通信を許可

```
ciscoasa(config)#access-list OUTSIDE-to-INSIDE extended permit ip any any
ciscoasa(config)#access-group OUTSIDE-to-INSIDE in interface OUTSIDE
ciscoasa(config)#
ciscoasa(config)#exit
ciscoasa#
```

Sougo-1-Mihon-FW.pkt （総合実習でのNWにASAを追加）は ”②” のaccess-listを適用しています！

①のAccess-Listに変更して動作を確認してみてください。

3 Firewall設定と確認

ASAに適用するAccess-List

② OUTSIDE→INSIDE: HTTPのみ許可 OUTSIDE→INSIDE: 全ての通信を許可

```
C:\>
C:\>ping 172.19.10.1

Pinging 172.19.10.1 with 32 bytes of data:

Ping statistics for 172.19.10.1:
    Packets: Sent = 1, Received = 0, Lost = 1 (100% loss),

Control-C
^C
C:\> ftp 172.19.10.1
Trying to connect...172.19.10.1

C:\>
C:\>
```

全許可していた場合に
通信できていた
PING/FTPはASAでブロックされます！



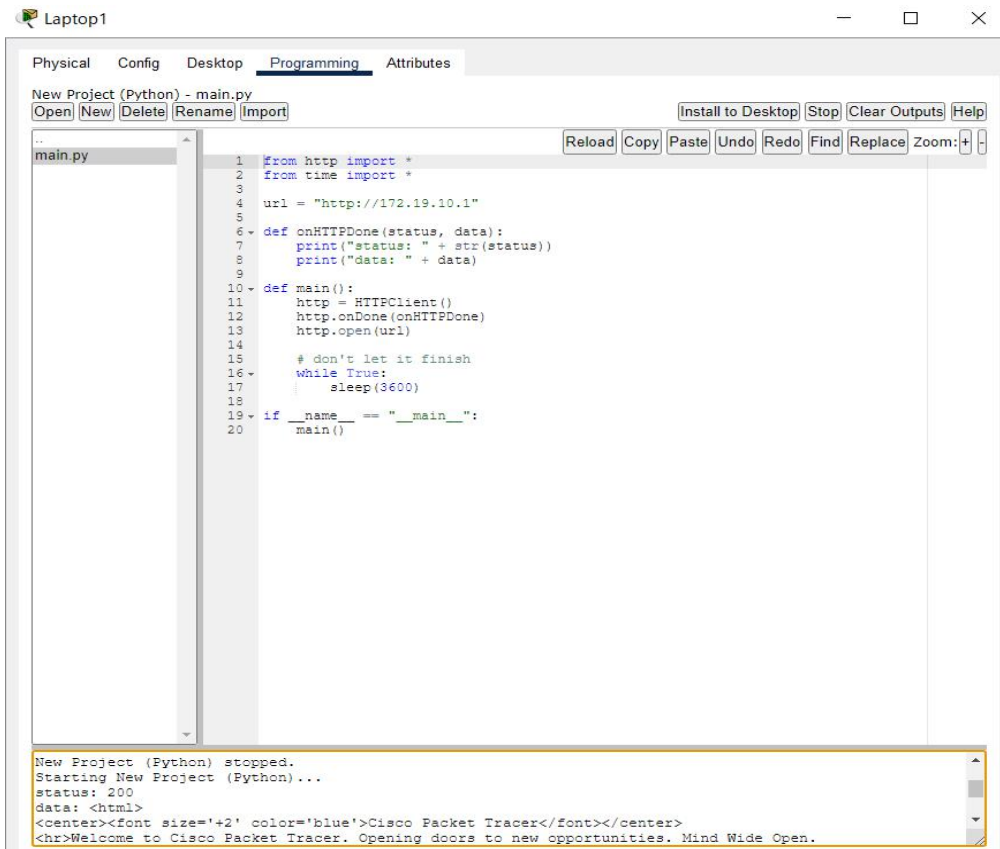
3 Firewall設定と確認

ASAに適用するAccess-List

② OUTSIDE→INSIDE: HTTPのみ許可

OUTSIDE→INSIDE: 全ての通信を許可

PythonによるWebアクセス



```
1 from http import *
2 from time import *
3
4 url = "http://172.19.10.1"
5
6 def onHTTPDone(status, data):
7     print("status: " + str(status))
8     print("data: " + data)
9
10 def main():
11     http = HTTPClient()
12     http.onDone(onHTTPDone)
13     http.open(url)
14
15     # don't let it finish
16     while True:
17         sleep(3600)
18
19 if __name__ == "__main__":
20     main()
```

New Project (Python) stopped.
Starting New Project (Python)...
status: 200
data: <html>
<center>Cisco Packet Tracer</center>

Welcome to Cisco Packet Tracer. Opening doors to new opportunities. Mind Wide Open.

WebブラウザによるWebアクセス

