FTP/FTPS通信とASA

1. FTP
   - -Active TCP/21(control), 20(data)
   - -Passive TCP/21(control)

2. FTPS - FTP over SSL
   - -Implicit (Active, Passive) : TCP/990 (TCP/989 -data)
   - -Explicit (Active, Passive) : TCP/21 (TCP/20 -data)

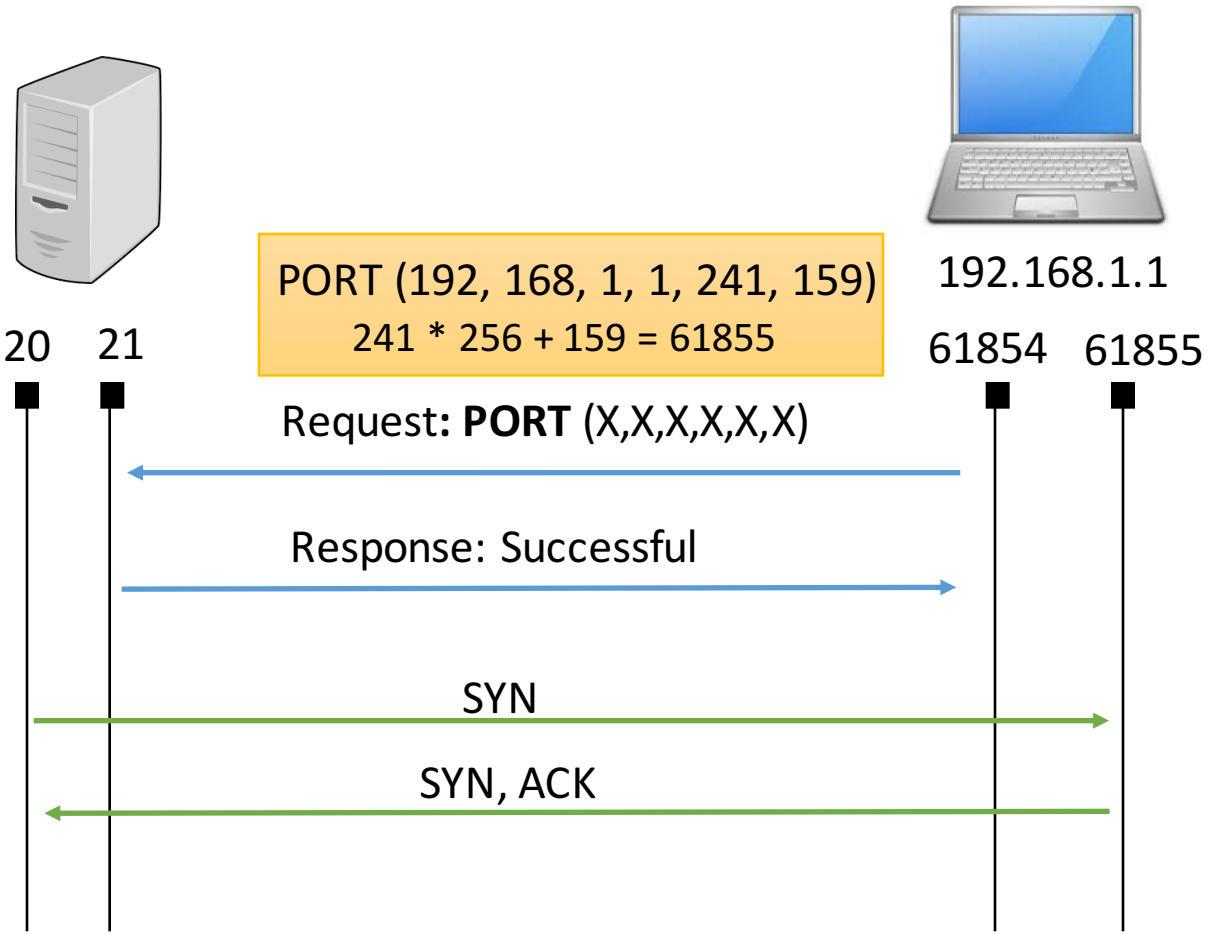
注) SFTP - SSH File Transfer Protocol
Port TCP/22

FTP

FTP Active Mode

TCP/21(control) 20(data)を使用

Active mode
リクエストに対し、サーバーからクライアントへ
データ通信のためのSYNを送信



PORT (X_1,X_2,X_3,X_4,X_5,X_6)

IP address

Data Port = X_5 * 256 + X_6

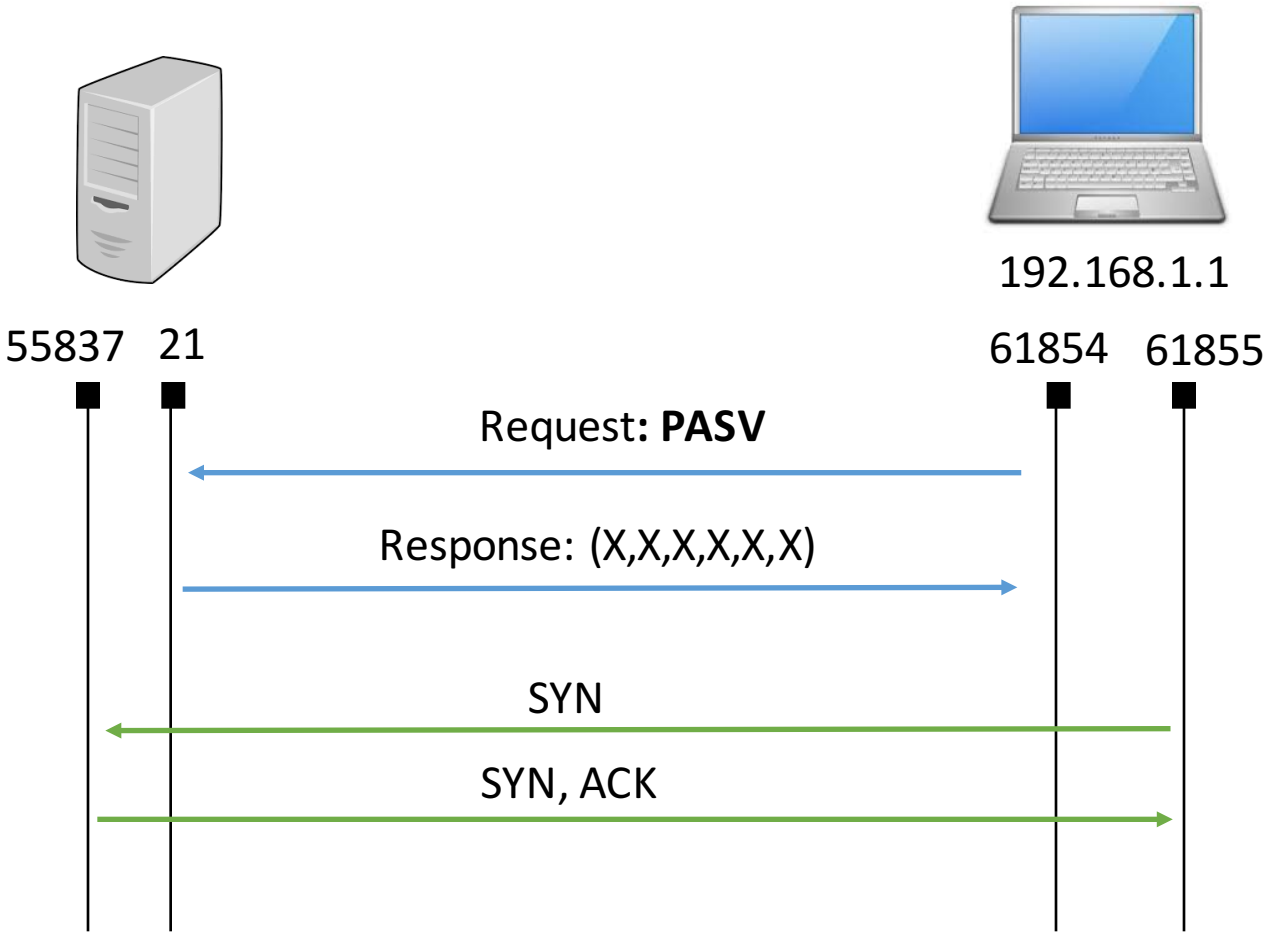
FTP- Control

FTP- Data

FTP Passive Mode

TCP/21(con) を使用

Passive mode
リクエストに対し、クライアントからサーバへ
データ通信のためのSYNを送信



$(\underline{X_1},\underline{X_2},\underline{X_3},\underline{X_4},\underline{X_5},\underline{X_6})$

IP address

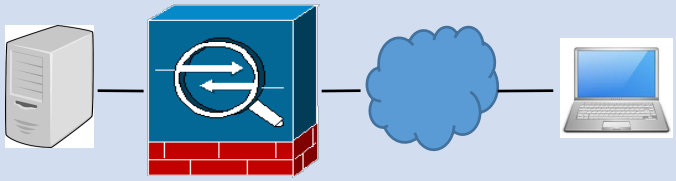
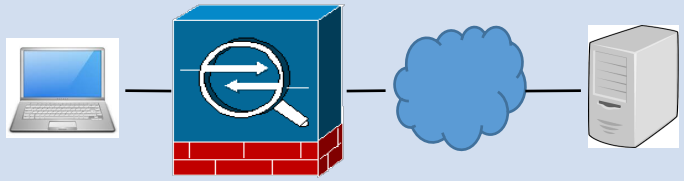
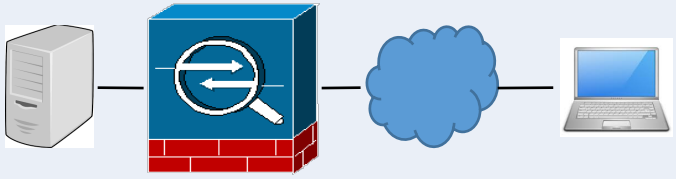
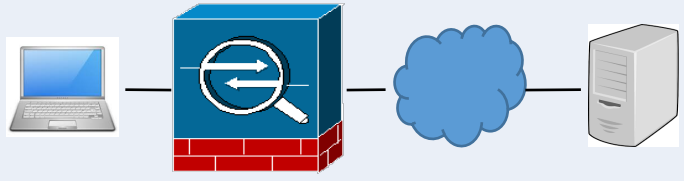
Data Port = $X_5 * 256 + X_6$

FTP- Control

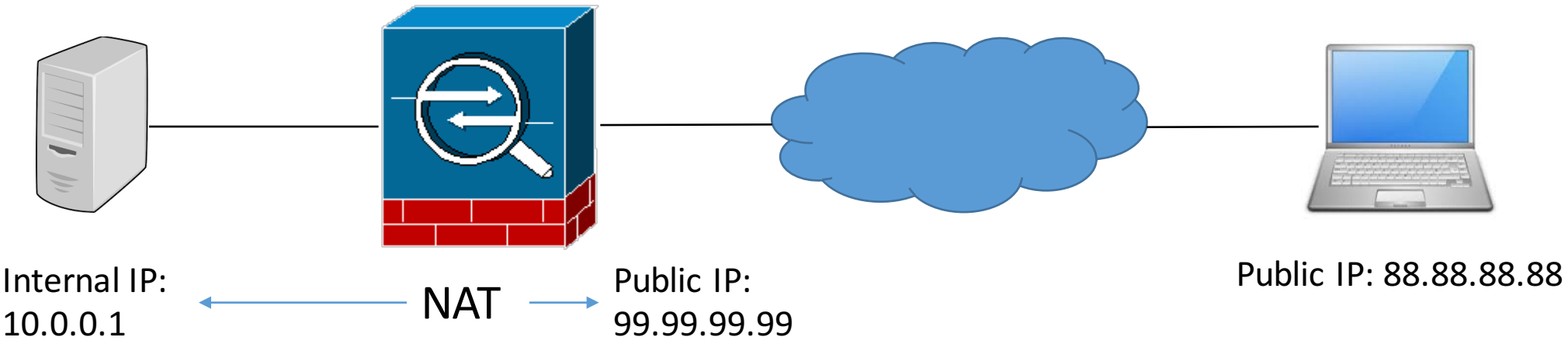
FTP- Data

ASAとFTP通信

Inbound: 自社ネットワークにリクエストが来る場合
Outbound: 自社ネットワークからリクエストを送る場合

	Inbound	Outbound
Active	1 	3 
Passive	2 	4 

1. Inbound/Active



Request: **PORT** (88,88,88,88,X,X)

Dest TCP/21

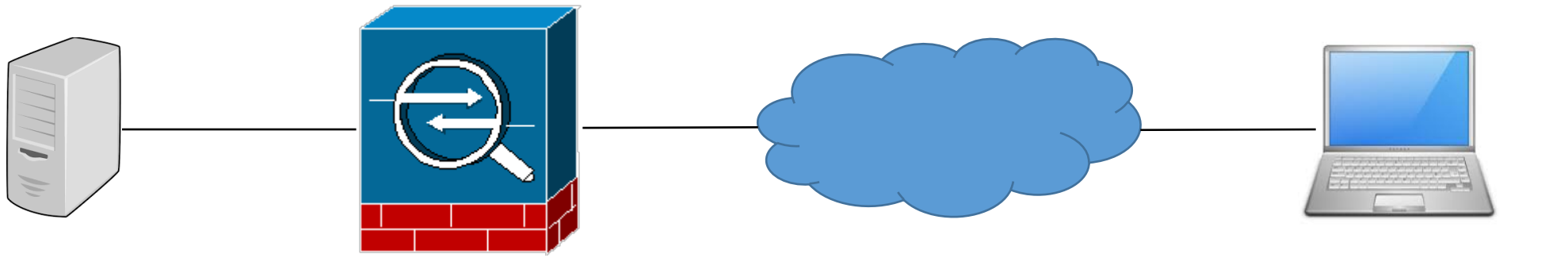
SYN

Sour TCP/20

Dest 88.88.88.88 / tcp X

データ通信用SYNは既知ポートのinside -> outside通信となり通過できる

2. Inbound/Passive



Request: **PASV**

Dest tcp21

Response: (10,0,0,1,X,X) - FTP inspection -> (99.99.99.99,X,X)

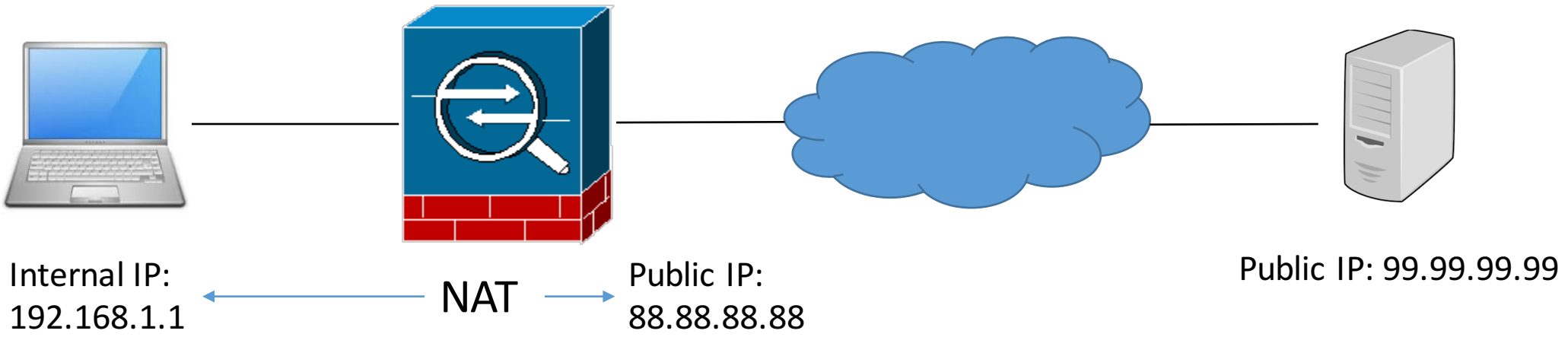
SYN

Dest 99.99.99.99 / tcp X

(-> Dest 10.0.0.1/ tcp X)

データ通信用SYNはFTP inspectionの機能でペイロード変換と一時的に特定ポートを許可することにより通過できる

3. Outbound/Active



Request: **PORT** (192.168.1.1,X,X) - FTP inspection -> **PORT** (88,88,88,88,X,X)

Dest TCP/21

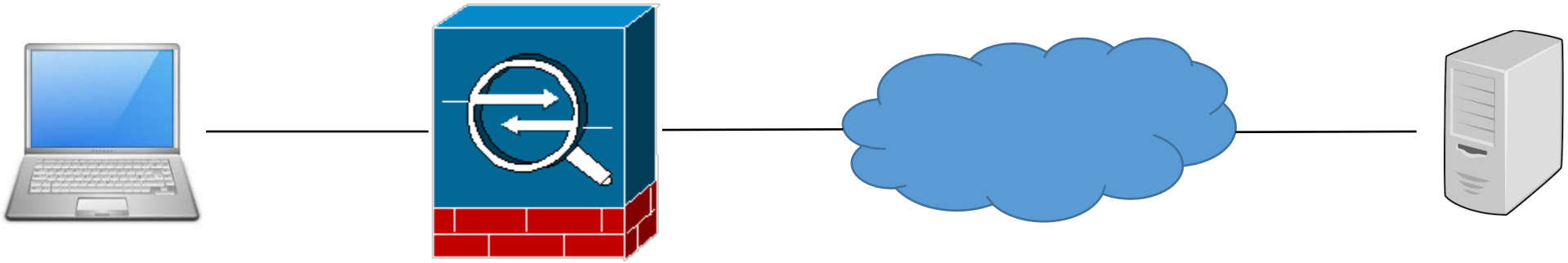
SYN

Dest 88.88.88.88 / tcp X
(-> Dest 192.168.1.1/ tcp X)

Sour TCP/20

データ通信用SYNはFTP inspectionの機能でペイロード変換と一時的に特定ポートを許可することにより通過できる

4. Outbound/Passive



Dest tcp21

Request: **PASV**

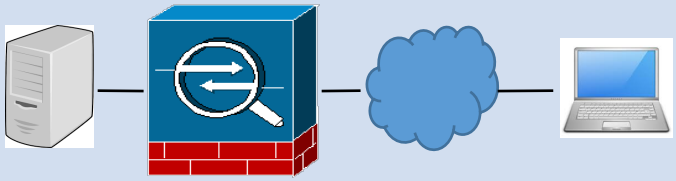
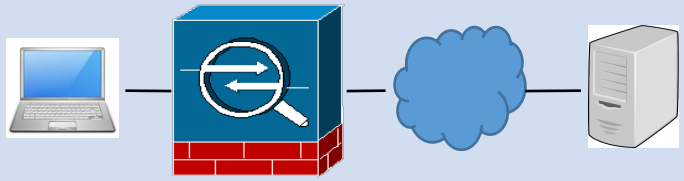
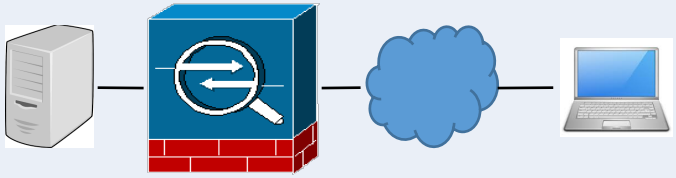
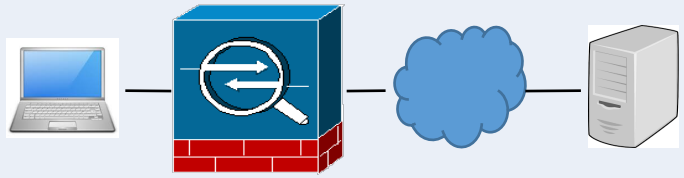
Response: (99.99.99.99,X,X)

SYN

Dest 99.99.99.99 / tcp X

データ通信用SYNはinside -> outside通信となり通過できる

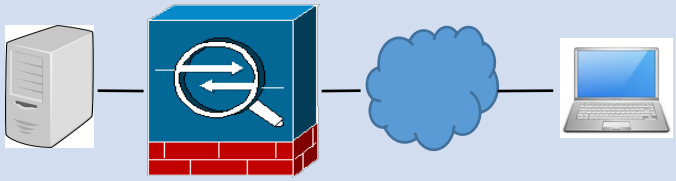
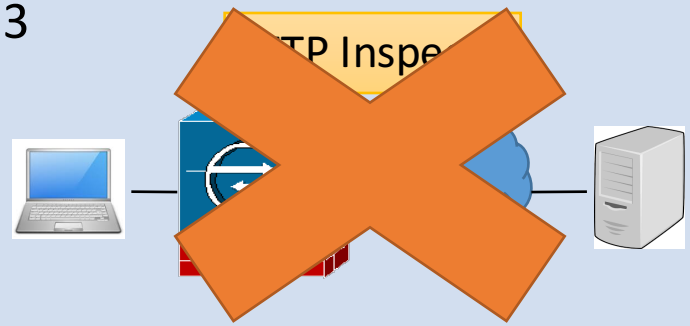
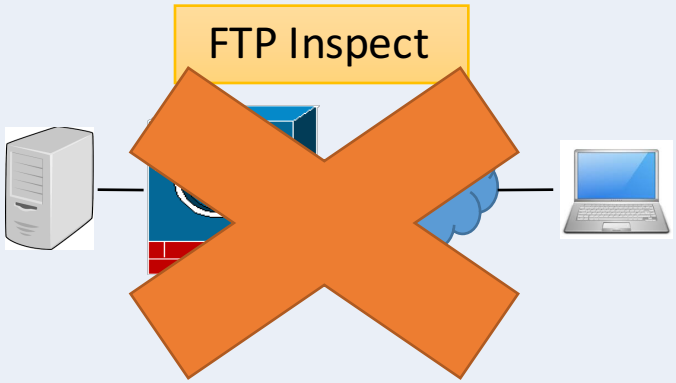
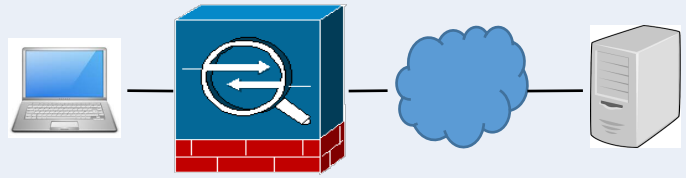
ASAとFTP通信

	Inbound	Outbound
Active	1 	3 FTP Inspect (NAT) 
Passive	2 FTP Inspect (NAT) 	4 

※データ通信用SYNはFTP Inspectが有効でないと通過しない場合がある

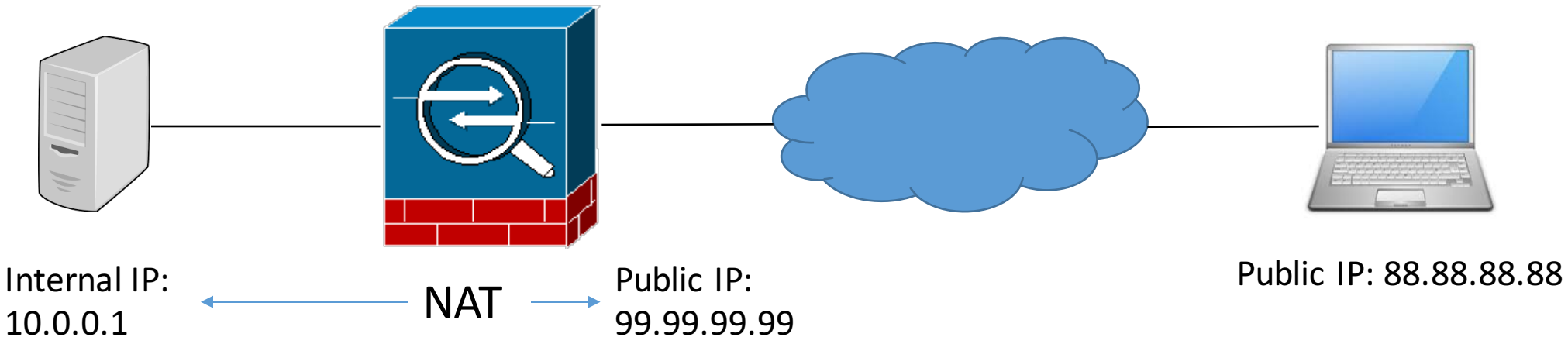
FTPS - FTP over SSL

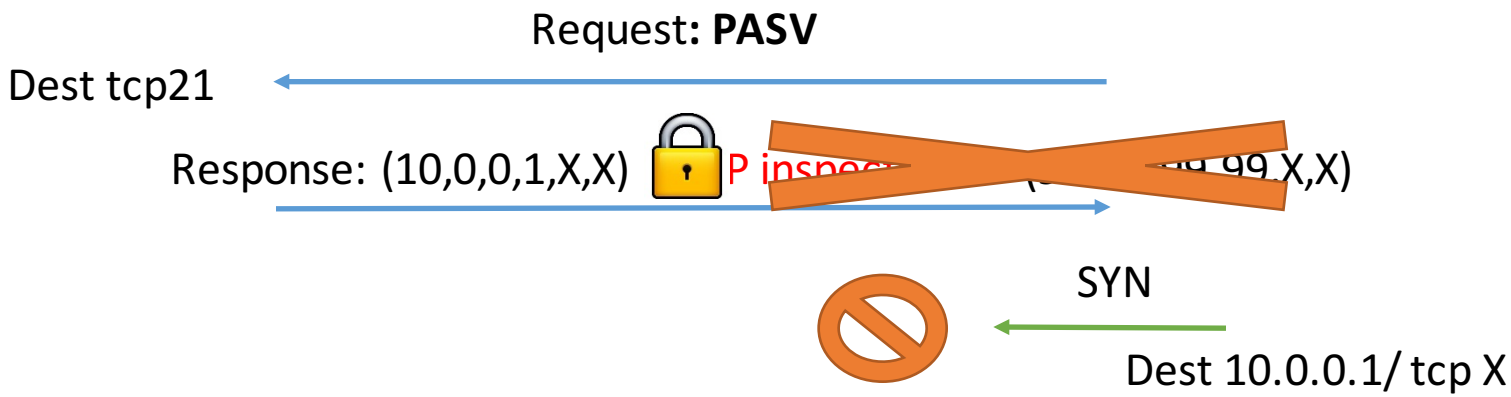
ASAとFTPS通信

	Inbound	Outbound
Active	1 	3 
Passive	2 	4 

※FTP Inspectが有効でないと通過しない通信では、FTPS通信は許可できない

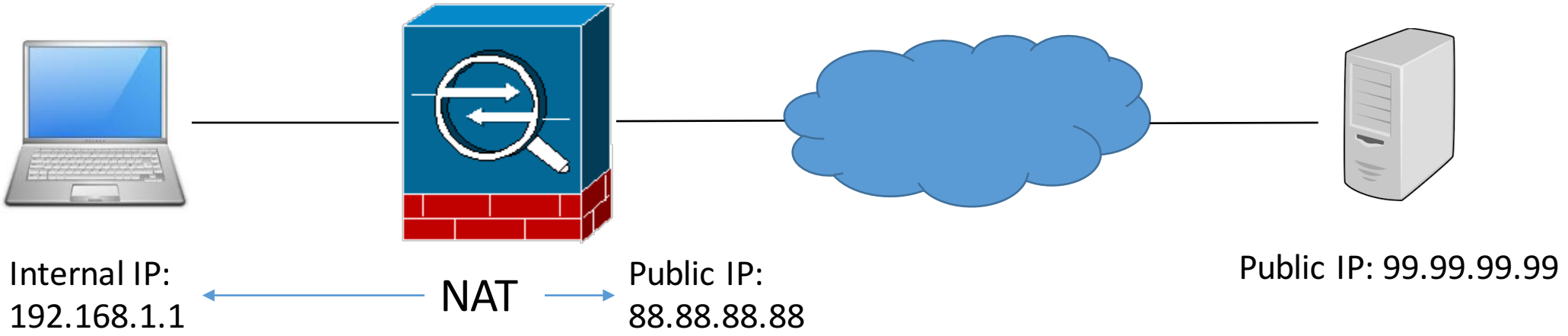
Inbound/Passiveで通信を許可できない理由

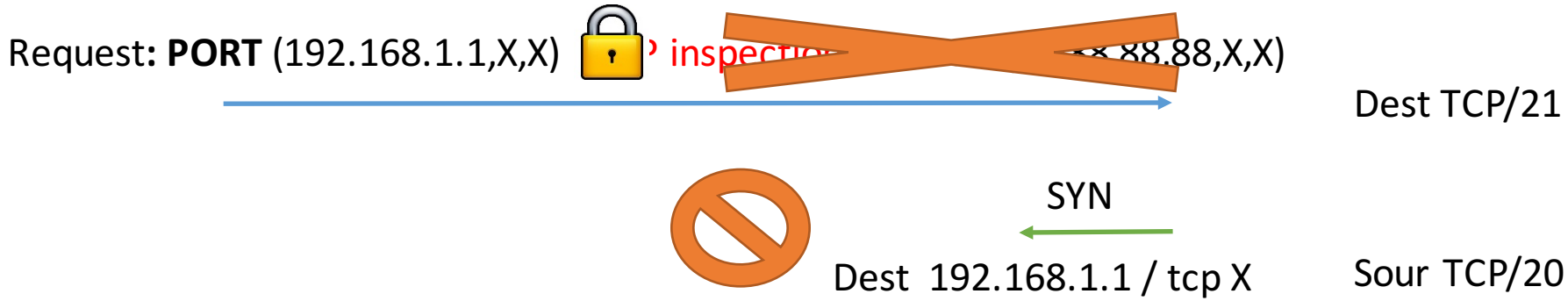




制御用通信のResponseが暗号化されていて、ペイロードが変換できず
クライアントが社内(NAT変換前)IP addressをSYNを送信してしまう

Outbound/Activeで通信を許可できない理由





制御用通信のPORTが暗号化されていて、ペイロードが変換できず
サーバーが社内(NAT変換前)IP addressにSYNを送信してしまう

対策

-Explicit (Active, Passive) ：TCP/21 –control (TCP/20 -data)の場合

CCC(Clear Channel Command)の利用。

CCC:認証(ユーザー/PASS)は暗号化し、その後の制御通信を平文化する

->(X,X,X,X,X,X)ペイロードをインスペクト可能

-Implicit (Active, Passive) ：TCP/990 -control (TCP/989 -data)の場合

対策なし