CS5333
Computer and Network Security

January 8th, 2018

Kotaro Kataoka

Security

- How to secure your host?
- How to secure our network?
  - ACL and Firewall
  - How to avoid to disturb other network?

Securing Your Hosts

- Account security
- Secure shell
- Network servers
- Firewall
- Keeping your system up-to-date
- Minimum requirement

Account Security

- No group and shared accounts
  - An account should correspond to only one person
- “Good” password
  - Mix alphanumeric + symbolic characters
- Password ageing
  - When should you change the password?
- Limit who can access to root
  - wheel group + sudo access
- Do not become root
  - Login as your account, then sudo to execute a privileged command
- Never leave idle console

Secure Shell

- A secure way for remote access
- Default remote access method
- More security by limiting access only from certain hosts
  - use firewall
- But, sometimes a vulnerability is found
  - patch ASAP!!

SSH: Dos and Don’ts

- Use Public Key Authentication
- Use access list to limit the network that can access your server
- Don’t permit Password Authentication
- Don’t permit Root Login

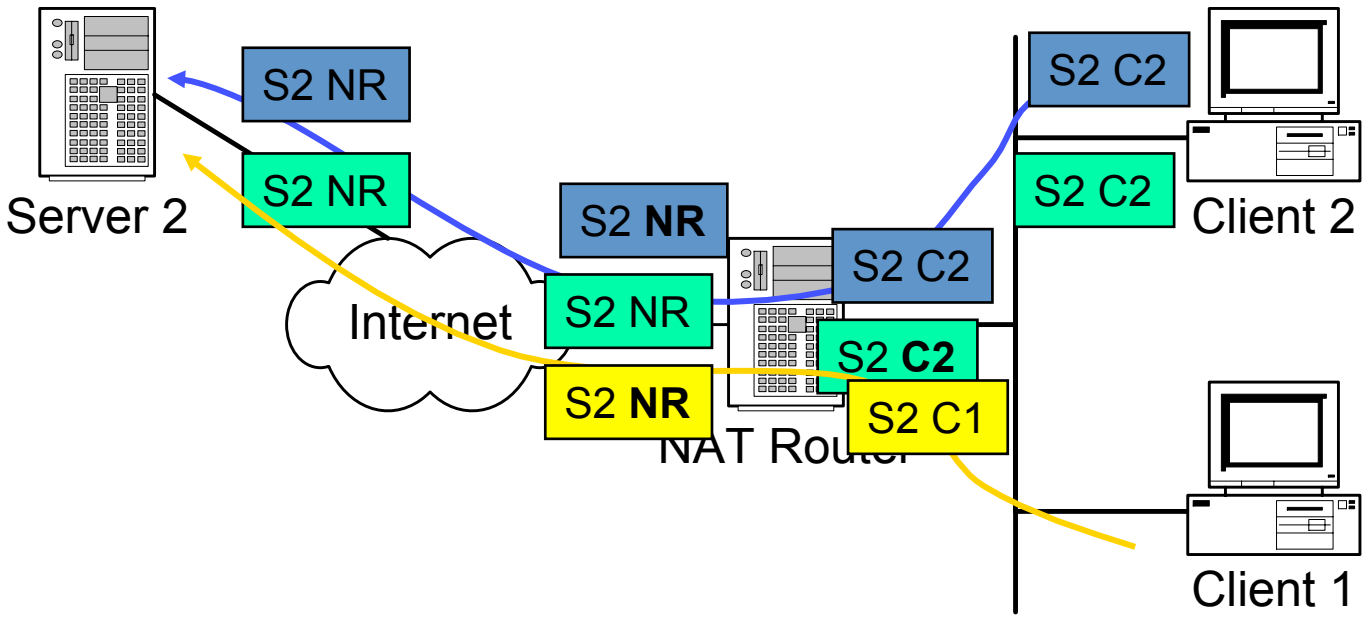
Network Servers

- Disable unnecessary network servers
- Make sure that the network servers do not have vulnerabilities
  - keep up to date

Network Security

- Preventing and detecting unauthorized use of your computers and networks
- Why you have to care for network security
  - protect your data
  - prevent your network to be used as a source of attacks
- What you can do
  - secure your hosts and networks
  - keep up to date to the latest security threats

Network Address Translation



NAT is Dangerous

- Masquerade source address
- No log file
- If an attack is launched from behind NAT, difficult to track the culprit

Firewall

- Block packets
- Rule based: protocol, source & destination address & port, other flags
- First match
- Example:

  0500 allow tcp from 10.0.0.0/8 to 10.1.1.1 80

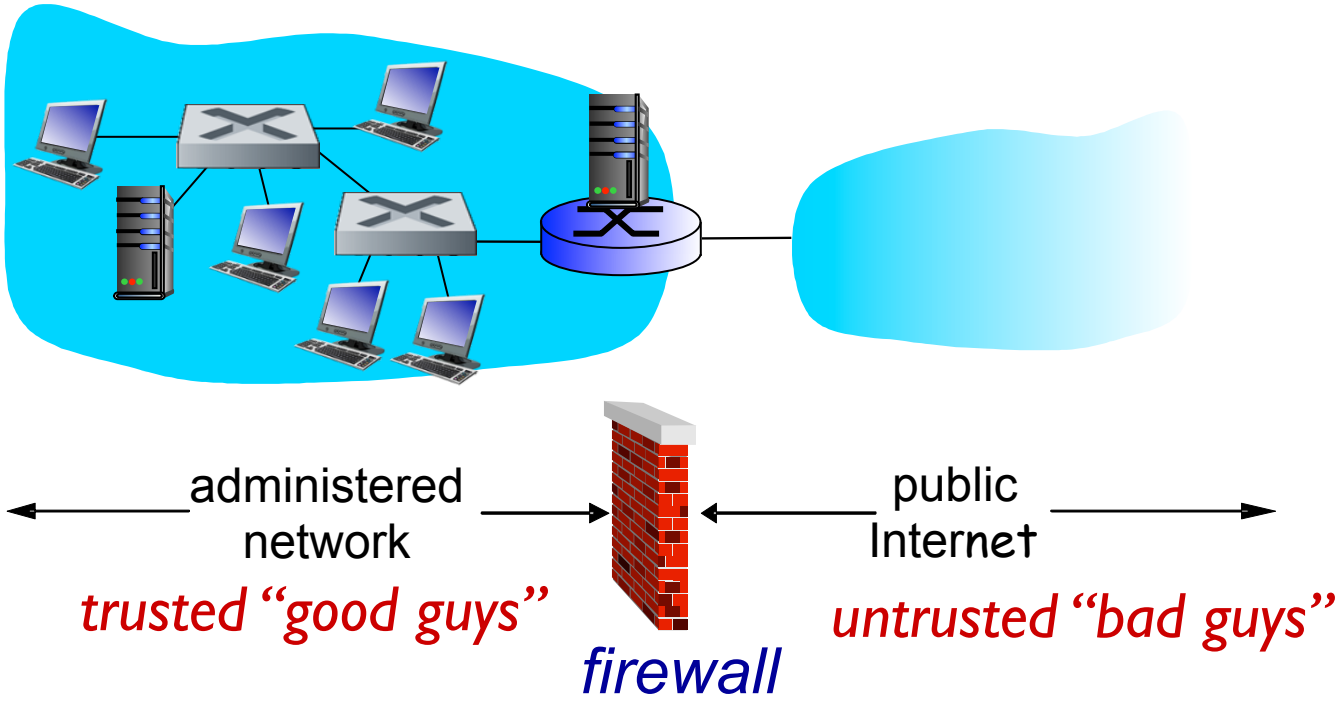
  0600 deny tcp from any to 10.1.1.1 80

Securing Network with Firewall

Firewalls

firewall

isolates organization's internal net from larger Internet, allowing some packets to pass, blocking others



Firewalls: why

prevent denial of service attacks:

- SYN flooding: attacker establishes many bogus TCP connections, no resources left for "real" connections

prevent illegal modification/access of internal data

- e.g., attacker replaces CIA's homepage with something else

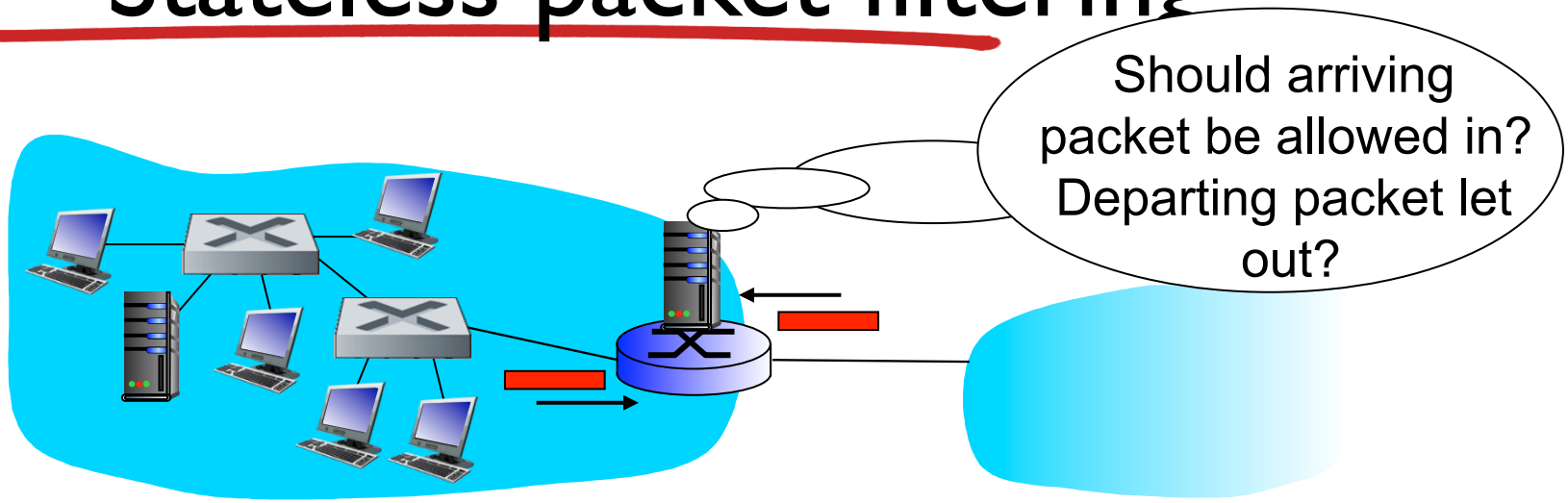
allow only authorized access to inside network

- set of authenticated users/hosts

three types of firewalls:

- stateless packet filters
- stateful packet filters
- application gateways

Stateless packet filtering



- internal network connected to Internet via *router firewall*
- router *filters packet-by-packet,* decision to forward/drop packet based on:
  - source IP address, destination IP address
  - TCP/UDP source and destination port numbers
  - ICMP message type
  - TCP SYN and ACK bits

Stateless packet filtering: example

- *example 1:* block incoming and outgoing datagrams with IP protocol field = 17 and with either source or dest port = 23
  - *result:* all incoming, outgoing UDP flows and telnet connections are blocked
- *example 2:* block inbound TCP segments with ACK=0.
  - *result:* prevents external clients from making TCP connections with internal clients, but allows internal clients to connect to outside.

Stateless packet filtering: more examples

Policy	*Firewall Setting*
No outside Web access.	Drop all outgoing packets to any IP address, port 80
No incoming TCP connections, except those for institution's public Web server only.	Drop all incoming TCP SYN packets to any IP except 130.207.244.203, port 80
Prevent Web-radios from eating up the available bandwidth.	Drop all incoming UDP packets - except DNS and router broadcasts.
Prevent your network from being used for a smurf DoS attack.	Drop all ICMP packets going to a "broadcast" address (e.g. 130.207.255.255).
Prevent your network from being tracerouted	Drop all outgoing ICMP TTL expired traffic

Access Control Lists

- *ACL:* table of rules, applied top to bottom to incoming packets: (action, condition) pairs

action	source address	dest address	protocol	source port	dest port	flag bit
allow	222.22/16	outside of 222.22/16	TCP	> 1023	80	any
allow	outside of 222.22/16	222.22/16	TCP	80	> 1023	ACK
allow	222.22/16	outside of 222.22/16	UDP	> 1023	53	---
allow	outside of 222.22/16	222.22/16	UDP	53	> 1023	----
deny	all	all	all	all	all	all

Stateful packet filtering

- *stateless packet filter:* heavy handed tool
  - admits packets that "make no sense," e.g., dest port = 80, ACK bit set, even though no TCP connection established:

action	source address	dest address	protocol	source port	dest port	flag bit
allow	outside of 222.22/16	222.22/16	TCP	80	> 1023	ACK

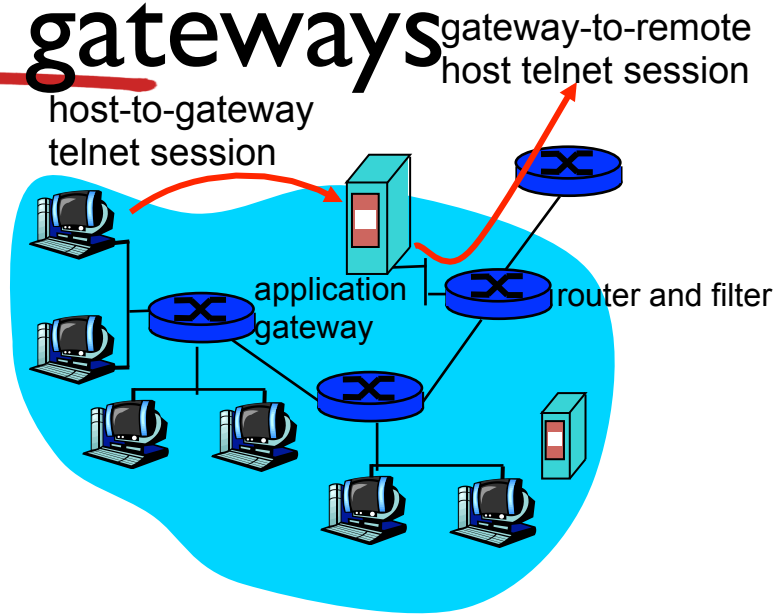
- *stateful packet filter:* track status of every TCP connection
  - track connection setup (SYN), teardown (FIN): determine whether incoming, outgoing packets "makes sense"
  - timeout inactive connections at firewall: no longer admit packets

Stateful packet filtering

- ACL augmented to indicate need to check connection state table before admitting packet

action	source address	dest address	proto	source port	dest port	flag bit	check conxion
allow	222.22/16	outside of 222.22/16	TCP	> 1023	80	any	
allow	outside of 222.22/16	222.22/16	TCP	80	> 1023	ACK	X
allow	222.22/16	outside of 222.22/16	UDP	> 1023	53	---	
allow	outside of 222.22/16	222.22/16	UDP	53	> 1023	----	X
deny	all	all	all	all	all	all	

Application gateways

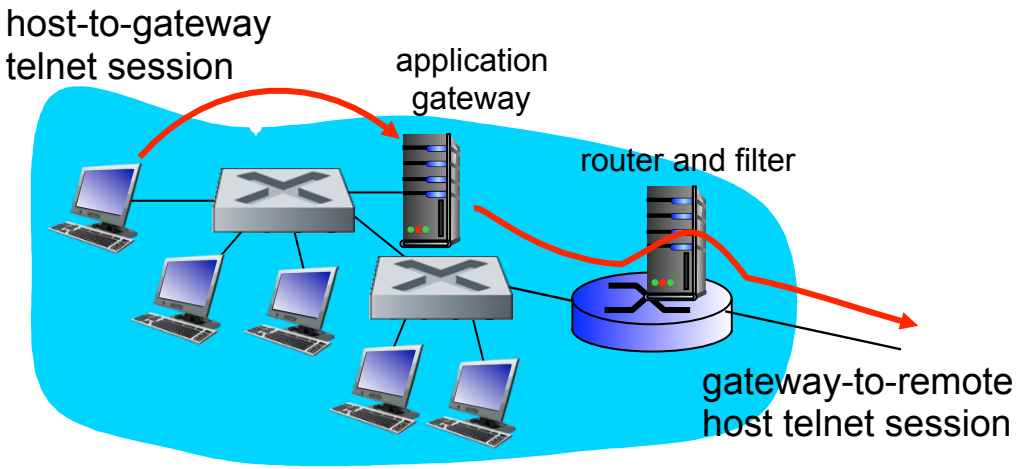


- filters packets on application data as well as on IP/TCP/ UDP fields.
- *example:* allow select internal users to telnet outside.

1. require all telnet users to telnet through gateway.
2. for authorized users, gateway sets up telnet connection to dest host. Gateway relays data between 2 connections
3. router filter blocks all telnet connections not originating from gateway.

Application gateways

- filter packets on application data as well as on IP/TCP/UDP fields.
- *example:* allow select internal users to telnet outside



1. require all telnet users to telnet through gateway.
2. for authorized users, gateway sets up telnet connection to dest host. Gateway relays data between 2 connections
3. router filter blocks all telnet connections not originating from gateway.

Black List vs. White List

- Black List
  - Open access with prohibited rules
  - More freedom on network activity compared to White List
  - Malicious traffic can pass through the firewall before it gets blocked
- White List
  - Closed access with permitted rules like Intranet
  - Sometimes prohibits activity in the network unnecessarily
  - Online banking, Honey pot (experiment of petting malware-infected PCs) should go this way

Inbound Filtering and Outbound Filtering

- Inbound filtering for protecting own network from external threats

- Outbound filtering for not disturbing other networks
  - Blocking malware happening in intranet not to go out
  - Blocking, for example, open SMTP relay server (OP25B)

Q: Does Firewall Provide Perfect Security?

A: No. Why?

Limitation of Firewalls

- Firewalls can be bypassed by many ways
  - Unsecure Wi-Fi APs
  - Cracked VPN connections
- Malicious traffic that matches a white listed rule can pass through the firewall
- Mobile devices get infected outside the network and come back inside

Limitations of firewalls, gateways

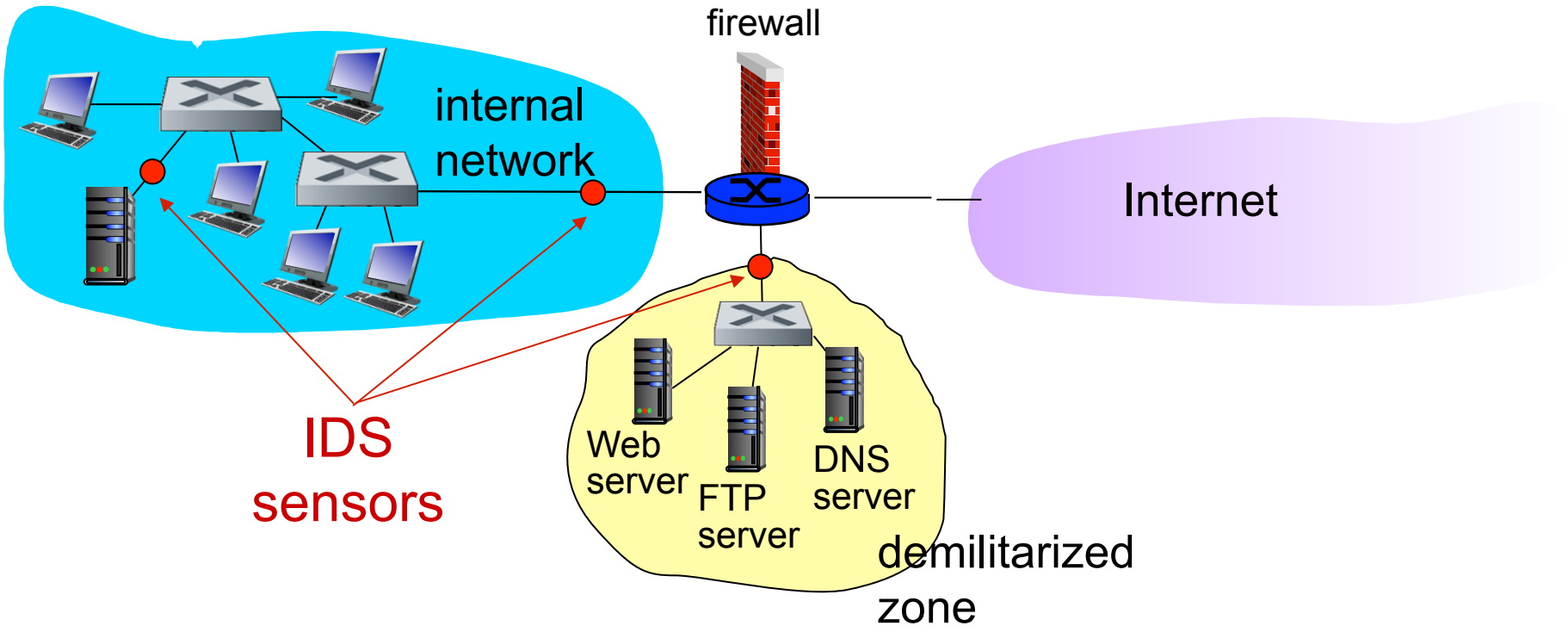
- *IP spoofing:* router can't know if data "really" comes from claimed source
- if multiple app's. need special treatment, each has own app. gateway
- client software must know how to contact gateway.
  - e.g., must set IP address of proxy in Web browser
- filters often use all or nothing policy for UDP
- *tradeoff:* degree of communication with outside world, level of security
- many highly protected sites still suffer from attacks

Intrusion detection systems

- packet filtering:
  - operates on TCP/IP headers only
  - no correlation check among sessions
- *IDS: intrusion detection system*
  - *deep packet inspection:* look at packet contents (e.g., check character strings in packet against database of known virus, attack strings)
  - examine correlation among multiple packets
    - port scanning
    - network mapping
    - DoS attack

Intrusion detection systems

- multiple IDSs: different types of checking at different locations



What happens if IDS sensor is installed outside FW?

Assignment

- Setting up an SSH server with a proper access method
  - Setup 1 VM using Ubuntu in your laptop computer
  - Generate an SSH Key Pair
  - Place Private Key at Host OS
  - Place Public Key at Ubuntu VM
  - Give proper setup to SSH Server un Ubuntu VM
  - Demonstrate that your SSH login properly uses Public Key Authentication

- Deadline: 23:59 January 26^{th,} 2018
  - Demo slots/venues will be announced by TAs

- Hints / References
  https://help.ubuntu.com/community/SSH/OpenSSH/Keys

Marks Distribution of Assignment

- Point 1: 10 Marks
  - Is /etc/ssh/sshd_config is properly configured?
  - 5 Marks PermitRootLogin: no
  - 5 Marks PermitPasswordAuthentication: no

- Point 2: 10 Marks
  - Does remote login use Public Key Authentication?
  - If his/her key pair is properly generated and configured, then the default mode of authentication shall be Public Key Authentication.
  - If Public Key Authentication is not initiated properly for the remote login, misplacement of the keys, wrong file permission, etc. maybe the course.
  - The marks must be given only successful remote login using Public Key Authentication is confirmed.

- Point 3: 10 Marks
  - 5 Marks Make sure that root login is refused immediately.
  - 5 Marks Make sure that the login procedure DOES NOT fall back to Password Authentication
  - If the Public Key Authentication fails AND password authentication is still allowed, then the password authentication may come up. It is not allowed in this assignment. To check this, type wrong pass phrase (empty password) several times. If the authentication is terminated after the failure of entering pass phrase, that mean the configuration is correct 5 marks will be given.

- Why must the point 1 and other points be separately checked?
- Answer: The sshd configuration gets active after the sshd is restarted with the updated configuration. If there is an inconsistency in the configuration, then the sshd will not be launched properly. You're suggested to check both configuration and actual behavior of the remote longin.