# Security Standard on Firewall Configuration

## Background

Incorporated with the University Firewall Policy approved in Aug 2015, this document is served as a minimum security standard on firewall configuration to comply with and stated clearly the operating procedures for raising exception services.

## Roles and Responsibilities

The following table is to specify the roles and tasks involved in configuring and operating the firewalls, monitoring policy compliance, so that all parties involved in the University can follow easily and unambiguously.

| Tasks | Timeframe | Responsible Party | | |
|---|---|---|---|---|
| | | ITSC | IT Coordinator | LAN Admin |
| Conduct consultation on firewall configuration | Nov 2015 | Y | | |
| Review and comment on firewall configuration | Nov 2015 | Y | Y | Y |
| Setup and configure the firewalls | Dec 2015 | Y | | Y |
| Monitor firewall setup and configuration | Jan 2016 | Y | | |
| *Proposal of Vulnerability Scanning procedures | Mar 2016 | Y | Y | Y |
| Migrate all Internet-facing servers to the DMZ | Jun 2016 | Y | | Y |
| Monitor policy compliance | Jul 2016 | Y | | |
| Raise exception request, if necessary | Ongoing | Y | Y | Y |

* Proposal of Vulnerability Scanning procedures - Detailed vulnerability scanning procedures would be written in a separate proposal paper of University-wide Vulnerability Scanning.

# A. Security Standard on Firewall Configuration

## Network and Platform Definition

These definitions are used in this document.

- CUHK Campus Network ( 137.189.0.0/16) : Could be both intranet and DMZ, depending on department's firewall zoning setup.

- Special Virtual Machine (SVM) Platform : Each SVM host has its individual virtual firewall, SVM platform would be treated as either intranet or DMZ, depending on the requirement of SVM host.

## Minimum security standard on Firewall Configuration

The University will have two security regions – trusted (intranet) and untrusted (DMZ) regions.

| Region | Coverage |
|---|---|
| Trusted (Intranet) | The trusted region is used to host computers that do not need direct connection from the outside world. Firewalls are like gates that outsiders cannot come in but insiders can go out. |
| Untrusted (DMZ) | The untrusted region contains computers, such as web and email servers, that by necessity need to be accessible from the outside, which, unfortunately, also includes hackers. |

Department will configure firewall according to the security standard on firewall configuration with principle of least privileges access control. A default deny rule is set for blocking all incoming traffic with explicit allow rules for legitimate traffic.

To prevent unwanted incoming traffic entering CUHK campus network, direct access from the Internet is limited to Untrusted region, that is DMZ and would be restricted to the authorized internet services listed in Appendix 1. Apart from these, other services can be accessed via CUHK VPN.

| Region | Minimum security standard on Firewall Configuration | Vulnerability Scanning |
|---|---|---|
| Trusted (Intranet) | **Incoming connection :**<br>• Block all incoming traffic from the Internet<br>• Block all incoming traffic from DMZ except for required services[1], such as the connection to database in the intranet<br>• Allow incoming traffic from the intranet except for exceptional cases, such as from a compromised node<br>**Outgoing connection :**<br>• Allow all outgoing traffic from intranet | Non-credential Scanning |
| Untrusted (DMZ) | **Incoming connection :**<br>• Allow only authorized internet services[2] access from Internet<br>• Allow incoming traffic from DMZ and intranet except for exceptional cases, such as from a compromised node<br>**Outgoing connection :**<br>• Allow all outgoing traffic from DMZ | Credential Scanning |

Notes:
[1] Required services – services which department is required and would like to grant access for.

[2] Authorized internet services – Web, Email, Ping services allow to be accessed from the Internet. For detail protocol and ports, please refer to Appendix I.

## B. Procedures for Raising Exception Request for Authorized Internet Services

### Purpose

Departments/units may raise exception request for releasing recommended security protection and/or substantial access to the CUHK network devices.

### Frequency

Ad-hoc on request

### Direct Approval

ITSC might directly approve exception requests to accelerate the process, provided that the application at least fulfilled the following criteria:-

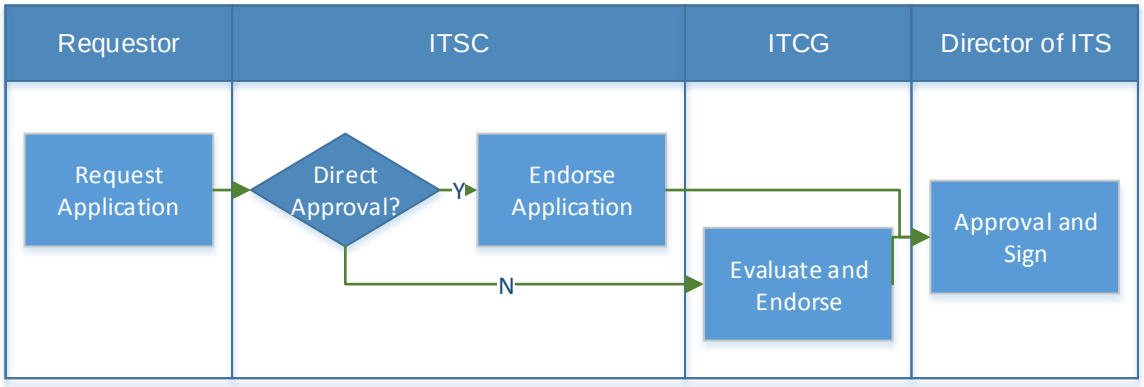
- Same or more restricted security level
- Not violating the rationale of minimum security standard
- With actual need and reasonable justification, normally convenience is not a valid justification.

### Extensive Evaluation

For application that does not meet criteria for direct approval, or needs more thorough evaluation, it would undergo a more extensive evaluation by ITSC and seek endorsement on IT Coordinator Group (ITCG) Meeting.

### Procedures

As a whole, exception request would go through the approval workflow, as illustrated below.




| Steps | Responsibility Role | Task |
|---|---|---|
| **1** | LAN Admin or System Support | Submit request application via eForm "Firewall Exception Request for Releasing / Revoking Authorized Service" |
| **2** | ITSC Information Security Section (ISS) | Evaluate submitted request and determine if it could be approved directly |
| **3** | *Direct Approval* | |
| **3.1** | ITSC Information Security Section (ISS) | Endorse the application |
| **4** | *Extensive Evaluation* | |
| **4.1** | ITSC Information Security Section (ISS) | Consolidate requests and submit to IT Coordinator Group (ITCG) |
| **4.2** | IT Coordinator Group (ITCG) | Evaluate all submitted requests and endorse the application in IT Coordinator Group (ITCG) meeting |
| **5** | Director of ITS | Approve and sign the request |
| **6** | ITSC | Keep record and monitor the request |

1. Requesting party should submit the request with justification to ITSC via eForm "Firewall Exception Request for Releasing / Revoking Authorized Service".
2. Information Security Section (ISS) of ITSC should evaluate the submitted request and determine if it could be approved directly.
3. For requests that could be approved directly, ISS endorses and passes to the Director of ITS for approval.
4. For requests that requires extensive evaluation,
   4.1. ITSC should consolidate the requests and submit to IT Coordinator Group (ITCG).
   4.2. IT Coordinator Group (ITCG) should evaluate justification of the requests and endorse the application in IT Coordinator Group (ITCG) meeting.
5. Director of ITS should review and approve acceptance of the requests and forward to ITSC for recording.
6. ITSC would record down the request details, and update monitoring configuration such as that in vulnerability scanning.

Besides, colleagues should update ITSC for any changes of approved request.

## C. Enquiry and Support

This document may not cover all cases and situations and there may be some exceptional situations which need to be assessed and considered individually. If you have any enquiries, please contact ITSC Information Security Section (ISS) at infosec@cuhk.edu.hk.

**Appendix I :**

Authorized Internet services – services allow to be accessed from Internet.

| Service Name | Protocol | Port | Service Description |
|---|---|---|---|
| Echo/Trace Route | UDP | 7 | Ping service |
| HTTP | TCP | 80 | Web service |
| HTTPS | TCP | 443 | Secure web service |
| SMTP | TCP | 25 | Simple mail transfer protocol (SMTP) |
| SMTP (SSL) | TCP | 465 | SMTP over SSL service |
| SMTP over TLS | TCP | 587 | SMTP over TLS service |
| IMAPS | TCP | 993 | Secure IMAP service |
| POPS | TCP | 995 | Secure POP service |