WARCS (Wide Area Remote Control for SPring-8)

A. Yamashita and Y.Furukawa

SPring-8, Japan

Control System Cyber-Security Workshop (CS)2/HEP

Oct.14 2007 Knoxville,TN USA

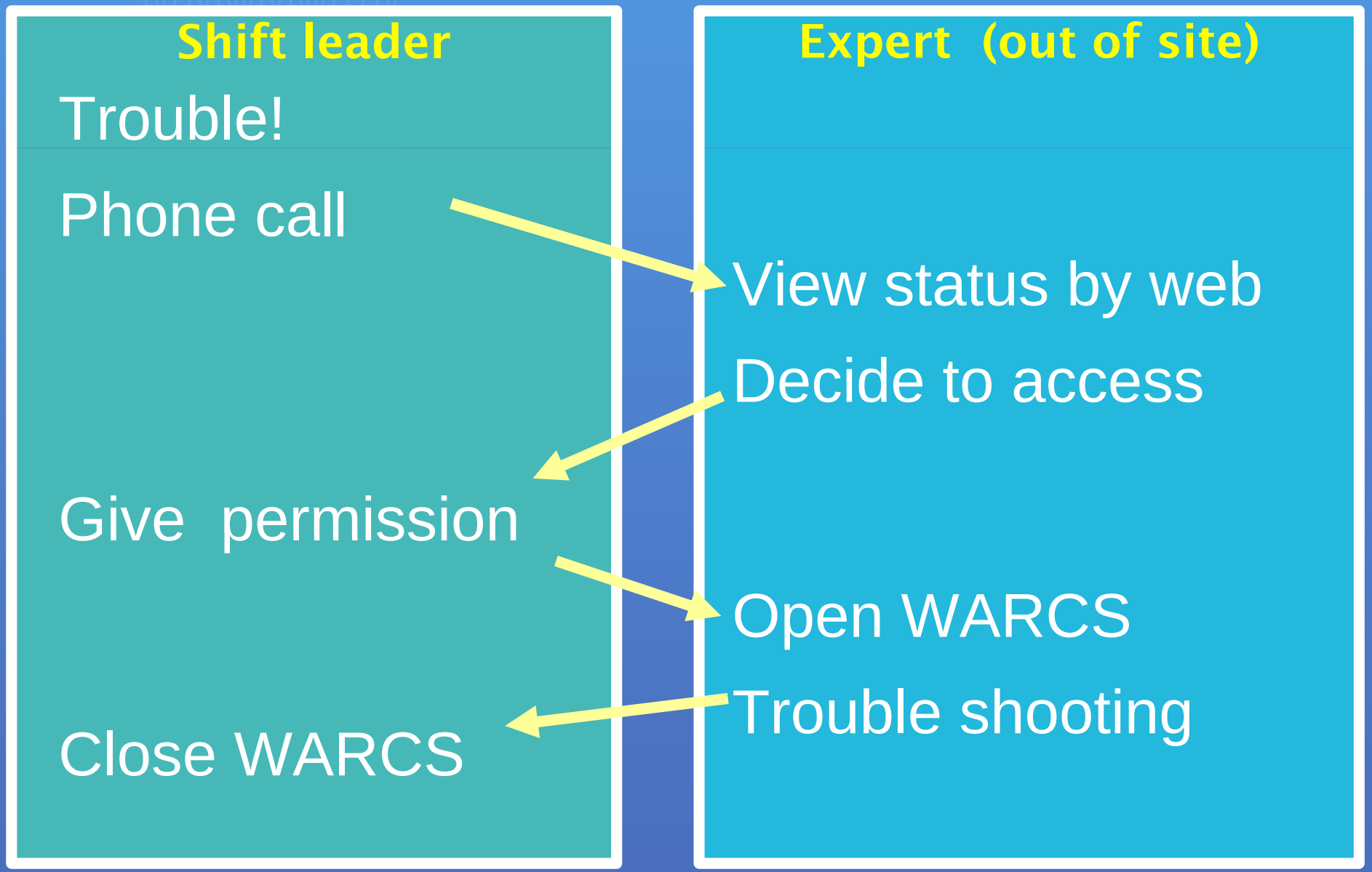
Contents

- What is WARCS?
- Requirements
  - SPring-8 operation policy
- Implementation
- Operation
- Conclusion

What is WARCS?

- Access tool for SPring-8 control system from the Internet.
- It is used at the trouble time
  - CALL the expert(s) by phone
  - The expert can access SPring-8 control network from internet using WARCS.
  - Mobile client, not fixed PC.
- Originally developed at SPring-8
  - NO ssh (Secure Shell), NO VPN (virtual private network)
  - Combination of open sources.

Scinario


Shift leader
Trouble!
Phone call
Give permission
Close WARCS
Expert (out of site)
View status by web
Decide to access
Open WARCS
Trouble shooting

SPring-8 operation policy

Every activity
on the accelerators
must be
under control
of the shift leader.

Requirements 1

- Connect under permission of the shift leader.
  - **No free access** from the outside.
  - Shift leader monitors connection status.
  - Shift leader can disconnect at any time.
- Two type of clients
  - telnet for terminal access.
  - Remote screen (VNC)
- Multi-platform
  - Client: Windows, Mac, Linux
  - Server: HP-UX, Linux

Requirements 2

- Easy operation.
  - Installation.
    - Install client software to individual note PC.
  - Operation.
    - Just type password.
- Secure
  - Encrypted communication.
  - One time password.
- Multi-user
  - Multiple-connection at one time.

Software Tools

Server

Server/Client

- Zebedee
  - Encryption
  - Authentication
- VNC
  - Screen sharing.
- Python
  - glueing

- Apache
  - Communication
- SQLite
  - Data store
- iptable
  - Embedded firewall for Linux

Zebedee

- IP tunneling tool
  - **Z**lib compression
  - **B**lowfish encryption
  - **D**iffie-Hellman key agreement (authentication)
- Open arbitrary ip-port
  - Client ip-port
    - For multiple connection
  - Host ip-port
    - Specify target application

Zebedee

- Multiple zebedee process can run simultaneously
  - One zebedee server for one user connection.
  - Individual control to zebedee process.

Why not ssh nor VPN

- SSH/VPN
  - Tools for free access
    - Difficult to be controlled from outside.
    - Security problem
      - If a note PC with private key is stolen?
  - Account base
    - Administration effort – new or obsolete account
    - Common account is risky.
- VPN (SSL-VPN)
  - Appliance
    - Hard to customize

VNC (Virtual Network Computer)

- Screen sharing program
  - With multiple users (not only 1-1, 1 to many)
- Free
- Multi platform
  - Not only Win, Mac, UNIX but also PDA
- Open standard
  - Many implementation
  - Ultr@VNC for Win
    - Shrink large screen to fit small screen
    - 20” screen into 11” note PC's screen
- Image compression level can be selected.
  - Select by connection condition.

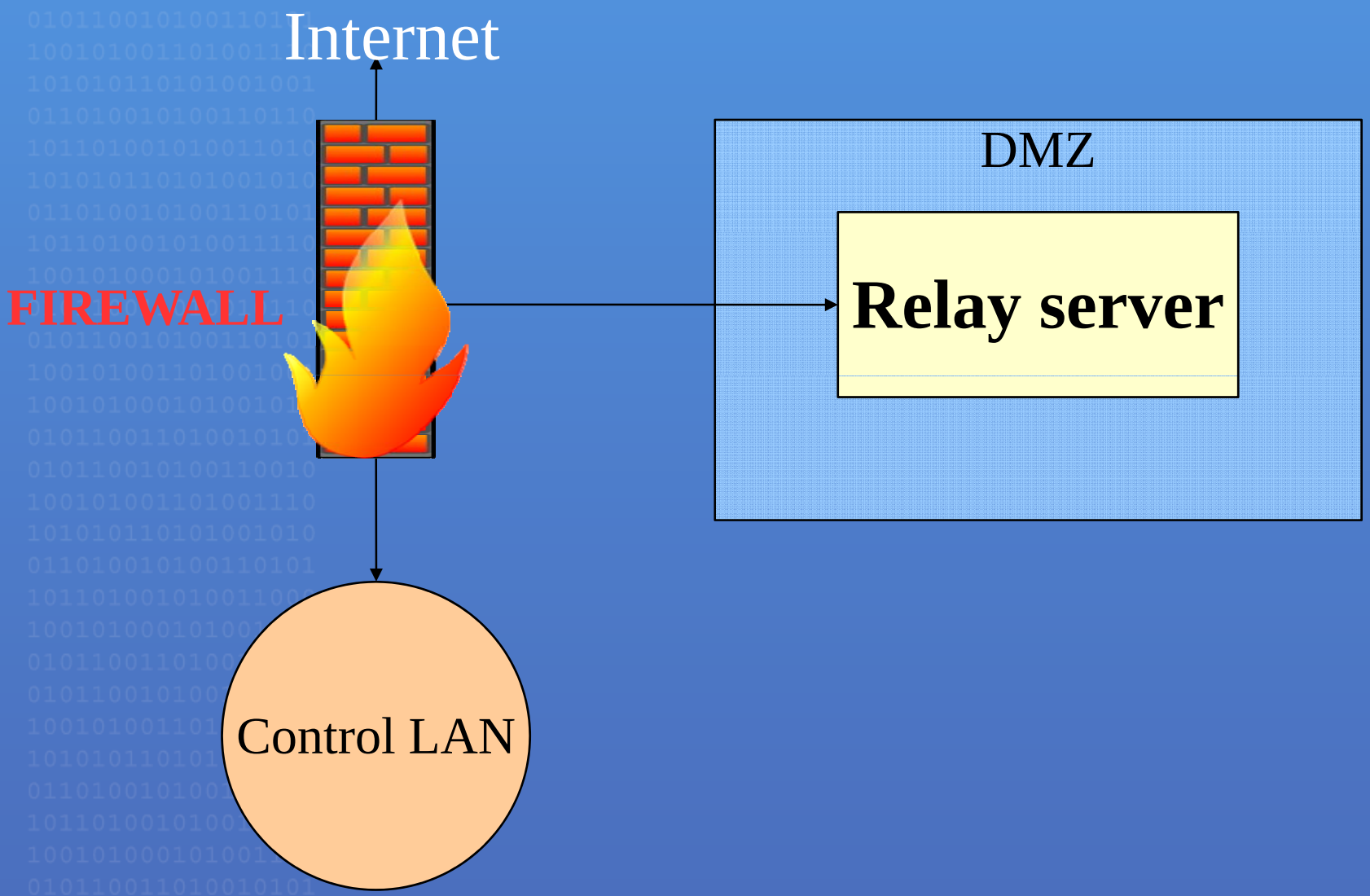
Other tools

- Apache (http server)
  - Know user's address by REMOTE_ADDR environment variable.
    - Users behind NAT don't know their global ip-addresses.
- SQLite
  - File and library based database.
    - No client-server
    - No configuration
  - Share information between processes.

Other tools

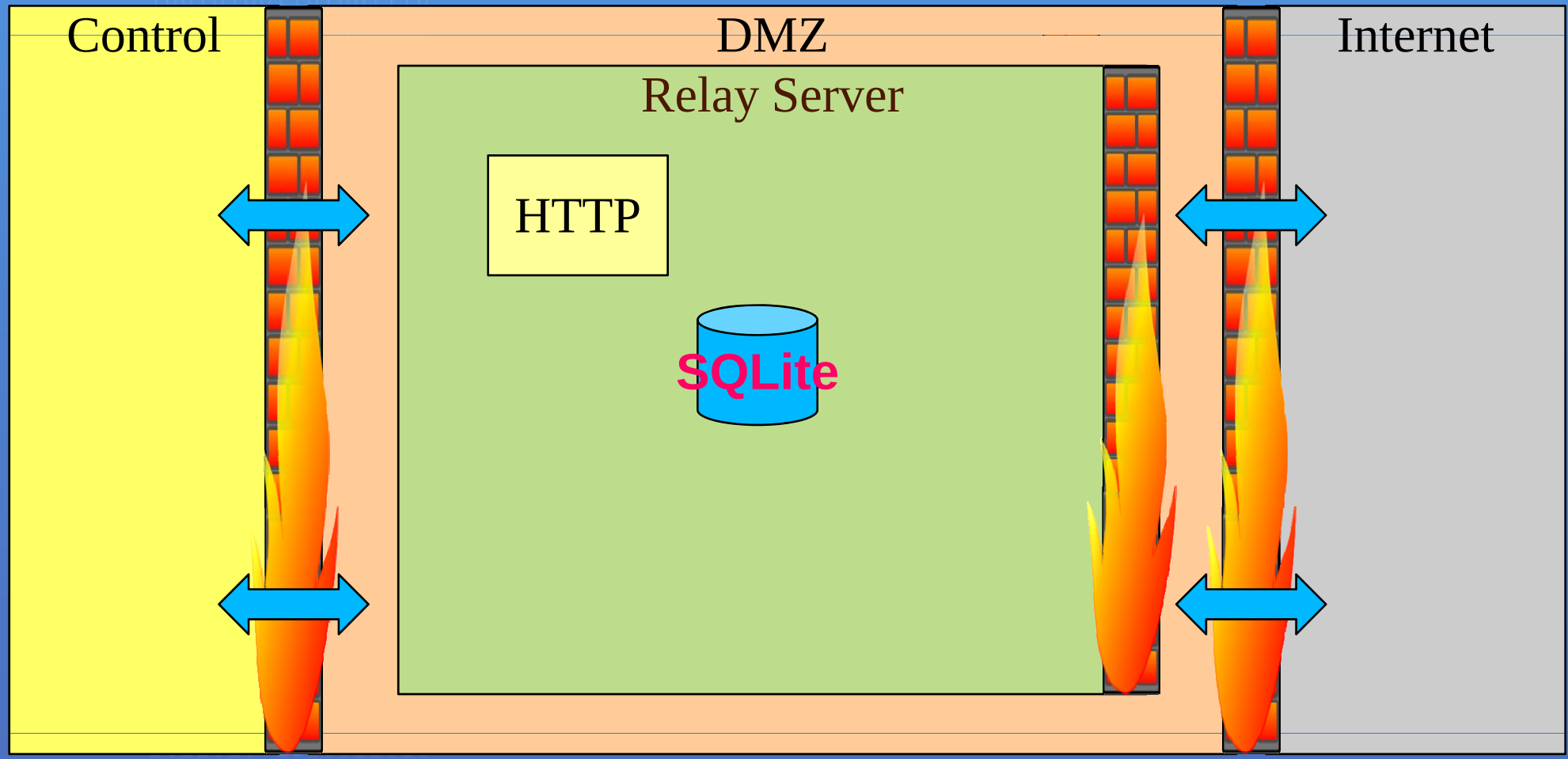
- Iptables
  - Linux firewall in its kernel.
  - Tunnel can be added/removed without restarting

Network scheme

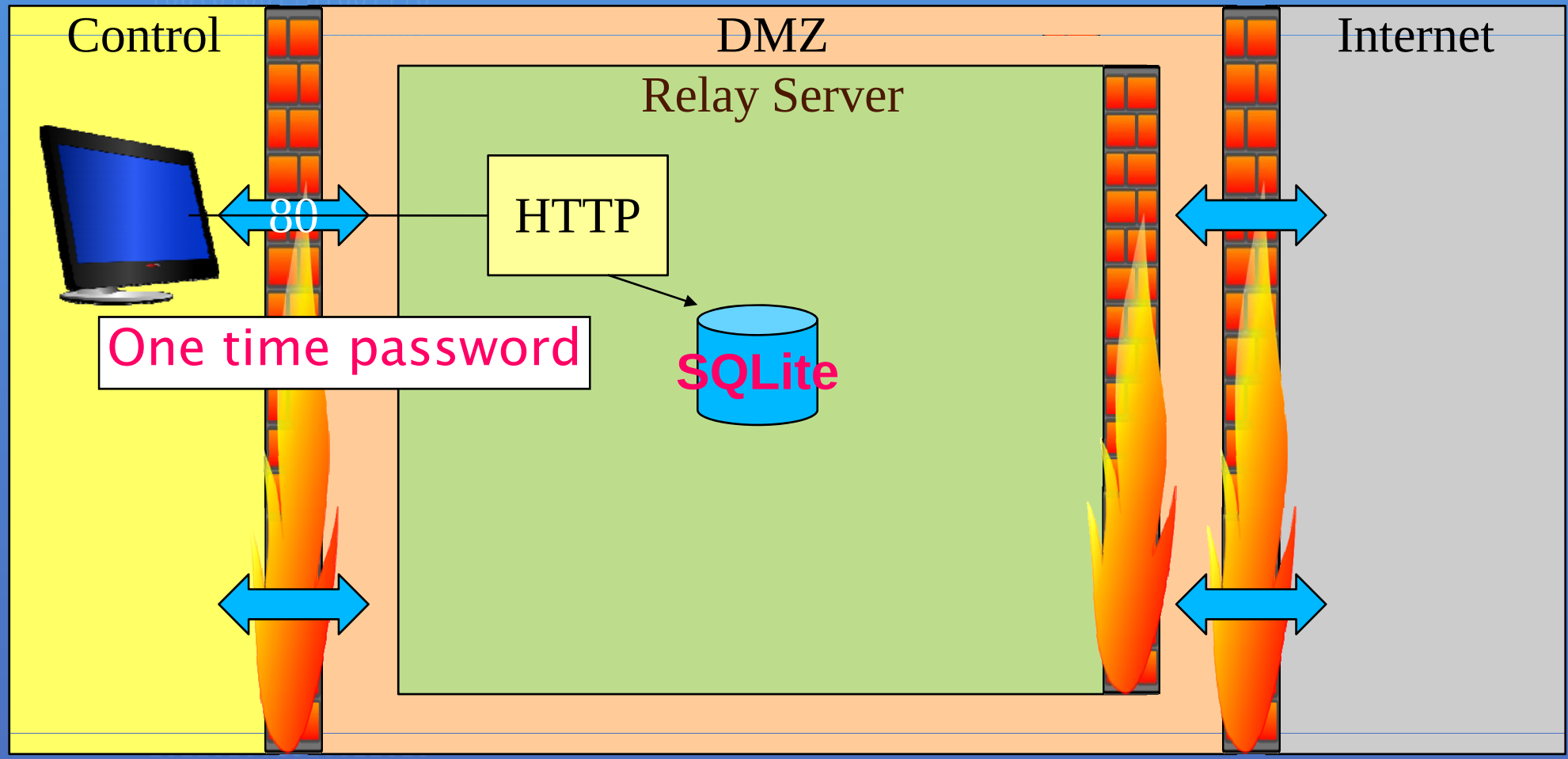


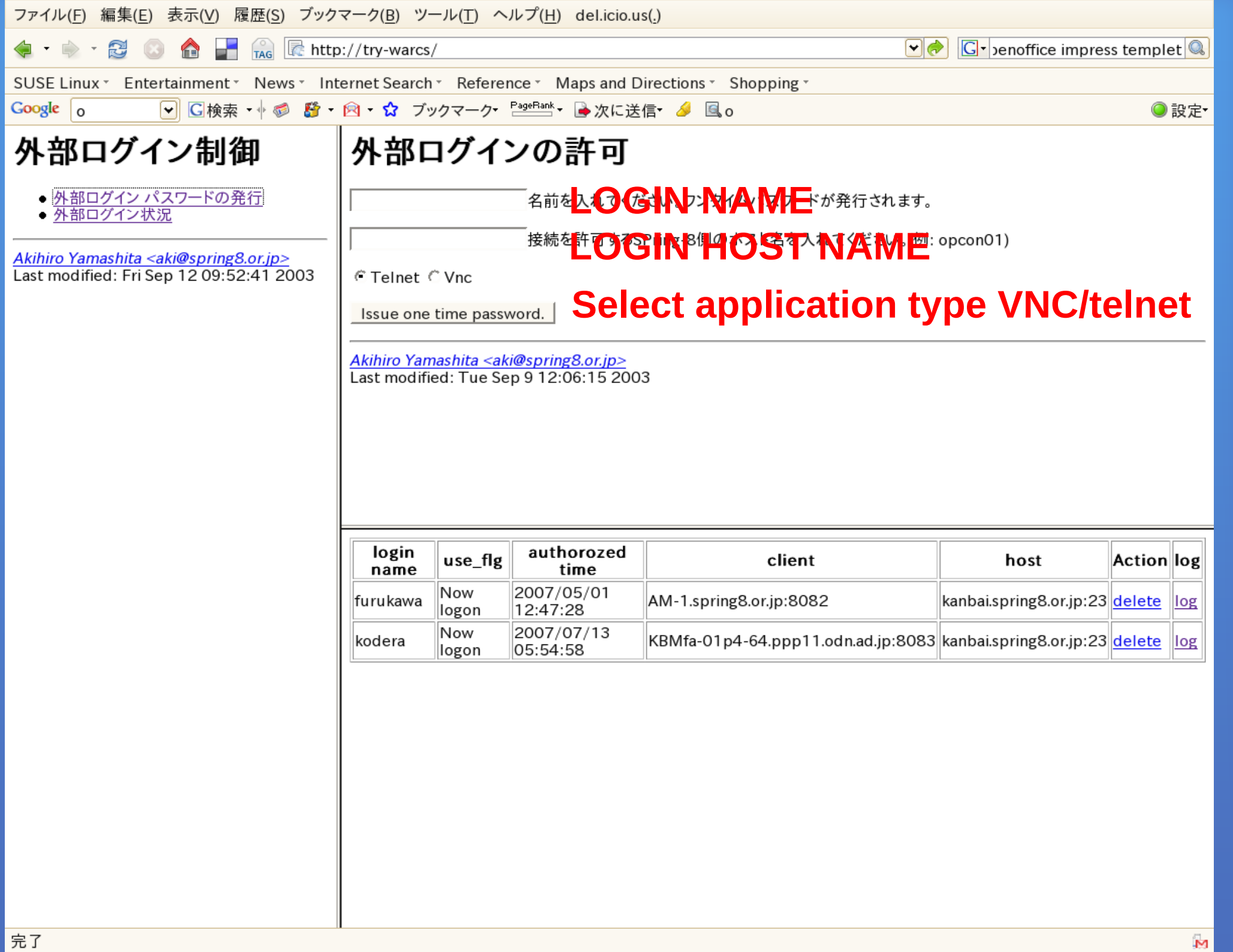
How WARCS works?

At the beginning



Issue one time password and record




ファイル(F) 編集(E) 表示(V) 履歴(S) ブックマーク(B) ツール(T) ヘルプ(H) del.icio.us(.)
http://try-warcs/
SUSE Linux Entertainment News Internet Search Reference Maps and Directions Shopping
Google 検索 ブックマーク PageRank 次に送信 設定
外部ログイン制御
外部ログイン パスワードの発行
外部ログイン状況
Akihiro Yamashita <aki@spring8.or.jp>
Last modified: Fri Sep 12 09:52:41 2003
外部ログインの許可
LOGIN NAME
LOGIN HOST NAME
Select application type VNC/telnet
名前を入れてください。ワンタイムパスワードが発行されます。
接続を許可するSPring-8側のホスト名を入れてください。(例: opcon01)
Telnet Vnc
Issue one time password.
Akihiro Yamashita <aki@spring8.or.jp>
Last modified: Tue Sep 9 12:06:15 2003
login name
use_flg
authorozed time
client
host
Action
log
furukawa
Now logon
2007/05/01 12:47:28
AM-1.spring8.or.jp:8082
kanbai.spring8.or.jp:23
delete
log
kodera
Now logon
2007/07/13 05:54:58
KBMfa-01p4-64.ppp11.odn.ad.jp:8083
kanbai.spring8.or.jp:23
delete
log
完了

外部ログイン制御

- 外部ログイン パスワードの発行
- 外部ログイン状況

Akihiro Yamashita <aki@spring8.or.jp>
Last modified: Fri Sep 12 09:52:41 2003

外部ログインの許可

yamashita 名前を入れてください。ワンタイムパスワードが発行されます。

conti 接続を許可するSPring-8側のホスト名を入れてください。(例: opcon01)

Telnet Vnc

Issue one time password.

Akihiro Yamashita <aki@spring8.or.jp>
Last modified: Tue Sep 9 12:06:15 2003

login name	use_flg	authorozed time	client	host	Action	log
furukawa	Now logon	2007/05/01 12:47:28	AM-1.spring8.or.jp:8082	kanbai.spring8.or.jp:23	delete	log
kodera	Now logon	2007/07/13 05:54:58	KBMfa-01p4-64.ppp11.odn.ad.jp:8083	kanbai.spring8.or.jp:23	delete	log

外部ログイン制御

- 外部ログイン パスワードの発行
- 外部ログイン状況

Akihiro Yamashita <aki@spring8.or.jp>
Last modified: Fri Sep 12 09:52:41 2003

[(8083.0, 8082.0)]

OK!

user	yamashita
host	conti
port	8081
host port	23
password	9930771

ONE TIME PASSWORD

login name	use_flg	authorozed time	client	host	Action	log
furukawa	Now logon	2007/05/01 12:47:28	AM-1.spring8.or.jp:8082	kanbai.spring8.or.jp:23	delete	log
kodera	Now logon	2007/07/13 05:54:58	KBMfa-01p4-64.ppp11.odn.ad.jp:8083	kanbai.spring8.or.jp:23	delete	log

外部ログイン制御

- 外部ログイン パスワードの発行
- 外部ログイン状況

Akihiro Yamashita <aki@spring8.or.jp>
Last modified: Fri Sep 12 09:52:41 2003

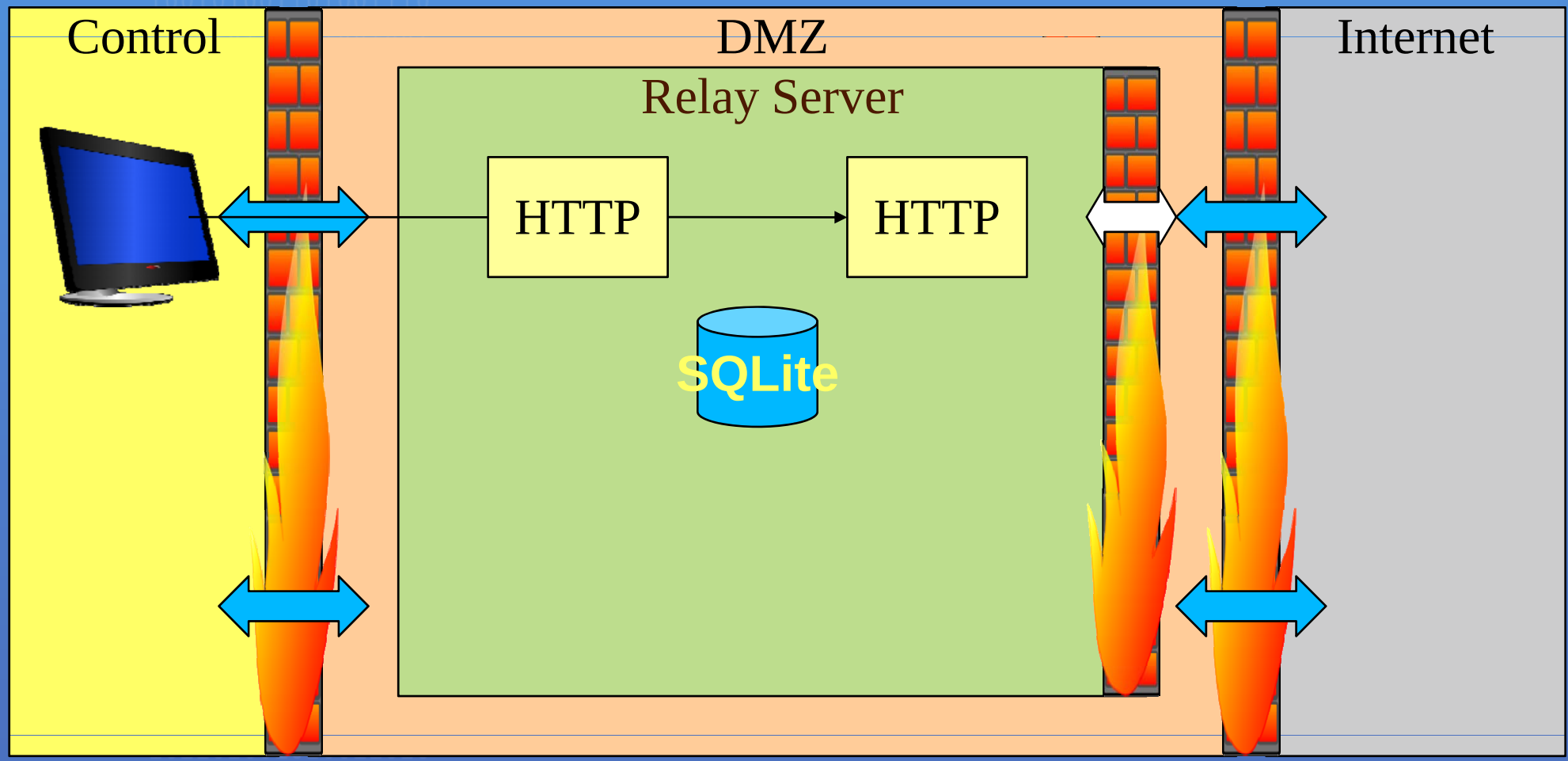
[(8083.0, 8082.0)]

OK!

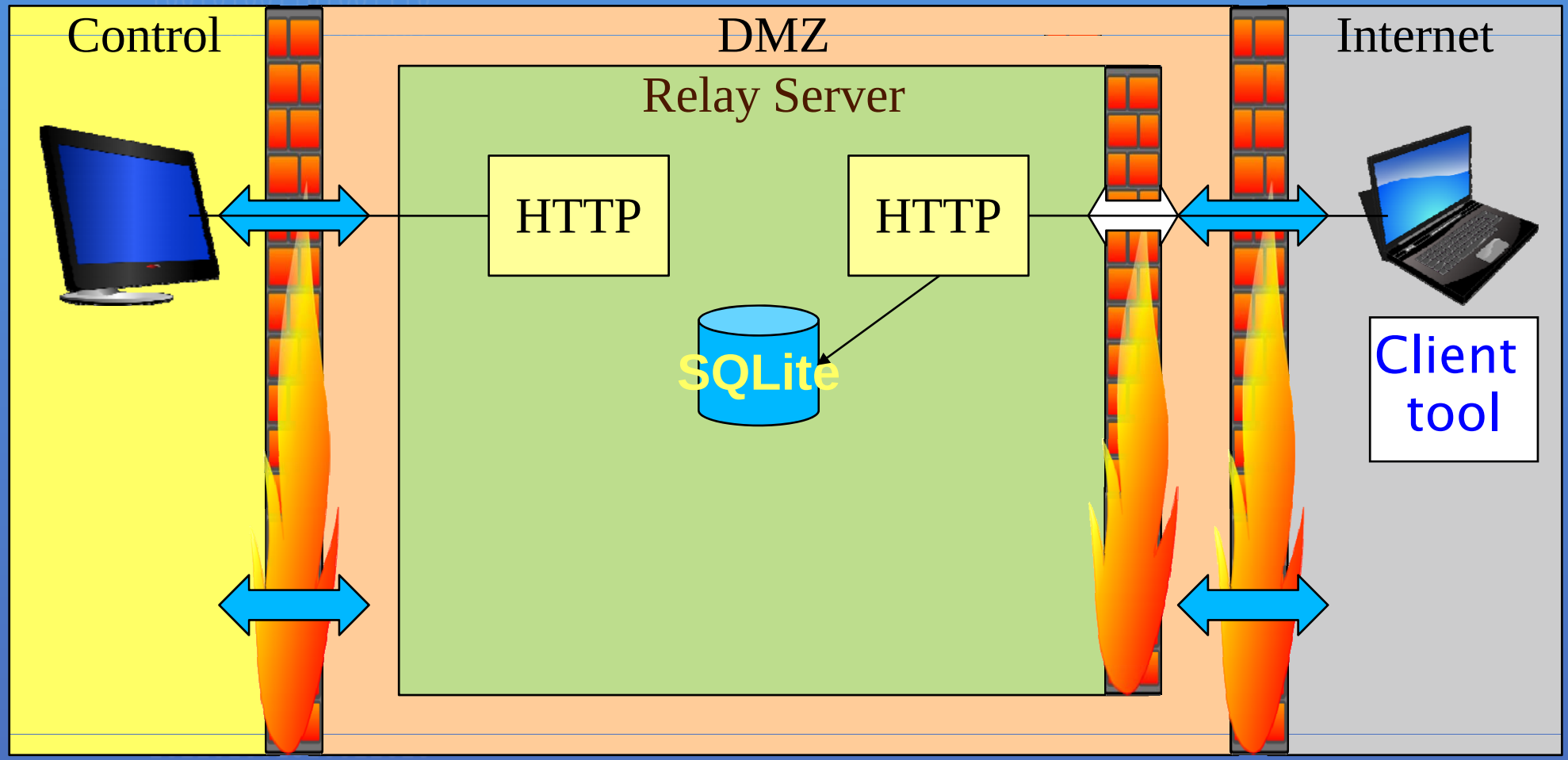
user	yamashita
host	conti
port	8081
host port	23
password	9930771

login name	use_flg	authorozed time	client	host	Action	log
furukawa	Now logon	2007/05/01 12:47:28	AM-1.spring8.or.jp:8082	kanbai.spring8.or.jp:23	delete	log
kodera	Now logon	2007/07/13 05:54:58	KBMfa-01p4-64.ppp11.odn.ad.jp:8083	kanbai.spring8.or.jp:23	delete	log
yamashita	Not yet login	2007/10/04 10:07:04	NOTYET:8081	conti.spring8.or.jp:23	delete	log

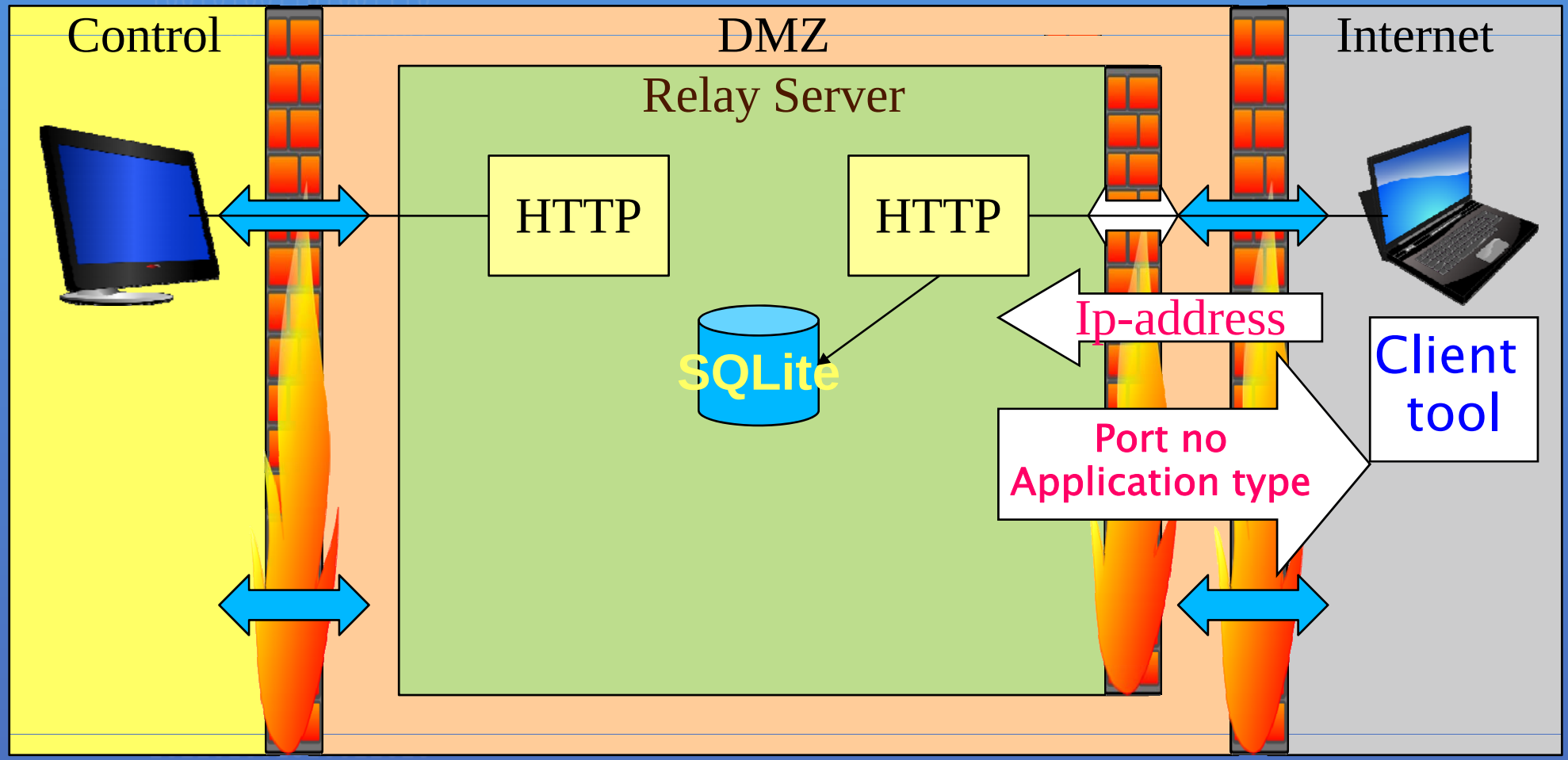
Launch another HTTP and open tunnel in iptables firewall for http



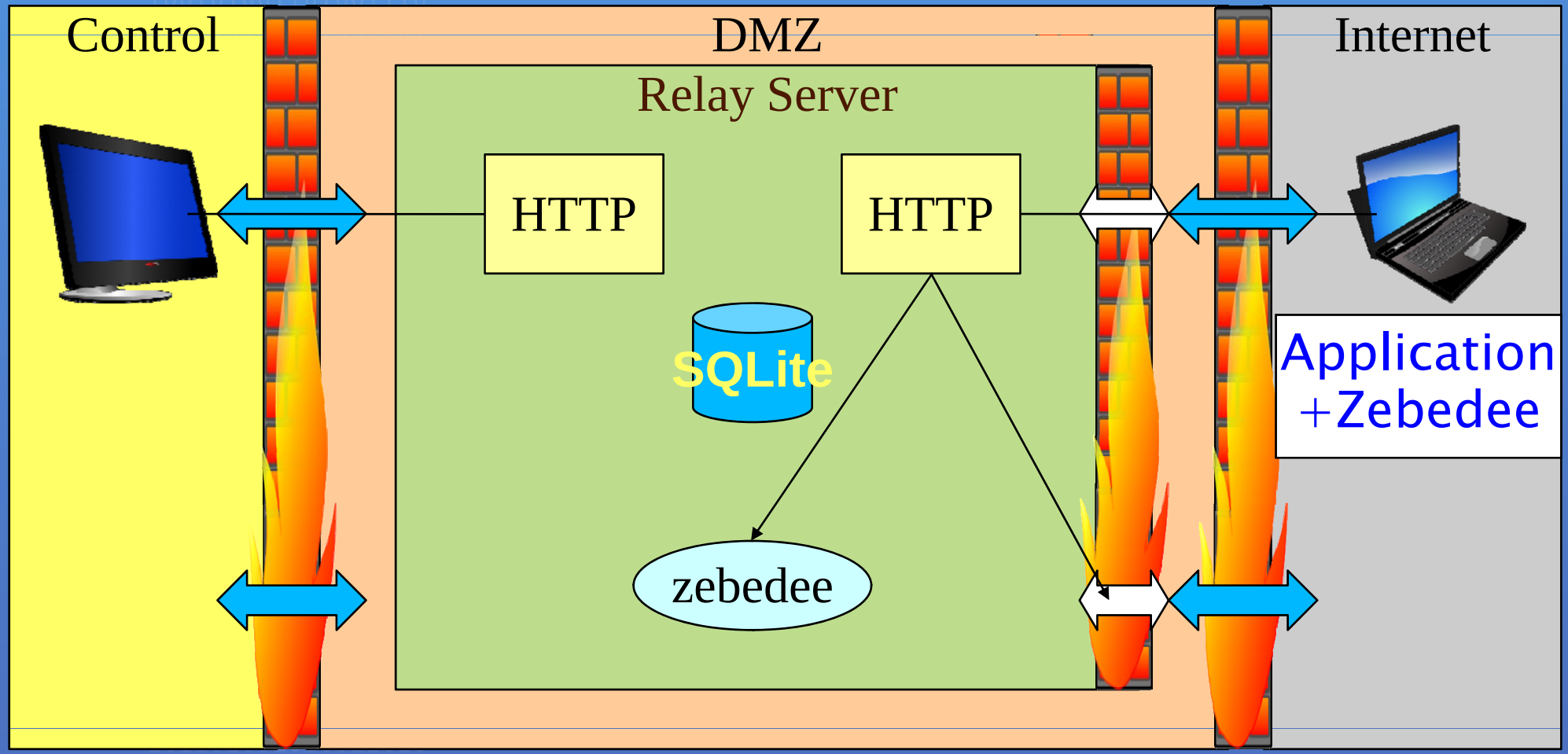
Client launches client tool and enter one time password



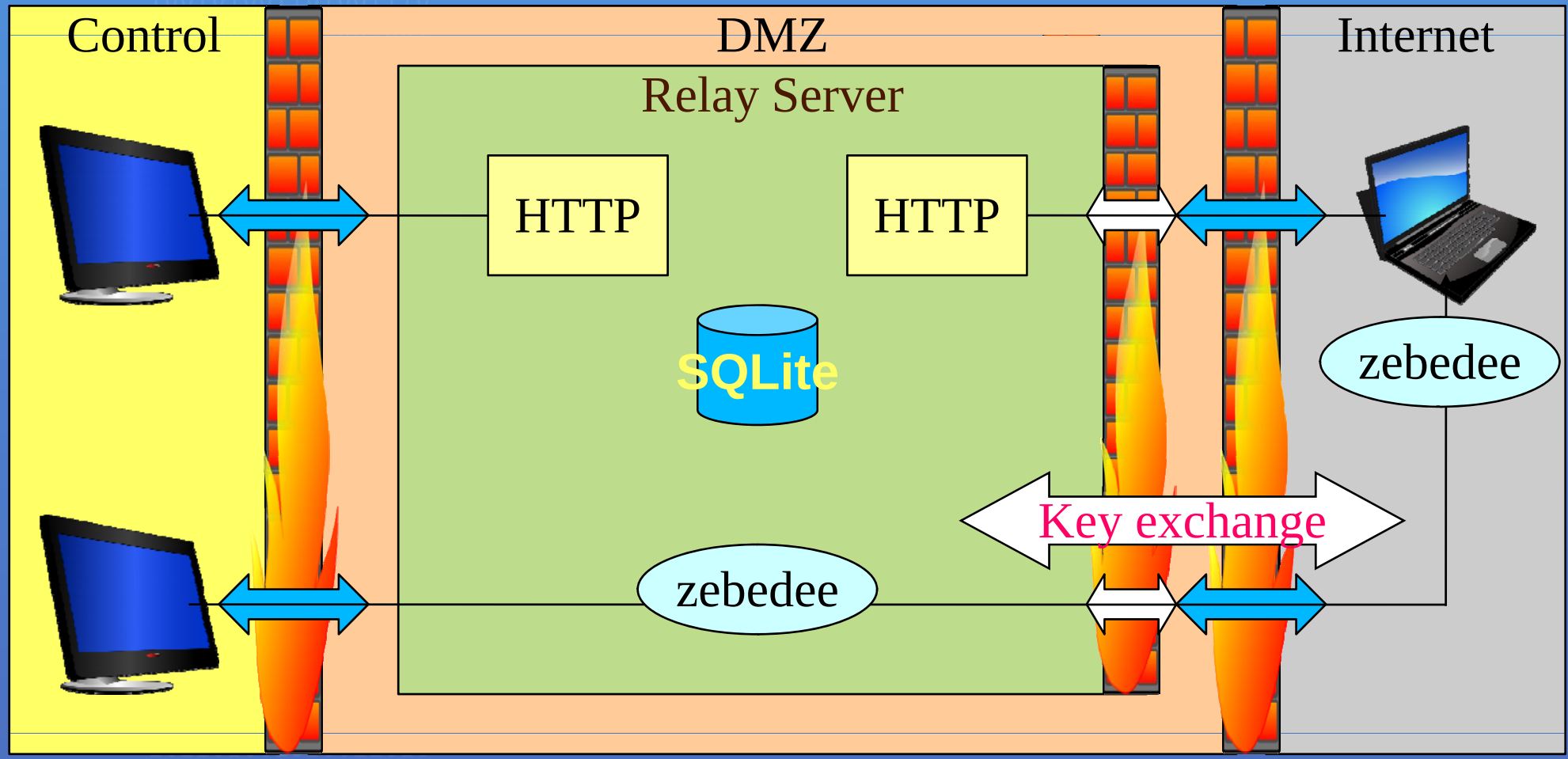
Exchange ip-address and port no, application type



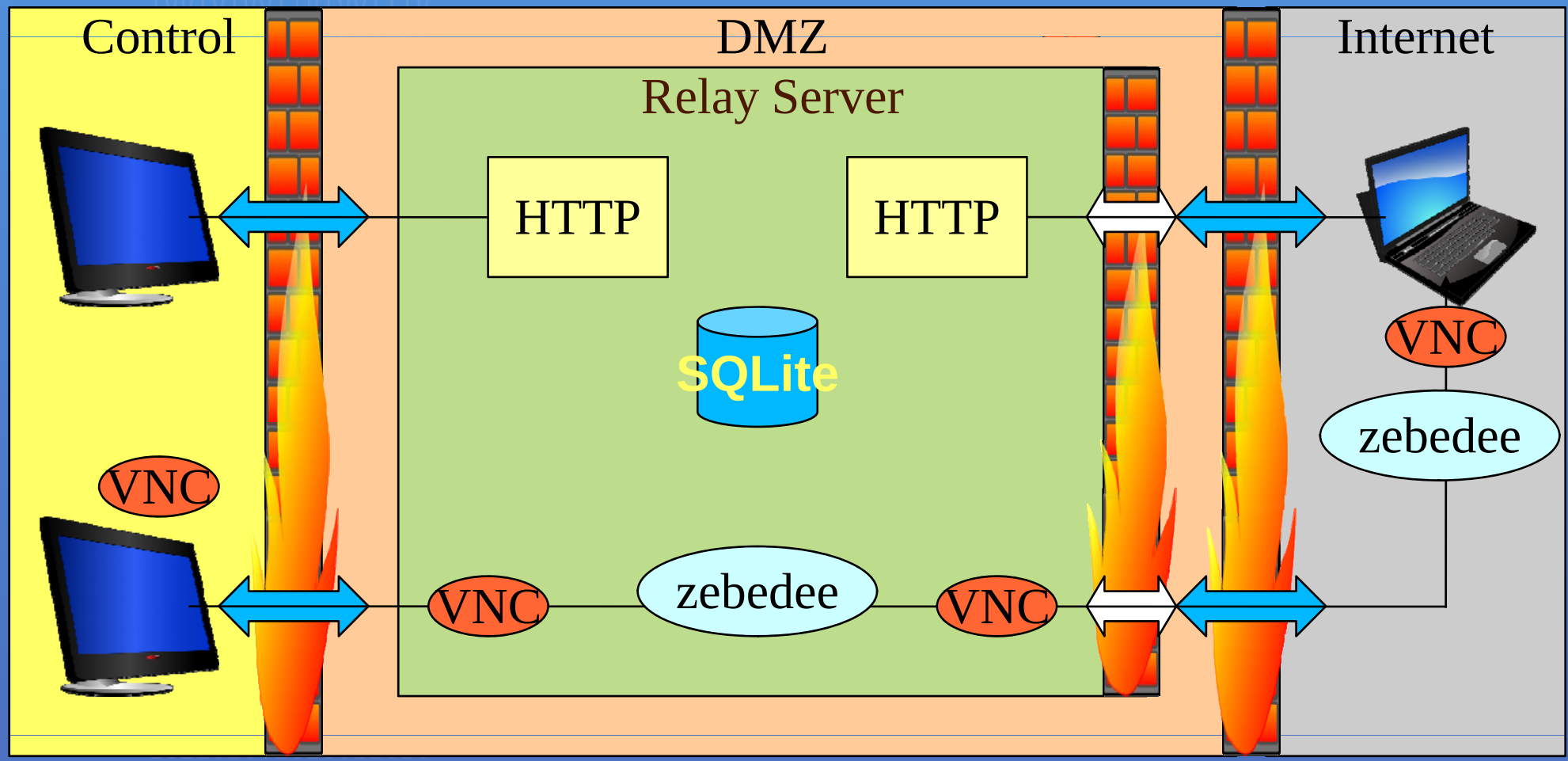
Open tunnel and launch zebedee.

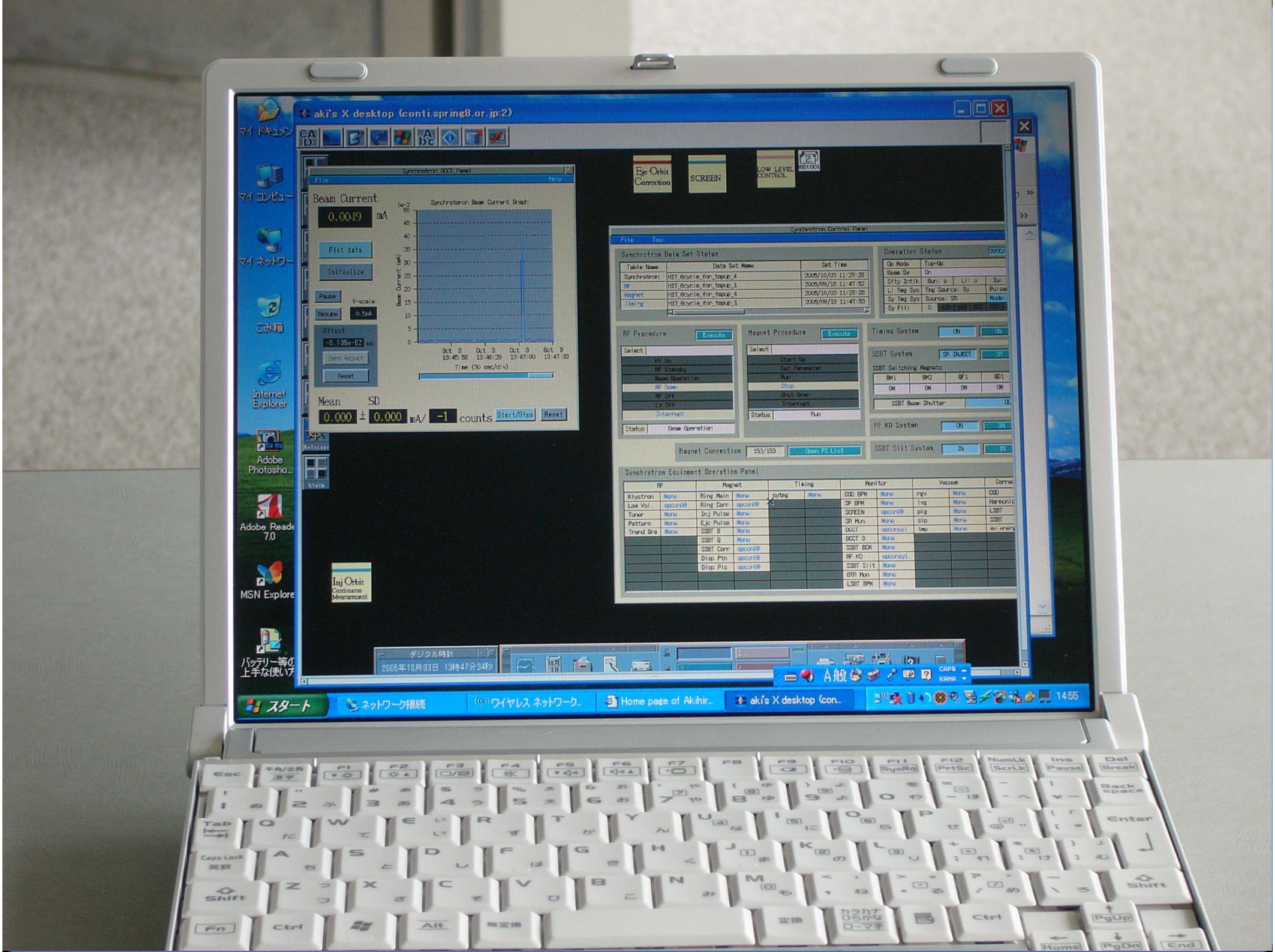


Establish connection with authentication

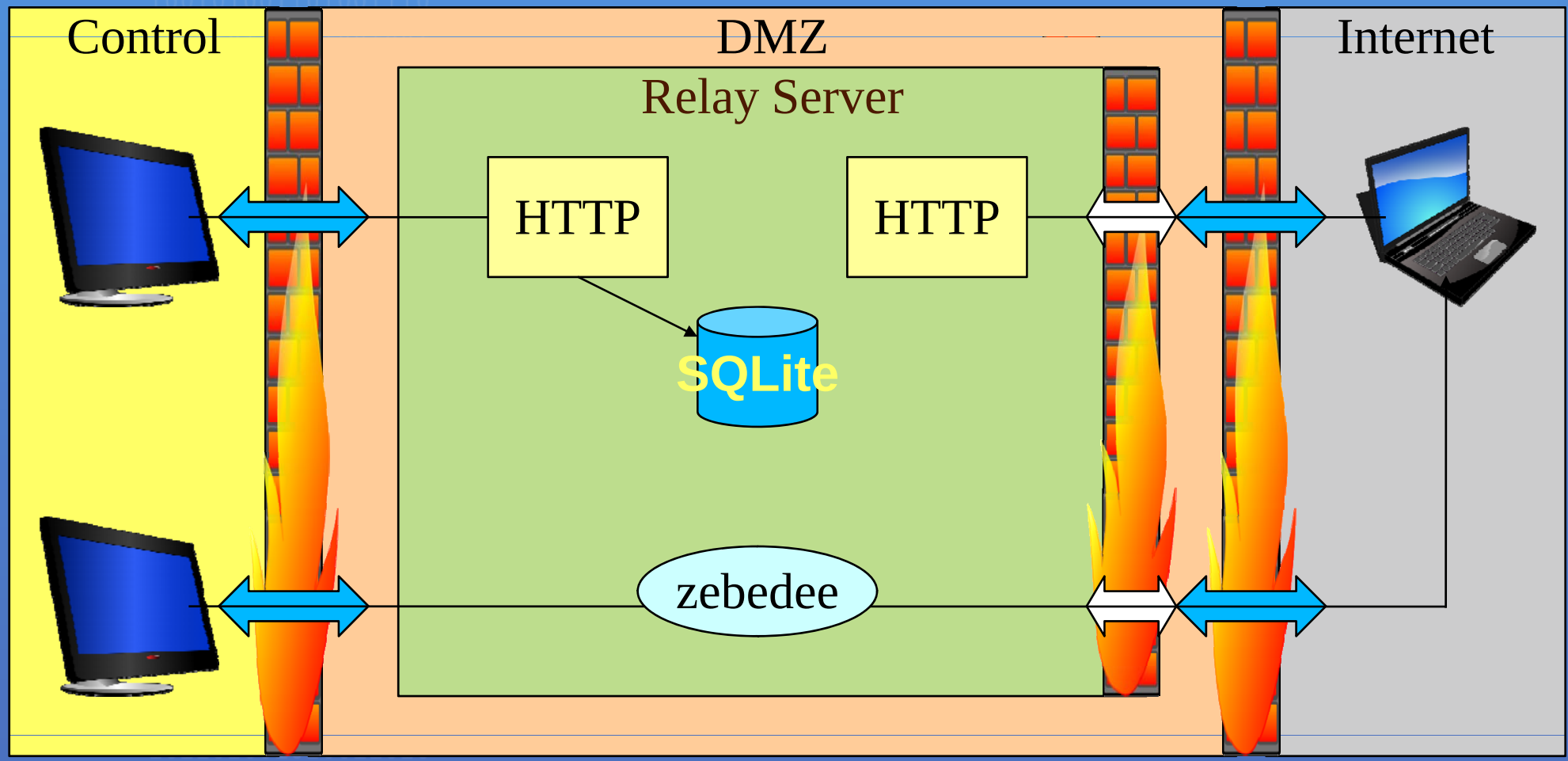


VNC (Virtual network computer) is also available.




aki's X desktop (conti.spring8.or.jp:2)
Beam Current
0.0049
mA
Plot data
Initialize
Pause
Resume
Offset
Reset
Mean
SD
0.000
0.000
counts
Start/Stop
Reset
Eje Orbit Correction
SCREEN
LOW LEVEL CONTROL
Synchrotron Control Panel
Synchrotron Data Set Status
Operation Status
RF Procedure
Magnet Procedure
Timing System
SSBT System
SSBT Switching Magnets
SSBT Beam Shutter
RF KO System
SSBT Slit System
Magnet Connection
Synchrotron Equipment Operation Panel
Inj Orbit Continuous Measurement
スタート
ネットワーク接続
ワイヤレス ネットワーク
Home page of Akihir...
aki's X desktop (con...
14:55

Shift leader monitors and controls status by Web



外部ログイン制御

- 外部ログイン パスワードの発行
- 外部ログイン状況

Akihiro Yamashita <aki@spring8.or.jp>
Last modified: Fri Sep 12 09:52:41 2003

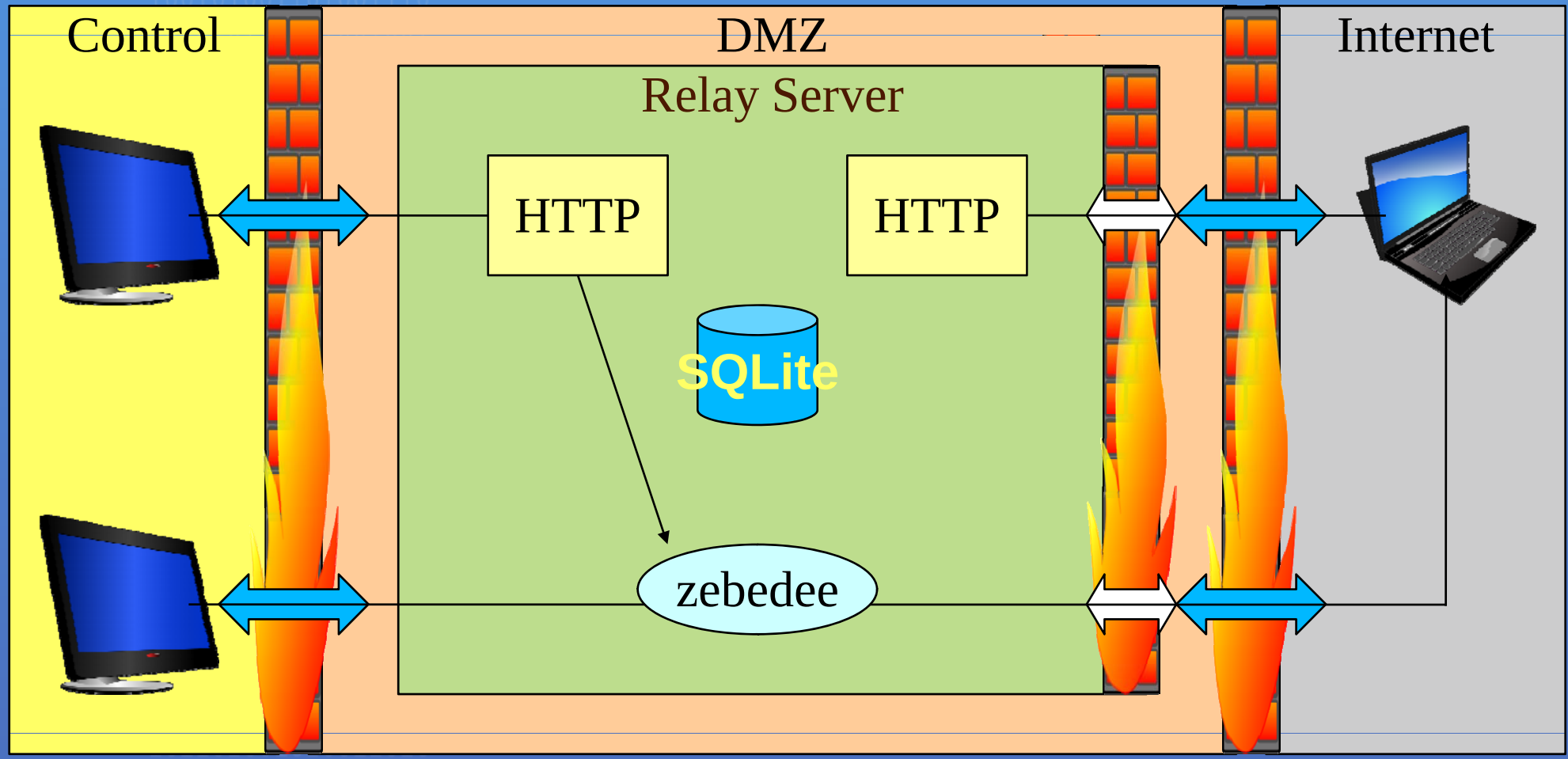
[(8083.0, 8082.0)]

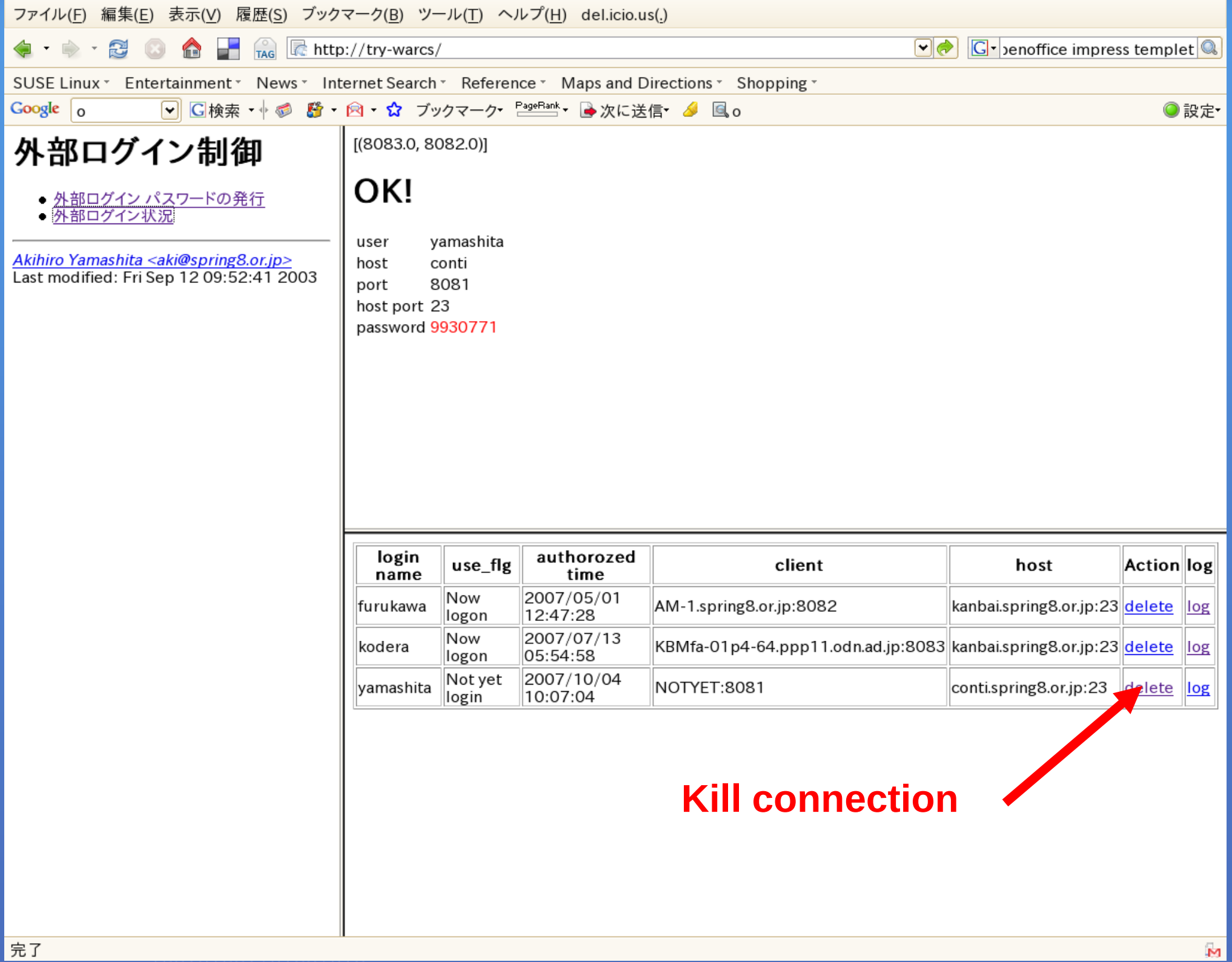
OK!

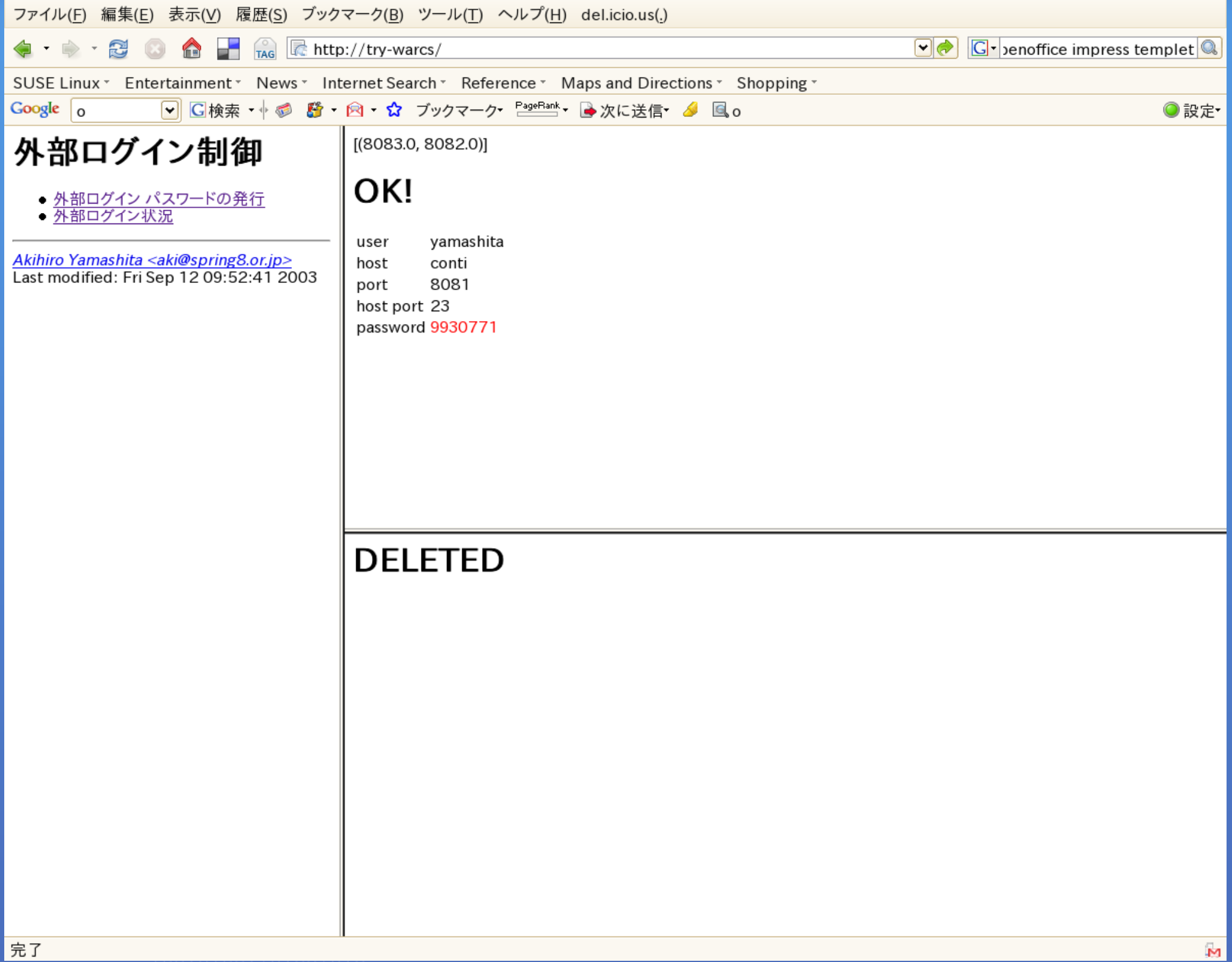
user	yamashita
host	conti
port	8081
host port	23
password	9930771

login name	use_flg	authorozed time	client	host	Action	log
furukawa	Now logon	2007/05/01 12:47:28	AM-1.spring8.or.jp:8082	kanbai.spring8.or.jp:23	delete	log
kodera	Now logon	2007/07/13 05:54:58	KBMfa-01p4-64.ppp11.odn.ad.jp:8083	kanbai.spring8.or.jp:23	delete	log
yamashita	Not yet login	2007/10/04 10:07:04	NOTYET:8081	conti.spring8.or.jp:23	delete	log

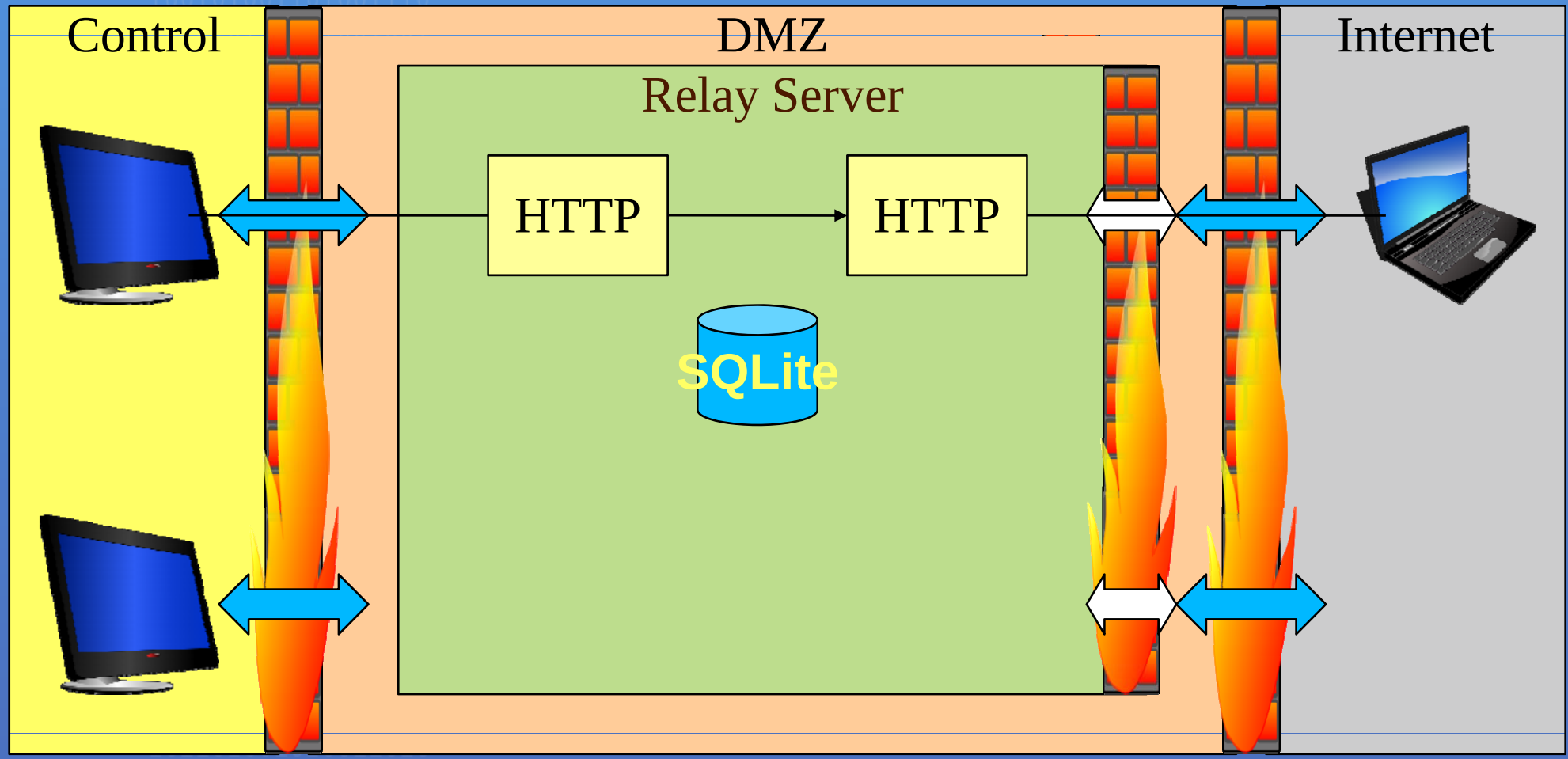
Shift leader ends WARCS (kill zebedee)



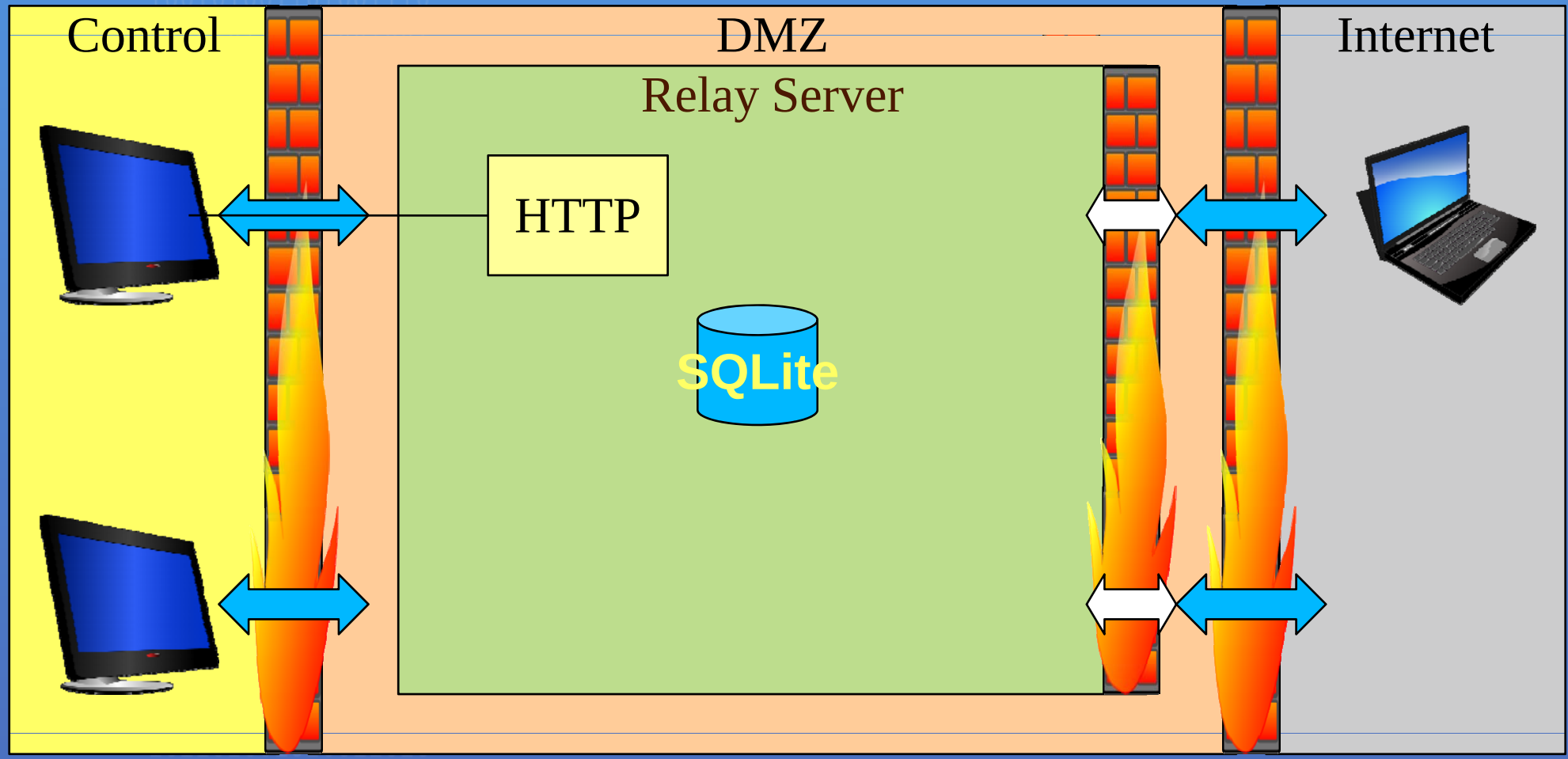

ファイル(F) 編集(E) 表示(V) 履歴(S) ブックマーク(B) ツール(T) ヘルプ(H) del.icio.us(.)
http://try-warcs/
SUSE Linux Entertainment News Internet Search Reference Maps and Directions Shopping
Google 検索 ブックマーク 次に送信 設定
外部ログイン制御
外部ログイン パスワードの発行
外部ログイン状況
Akihiro Yamashita <aki@spring8.or.jp>
Last modified: Fri Sep 12 09:52:41 2003
[(8083.0, 8082.0)]
OK!
user yamashita
host conti
port 8081
host port 23
password 9930771
login name
use_flg
authorozed time
client
host
Action
log
furukawa
Now logon
2007/05/01 12:47:28
AM-1.spring8.or.jp:8082
kanbai.spring8.or.jp:23
delete
log
kodera
Now logon
2007/07/13 05:54:58
KBMfa-01p4-64.ppp11.odn.ad.jp:8083
kanbai.spring8.or.jp:23
delete
log
yamashita
Not yet login
2007/10/04 10:07:04
NOTYET:8081
conti.spring8.or.jp:23
delete
log
Kill connection
完了


ファイル(F) 編集(E) 表示(V) 履歴(S) ブックマーク(B) ツール(T) ヘルプ(H) del.icio.us(.)
http://try-warcs/
SUSE Linux Entertainment News Internet Search Reference Maps and Directions Shopping
Google 検索 ブックマーク PageRank 次に送信 設定
外部ログイン制御
外部ログイン パスワードの発行
外部ログイン状況
Akihiro Yamashita <aki@spring8.or.jp>
Last modified: Fri Sep 12 09:52:41 2003
[(8083.0, 8082.0)]
OK!
user yamashita
host conti
port 8081
host port 23
password 9930771
DELETED
完了

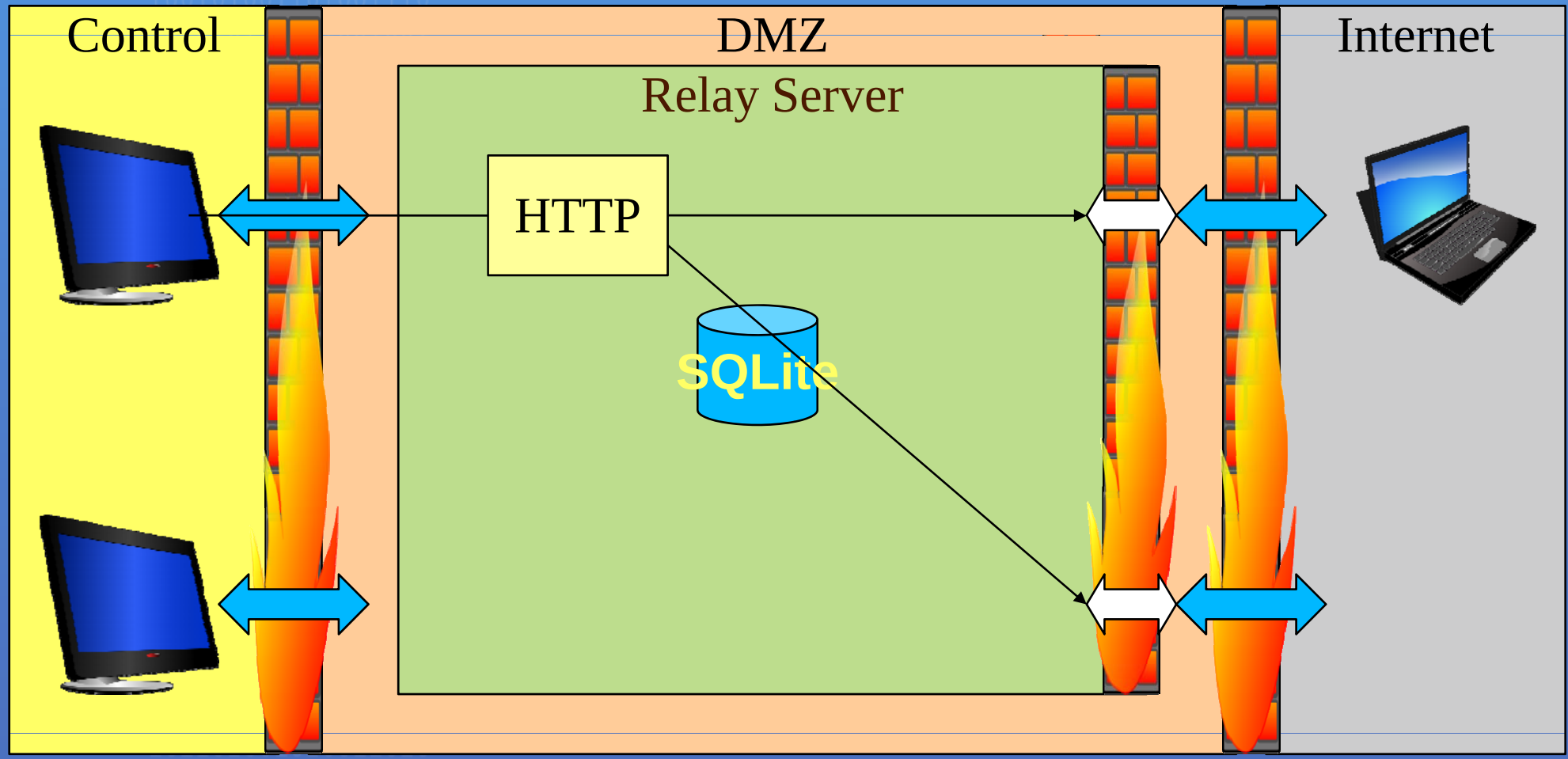
Shift leader ends WARCS kills http



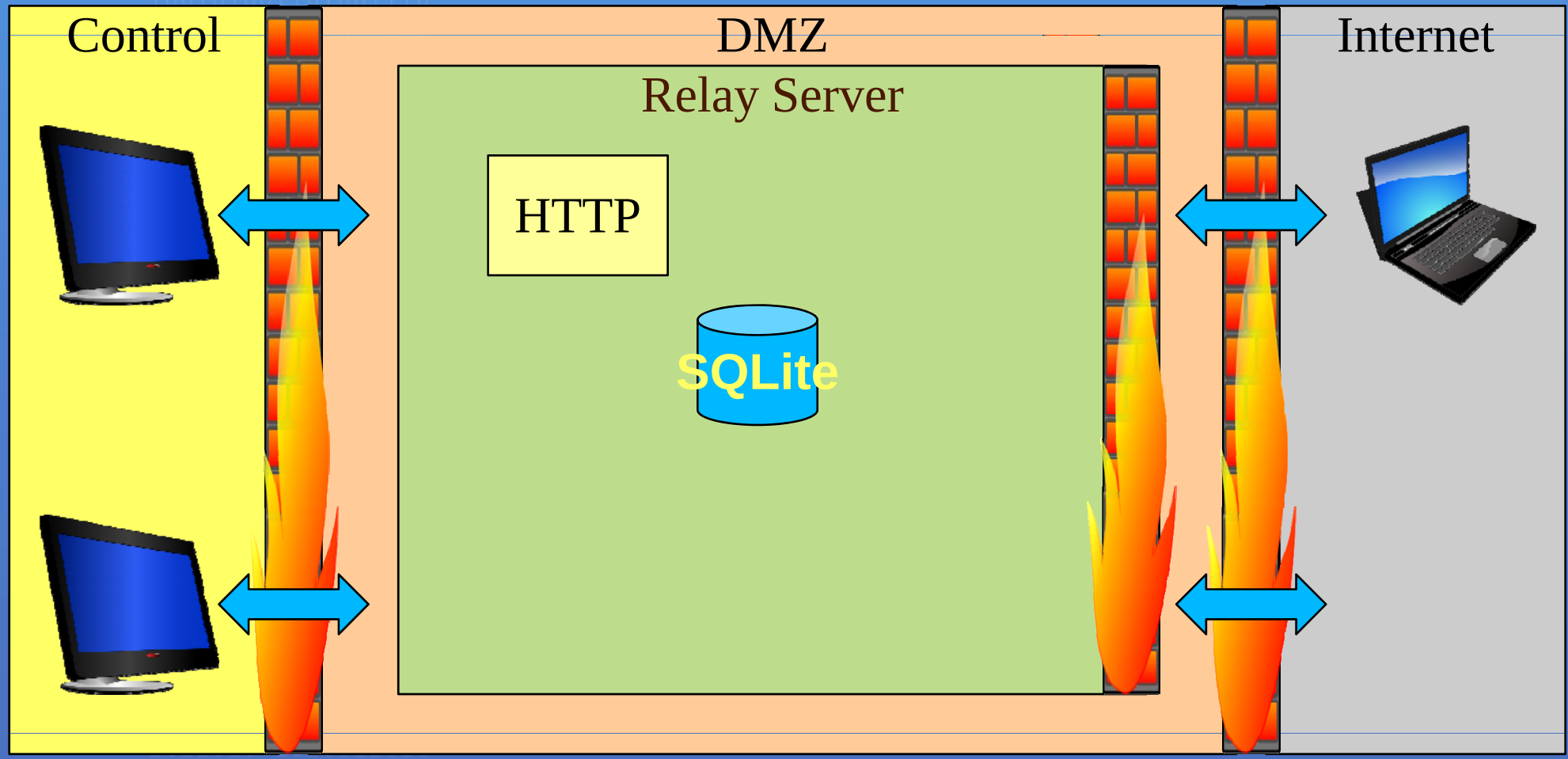
Shift leader ends WARCS



Shift leader ends WARCS (closes tunnel)



Shift leader ends WARCS



外部ログイン制御

- 外部ログイン パスワードの発行
- 外部ログイン状況

Akihiro Yamashita <aki@spring8.or.jp>
Last modified: Fri Sep 12 09:52:41 2003

外部ログインの許可

名前を入れてください。ワンタイムパスワードが発行されます。

接続を許可するSPring-8側のホスト名を入れてください。(例: opcon01)

Telnet Vnc

Issue one time password.

Akihiro Yamashita <aki@spring8.or.jp>
Last modified: Tue Sep 9 12:06:15 2003

login name	use_flg	authorozed time	client	host	Action	log
furukawa	Now logon	2007/05/01 12:47:28	AM-1.spring8.or.jp:8082	kanbai.spring8.or.jp:23	delete	log
kodera	Now logon	2007/07/13 05:54:58	KBMfa-01p4-64.ppp11.odn.ad.jp:8083	kanbai.spring8.or.jp:23	delete	log

Operation

- Since 2004, WARCS has been used.
- Experts go abroad must have WARCS installed notebook PC and cellular phone.
  - They must be trained before they go.
  - Windows, Mac or Linux.
- Another server for training is available.
- In the worst case, client software can be installed easily.
  - Access an instruction web page.

Problem

- VNC became hard to use.
  - Large screen monitors (24”x2) are going to be installed for the control room.
  - Does not fit notebook PC's screen.
- VNC can export partial screen?

Conclusion

- WARCS provides
  - Secure, controlled and stable connection to SPring-8 control LAN since 2004.
  - It fits to SPring-8 operation policy
  - Easy operation
    - Shift leader
      - WEB -based
    - Clients
      - Just enter one-time password.
- No special hardware is required
- Open-source base
  - No commercial licence