



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



1001010001010011
010110011010010010
100101000101001110
010110011010010100
010110010100110001
100101001101001010
101010110101001001
011010011011001001
101101001010011110
100101000101001001
010110011010010101
010110010100110101
100101001101001110
101010110101001001
011010010100110110
101101001010011010
101010110101001010
011010010100110101
101101001010011110
100101000101001110
010110011010010010
010110010100110101
100101001101001001
100101000101001010
010110011010010101
010110010100110010
100101001101001110
101010110101001010
011010010100110101
101101001010011000
100101000101001001
010110011010010010
010110010100110001
100101001101001111
101010110101001001
011010010100110101
101101001010011010
100101000101001101
010110011010010101
00110010100110001
100101001101001010

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
 - Zlib compression
 - Blowfish encryption
 - Diffie-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.

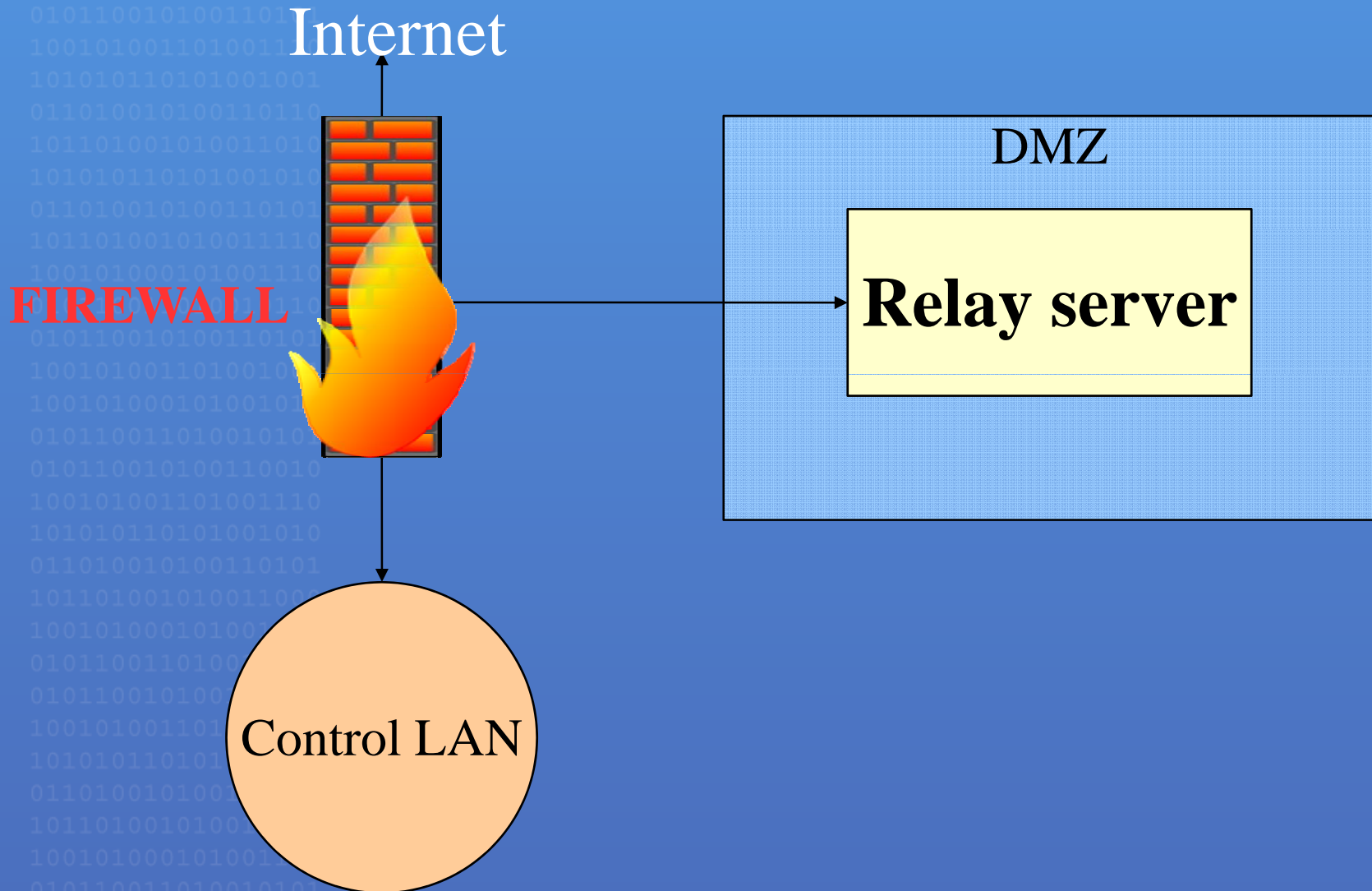
Other tools

- 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

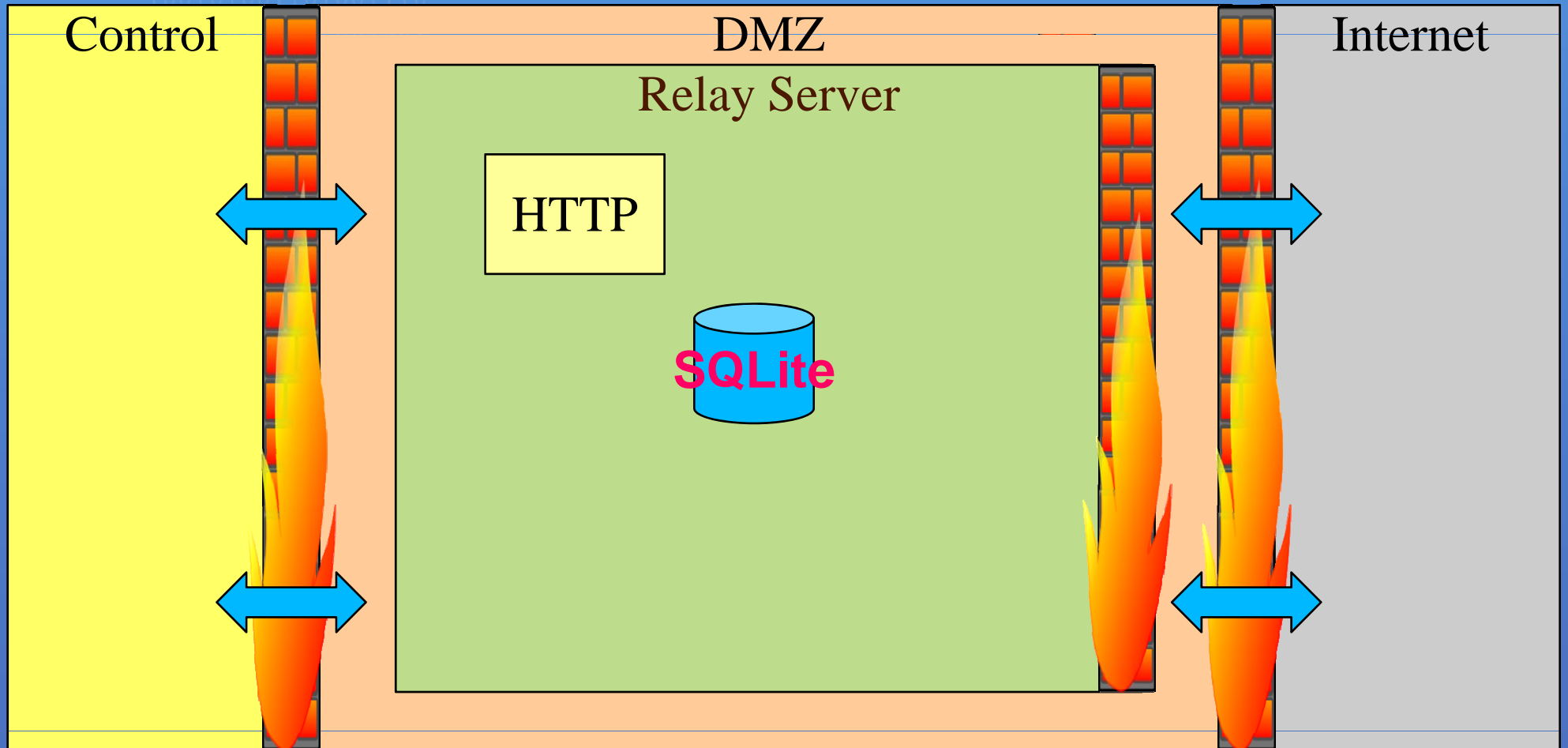
- Iptables
 - Linux firewall in its kernel.
 - Tunnel can be added/removed without restarting

Network scheme

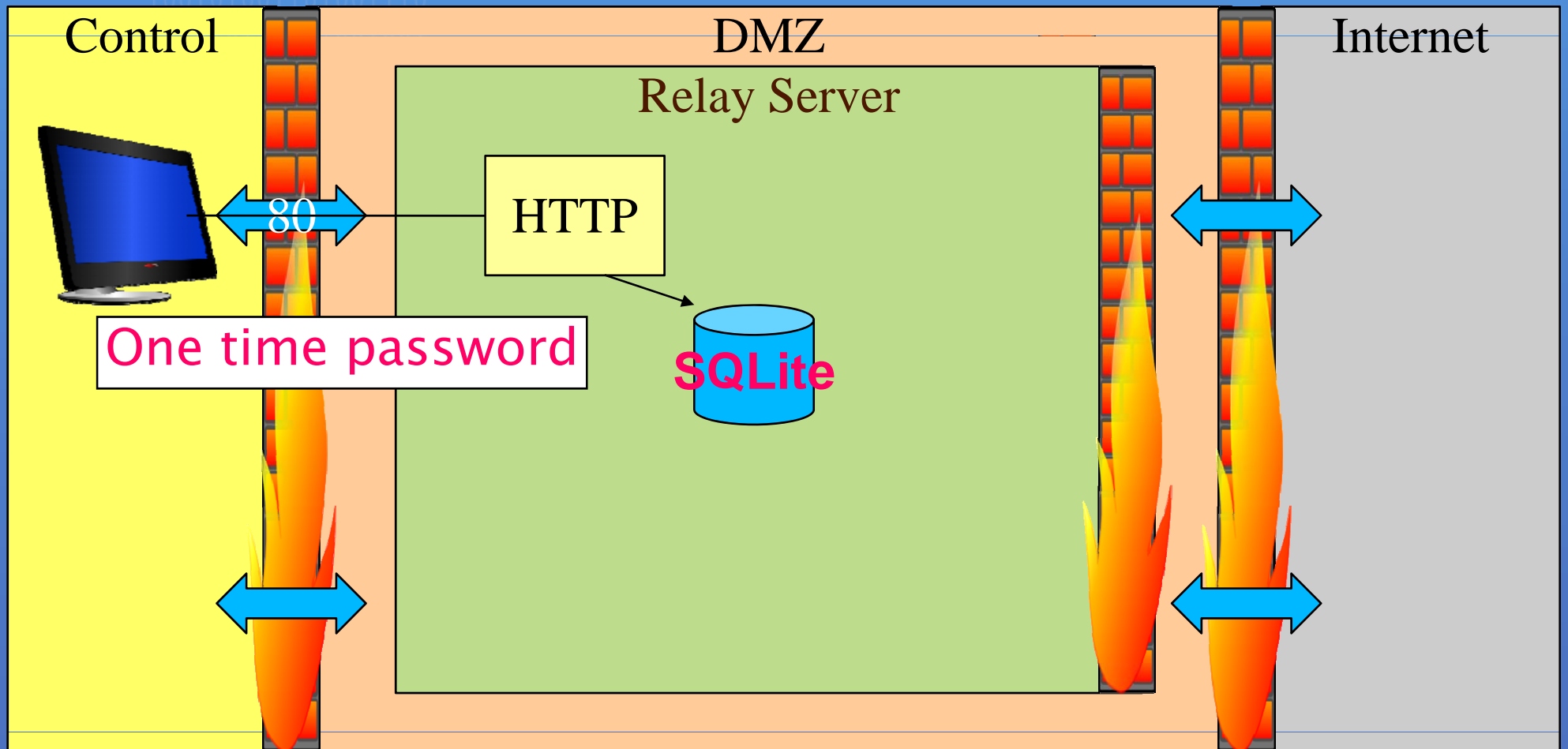


How WARCS works?

At the beginning



Issue one time password and record



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、ただし、ワンタイムパスワードが発行されます。

接続を許可するSPIDを8桁のホスト名を入力してください。(例: opcon01)

Telnet Vnc

Issue one time password.

LOGIN NAME
LOGIN HOST NAME
Select application type VNC/telnet

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

login name	use_flg	authorized 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

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

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

login name	use_flg	authorized 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	authorized 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-01 p4-64.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

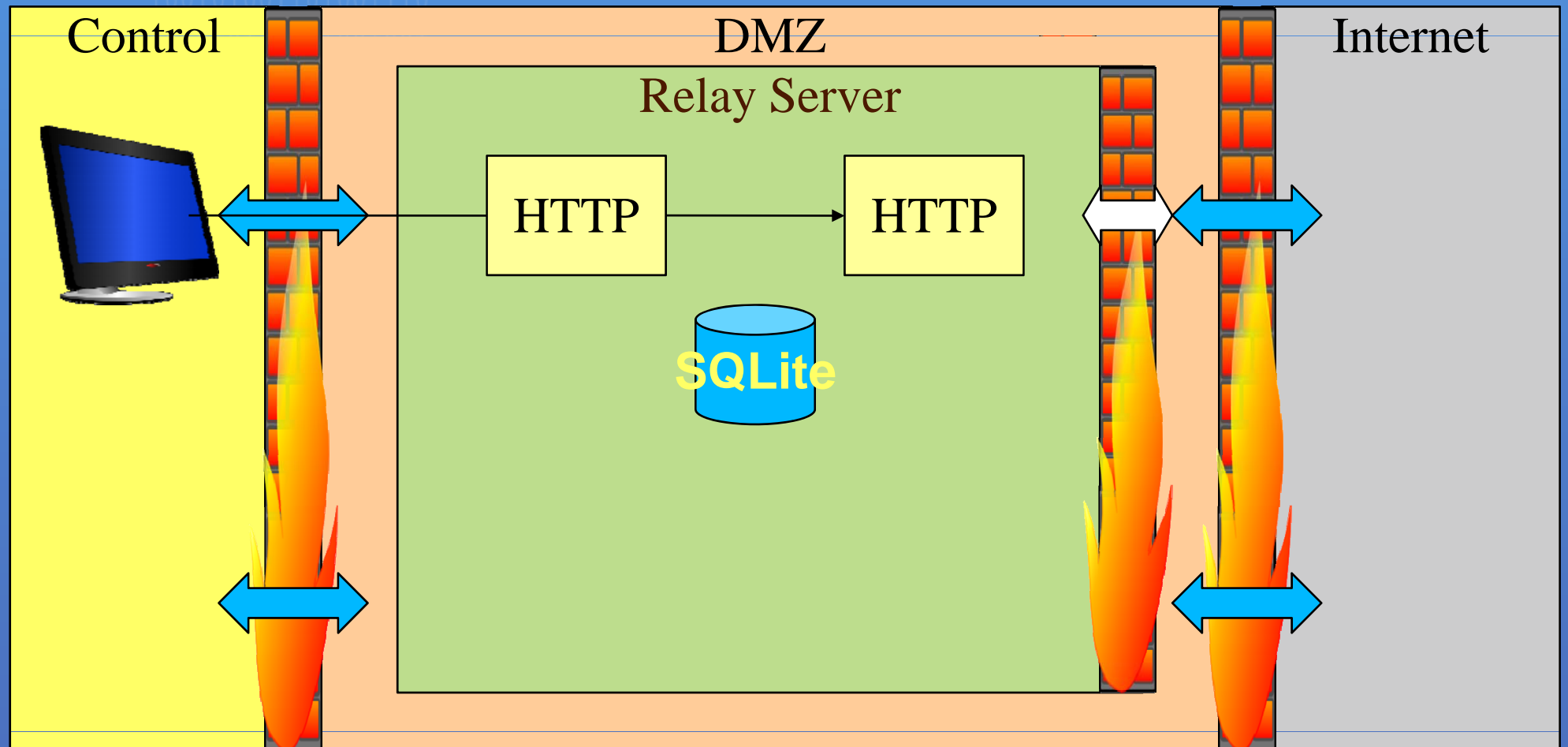
[(8083.0, 8082.0)]

OK!

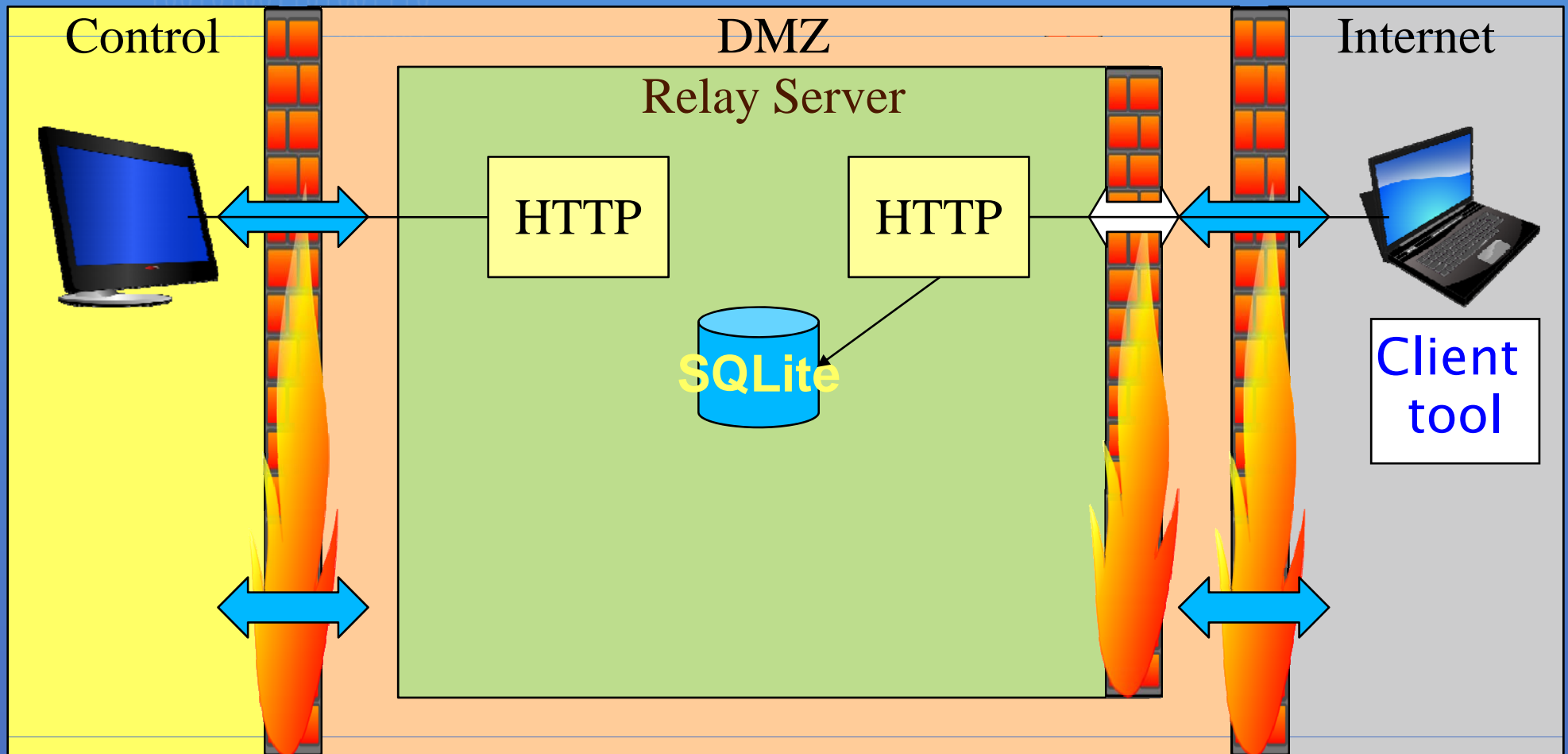
```
user      yamashita
host      conti
port      8081
host port 23
password  9930771
```

login name	use_flg	authorized 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

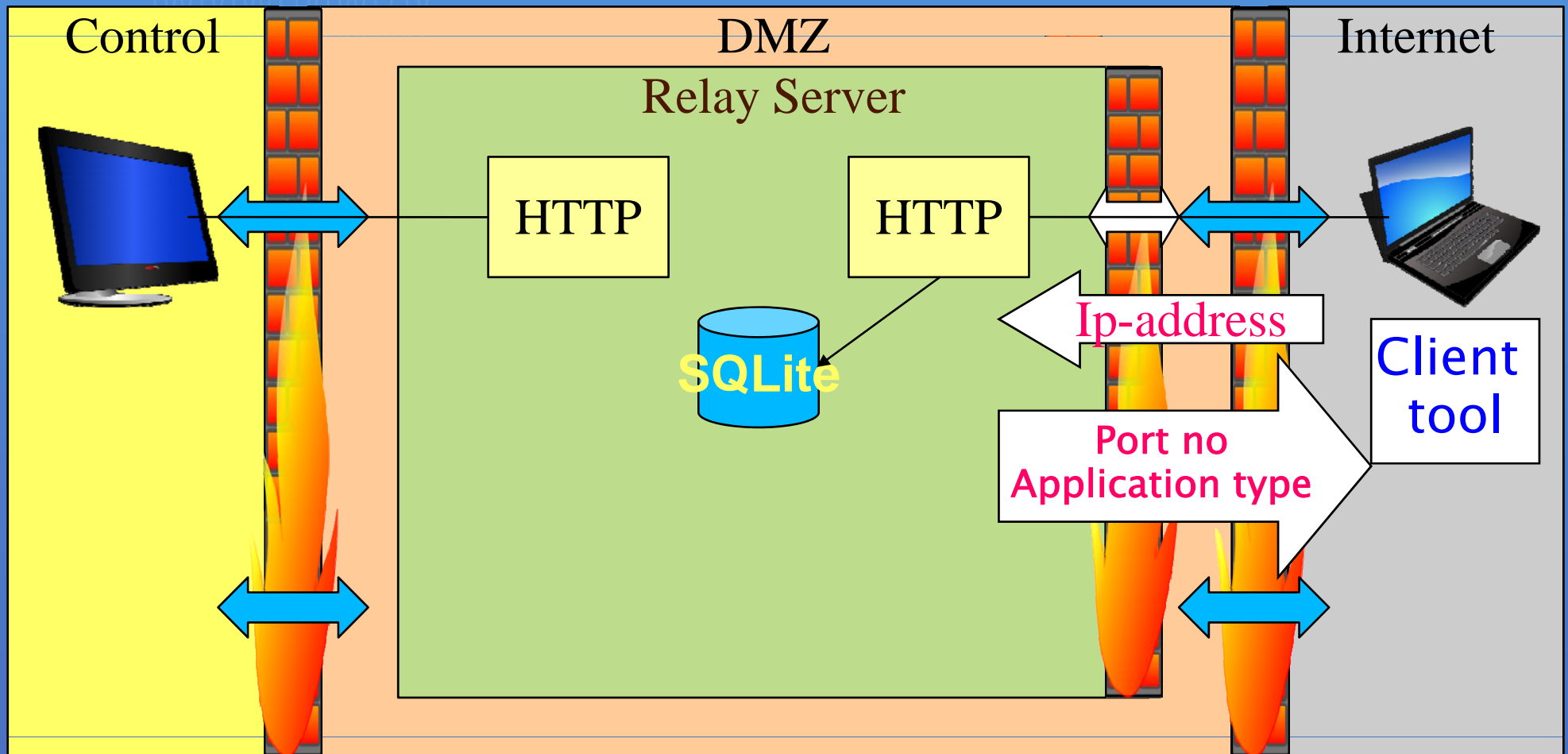
Launch another HTTP and open tunnel in iptables firewall for http



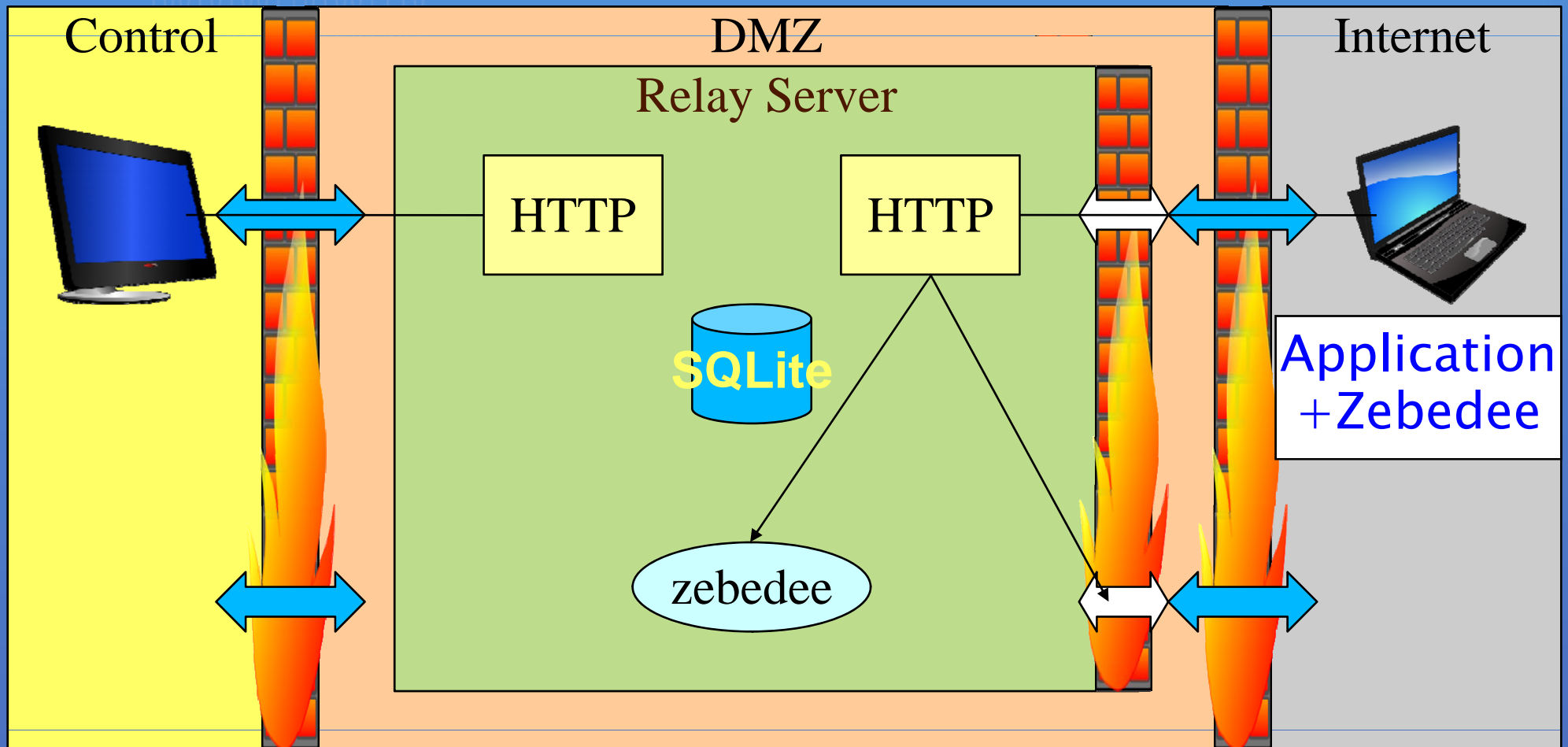
Client launches client tool and enter one time password



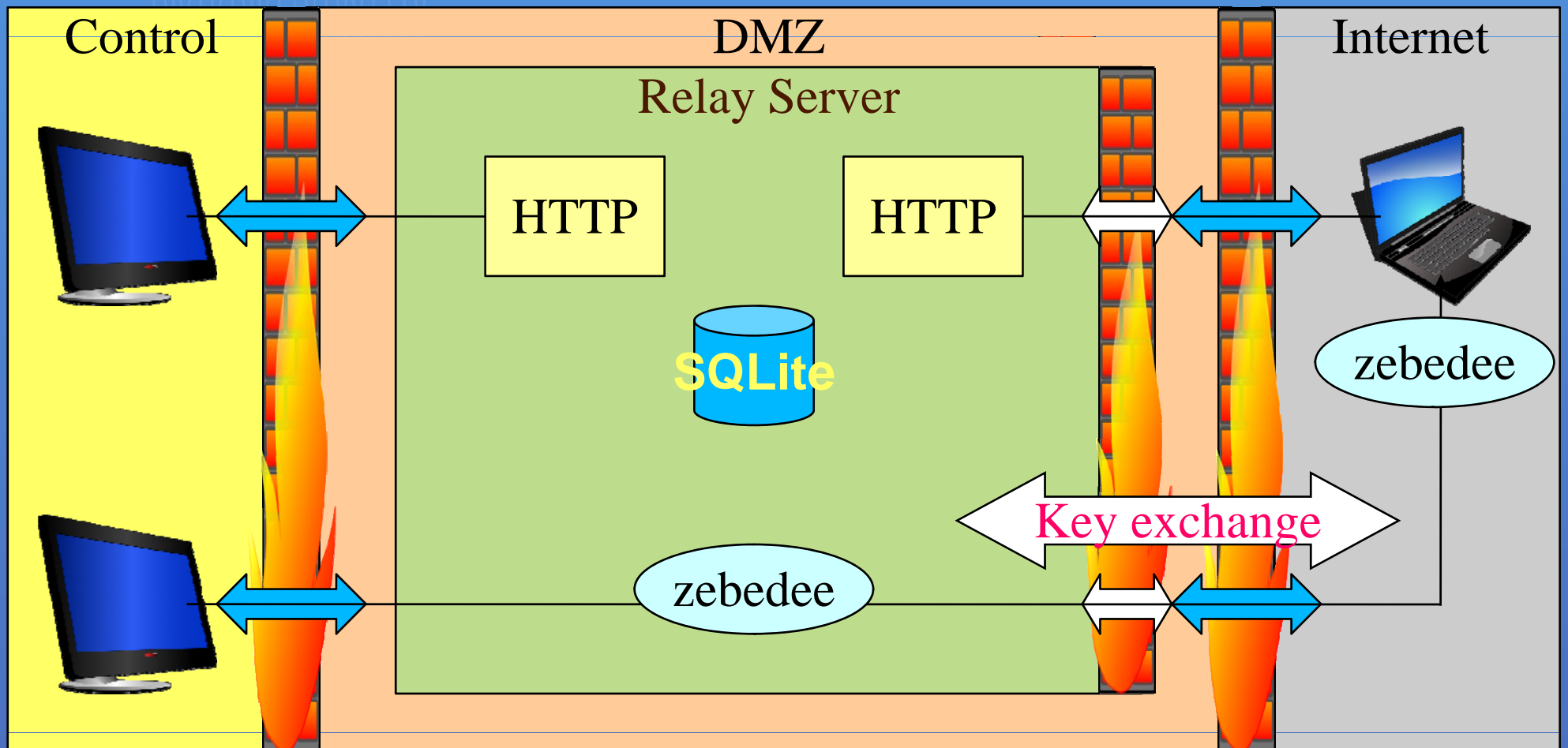
Exchange ip-address and port no, application type



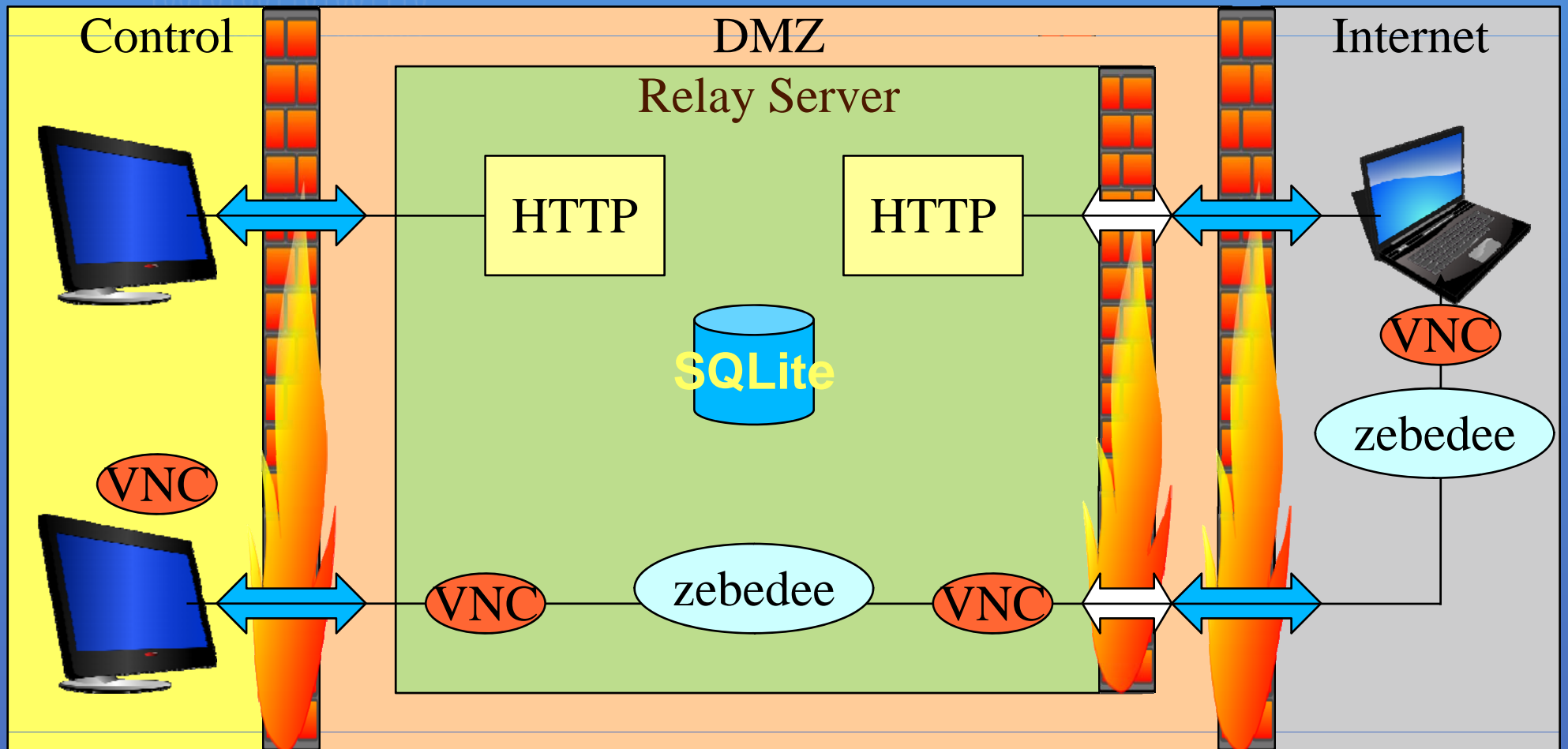
Open tunnel and launch zebedee.



Establish connection with authentication



VNC (Virtual network computer) is also available.



Windows XP desktop environment showing a Synchrotron control interface. The desktop background is a blue sky with clouds. The taskbar at the bottom shows the Start button, network status, and several open applications including 'aki's X desktop (con...' and 'Home page of Akihir...'. The system tray shows the date and time as 2005年10月03日 13時47分34秒 and 14:55.

The main application window is titled 'aki's X desktop (conti.spring8.or.jp:2)'. It contains several sub-windows:

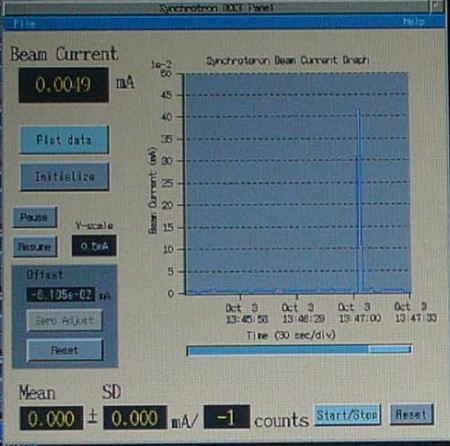
- Synchrotron Beam Current Graph:** A plot showing beam current (mA) over time. The current is stable at approximately 0.0049 mA. The x-axis is labeled 'Time (30 sec/div)' and the y-axis is 'Beam Current (mA)'. Below the plot, statistics are shown: Mean: 0.000 ± 0.000 mA, SD: -1 counts. Buttons for 'Start/Stop' and 'Reset' are present.
- Synchrotron Control Panel:** A complex control interface with multiple sections:
 - Synchrotron Data Set Status:** A table listing data sets and their set times.
 - RF Procedure:** A list of RF-related operations with 'Execute' and 'Status' buttons.
 - Magnet Procedure:** A list of magnet-related operations with 'Execute' and 'Status' buttons.
 - Timing System:** Control buttons for the timing system.
 - SSBT System:** Control buttons for the SSBT system.
 - RF KD System:** Control buttons for the RF KD system.
 - SSBT Silt System:** Control buttons for the SSBT Silt system.
- Synchrotron Equipment Operation Panel:** A large table monitoring various equipment parameters.

Eye Orbit Correction

SCREEN

LOW LEVEL CONTROL

WST001



Synchrotron Control Panel

Table Name	Date Set Name	Set Time	Operation Status
Synchrotron	HIT_Boyle_for_trap_4	2005/10/03 11:28:28	Op Mode Top-Up
RF	HIT_Boyle_for_trap_1	2005/09/18 11:47:02	Beam Sv On
Magnet	HIT_Boyle_for_trap_4	2005/10/03 11:28:28	Sfty Intlk Gun: 0 LI: 0 Sv
Timing	HIT_Boyle_for_trap_1	2005/09/18 11:47:03	LI Trig Sys Trig Source: Sv Pulse
			Sy Trig Sys Source: SR Mode: 0

RF Procedure	Magnet Procedure	Timing System
Select: RF On	Select: Start-Up	Timing System: ON
RF Standby	Set Parameter	SSBT System: SR TRUOCT
Beam Operation	Run	SSBT Switching Magnets: BK1 BK2 QF1 Q01
RF Down	Stop	DK DK QF1 Q01
RF Off	Shut Down	SSBT Beam Shutter: 0
LV Off	Interlock	RF KD System: ON
Interlock	Status: Run	SSBT Silt System: IN

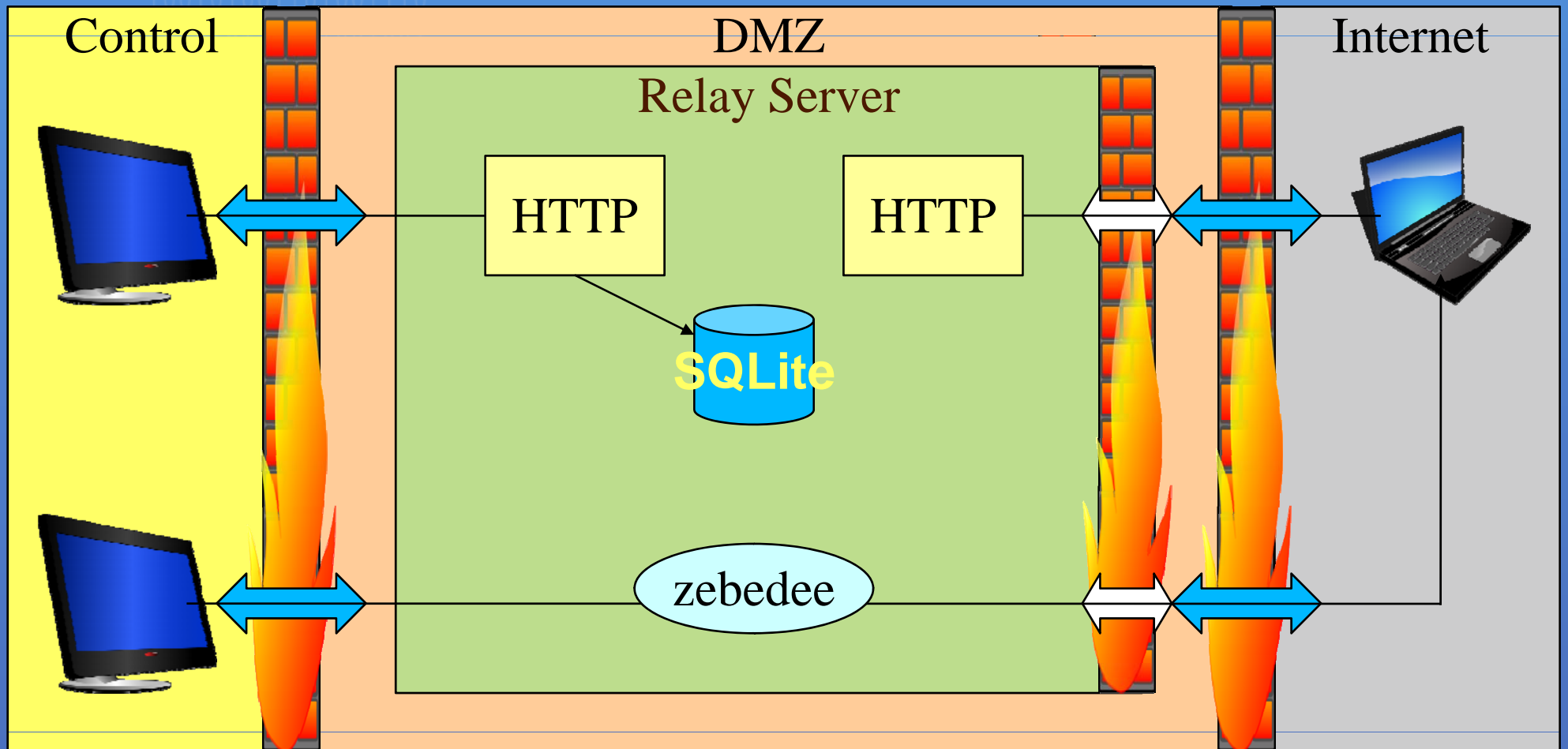
RF	Magnet	Timing	Monitor	Vacuum	Corner
Klystron	Ring Main	None	DD BPM	None	DD
Low Vol	Ring Drive	apocor08	SP BPM	None	Hannonic
Tuner	Inj Pulse	None	SCREEN	None	LSBT
Pattern	Ejc Pulse	None	SR Mon	None	SSBT
Trend Dis	SSBT B	None	DOCT	apocor01	ap-ones
	SSBT Q	None	DOCT 3	None	
	SSBT Conn	apocor08	SSBT BOM	None	
	Disp Pth	apocor08	RF KD	apocor01	
	Disp Pts	apocor08	SSBT Silt	None	
			OTR Mon	None	
			LSBT BPM	None	

バッテリー等の上手な使い方

Inj Orbit Continuous Measurement

スタート ネットワーク接続 (C:) 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>](mailto:aki@spring8.or.jp)
 Last modified: Fri Sep 12 09:52:41 2003

[(8083.0, 8082.0)]

OK!

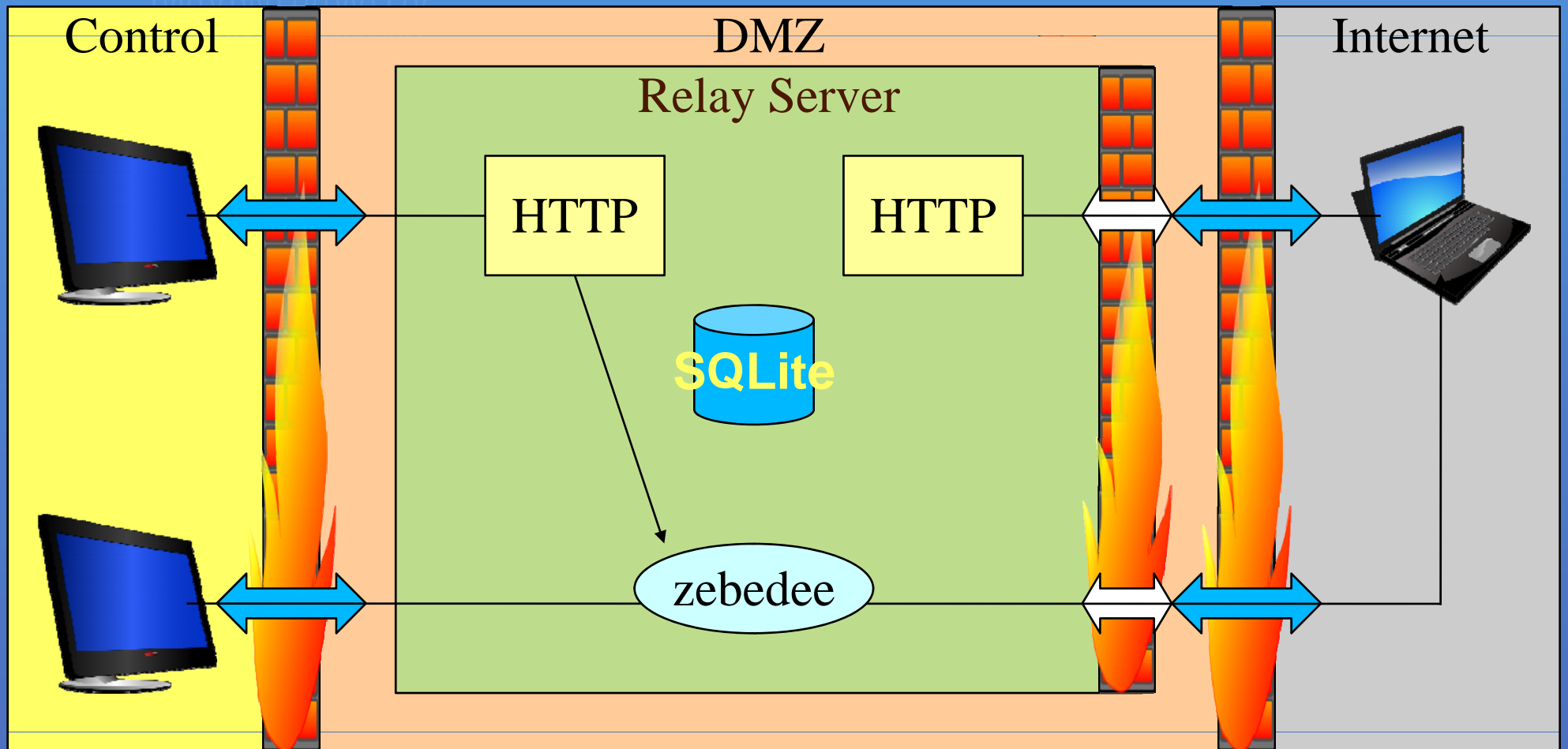
```

user      yamashita
host      conti
port      8081
host port 23
password  9930771
  
```

login name	use_flg	authorized 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)



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>](mailto: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	authorized 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 logon	2007/10/04 10:07:04	NOTYET:8081	conti.spring8.or.jp:23	delete	log

Kill connection



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

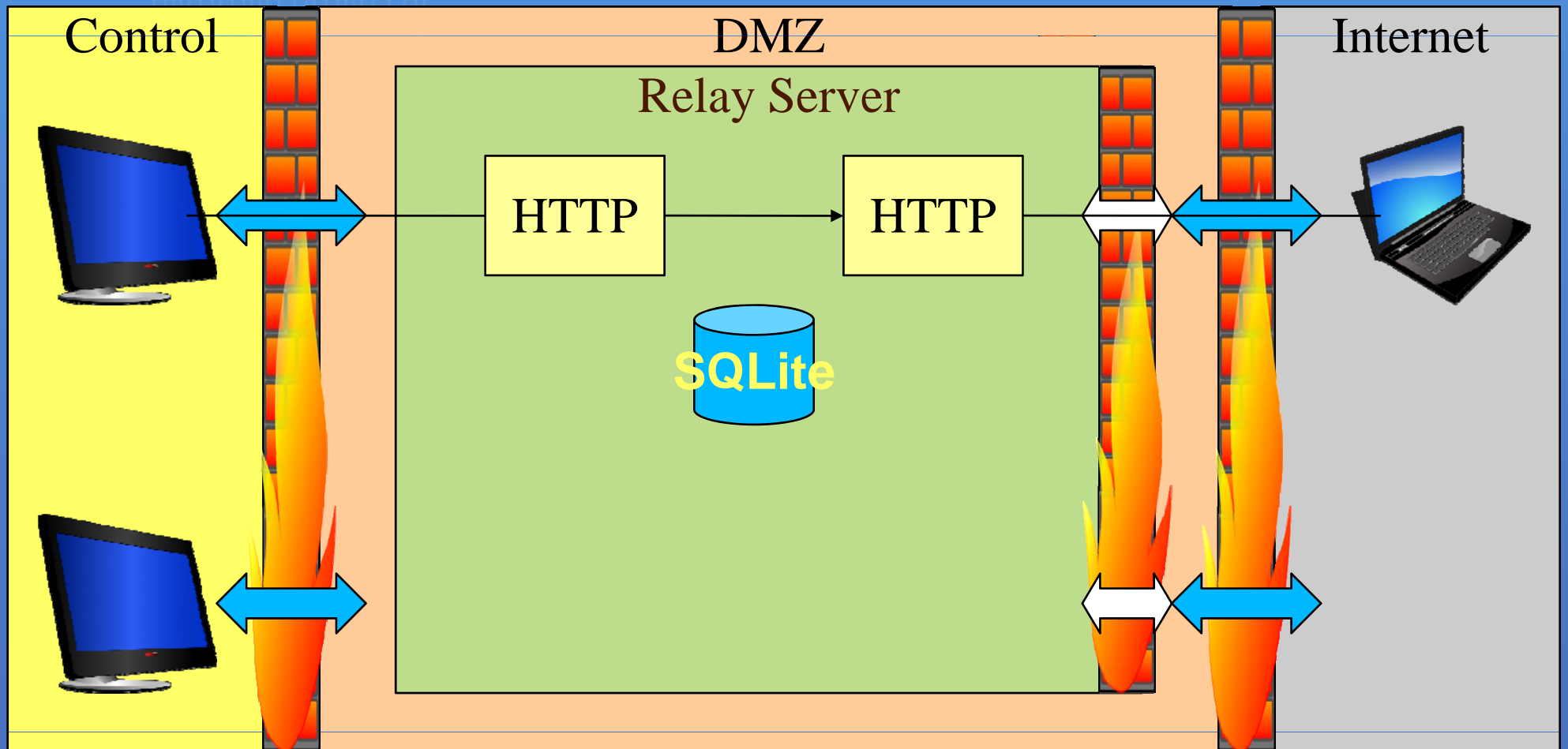
[(8083.0, 8082.0)]

OK!

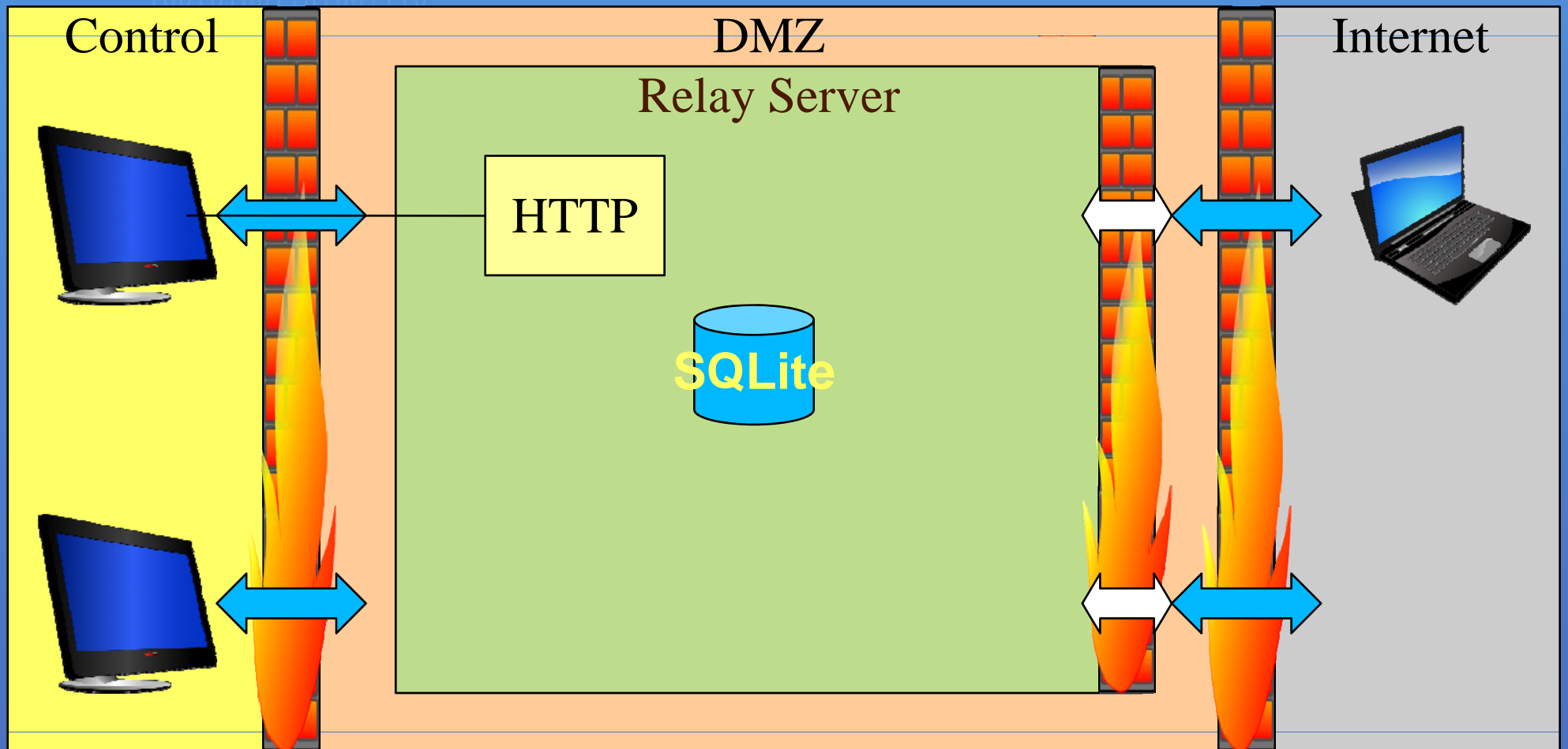
user yamashita
host conti
port 8081
host port 23
password 9930771

DELETED

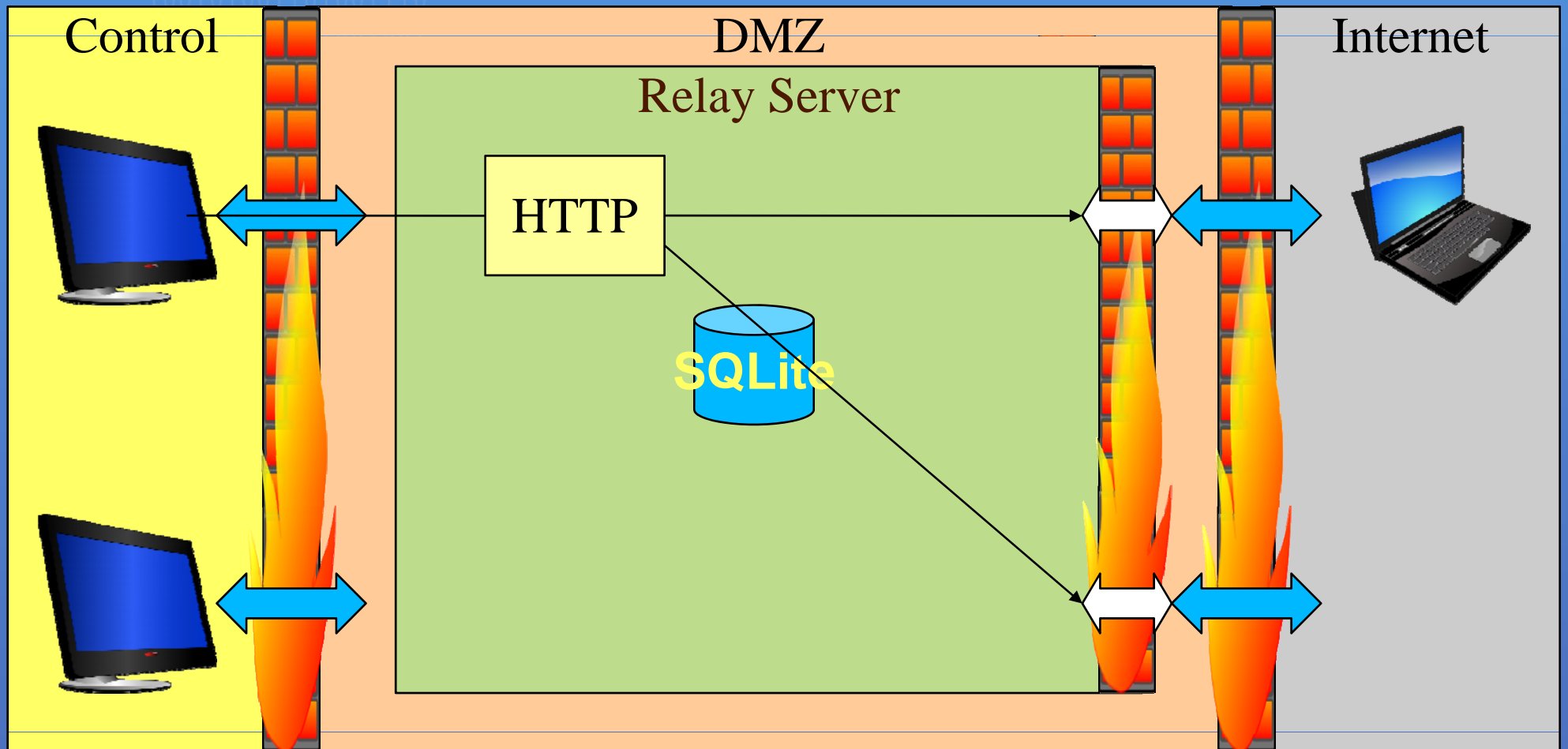
Shift leader ends WARCS kills http



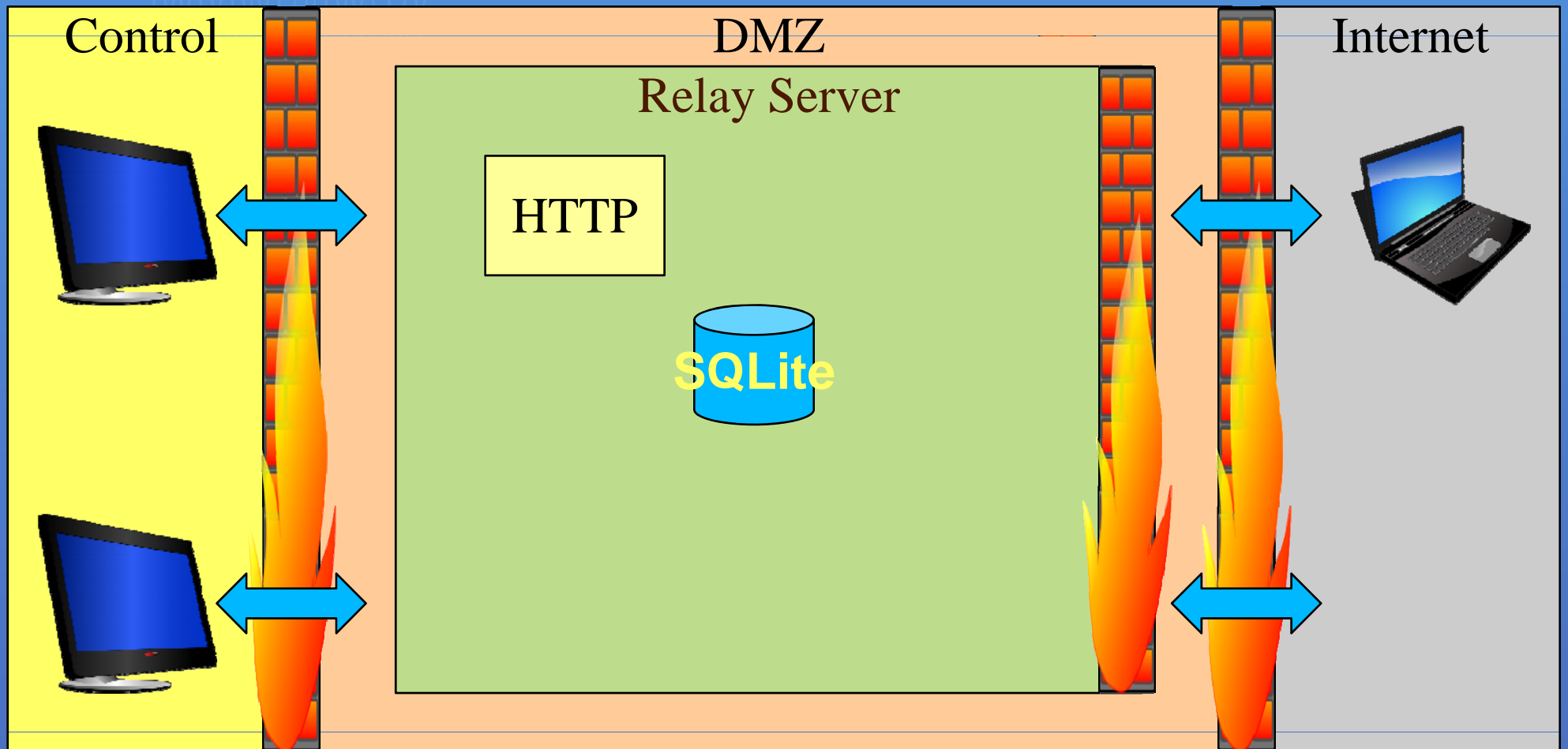
Shift leader ends WARCS



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

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

login name	use_flg	authorized 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