

# ***SBOX Firewall Configuration for VSP Service***



# Allow Rules – Step 1

The screenshot displays the Check Point SmartDefense console interface. At the top, the navigation menu includes 'Firewall', 'Servers', 'Rules', 'SmartDefense', and 'Exposed Host'. The main header shows 'Safe@Office 500' and version '6.0.42x'. A sidebar on the left contains a menu with 'Welcome', 'Reports', 'Security', 'Antivirus', 'Services', 'Network', 'Setup', 'Users', 'VPN', and 'Help', along with a 'SofaWare Embedded' logo.

The central area shows a 'Rules' table with 7 entries, all with 'Allow' status. A 'Firewall Rule Wizard' dialog box is open, titled 'Safe@Office Firewall Rule Wizard'. It is at 'Step 1: Rule Type' and asks 'Which type of rule do you want to create?'. The 'Allow and Forward' option is selected and highlighted with a red box. Below the options, a 'Certificate Error' dialog box is also visible, with its 'Next >' button highlighted in red. The wizard dialog has 'Next >' and 'Cancel' buttons at the bottom right.

No	▲ ▼	Allow	▲ ▼	▲ ▼	▲ ▼	▲ ▼	▲ ▼	▲ ▼	▲ ▼	Log	Enabled	▲ ▼	Edit
1	▲ ▼	Allow	▲ ▼	▲ ▼	▲ ▼	▲ ▼	▲ ▼	▲ ▼	▲ ▼	✓	✓	▲ ▼	Edit
2	▲ ▼	Allow	▲ ▼	▲ ▼	▲ ▼	▲ ▼	▲ ▼	▲ ▼	▲ ▼	✓	✓	▲ ▼	Edit
3	▲ ▼	Allow	▲ ▼	▲ ▼	▲ ▼	▲ ▼	▲ ▼	▲ ▼	▲ ▼	✓	✓	▲ ▼	Edit
4	▲ ▼	Allow	▲ ▼	▲ ▼	▲ ▼	▲ ▼	▲ ▼	▲ ▼	▲ ▼	✓	✓	▲ ▼	Edit
5	▲ ▼	Allow	▲ ▼	▲ ▼	▲ ▼	▲ ▼	▲ ▼	▲ ▼	▲ ▼	✓	✓	▲ ▼	Edit
6	▲ ▼	Allow	▲ ▼	▲ ▼	▲ ▼	▲ ▼	▲ ▼	▲ ▼	▲ ▼	✓	✓	▲ ▼	Edit
7	▲ ▼	Allow	▲ ▼	▲ ▼	▲ ▼	▲ ▼	▲ ▼	▲ ▼	▲ ▼	✓	✓	▲ ▼	Edit

# Allow Rules – Step 2

**Check Point**  
SOFTWARE TECHNOLOGIES LTD.  
We Secure the Internet.

Safe@Office 500  
6.0.42x

Firewall Servers Rules SmartDefense Exposed Host

Rules

No	↑	↓	Allow	Log	Enabled	Edit
1	↑	↓	Allow	✓	✓	Edit
2	↑	↓		✓	✓	Edit
3	↑	↓		✓	✓	Edit
4	↑	↓		✓	✓	Edit
5	↑	↓	Allow	✓	✓	Edit
6	↑	↓	Allow	✓	✓	Edit
7	↑	↓		✓	✓	Edit

**Firewall Rule Wizard** -- Webpage Dialog  
https://62.219.213.189:981/pop/WizardFrame.html

**Safe@Office Firewall Rule Wizard**

**Step 2: Service**

Allow and Forward connections to the following service:

Any Service  
 Standard Service  
 Custom Service

Protocol: TCP  
Port Range: [ ] - [ ]

Mail Server (SMTP)

< Back Next > Cancel

Internet

https://62.219.213.189:981/pop/WizardFrame.html

SSL

Welcome  
Reports  
Security  
Antivirus  
Services  
Network  
Setup  
Users  
VPN  
Help

**SofaWare**  
Embedded

# Allow Rules – Step 3

**Safe@Office 500**  
6.0.42x

**Check Point**  
SOFTWARE TECHNOLOGIES LTD.  
We Secure the Internet.

Firewall Servers Rules SmartDefense Exposed Host

**Rules**

No	Rule Type	Source	Destination	On/Off	Log	Enabled
1	Allow and Forward	ANY	192.168.0.200:3389 (TCP)			
2	Allow	212.79.211.192	192.168.0.200:Any Service			
3	Firewall Rule Wizard -- Webpage Dialog					
4	Https://62.219.213.189:981/jpop/WzrFrame.html					
5						
6						
7						

**Safe@Office Firewall Rule Wizard**  
Step 3: Destination & Source

If the connection source is:  
Specified Range  
Then forward the connection to:  
Specified IP

Advanced  
Quality of Service class  
 Redirect to port  
 Log accepted connections

Default

< Back Next > Cancel

https://62.219.213.189:981/jpop/WzrFrame.html Internet 551

**Specific VSP Range**

**Local Mail Server IP**

# Allow Rules – Step 4

The screenshot displays the 'Safe@Office Firewall Rule Wizard' interface. The main window title is 'Safe@Office Firewall Rule Wizard' and the URL is 'https://62.219.191.109:981/pop/WizRFrame.html?0'. The interface is divided into several sections:

- Header:** 'Safe@Office 110' and '6.0.53x'.
- Navigation:** 'Firewall', 'Servers', 'Rules', 'SmartDefense', 'HotSpot', 'Exposed Host'.
- Rules Table:** A table with 4 rows, each with a 'No' column and an 'All' dropdown menu. The status 'Saved successfully' is shown above the table.
- Wizard Steps:** 'Step 4: Done'. Below this, it states: 'This rule will Allow and Forward connections to Mail Server (SMTP) if the connection source is 212.79.238.66-212.79.238.126 and forward them to 192.168.0.2'.
- Buttons:** '< Back', 'Cancel', and 'Finish'.
- Footer:** 'Check Point SOFTWARE TECHNOLOGIES LTD. We Secure the Internet.' and 'SofaWare Embedded' logo.

On the right side of the interface, there is a 'Log' section with a table of log entries:

Log	Enabled
	<input checked="" type="checkbox"/>
	<input checked="" type="checkbox"/>
	<input checked="" type="checkbox"/>
	<input checked="" type="checkbox"/>

Each log entry has an 'Erase' button and an 'Edit' button.

# Deny Rule – Step 1

Check Point  
SOFTWARE TECHNOLOGIES LTD.  
We Secure the Internet.

Safe@Office 110  
6.0.53x

Firewall Servers Rules SmartDefense HotSpot Exposed Host

Rules

Saved successfully

No	Action	Log	Enabled	Edit
1	All	X	✓	Edit
2	All	X	✓	Edit
3	All	X	✓	Edit
4	All	X	✓	Edit

Firewall Rule Wizard -- Webpage Dialog  
https://62.219.191.109:981/pop/WizRFrame.html

### Safe@Office Firewall Rule Wizard

#### Step 1: Rule Type

This wizard will guide you through the process of creating a firewall rule.  
Which type of rule do you want to create?

Allow and Forward:  
Allows incoming connections, and forwards them to a local computer

Allow:  
Allows incoming or outgoing connections

Deny:  
Blocks incoming or outgoing connections

Next > Cancel

Internet

SSL

https://62.219.191.109:981/pop/WizRFrame.html

# Deny Rule – Step 2

The screenshot shows the 'Safe@Office Firewall Rule Wizard' in Step 2: Service. The wizard is titled 'Safe@Office 110' and '6.0.53x'. The main configuration area shows 'Block connections to the following service:' with the following options:

- Any Service
- Standard Service
- Custom Service

The 'Standard Service' option is selected, and the service is set to 'Mail Server (SMTP)'. The 'Protocol' is set to 'TCP' and the 'Port Range' is empty. The 'Log' column in the table below is set to 'Enabled'.

No	▲ ▼	All	Log	Enabled	Eraser	Edit
1	▲ ▼	All	✗	✓	✗	✗
2	▲ ▼	All	✗	✓	✗	✗
3	▲ ▼	All	✗	✓	✗	✗
4	▲ ▼	All	✗	✓	✗	✗

The bottom of the wizard shows navigation buttons: '< Back', 'Next >', and 'Cancel'. The status bar at the bottom indicates 'Internet' and 'SSL'.

# Deny Rule – Step 3

**Check Point**  
SOFTWARE TECHNOLOGIES LTD.  
We Secure the Internet

Safe@Office 110  
6.0.53x

Firewall Servers Rules SmartDefense HotSpot Exposed Host

**Rules**  
Saved successfully

No	Action	Enabled	...
1	Allow	✓	Edit
2	Allow	✓	Edit
3	Allow	✓	Edit
4		✓	Edit

**Firewall Rule Wizard -- Webpage Dialog**  
https://62.219.191.109:981/pop/WiFiFrame.html

### Safe@Office Firewall Rule Wizard

**Step 3: Destination & Source**

Block the connection if:  
The source is: ANY

And the destination is: LAN

**Advanced**  
 Log blocked connections

< Back Next > Cancel

https://62.219.191.109:981/pop/WiFiFrame.html Internet

# Deny Rule – Step 4

Check Point  
SOFTWARE TECHNOLOGIES LTD.  
We Secure the Internet

Safe@Office 110  
6.0.53x

Firewall Servers Rules SmartDefense HotSpot Exposed Host

Rules

Saved successfully

No	▲	▼	All	Log	Enabled	Eraser	Edit
1	▲	▼	All	✗	✓	Eraser	Edit
2	▲	▼	All	✗	✓	Eraser	Edit
3	▲	▼	All	✗	✓	Eraser	Edit

Firewall Rule Wizard -- Webpage Dialog  
https://62.219.191.109:981/pop/WizardFrame.html

### Safe@Office Firewall Rule Wizard

**Step 4: Done**

This rule will **Block** connections to Mail Server (SMTP) if the connection source is **ANY** and the destination is LAN  
Blocked connections will be **logged**.

Click **Finish** to save the rule into your settings.  
Click **Back** to review your settings.  
Click **Cancel** to quit without saving.

< Back Cancel Finish

Internet

https://62.219.191.109:981/pop/WizardFrame.html

SSL

Welcome  
Reports  
Security  
Antivirus  
Services  
Network  
Setup  
Users  
VPN  
Help

SofaWare  
Embedded

# SBOX rules configuration

Safe@Office 110  
6.0.53x

Firewall Servers Rules SmartDefense HotSpot Exposed Host

Rules

Saved successfully

No	Rule Type	Source	Destination	Log	Enabled
1	Allow and Forward	212.79.238.66-212.79.238.126	192.168.0.2:Mail Server (SMTP)	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
2	Allow and Forward	212.79.242.192-212.79.242.254	192.168.0.2:Mail Server (SMTP)	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
3	Allow and Forward	193.28.13.1-193.28.13.254	192.168.0.2:Mail Server (SMTP)	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
4	Block	ANY	LAN:Mail Server (SMTP)	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>

Add Rule

VSP - Allow Rules

SMTP - General Deny Rule