

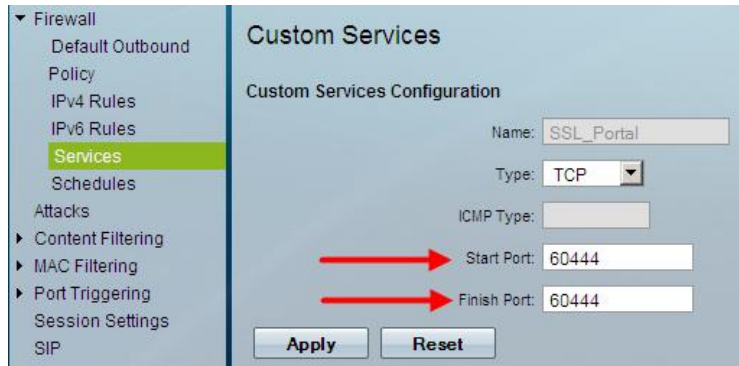
Workaround for SSL Portal access with port 443 forwarded for other service.

To change the default port for SSL VPN on SA5xx security appliance routers follow these steps:

NOTE: this tutorial already assumes that users have already been created and or an authentication method has been applied to the router for SSL access. You can use either RADIUS, or LDAP (being ADS or OpenLDAP).

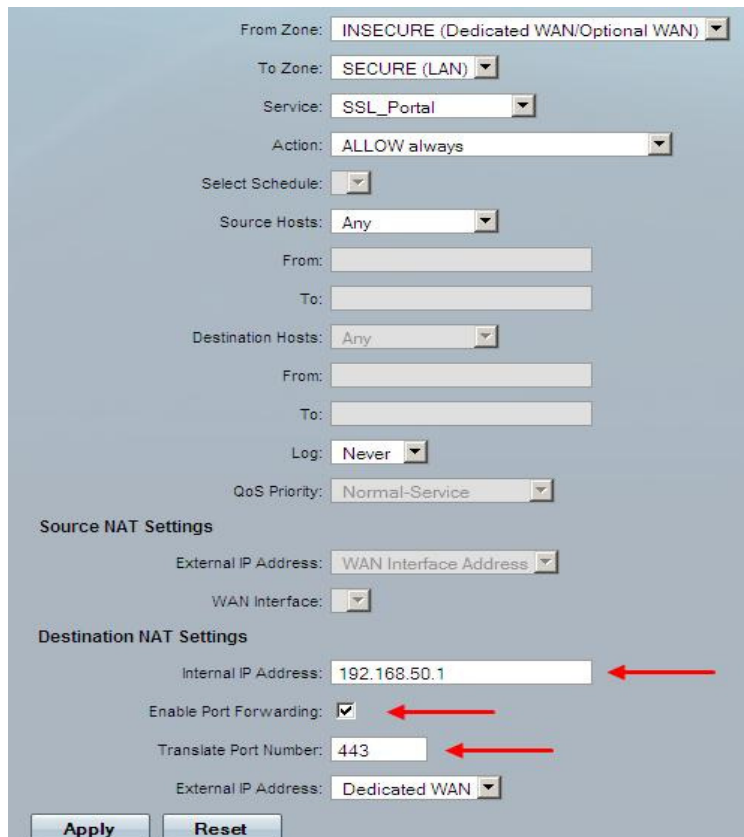
First we need to create the service:

- Log into router and select “Firewall” tab, then select “Services” and click “Add”
- Add the service as shown. The port number just needs to be above 1024 not necessarily what is shown.



For this example we will use external ports 60444.

Second, we will need to create the IPv4 firewall rule to forward 60444 to 443 like this:



- The Internal IP Address is the LAN IP of the SA appliance.
- Enable Port Forwarding
- Translate to our SSL VPN of 443
- Don't forget about the External IP Address. If you have multiple WAN addresses make sure to select the appropriate IP.

Workaround for SSL Portal access with port 443 forwarded for other service.

Lastly make sure your rule is what you want. The end result should look similar to the picture below. The rule is stating this:

Allow conversations traveling on port 60444 access from any host on the WAN inbound. Once accepted translate the conversation to port 443 and send it to host on LAN that is specified. Do not log this action.



The screenshot displays the Cisco ASA Firewall configuration interface, specifically the IPv4 Firewall Rules section. The 'SSL_Portal' rule is highlighted in red, indicating it is the active rule. The rule is enabled, allowing traffic from the WAN zone to the LAN zone on port 443. The local server is set to 192.168.50.1, and the internet destination is WAN1. The rule is configured to allow traffic from any source hosts to any destination hosts.

Status	From Zone	To Zone	Service	Action	Source Hosts	Destination Hosts	Local Server	Internet Destination	Log	Edit
<input type="checkbox"/>	Enabled	WAN	LAN	HTTPS	ALLOW always	Any	192.168.50.250	WAN1	Never	
<input type="checkbox"/>	Enabled	WAN	LAN	SMTP	ALLOW always	Any	192.168.50.250	WAN1	Never	
<input type="checkbox"/>	Enabled	WAN	LAN	DNS:UDP	ALLOW always	Any	192.168.50.251	WAN1	Always	
<input type="checkbox"/>	Enabled	WAN	LAN	FTP	ALLOW always	Any	192.168.50.230	WAN1	Always	
<input type="checkbox"/>	Enabled	WAN	LAN	AthensFTP	ALLOW always	Any	192.168.50.230	WAN1	Never	
<input type="checkbox"/>	Enabled	WAN	LAN	XPVM1	ALLOW always	Any	192.168.50.61:3389	WAN1	Never	
<input type="checkbox"/>	Enabled	WAN	LAN	QVPN	ALLOW always	Any	192.168.50.1	WAN1	Never	
<input checked="" type="checkbox"/>	Enabled	WAN	LAN	SSL_Portal	ALLOW always	Any	192.168.50.1:443	WAN1	Never	