



securing your web



**Feature Description**

**Port Mapping**

**SOFTWARE VERSION 9.2**

## VSOS 9.2 Port Mapping

To ensure correct functionality for Vital Security Web Appliance Series Version 9.2, the following ports must be opened between the devices. Any firewalls in your topology must be configured as required.



**NOTE: All ports mentioned in this document are TCP unless otherwise listed.**

**All ports mentioned in this document are inbound.**

### 1. Scanning Server Role:

- The Scanning Server does not need to initiate communication with the Policy Server.
- The Scanning Server needs access to DNS, HTTP, FTP and HTTPS.
- The Scanning Server also needs to pre-fetch data from the Internet using HTTP and HTTPS when working in ICAP mode.

When the scanning server needs to authenticate the users the following ports should be accessible to the Authentication Server:

- UDP/137
- UDP/138
- TCP/139
- TCP/445

Port Number	Application	Comment
8000	Log relaying HTTP port	Between Policy Servers and all other devices
8001	Log relaying HTTPS port	Between Policy Servers and all other devices
1344	Scanning server default ICAP port	If using ICAP client, port must be open between ICAP client and Scanning Server. This port is configurable.
8080	Scanning server default HTTP port	This port is configurable.

5222	Configuration Port (Notifier/Manager)	Between Policy Servers and all other devices.
5224	Secure Configuration Port Notifier/Manager	Between Policy Servers and all other devices.
161 UDP	SNMP Management Tools	
2121	FTP Clients	This port is configurable.
8443	HTTPS Clients	This port is configurable.
22	SSH, SFTP	Administrator's PC must have access to this port
2048	WCCP	The port should be opened only if there is a firewall between the router and the Scanning Server. The administrator should enable the passage of GRE traffic – IP protocol 47

## 2. Policy Server Role:

In order to download updates, the Policy Server must be able to connect to the Internet using DNS and HTTPS.

The following two sites need to be allowed for downloading purposes:

- [updateng.finjan.com](http://updateng.finjan.com)
- [mirror.updateng.finjan.com](http://mirror.updateng.finjan.com)

In order to utilize the Archiving and Policy Export/Import features, the Policy Server needs access to HTTPS, SAMBA, SFTP or FTP on another machine.

In order to utilize the Active Directory features, the Policy Server needs access via Port 389 to any Active Directory Domain Controller.

Port Number	Application	Comment
8000	Log relaying HTTP port	Used by standby Policy Server in High Availability mode
8001	Log relaying HTTPS port	Used by standby Policy Server in High Availability mode
5226	High-Availability Rsync	Used by standby Policy Server in High Availability mode
443	Policy Server Console HTTPS interface	Administrator's PC must have access to this port

	Setup Console HTTPS Interface	Administrator's PC must have access to this port
161	UDP SNMP Management Tools	Administrator's PC must have access to this port
22	SSH, SFTP	Administrator's PC must have access to this port
162	UDP Policy Server, add port SNMP traps	This port should be opened if there is a firewall between scanning servers and policy servers for the Dashboard
389	Start TLS	Used by Policy Server when importing users from LDAP
636	SLDAP	Used by Policy Server when importing users from Secure LDAP

### 3. All in One Role:

- As an All in One, the connections mentioned above for the Policy Server and the Scanning Server are relevant here.

Port Number	Application	Comment
8000	Log relaying HTTP port	Used by standby Policy Server in High Availability mode
8001	Log relaying HTTPS port	Used by standby Policy Server in High Availability mode
8080	Scanning server default HTTP port	This port is configurable.
1344	Scanning server default ICAP port	If using ICAP client, port must be open between ICAP client and Scanning Server. This port is configurable.
2121	FTP	This port is configurable
443	Policy Server Console HTTPS interface	Administrator's PC must have access to this port
5222	Configuration port (Notifier/Manager)	Between Policy Servers and all other devices.
5224	Secure Configuration port (Notifier/Manager)	Between Policy Servers and all other devices.
161 UDP	SNMP	

<b>8443</b>	HTTPS	This port is configurable.
<b>22</b>	SSH, SFTP	Administrator's PC must have access to this port