Secure Web Gateway Port Mapping

To ensure correct Secure Web Gateway functionality, all the ports listed in this document 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 stated and are inbound.

1. Scanning Server Role:

The Scanning Server:

- Is not required to initiate communication with the Policy Server.
- Requires access to DNS, HTTP, FTP and HTTPS.
- When working in ICAP mode, must pre-fetch data from the Internet using HTTP and HTTPS.

Port Number	Application	Comment
8000	Log relaying HTTP port	Between Policy Server and all other devices.
8001	Log relaying HTTPS port	Between Policy Server and all other devices.
1344	Scanning server default ICAP port	If using ICAP client, the port must be opened 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 Server and all other devices.
5224	Hang Detection Port	Local machine tests to ensure that Apache is running and responding correctly to requests. The communication is between processes in the machine, and localhost: 5224.
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 must be opened only if there is a firewall between the router and the Scanning Server. The administrator enables the GRE traffic passage with IP protocol 47.

2. Policy Server Role:

To download updates, the Policy Server must be enabled to connect to the Internet using DNS and HTTPS.

The following sites must be enabled for downloading purposes:

- updateng.finjan.com
- mirror.updateng.finjan.com

Note: mirror.updateng.finjan.com is part of a Content Delivery Network (CDN). Some customers request Trustwave to provide the Trustwave update server IPs to lock down the customers firewall and ensure the SWG Policy Server can only communicate with specific IPs over port 443. This is not possible because there are multiple CDN IPs that are subject to change.

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

To utilize the Active Directory features, the Policy Server requires 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.
5222	Configuration Port (Notifier Manager)	Between Policy Server and all other devices.
5224	Hang Detection Port	Local machine tests to ensure that Apache is running and responding correctly to requests. The communication is between processes in the machine, and localhost: 5224.
443	Policy Server 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 must be opened if there is a firewall between scanning servers and Policy Server 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:

The connections previously described for the Policy Server and the Scanning Server are relevant for All-in-One.

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 ICAP port	This port is configurable.
1344	Scanning server default ICAP port	If using ICAP client, the port must be opened 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. This is configurable by issuing the command "config_psweb" from the CLI.
5222	Configuration port (Notifier/Manager)	Between Policy Server and all other devices.
5224	Hang Detection Port	Local machine tests to ensure that Apache is running and responding correctly to requests. The communication is between processes in the machine, and localhost: 5224.
161 UDP	SNMP	This port is configurable.
8443	HTTPS	Administrator's PC must have access to this port.
22	SSH, SFTP	Administrator's PC must have access to this port.

Legal Notice

The most current version of this document may be obtained by contacting:

Trustwave Technical Support:
Phone: +1.800.363.1621
Email: support@trustwave.com

Trademarks

About Trustwave®

Trustwave is a leading provider of information security and compliance management solutions to large and small businesses thought the world. Trustwave analyzes, protects and validates an organization's data management infrastructure from the network to the application layer – to ensure the protection of information and compliance with industry standards and regulations such as the PCI DSS and ISO 27002, among others. Financial institutions, large and small retailers, global electric exchanges, educational institutions, business service firms and government agencies rely on Trustwave. The company's solutions include on-demand compliance management, managed security services, digital certificates and 24x7 multilingual support. Trustwave is headquartered in Chicago with offices throughout North America, South America, Europe, the Middle East, Africa, Asia, and Australia.