eScan for Windows: What ports should be opened on Firewall for communication between eScan Server and client computers?

What ports should be opened on Firewall for communication between eScan Server and client computers?

An Enterprise or Corporate customer uses firewall, to block attacks and to prevent unwanted traffic from passing to and fro within a network.

Wide Area Network includes remote branches or roaming clients. Considering this environment, this document guides you through the ports being used by eScan server, Update agents and Clients, and which ports needs to be open on firewall for smooth deployment of virus signatures and policies.

Ports	Purpose
On eScan Server	
TCP 10443	On which eScan Server Web Console listens Administrator can access eScan Web console using this port to manage eS Deployment, Policies and tasks
TCP 3333	To provide update version to Update agents and clients. Client PC uses this connection to request if there is any new updat not.
TCP 2021	FTP port from where Update Agents and clients download Virus signatures information and mwav.log.

eScan for Windows: What ports should be opened on Firewall for communication between eScan Server and client computers?

If this port is closed UA and clients will not download virus signatures or polici

eScan for Windows: What ports should be opened on Firewall for communication between eScan Server and client computers?

TCP 2221	HTTP port from where Update Agents and clients download Viru
	If this port is closed UA and clients will not download virus signatures or po
TCP 2222	eScan agent listens on this port
TCP 2225	eScan server accepts client events on this port
TCP 2226	eScan Server listen on this port in system mode. This port need NOT be allowed/opened on firewall
TCP 2227	eScan accepts self-events on this port. This port need NOT be allowed/ope firewall

On a PC assigned with Update Agent Role

TCP 3333	To provide update version to Update agents and clients. Client PC uses this connection to request if there is any new updat to download or not.
TCP 2021	FTP ports from clients downloads Virus signatures
TCP 2222	eScan agent listens on this port
TCP 2227	eScan accepts self-events on this port

On eScan Client

TCP 2222	eScan agent listens on this port and Used to receive requests sent from eS If this port is closed eScan server will not be able to send an requests/tasks to the client.
TCP 2227	eScan accepts self-events on this port

****eScan Server use FTP port 2021 to distribute virus signatures and policies to clients. If eScan server or clients are behind Firewall, customer needs to enable **PASV mode i.e. Passive mode**

Passive mode is an alternative mode for establishing File Transfer Protocol (FTP) connections.

eScan for Windows: What ports should be opened on Firewall for communication between eScan Server and client computers?

PASV mode is designed for FTP clients behind firewalls.

PASV mode works by allowing FTP clients to initiate sending of both control and data messages. Ordinarily, only FTP servers initiate the data requests. Because many client firewalls reject incoming messages like these FTP requests, PASV mode makes FTP "firewall-friendly."

If eScan server or clients are behind firewall, then you need to open following ports on Firewall to make sure downloading of virus signatures and policy updates doesn't stop.

TCP port 10443

TCP port 3333

TCP Port 2222

TCP port 2021

TCP port 2225

TCP port range 3023 – 4023 (These port numbers can be different, depending upon the configuration)

[**Port range 3023 – 4023 are examples given in the document, administrator can open any range after 3333 port, since 3333 port is being used by eScan server. In this guide we have opened 1000 ports from 3023 to 4023, this is an example and actual range can be depends on the number of clients connect to the server over the WAN. If you have 100 users you can open range of 100 ports on your firewall and so on.]**

Once these ports are open on firewall make the below changes on eScan Server to synchronize.

Open the eserv.ini file from %program files%\eScan folder and insert the following entries under the

[General] section.

eScan for Windows: What ports should be opened on Firewall for communication between eScan Server and client computers?

AddPassivePort=1
StartingPassivePort=3023
NoofPassivePorts=1000

Ser_Pasv_IPAddr=192.x.x.x - (eScan server public ip)

In case of, roaming clients or remote branches which are connected to eScan Server over the internet, may force administrator to install eScan Server on a Public IP or NAT it with Firewall Public IP. If you NAT it with Firewall Public IP, then you need to add the NATTED IP address in front of “Ser_Pasv_IPAddr=” entry.

This settings are cumbersome and it pose a security risk when you open n number of ports in your firewall, what if we open only few ports instead of opening 1000 number of ports. Hence we provided an option of HTTP download along with FTP.

***By default, eScan server installs with FTP port enabled, if you want to change it to HTTP please refer to the document called “http_readme.txt” which resides in eScan server Installation folder. Open this file and search for point number 3. How to Add HTTP download along with FTP download for Signature update and policies?

Once you are done with the settings, you need to open below ports on Firewall.

TCP port 10443

TCP port 2221

TCP Port 2222

TCP port 2225

eScan for Windows: What ports should be opened on Firewall for communication between eScan Server and client computers?

[HTTP Port for downloading Virus signature and policies, this option is available in eScan version 11.0.1139.1229 and later]

Unique solution ID: #1236
Author: Nitin G Shivtarkar
Last update: 2014-08-18 09:15