eScan Antivirus Signatures

White Paper
Document Version (esnvs 14.0.0.1)
Creation Date: 19th Feb, 2013

Anti-Virus Signatures

This paper explains about Virus signatures and how eScan downloads them to combat against latest threats. Virus Signatures are the core part of any Anti-virus, without virus signatures Anti-virus would not be able to eliminate viruses that are exist in-the-wild. It is like a gun without bullets. In order to keep your anti-virus up-to-date, you need to download the virus signatures from your AV vendor's website. AV vendor automatically downloads them from internet, once they installed on a system.

In this whitepaper, we will see how eScan downloads virus signatures? From where it downloads them? How SOHO products update themselves? How corporate product downloads the updates and distributes them?

Before digging deeper into the Virus signatures, we need to understand what do we mean by virus signatures?

Virus signatures are the updates provided by Anti-virus vendors to combat new threats. Once the virus signatures are downloaded and updated. The Threats for which the signatures have been designed can be removed using Anti-virus engine. It needs lot of efforts and testing to create virus signatures.

How this is achieved?

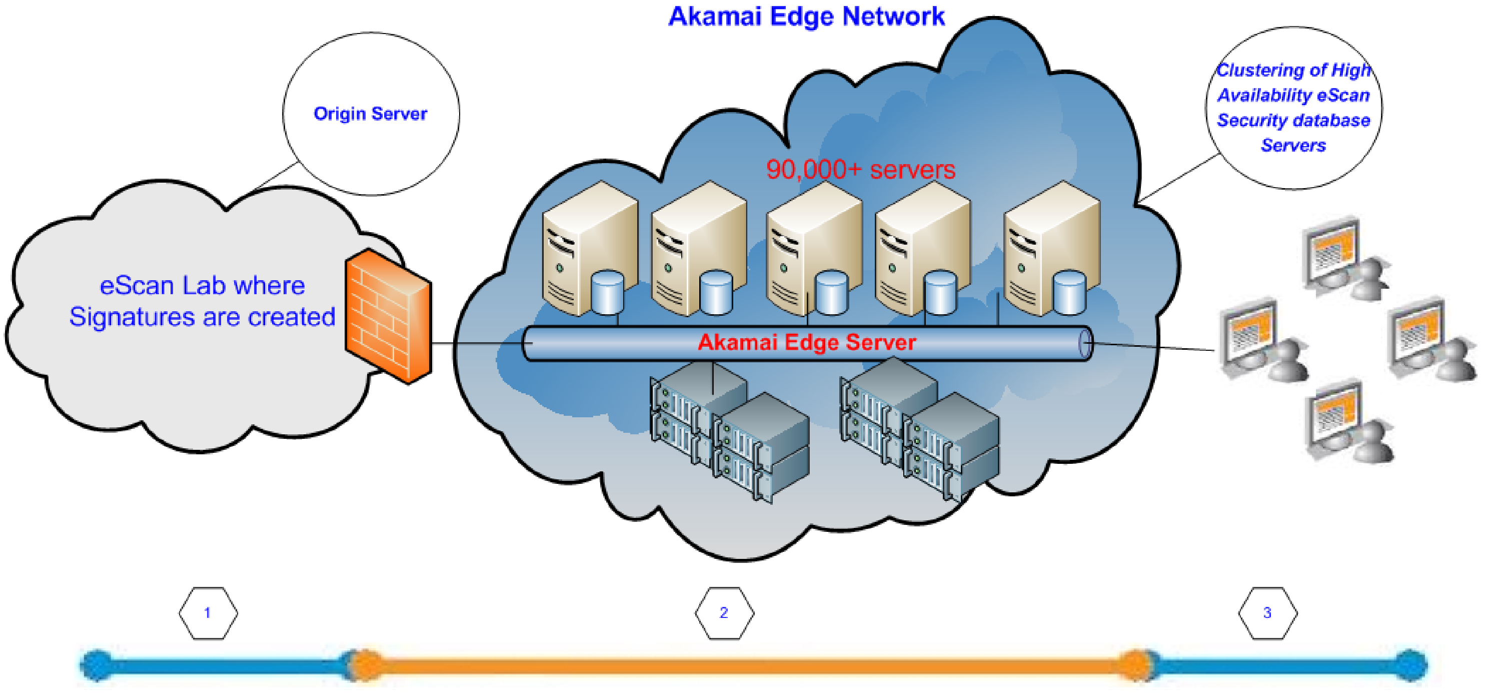
Once the sample is received at eScan Lab, it goes through number of procedures to create virus signatures. Malware analyst run static and dynamic test to see how the system behaves, when the sample is executed, based on the collected information from Malware Analyst, Virus signature is created and then again it needs to be tested whether it is remediating the infection correctly and no false positives are detected and then these signatures needs to be released.

Today, more than hundreds of malwares are found every day, and it is very difficult task for AV vendors to release the signature for each virus. But it is necessary to release the signature to prevent these threats.

Infrastructure plays a major role when it comes to distributing updates to all our customers, reason being the number of customers using eScan AV engine, eScan is popular in all the countries worldwide and it is being used worldwide. To cater all the customers worldwide eScan has deployed more than 90,000 servers to update eScan products all over the world, while distributing virus signatures, we need to consider the download speed of the signatures and the availability more servers to distribute the load evenly to all our customers worldwide.

The mechanism used to update these entire 90,000+ servers all over the world is robust. Akamai is playing vital role in doing the same. eScan lab updates the virus signatures to Akamai Edge server and then Akamai edge server synchronize the updates to its entire 90,000+ server within few minutes.

Below diagram shows us how virus signatures are distributed.


Akamai Edge Network
Origin Server
Clustering of High Availability eScan Security database Servers
90,000+ servers
eScan Lab where Signatures are created
Akamai Edge Server
1
2
3

Malware Analyst creates virus Signatures at eScan Lab, and update them on Origin Server

Then eScan customers can Download them once they Are connected to internet

Once It is updated on Origin Server. After every 2 hours A script is run to synchronized data between origin server And the servers located on Internet for distribution.

eScan has Deployed 90,000+ servers on Internet, To distribute virus signatures to their customers.

It hardly takes few minutes to synchronized the data

Above Figure shows you how updates are distributed and synchronized between multiple servers. eScan has deployed over 90,000+ servers to distribute virus signatures to its customers.

1. eScan Experts create virus signatures.
2. eScan Lab upload the virus signatures to eScan Origin Server.
3. eScan Origin Server uploads its signatures to Akamai Edge server using FTP protocol after every 2 hours.
4. These signatures get automatically mirrored to Akamai Edge network.
5. eScan Clients then download those signatures using Akamai network.

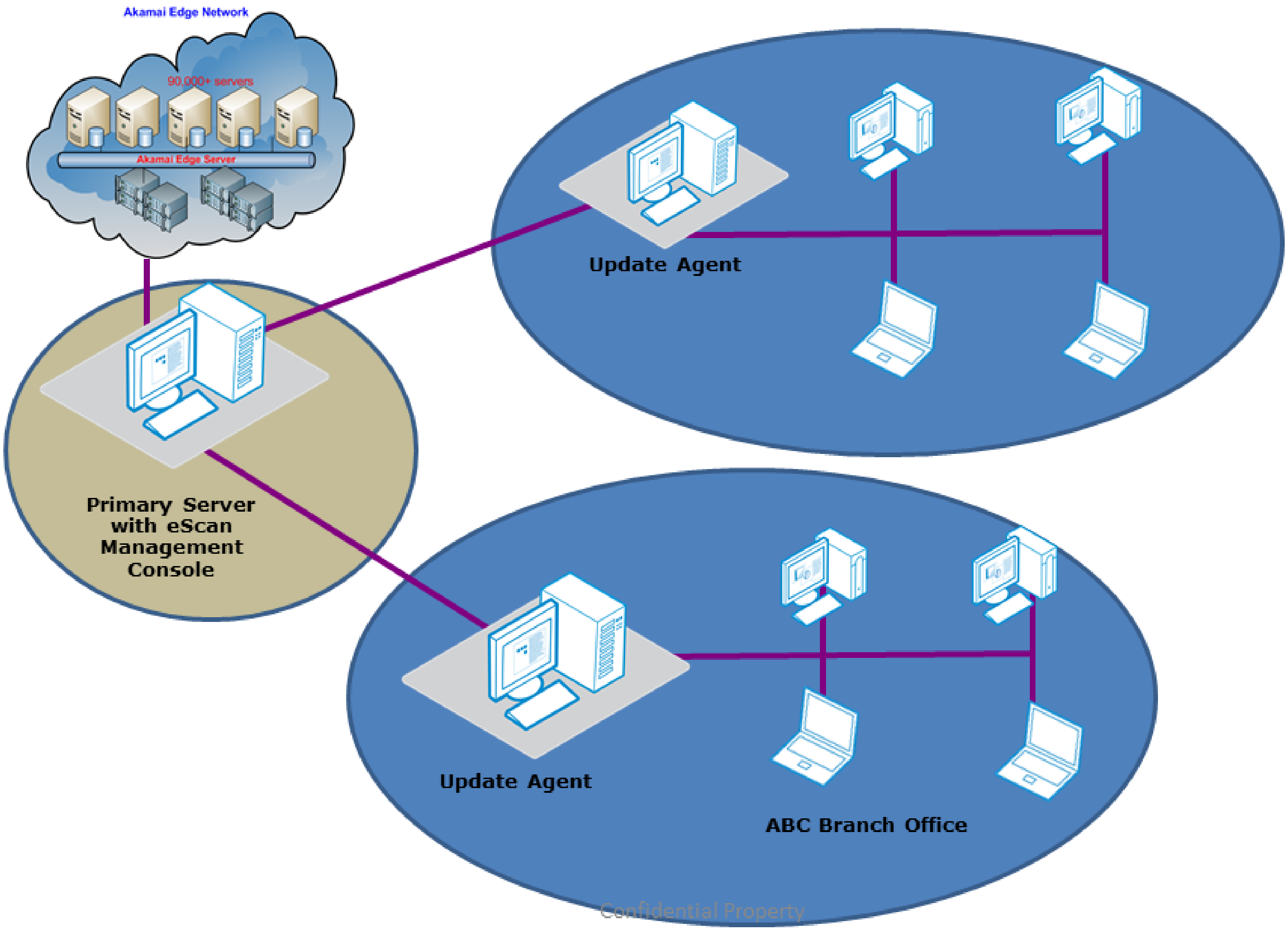
This is how eScan releases virus signatures to its customers. Once Virus Signatures are available for download, eScan products automatically query to eScan update servers after every 2 hours, to check, if any new signature is available or not. In this process, Following conditions are checked:

1. eScan products queries to the eScan updates server on internet, to check if any new signature is available or not.
2. If New Signature is available then eScan invoke its downloader to download the new signatures automatically, and updates the virus database.
3. If new signature is not available then it does not invoke the downloader till next cycle (i.e. after 2 hours).
4. If it does not found internet connection at the time of query, it will retry the query after every 3 minutes till the query succeeds.

In corporate products, same steps are followed but eScan clients download the updates from eScan server instead of internet. And eScan server downloads the updates from internet. Otherwise all the above mentioned 4 steps remain same. In Corporate environment, it might happen that eScan client is not in the local network, then eScan client will switch to internet to download virus signature and this switching will happen after 6 hours when eScan recognize that it is not in the local network where eScan server resides.

Following Diagram shows how Different branches download updates from eScan Corporate Server and update agents:

Updates Distribution in Enterprise environment


Akamai Edge Network
90,000+ servers
Akamai Edge Server
Primary Server
with eScan
Management
Console
Update Agent
Update Agent
ABC Branch Office