

**SOLUTION PAPER
CONSOLIDATE SERVERS
SECURELY**

An introduction to Secure Consolidation

Everybody wants to consolidate their Network

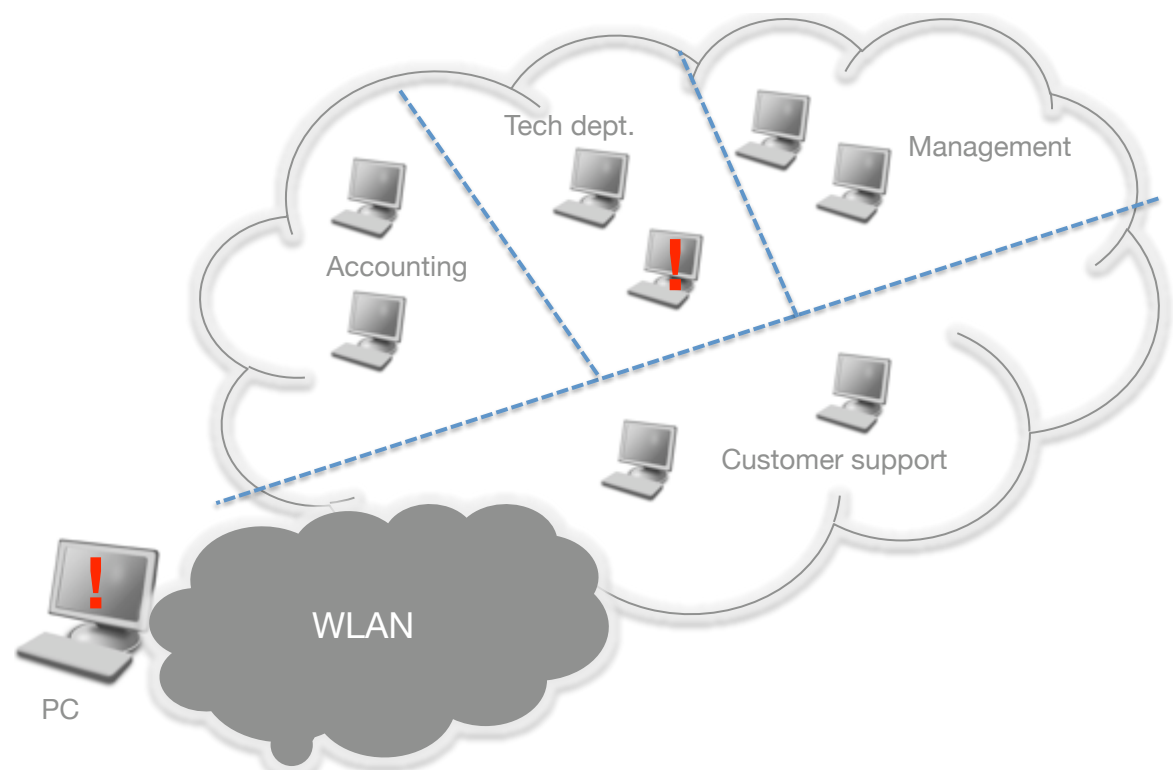
- So why does not everybody do it?
- Because the problems are many and costly to overcome!

Introduction

Segmentation of networks increases security and can be a business enabler

Segmentation of networks simply means that network traffic no longer can flow freely between all systems on the internal network. This has many advantages, such as better possibilities to react on security incidents and a very high level of security can be achieved. It may, for example, be desirable to allow a remote partner to access a shared project server, and the segmentation will automatically prevent project members from seeing or sending traffic to other systems on the internal network if they belong to other segments.

The picture shows if for example a virus outbreak is found within the tech-department, it is fairly simple to isolate this segment from the other until the problem is solved.



Segmentation creates problems

So why does not everyone segment their networks? There are several reasons why this is not as easily done as it may seem to be:

Segmentation as shown in the picture seems simple – but in reality, users are located not just in one building or in one site. This logical picture does not match the physical corporate structure.

Servers have the same problem: they are found at different physical locations.

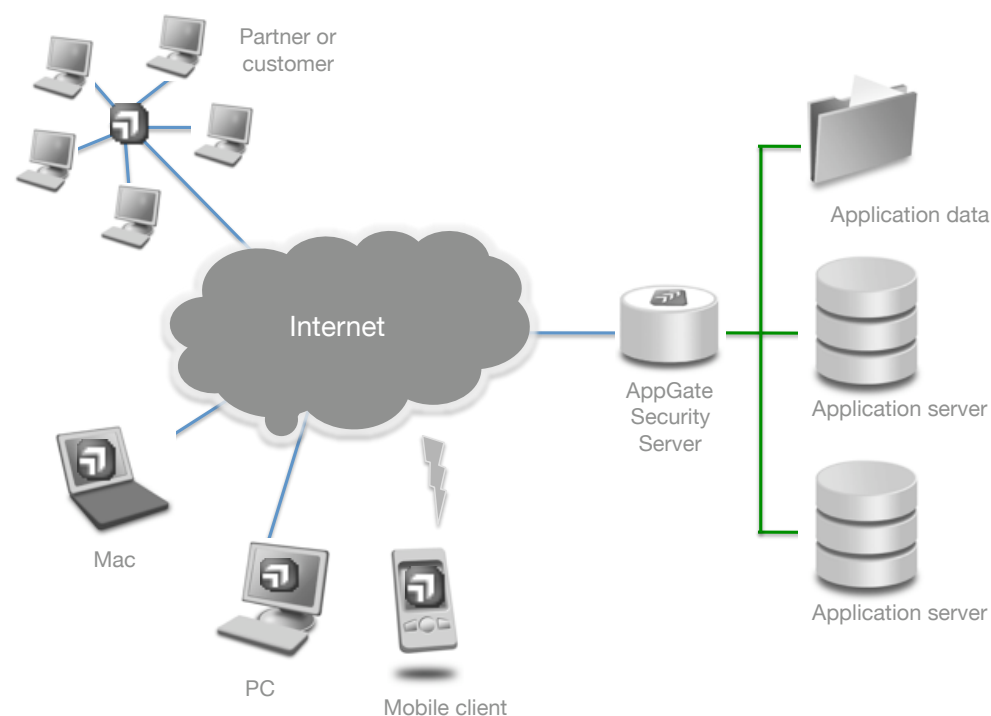
This model limits the use of shared resources. Many services must be duplicated if segmentation is introduced. There will even be servers that cannot be duplicated since their information must be available not just within one segment. It prohibits organizational changes and makes it hard to create “virtual” organizations quickly. And how should a user be treated if he/she belongs to more than one segment? Or if a user gets new assignments without moving across the street?

So, higher security results in lower flexibility.

And in many situations, security will be sacrificed in this battle.

The AppGate solution

By moving security closer to the applications servers, it is possible to offer controlled access from any device over any network infrastructure in a totally secure way. If clients encrypt all network traffic, we will have separation of traffic virtually identical to giving everyone their own network connection. Traffic cannot be read or modified by anyone else on the network. Adding an AppGate server in front of the application servers will take care of user authentication, access authorization and the application servers will be protected by AppGate's unique and prize winning security solution.



The solution has many advantages:

- Network encryption gives each user a private secure connection comparable to his/her own network cable. It does not matter where users are located. Access is granted based on who the user is, type of device being used, etc., but access can be granted from everywhere if desired.
- External authentication methods are easy to use. Application servers do not have to deal with certificates, token devices or smart cards, this is handled by the AppGate server.
- Users can easily belong to more than one user group
- Virtual organisations are easily created and deleted
- Client configuration can be checked before access is granted, for example to make sure a personal firewall is being used if the user connects over the Internet.
- Customers, business partners, remote workers and other categories of users are easily handled by the system. The administrator will always be in full control of the system.
- It is easy to offer external users access in a secure way
- Internal access is as easy to control as external access
- It is possible to grow with the solution
- Different user roles can be granted access to different systems or applications
- Fits in data center solutions
- Networks are no longer security sensitive



appGATE™
NETWORK SECURITY



www.appgate.com