ARCHITECT JOURNEY

FrieslandCampina

An International Dairy Conglomerate's Network and Security Transformation Journey

Company:	FrieslandCampina	**Revenue:**	$14 billion
Sector:	Dairy	**Employees:**	20,000
Driver:	Erik Klein	**Countries:**	34
Role:	Infrastructure Architect	**Locations:**	120

Company IT Footprint: FrieslandCampina has 120 locations. It employs over 20,000 people worldwide, but, because those people work in shifts, the number of endpoints are not related to the number of employees. Within the office and industrial workspace, there are about 7,000 to 8,000 endpoints. It currently also has over 80 factories worldwide.

"I'm looking towards making the network totally irrelevant in the next five to seven years. The network will only be a transport mechanism that makes sure the application goes from A to B, but the data security itself is completely embedded in the communication stream."

Erik Klein, Infrastructure Architect, FrieslandCampina

zscaler™

Excerpt from: Stiennon, Richard "Moving Applications to the Cloud," *Secure Cloud Transformation: The CIO's Journey*. IT-Harvest Press, 2019, pp. 51-59.

FrieslandCampina Journey Overview

Business Objectives

- Align IT with both operations technology (OT) and IoT priorities, processes
- Improve security
- Reduce MPLS costs, WAN dependence
- Resolve Office 365 deployment challenges

The Solution

- Introduce dynamic application-routing, local internet breakouts
- Overcome cultural hurdles to cloud security
- Move applications to AWS
- Transition to Office 365
- Deploy SD-WAN

Impact

- Reduced costs: MPLS, hardware security stack, “turning off apps on weekends”
- Faster application access, better user experience
- Better security, delivered inline
- “Making the network totally irrelevant”

FrieslandCampina is a global producer of milk products and has created a sophisticated network to provide consistent and secure global connectivity. Erik Klein, lead infrastructure architect, tells its network and security transformation story.

In the words of Erik Klein:

Bringing milk products to the world

I joined FrieslandCampina in 2012. We are a global producer of milk products—we make cheese, infant and toddler nutrition, yogurts, skimmed and semi-skimmed milk, condensed milk, and health foods for athletes. We are based in the Netherlands, and over time we have expanded into other countries, such as Indonesia, Vietnam, Nigeria, Ghana, the U.S., and many others.

IT has an important role in manufacturing goods. From a production perspective, the availability of the operations technology (OT) environment (which is IT within the production environment with specific requirements) has a huge impact. For example, the raw milk can't be stored for more than seventy-two hours. Any longer and it gets discarded, but it can't be thrown away into a sewer, so it is a costly process to dispose of the spoiled product. Therefore, OT is used within the production environment to make sure that the production processes aren't disrupted and work within the strict timeframes.

Within the OT environment, with the introduction of next generation PLCs (programmable logic controls), smart sensors, and other IoT developments, the number of IP-based endpoints will grow considerably over time.

Currently, we have about 80 factories worldwide. Some are more traditional, but some are really sophisticated and the Smart Factory is emerging. Therefore, the number of endpoints will grow in the OT environment.

Our cloud transformation

By the end of 2013, the cloud hype cycle started and there were more and more people looking at software as a service, localized content, and moving stuff to the cloud—in our case, Amazon Web Services.

Eventually, we realized, when going in that direction, the wide area network we had was no longer valid. We needed to go into a transformation from a private MPLS-centered network to a public internet-centric network.

"We needed to go into a transformation from a private MPLS-centered network to a public internet-centric network."

At that time, the designs we made consisted of several boxes on location, and we realized that this would be too complicated and expensive to execute. So in 2014, we embarked on the transformation journey by moving the centralized proxy server to the cloud with the Zscaler cloud service, but still relying on the capabilities of Cisco routers for all other functions.

As cybersecurity became more of an issue, the Zscaler Cloud Firewall came into play. Moving security to the cloud was harder, because I had some internal push back, and there were some reorganization issues. But in 2016, we started a project to extend the boundaries of our network from a stateful firewall on a Cisco router at the FrieslandCampina location to cloud security, the Zscaler Cloud Firewall.

From every location, we then built IPsec tunnels to the Zscaler security service and used the proxy functionality as well as firewall functionality of Zscaler.

To overcome the limitations using PAC (proxy auto-configuration) files in the browser to get to the internet, we also transferred the routing within the whole LAN environment, so that the default route from every location would end up at the security layer of Zscaler. And that's where we are today.

And then it was time for testing dynamic application routing.

Why secure internet local breakouts?

There are two reasons why we switched from a centralized proxy environment to the cloud-based proxy environment with local breakouts. Firstly, from a marketing perspective, the driver to break out locally was to get localized content. The web servers that you're connecting to from each country should automatically give the content of the website in the local language, for example.

Secondly, FrieslandCampina had been using a number of different SaaS applications worldwide, so having it all centrally break out was, from a performance perspective, not a way forward. Also, the web content became richer and files were getting bigger, so there was more data to transport. From a localized content perspective, and the fact that users are using more and more SaaS applications, we realized that we would need to bring the end user to the internet (cloud) quicker.

"The 2016 phase of the network transformation went very quickly and was completely non-disruptive."

Except for our private cloud, direct-connected VPC (virtual private cloud) on AWS—and we have connected that to our MPLS backbone so that's still going over an MPLS link—everything else is being offloaded at the local site level and then travels to the closest Zscaler data center based on lowest latency, with a second closest Zscaler data center as backup. We do a measurement every six months to see if indeed those Zscaler nodes are still the quickest to reach.

Moving applications to AWS

FrieslandCampina is currently migrating applications to AWS based on various criteria, such as those applications that only need to be accessed at certain times. This service can't be provided by our existing hosting provider, and keeping those servers at their location will be too expensive. On the other hand, T-Systems couldn't always meet the requirements of the applications, resulting in an instance that was too big (too expensive) or too small (poor performance). And thirdly, AWS gives us the flexibility to temporarily upscale and downscale when required. With the capabilities of AWS, we could tailor to the actual requirements of the applications.

Last but not least, since not all applications are 24/7, we could use AWS elasticity to turn them off on the weekends, saving money in the process.

Improving SaaS access

In the early days, when we moved to the cloud proxy, we had our share of difficulties with the performance of Office 365. We really struggled to get that done correctly and have good performance now.

The 2016 phase of the network transformation went very quickly and was completely non-disruptive—people didn't even know we moved security to Zscaler. Nobody really noticed that we went from centralized to decentralized, except that some of the applications became quicker.

Also, Zscaler was very quick in communicating what they were doing about cyber security threats like, but not limited to, WannaCry and NotPetya. They were quicker to communicate the impact within their environment than other partners. They really did a good job on that one.

Deploying SD-WAN

Right now, we are going towards a full SD-WAN (software-defined wide area network). Our strategy involves connecting five FrieslandCampina locations to the SD-WAN environment, and that the SD-WAN environment has an NNI (network-to-network interface) with our existing Verizon network. With a full-blown SD-WAN deployment our redundancy plan includes redundant internet lines and universal customer premises equipment.

For locations that use applications that require MPLS services, a fit for purpose MPLS line that is smaller than our legacy MPLS circuit is supplied.

Historically for every location, except locations with call center functionality, the MPLS line was approximately 5 megabits per second, while the internet lines are a lot bigger. We also have a failover from MPLS to the internet and the two internet lines back each other up. Our goal is to guarantee an experience level agreement (XLA) at the application level, rather than a service level agreement (SLA) based on availability and time to repair. We are aiming for predictable behavior and end-user experience on an application-based context (device, location, connectivity).

The SD-WAN has what they call universal CPEs at each location. And those universal CPEs will have network function virtualization on them. Actually it's a device for compute and storage with a hypervisor, which runs virtual services which are required by either the SD-WAN service itself or the application acceleration. Other virtual network functions can be added if and when required. There will be a growing number of network function virtualizations that we can deploy on those devices.

Picking an SD-WAN partner

In 2017, we initiated an RFI for, amongst other services, a new WAN service.

The vendors invited to the RFI were only given business requirements and we asked them to really innovate with a disruptive approach. We selected eight vendors to enter the RFP phase, and we started eliminating vendors based on their offering and presentation of the solution. In the end, three vendors were selected to give us their best and final offer, namely NTT, Interoute (both proposing the Silver Peak SD-WAN solution), and Verizon (proposing a combination of Viptela and Riverbed).

"Do not invest in a traditional network. Don't do any investments in your existing MPLS with an internet backup network. That's old school."

As part of the RFP process, we asked each vendor to present a reference customer where they had already deployed the proposed solution. And based on discussions with those customers, we made the final selection. The vendor testimonials were very important to us in the final phase of the RFP process.

Things to consider

- Do not invest in a traditional network. Don't do any investments in your existing MPLS with an internet backup network. That's old school. Just make sure that you know how your traffic is routing—so where your end users are and where your applications are—and make sure that you create a network where, based on the applications, the quickest, most efficient route will be taken. In the end, users are not interested in technology, they are only concerned that the applications they are working with on a day-to-day basis perform well and perform constantly. If you have an application that has a 2.5 millisecond response time throughout all of Asia, nobody is complaining. But if you have one country that has a response time of one and another of four, then they start talking to each other and start complaining.

- People are traveling more and working outside of the office, and those people are diverse. Currently, we are bringing people that are roaming back into our network via two central remote access (VPN concentrated) locations. With the use of tools like the Zscaler App, we are looking at alternatives to connect roaming users to internal applications.

- In the end, if you have your software-defined wide area network, local area network, and software-defined data centers, you need an orchestrator of orchestrators above that to make sure the policies you set on an application, or at a higher level, flows down to the LAN, the WAN, and the data center. And the next step is to invest in security in the session between consumer and application.

- I'm looking towards making the network totally irrelevant in the next five to seven years. The network will only be a transport mechanism that makes sure the application goes from A to B, but the data security itself is completely embedded in the communication stream. For example, based on the identity of the client and on the identity of the application, a secure communication will be set

up between them. That will be my next focus, and will be around the 2025-28 timeframe. It could happen sooner, but developments within our company need a business case for change; there needs to be funding for it, and so on. Not only is the development of the technology driving this, but also the adaptation and the willingness to spend money in new areas.

Ready to transform your company?

Create business value with Zscaler today.

CONTACT US

REQUEST DEMO

https://www.zscaler.com/company/contact

https://www.zscaler.com/custom-product-demo

About Zscaler Zscaler was founded in 2008 on a simple but powerful concept: as applications move to the cloud, security needs to move there as well. Today, we are helping thousands of global organizations transform into cloud-enabled operations.