

# Toyota Financial Services, a safer company network with Cisco NAC Access Control



**Company:**

Toyota Financial Services

**Business Sector:**

Finance, Lease, Rent.

**Our Challenges:**

Providing our infrastructure with a proactive safety solution with wide-ranging efficacy within the Web.

Setting the safety solution to guarantee Security Policy standards for all assets, both inside and outside the company.

Optimizing all processes and reducing risks of vulnerability.

**Met Targets:**

We protect our business environment with an efficient Access System Control (for mobile users, remotely connected users, partners with outsourcing contracts, guests and temporary staff).

We allow safe accesses to our company network to inner and external users, protecting all data from unauthorized intrusions with guaranteed efficiency anytime, anywhere.

We have improved our employees productivity, shielded our confidential information and cut down expenses thanks to Cisco NAS Access Control. We have therefore optimized our ROI.

Toyota is the second worldwide car manufacturer: it produces more than 9 million vehicles a year throughout the world within its 67 plants. Toyota Italy has more than 233 points of sale and 227 assistance centers. "Financial Services" is the company division which deals with financing.

For companies like Toyota is not enough to rely on a perimetrical defense anymore. They have the urgency to implement integrated solutions with wide-ranging efficacy within the Web.

This is why the company asked for an innovative solution that complies with safety policies for all final devices (managed or not by the IT dept.), regardless of access mode, model type, applicative settings and remediation models. This mean a proactive safety solution for the company infrastructure that improves Web resiliency and widely protects the inner network infrastructure.

The company works in open business environment, where laptops and mobile devices go in and out the offices, connect to the company network or to the Web. Employees relate to customers remotely connected in public places, to partners with outsourcing contracts that need to access the company network, to guests and temporary staff who may need access to the Internet. This methodology of work needs a reliable and safe infrastructure in

compliance with the Security Policy for all assets, both inside and outside the company.

Because of those reasons **Cisco NAC** (Network Admission Control) technology was preferred. Cisco NAC is a solution that sets the network itself in control for all peripheral devices accessing the network. Access is allowed only to reliable and recognized devices (PC, servers, IP telephones and printers included), while is denied to not recognizable devices. These are redirected to a quarantine area for possible remediation.

Cisco NAC defines and makes use of complete and spot security policies, that can be processed and applied reliably, systematically, automatically and completely by the network itself. This can be realized with a scalar architecture, a centralized component that defines policies, verification and controlling components distributed throughout the network and the possibility to integrate with other security solutions and technologies.

In order to avoid not authorized accesses, a part of the network, entirely separated from the production LAN, has been farmed out to consultants. This way Internet access is granted without putting the company network at risk.

Furthermore NAC controls all connections from a remote location, which is very useful when partners with extranet applications have to be allowed connection. It is a delicate situation when it is impossible to know who is connecting from a partner's office. Having all accesses under control before, during and after users authentication, is the best way to keep the company information safe.

Cisco NAC was implemented using Cisco Clean Access (CCA) technology.

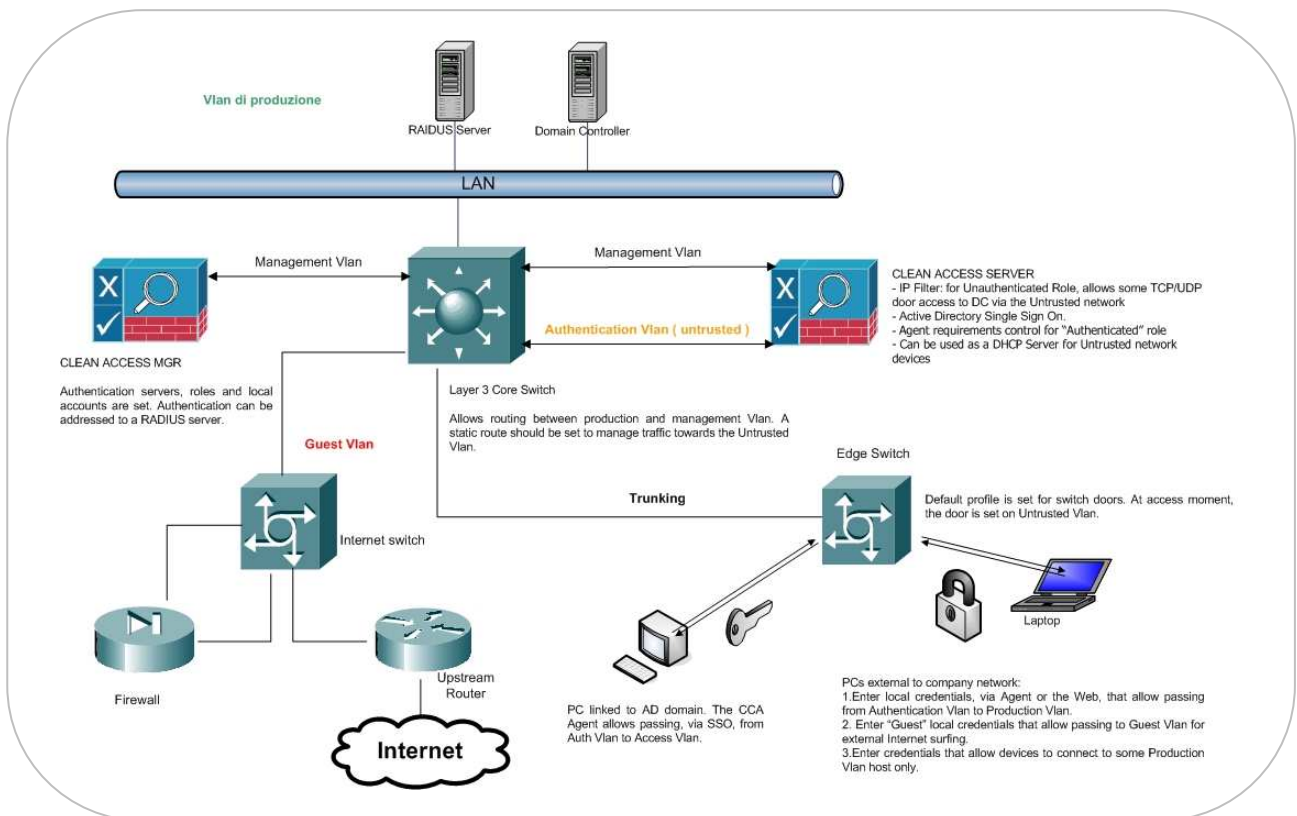




In Toyota's case two kind of technological equipments were used: Clean Access Manager (CAM) and Clean Access Server (CAS), both set on redundant mode. Clean Access Manager provides a Web interface that creates security policies and manages online users. It can work as a proxy authentication for servers as well. Administrators can use Clean Access Manager in order to manage role-users, conformity controls and remediation enquiries. Clean Access Manager communicates with Clean Access Server, NAC's activation element. Clean Access Server provides a Web interface that creates a security policy and manages online users. For Toyota this was realized in Out-of-Band Real-IP Gateway mode, in Layer 2 restricted and implemented in HQ offices. Within the frame of a steady, efficient and safe environment, Toyota has improved its productivity, protects confidential

information, cut down the solution life-cycle costs and can therefore be a winner on the markets. Assured Return of Investment (ROI) should not be forgotten. It can be quantified according to the risk the company is willing to face using NAC.

A complete and guaranteed security strategy has sure benefits: optimization of processes and reduction of expenses and accidents while investing a limited budget. Protecting the company resources with an efficient asset management reduces vulnerability risks and ensures protection to all devices on the network.





Headquarter: L.go G. Falcone, 4 – 00045 Genzano di Roma

Tel. +39 069391360 - [info@aminformatica.it](mailto:info@aminformatica.it)

<http://www.aminformatica.it>