FORTINET

NETWORK ACCESS CONTROL PROVIDES A STRONGER CYBER FENCE AROUND ICELAND'S AIRPORTS

Headquartered at Reykjavík Airport, Isavia is the national aviation authority for Iceland, dedicated to ensuring that flight operations are safe, secure and in accordance with international standards.

Isavia's nationwide network is critical to operations at Iceland's airports and air traffic control facilities serving vast areas of the northeastern Atlantic. The forecast for the main airport was at 8.8 million travelers a year by 2025. The company now expects more than 10 million passengers this year and more than 17 million annual travelers in 2030. Many different devices depend on access to the airport's network, including laptop and desktop PCs and a wide range of security and infrastructure devices. Network managers need to know what devices are on the network, where they're located, and that each is limited to its intended access. Given the need for heightened airport security, Isavia recognized that these challenges could best be addressed using a Network Access Control (NAC) solution.

With on-site assistance and integration provided by leading channel partner Khipu Networks, Isavia installed the Fortinet NAC solution to provide real-time network visibility and automated access control at airports across Iceland as well as at Isavia headquarters and satellite offices. The NAC solution identifies all devices on the network and allows access to resources based on pre-defined policies. Access decisions are made before the device connects so if a device is unauthorized, the connection is automatically blocked. NAC also simplifies the day-to-day logistics of configuring network devices. It automatically identifies devices and assigns access based on easy-to-manage profiles, providing plug-and-play provisioning in a fraction of the previous time.

"We wanted a solution that would enable us to know what was connecting to our networks and shut down unauthorized access."

– *Axel Einarsson*
  IT Manager
  Isavia

isavia

DETAILS

CUSTOMER: Isavia

INDUSTRY: Transportation/Airline

LOCATION: Reykjavik, Iceland

BUSINESS IMPACT

- Provides a real-time view of network activity at all facilities

- Ensures only authorized devices can access the network

- Automatically places devices on the correct VLAN based on predefined policies

- Blocks unauthorized devices before they can get on the network

- Saves time via plug and play provisioning

DEPLOYMENT

- Network Access Control

AUTOMATICALLY ENFORCES ACCESS POLICIES

"NAC is part of the security fence for our airports," Axel Einarsson, IT Manager at Isavia, explains. "We use it to control device access to ports according to their role. If an unauthorized device tries to connect, NAC shuts down the port immediately." New devices are sent to a registration VLAN where IT captures the MAC address and a few other details. "After that, we can plug a device in anywhere, and the NAC solution automatically assigns it to the correct VLAN according to predefined policies. It's a big time-saver," Axel adds.

The solution supports all Isavia facilities, including Kefkavik International airport, fifteen domestic airports across Iceland, Isavia's headquarters in Rekyavik and branch offices. NAC provides visibility and access control for thousands of devices, including staff PCs and headless devices like printers, badge readers and security cameras. It also provides access control for companies and stores that use the Isavia network.

IMPROVED OVERSIGHT AND CONTROL

NAC is now an integral part of Isavia's security perimeter that is used to protect Iceland's aviation infrastructure and the flying public who depend upon it. It provides complete visibility into all devices that access the network, and NAC's automatic quarantine of unauthorized devices has significantly improved Isavia's security posture. This increased security addresses major concerns for Isavia and the flying public.

Isavia needed a solution that offered the most efficient oversight and access control on a nationwide network. "Isavia has locations all around Iceland, and we need to protect the ports in those remote locations. We wanted a solution that would enable us to know what was connecting to our networks and shut down unauthorized access."

Axel and his colleagues explored the market for a comprehensive security solution, looking for a combination of functionality, ease of use, and price. "The NAC solution we chose was a better fit than the competition and integrated smoothly into our network environment," Axel says.

Isavia has greater control over its network while reducing the workload for network administrators at Isavia headquarters and IT staff at remote sites. Since NAC places each device on the correct VLAN, IT can install a device and have it network–ready instantly without assistance from administrators to configure ports. "The whole process has become smoother and faster," Axel observes.

WHAT'S NEXT

Continually improving the security posture is a key focus for Isavia. Isavia plans to extend NAC in a number of new directions, including its wireless network, to enable secure BYOD for employees and guests. The NAC solution offers real-time visibility and policy-based access control. NAC enables simplified security and antivirus compliance checks when devices connect to the network. Adding this requirement will ensure that devices have an up-to-date operating system and anti-virus software before being allowed access to the network. If users do not meet the requirements, NAC provides a link for users to self-remediate and limits access until they do. "NAC has given us better oversight and control over our network, Axel adds. "Now, we look forward to taking it further."