FireWall

Edge Airport France

Table des matières

network_configuration

Version originale

Réseaux et sécurité

Description générale

Le réseau aéroportuaire peut être complexe. Il est composé au minimum de 2 sous réseaux, eux-mêmes parfois sub-divisés en d'autres sous-réseaux généralement constitués de la sorte :

1. administratif,
2. opérationnel :
3. FIDS,
4. CUPPS,
5. Compagnies x…

Afin de garantir un haut niveau de sécurité, ces différents réseaux sont protégés par un ensemble de routeurs et de firewall. Les accès entre les différents sous-réseaux aéroportuaires sont alors segmentés par VLAN et protégés par un firewall central virtualisé ou non.

Chaque réseau peut avoir son propre accès internet. Dans ce cas les modems xDSL sont complétés par des routeurs « firewallant » paramétrés pour n'autoriser que les flux nécessaires aux systèmes informatiques aéroportuaires. Une séparation physique et logique par l'ajout de VLANs est réalisée entre les différents réseaux.

L'aéroport devant permettre d'exécuter des applications tierces des compagnies aériennes sur le réseau opérationnel CUPPS, des règles strictes de sécurité doivent être mises en place par les équipes réseaux de l'aéroport.

Chaque compagnie installant son propre routeur pour créer un accès applicatif via un VPN vers son système informatique, le réseau CUPPS et les réseaux des compagnies aériennes sont segmentés par autant de routeur que de compagnies.

Des règles de sécurité sont implémentées entre chaque équipement constituant les sous-réseaux et chaque système en fonction des flux qui lui sont nécessaires. En aucun cas, une compagnie ne doit pouvoir accéder à un sous-réseau de l'aéroport si aucun flux de ce type n'est nécessaire.

Chaque routeur physique dont Edge-airport à la charge peut être virtualisé sur la plateforme pour permettre un « backup » en cas de panne physique du routeur.

Edge-airport utilise principalement des routeurs de marque CISCO®, en fonction du besoin de sécurité de l'aéroport

Le Firewall Virtuel utilisé pour protéger les machines virtuelles ou remplacer un routeur physique est

pfSense, une solution libre de sécurité reconnue dans l'industrie de sécurité des réseaux.

Toutefois, si l'aéroport souhaite une garantie supplémentaire, tant pour la confidentialité que pour la sécurité de ses données, Edge-airport possède les qualifications nécessaires pour intégrer les solutions de sécurité Européennes de marque **STORMSHIELD**®(anciennement netasq) du groupe **AIRBUS DEFENSE&SPACE**. Ce sont actuellement les seuls équipements à être certifiés ANSSI EAL4+.

pfSense

1U Rack Mountable

The pfSense C2758 delivers a high performance, high throughput front-line security architecture at an excellent price per gigabit. The multi-core processors and extra memory make it great for medium to large networks or for a small network that is expanding.

High Availability

Two or more firewalls can be configured as a failover group. If one interface fails on the primary or the primary goes offline entirely, the secondary becomes active.

Multi-WAN

Enables the use of multiple Internet connections, with load balancing and/or failover, for improved Internet availability and bandwidth usage distribution.

Server Load Balancing

Used to distribute load between multiple servers. This is commonly used with web servers, mail servers, and others. Servers that fail to respond to ping requests or TCP port connections are removed from the pool.

Dynamic DNS

A Dynamic DNS client is included to allow you to register your public IP with a number of dynamic DNS service providers.

Virtual Private Network (VPN)

Multiple options for VPN connectivity, including IPsec, OpenVPN, and PPTP.

PPPoE Server

The pfSense software offers a PPPoE server. A local user database can be used for authentication, and RADIUS authentication with optional accounting is also supported.

Reporting and Monitoring

RRD and real time graphs that include information on everything from CPU utilization to real time throughput for each interface.

Captive Portal

Captive portal allows you to force authentication, or redirection to a click through page for network access. This is commonly used on hot spot networks, but is also widely used in corporate networks for an additional layer of security.

Edge Airport France

Airport Manager Solutions

Phone: +33 553 801 366

Service commercial : contact@edge-airport.com

Support technique : support@edge-airport.com

Edge Airport France SAS au capital de 150 000 €

RCS Bergerac 529 125 346 Les Lèches TVA : FR53529125346 / EORI : FR52912534600039

Tel : +33(0)553 801 366 contact@edge-airport.com www.edge-airport.com