Beacon
Your purchasing partner

Top 3 Reason Why Hotels Need to Protect Their Network:

A state-of-the-art firewall: This asset is an imperative part of ensuring that only authorized users have access to network resources. With a next-generation firewall in place, the hotel can be assured that malicious actors and hackers are effectively kept out of the network underpinning the Wi-Fi as well as the hotel's point-of-sales system.

Advanced filtering: The right filtering capabilities can help ensure that illegal activity doesn't take place in your hotel. Filtering means the hotel has complete control over the traffic traversing its network, and can work to prevent malicious advertisements, spam messages and unsafe websites.

Managed Service: The network security should be managed by experts who monitor the system 24/7 to ensure complete protection, whilst at the same time taking the management responsibility away from the hotel staff.

Block Peer 2 Peer Activity: Torrent sites and game downloads were taking up a lot of the internet bandwidth meaning guests were not having a good experience in the WiFi.

Managed Service: They don't have the expertise in house to manage such a solution so they need Altinet to manage this in-house.

Increased Ransomware Protection: Became aware of the threat to the business and they

Bandwidth Controls: The ability to reduce internet traffic for site such as Netflix or allocate more internet to different parts of the hotels such as conference rooms.

Meeting Legal Requirements: They have a responsibility to keep all their customer's data protected and unaccusable to outside cyber threats.

Application Management: Their current Draytek firewalls were not application aware so only 30% of traffic entering the system was able to be monitored or blocked.

altinet
take control

71% of global hotels, restaurants and other hospitality organizations jeopardize customers with inadequate security controls.

Free Wi-Fi was recently rated the most important in-room hotel amenity, above a bathroom with shower and daily housekeeping.

51% of global hospitality organizations do not monitor guest networks for suspect applications, malware or malicious activities; 62 percent do not monitor guest activity to limit bandwidth-intensive applications; and 48 percent do not use policy mapping or data visualization tools to monitor performance.

Increased internet speed:
Using the bandwidth controls we can dedicate internet to locations or certain types of traffic such as Social Media.

Ransomware Protection:
This is currently one of the biggest threats to all businesses and can only be prevented by having a Next-Generation Firewall to protect the network.

Web Filtering/Reporting:
Hotels have a legal requirement to be able to report on internet activity and identify the room/location that certain sites we accessed from.

Managed Service:
This is a fully managed service which includes installation, configuration and 24/7 monitoring.

Case Study Cairn Hotels Group

Customer: Cairn Hotel Group
Product: Barracuda Next-Generation Firewall
Number Deployed: 40 Live Firewalls
Replaced Solution: Draytek & Netgear Firewalls