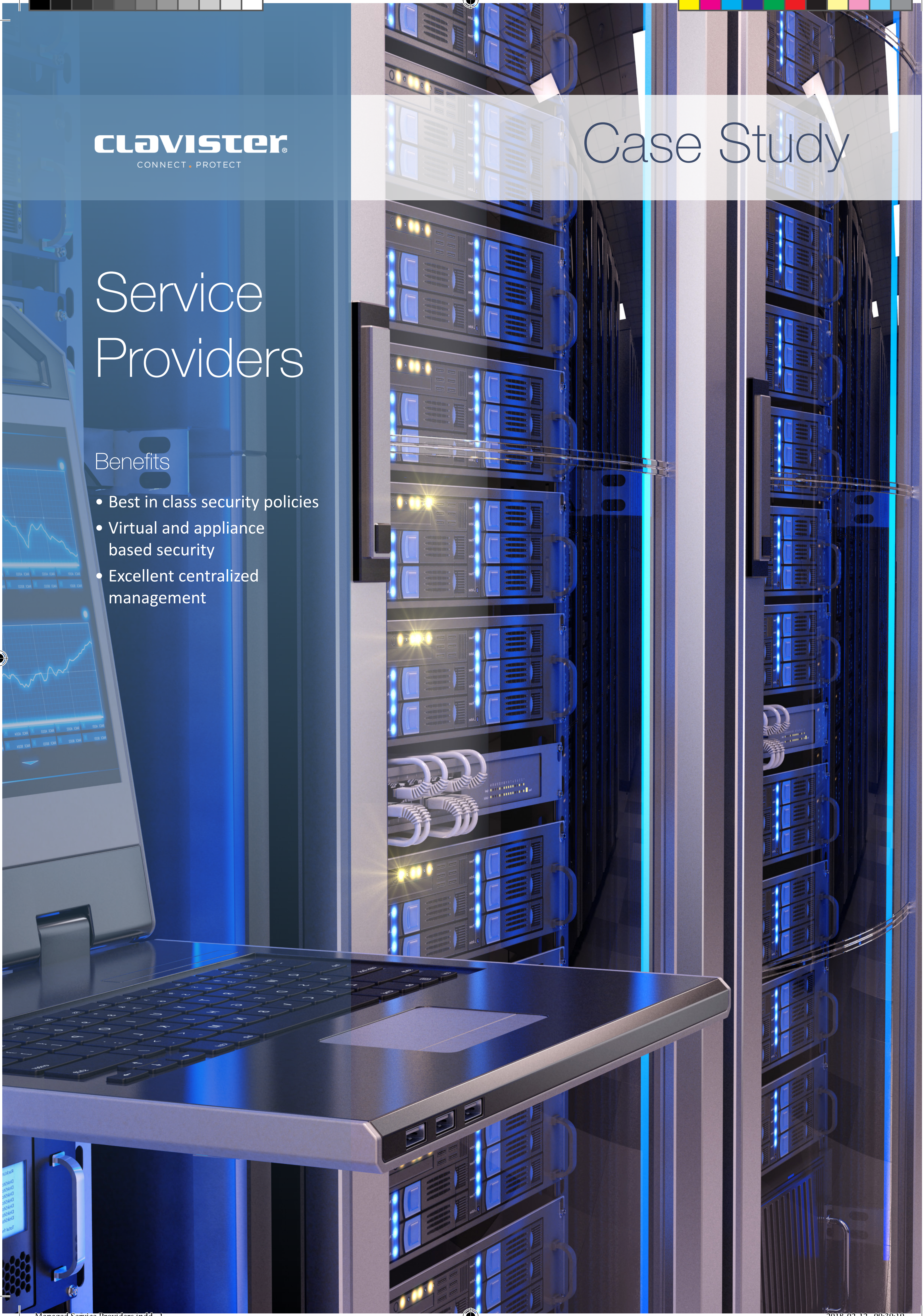


clavister
CONNECT . PROTECT

# Case Study

# Service Providers

## Benefits

- Best in class security policies
- Virtual and appliance based security
- Excellent centralized management

# Security for Managed Service Providers (MSPs)

In many ways, the nature of IT as an aspect of necessary infrastructure in business life has changed dramatically in the last few years. For decades, the paradigm of businesses buying a set of PCs for their employees to work from, buying software licenses for those machines, building a network and managing it through a staff of IT administrators and support.

However, with the rise of managed service providers, that paradigm has been deeply challenged by providing IT as a service and often in a cloud environment to keep operating costs minimized and efficiency high via cutting edge expertise. And to do that effectively, those service providers need a reliable, easy to deploy and affordable security solution that protects their customers data and business continuity.

# Customer Case: Core IT

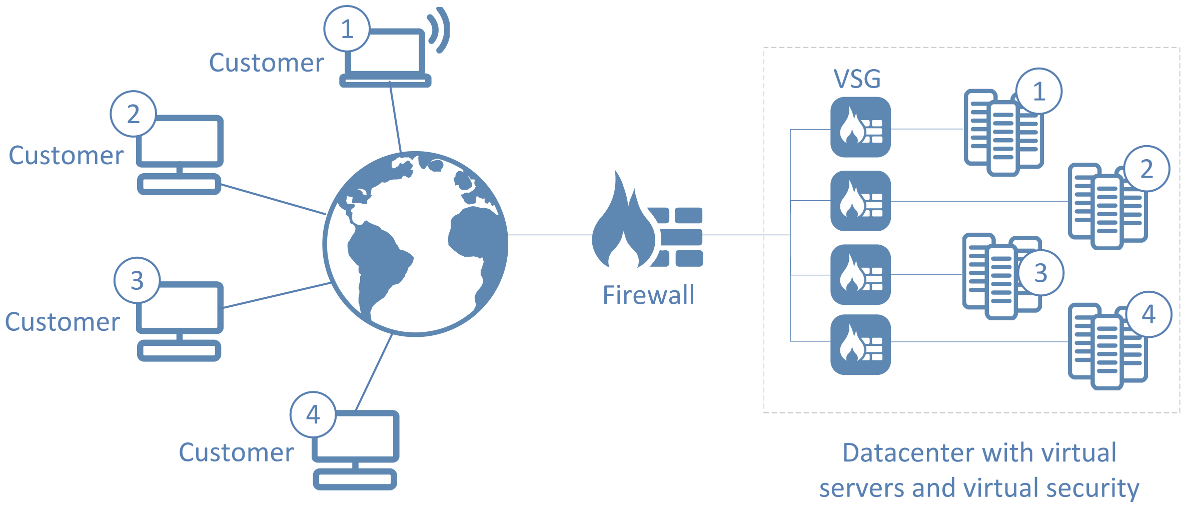
When firms contact Core IT—a Northern Swedish service provider and IT consultancy agency—they know they’re engaging one of most certified and competent suppliers of IT services. Versed in cloud infrastructure and deployment, they’ve been helping companies reap the full benefits of a service provider model.

Customers though have a major request as they host more and more data and services off premises: security is paramount. The solution Core IT provides is an elegant set of solutions by Clavister starting with a robust VPN tunnel between the remote office firewall and the main server one and adding other features that allow their mobile workers full protected access to their work platforms.

The firewall acts as a divider between an untrusted public Internet and a trusted network where customer resources reside. It can separate between trusted and untrusted resources and control network traffic access. This is the main building block for service providers for communication control and additional data content security. The main requirement for several different customers that wants access to their resources promptly and secure.

Users can be located both in offices and in the road—in remote locations, using one or more Internet access path over public networks that are not considered safe. Public access, encrypted access combined with different policies must be applied for customers based on service agreements with the service provider.

All of this is accommodated by yours truly—the service provider firewall as provided by Clavister’s state of the art cybersecurity NGFW.



Datacenter with virtual servers and virtual security

## Security policies

cOS Core security policies are configured to regulate which traffic can flow through the Clavister Next Generation Firewall and how traffic is examined and changed as it flows.

## Virtual routing

Virtual Routing is a feature that allows the creation of multiple, logically separated virtual systems within cOS Core, Clavister's proprietary operating system, each with its own routing table. This can be used if multiple different customers share a firewall where network addressing might be identical. These systems can behave as physically separated Clavister Next Generation Firewalls and almost everything that can be done with separate firewalls can be done with them, including dynamic routing with OSPF.

## Centralized management

Clavister InControl is our premium centralized management system built to manage thousands of Clavister NGFWs. By using Clavister InControl, service providers can easily handle anything from policy management to network troubleshooting and even produce insightful reports.

## VPN - Secure communication

When two internal networks need to be connected over the Internet securely—such as a remote office and a data center where resources are placed—each network becomes secured by an individual Clavister Next Generation Firewall with VPN tunnel set up between them. When many remote clients need to connect to an internal network over the Internet, an internal network is protected by the Clavister Next Generation Firewall to which the client connects and the VPN tunnel is set between them. In each case, the full power of Clavister's VPN is enforced to keep malicious intrusion from the network.

## Route failover

Clavister NGFWs are often used in mission-critical locations where availability and connectivity is crucial. For example, an enterprise relying heavily on access to the Internet could have operations severely disrupted if a single connection to the external Internet via a single Internet Service Provider (ISP) fails. It is therefore crucial to have backup Internet connectivity using a secondary ISP. The connections to the two service providers often use different routes to avoid a single point of failure. To allow for a situation with multiple ISPs, cOS Core provides a Route Failover capability so that should one route fail, traffic can automatically failover to another, alternate route.

# Clavister Features (Summary)

## Content Level Security

| | | | |
|---|---|---|---|
| Application Control | √ | Web Content Filtering | √ |
| Intrusion Detection and Prevention (IDP/IPS) | √ | Anti-Spam | √ |
| Anti-Virus | √ | File Integrity | √ |
| IP-Reputation | √ | Geo IP | √ |

| Network Level Security | | Network Infrastructure | |
|---|---|---|---|
| Firewalling | √ | High Availability Support* (HA) | √ |
| User Identity Awareness (UIA) | √ | Multiple WAN Connections | √ |
| User Authentication | √ | Server Load Balancing | √ |
| Single-Sign-On-Support | √ | WAN Load Balancing | √ |
| User-based Rules | √ | Traffic Management | √ |
| Scheduled Rules | √ | VLAN Support | √ |
| IPsec VPN | √ | Advanced Routing (Policy-Based, OSPF) | √ |
| SSL VPN | √ | Transparent and Routing Modes | √ |
| DoS and DDoS Protection | √ | DHCP Services | √ |

| Management | | Support and Maintenance | |
|---|---|---|---|
| Centralized Management | √ | 24/7 Support | √ |
| Web Management | √ | Unlimited Trouble-Tickets | √ |
| Command-Line Interface (CLI) | √ | Hardware Replacement | √ |
| Advanced Logging and Reporting | √ | Software Subscriptions | √ |
| Syslog- and Splunk-support | √ | Online License Center | √ |

* Optional service on Clavister E20.
Specifications are subject to change without notice.

CID: 9150-0040-24 (2017/04)

For a complete overview of the features included in the Clavister solutions please visit *www.clavister.com* or contact your local Clavister Representative directly.

clavister®
CONNECT . PROTECT

Clavister AB, Sjögatan 6 J, SE-891 60 Örnsköldsvik, Sweden
• **Phone:** +46 (0)660 29 92 00 • **Fax:** +46 (0)660 122 50 • **Web:** www.clavister.com