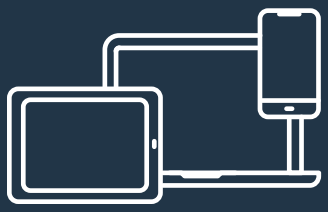
SECURITY



CLIENT COMPUTING

REFURBISMENT
TABLETS SERVICES
DESKTOPS **LAPTOPS** **CUSTOMIZATON**
SCREENS TEST ENVIRONMENT
PERIPIHALS **FREE UP CAPACITY**
INVENTORY **CHROMEBOOKS** SIMPLICITY
MANAGEMENT **FINANCING** WaaS TIME TO MARKET
ASSET RECOVERY **RE-USE** IMPROVE BUTTOM LINE
SCALABILITY DATA ERASE & SECURITY
IMPROVE CASH-FLOW

POWERED BY

dynabook FUJITSU

FLEXIBLE REMOTE ACCESS

EMPOWERING REMOTE WORKERS SECURELY

How we work has changed dramatically: we're now more mobile and global; we use BYOD, we access our workflow across complex and unsecured connections such as WiFi hotspots and other access points. Regardless of location or connection, an easy to manage and configure secure remote working solution is a key driver of organizational success and data protection. Nowadays a diverse number of different devices need to be supported.

SOLUTION

A flexible remote access solution supports a range of technologies including IPsec, SSL or L2TP enabling secure connectivity even in the most restricted remote environments. Compatibility with VPN clients with support for Windows, Mac and mobile operating systems allows all devices to get connected and purpose-built SSL VPN client provide easy of use for both the end user and IT administrator.

RESULT

Our technology providers remote access VPN solutions are quick to set-up on any and all of your devices without the need for IT administrators. You will have the confidence to know that all data is being shared confidentially and without malicious code inserted as it passes through your network. Our technology providers solution does this all without latency to allow your network (and employees) to perform at their best and works both in appliance and virtualized installations.

WEB CONTENT BLOCKING

RESTRICT ACCESS TO INNAPROPIATE CONTENT AND COMPLY WITH REGULATIONS

Specific locations on public networks, office policies on private networks, or general government regulations there may be many reasons on why certain type of web sites might have to be restricted.

SOLUTION

With a web content classification engine the URL and server hostname are in real-time matched to a database with content categories — then labelling the traffic flow with what kind of content it is. Policies in the engine can then take appropriate action or just log this information for statistical purposes. In this way administrators can easily restrict access to X-rated material or block social media sites during specific times in the day.

In addition the system can screen the traffic and block if malicious content is detected. The database is refreshed several times a day to ensure new sites are added continuously and secure accurate actions. In addition, for unencrypted traffic the Next Generation Firewall can screen the traffic and block if malicious content is detected.

RESULT

When implemented the results will not only avoid embarrassing situations but also help increase productivity to secure that business resources are used for the right purposes.

Created by: Claus Friberg Stensbjerg, Director of Business Transformation

PEDAB

SECURE NETWORK ZONES

NETWORK SEGMENTATION TO PROTECT COMPANY'S DIGITAL ACCESS

Employees expect to be able to bring their own devices (BYOD) to the office and connect them to the infrastructure. Often however these devices are not managed by the administrator and do not come with the same level of protection as corporate issued devices. This poses a risk towards internal systems from inside the secure perimeter.

"Only 3% of enterprises surveyed by Gartner have anti-malware protection on mobile Android devices and only 1% on iOS devices." - Gartner

SOLUTION

The solution is to segment your network into several zones and control the traffic allowed between them tightly. A complementary way is to setup an internal secure perimeter in front of the most critical business applications such as databases, file servers and collaboration servers.

RESULT

By protecting each of your digital assets with a virtualized dedicated firewall, you gain full control of the traffic even from inside your network. Due to our technology providers products small footprint, this takes very limited extra resources and can be run on the same virtualization infrastructure.

Created by: Claus Friberg Stensbjerg, Director of Business Transformation

THE IMPORTANCE OF BEING PROACTIVE

Advanced perimeter protection and secure connectivity between sites are the basis of a solid security infrastructure. But more often than not, users play an unintended key role in why cybercriminals anyway succeed in gaining access to the enterprises' digital assets and resources.

Multi factor authentication helps solve the problem of inferior passwords in a way that can also provide improved ease of use to connect to companies' systems. But for IT administrators, there is another key opportunity to help the user prevent from doing the wrong things by controlling access to safe applications and sites. Restricting malicious sites based on their global reputation and blocking dark-web, bitcoin mining and other specific applications reduces exposure to risks and secures that the company resources are used as intended. Controlling the traffic flows intimately can also provide an improved customer experience by differentiating real-time critical applications from background traffic and with that increasing the quality for web conferencing applications.

It's time to think pro-actively and implement preventative measures in order to avoid security incidents. Our technology providers provides the advanced technologies for preventative use-cases that does not require you to be an expert to implement and experience instant results.

Created by: Claus Friberg Stensbjerg, Director of Business Transformation

PEDAB