SpinnerTech

Network Security

Safe and Reliable Security

Be one step ahead of the next attack with our comprehensive plan to protect your infrastructure. Organizations face cyber threats every day, and with methods constantly changing, it's important to keep your networks up-to-date using resources and skills in the latest counter-measures. Utilizing multiple software, hardware and intricate methodologies, your network will be safeguarded against the most advanced attacks known today.

Proactive Safeguards

- Viruses, worms and Trojan horses
- Zero-day attacks
- Hacker attacks
- Denial of service attacks
- Ransomware, spyware and adware

SpinnerTech

> Traditional security products such as firewall and IPS cannot protect against distributed denial of service attacks.

Sophos UTM Gateways

There is no need to manage multiple security appliances to protect against every attack vectors: it's expensive and doesn't scale. We're familiar with Sophos' UTM line of products that provide all-in-one protection for email, wireless, web, network and web server. And, as the preferred solution for securing Amazon Web Services network infrastructure, we can set it up for your on-prem and/or cloud networks.

Cisco Gateways

Higher bandwidth IP-based wireless mobile networks such as 4G/LTE and 5G are exposing the corporate network to greater risk. Your data has the potential to be pulled down at any stage in transmission between the mobile device and Evolved Packet Core (EPC). We can configure your Cisco application to ensure that traffic is authenticated and encrypted from the eNodeB, providing end-to-end encryption and secure IPsec tunnels.

IPS/DDoS Systems

Traditional security products such as firewall and intrusion prevention system (IPS) cannot protect against distributed denial of service (DDoS) attacks. They are simply not designed to detect millions of legitimate packets sent in succession. There is an answer, however. We can setup a dedicated DDoS detection solution that will spot the attack and move it away from your network to a service, like Akamai, that has enough bandwidth and multiple locations around the web to handle the load.

Web Filtering

A good web filter as part of a proxy server and firewall solution is a great way to keep objectionable content out of your company. We'll set up the rules to screen incoming web pages and determine what, if anything, should be allowed through. We can also establish soft blocking procedures to issue warnings to users.

VLAN/Network Segmentation

The data center is protected from external threats by robust perimeter defenses that do little to protect against internal threats. Locally connected devices can access a flat network once authenticated. We break the network into a multiple layers to keep threats from reaching hardened systems. VLAN segmentation hinders access to systems, reduces packet-sniffing capabilities and restricts users to only see the devices necessary to perform their daily tasks.