SOPHOS

How to ensure a secure and productive remote workforce

The global spread of COVID-19 is rapidly changing the nature of work as we know it with many companies initiating voluntary or mandatory remote working to reduce the risk to their employees and business posed by this coronavirus.

To be productive, employees working from home will still need access to systems and applications on the office network, which can be easily and securely provisioned through the VPN capabilities of:

- Sophos XG Firewall
- Sophos SG UTM Firewall

To help you successfully enable the VPN capabilities in both these firewalls, here is the key information you will need:

Configuring the VPN

This is a straightforward process with easy to follow instructions. Please click on the appropriate link for your Sophos firewall:

- Sophos XG Firewall
- Sophos SG UTM Firewall

These video tutorials on YouTube are also useful:

- Sophos XG Firewall
- Sophos SG UTM Firewall

Capacity Planning

Having entire workforces remotely connecting to the office network at the same time will place additional loads on your infrastructure, including your Sophos firewall. The Sophos XG Firewall hardware appliances are purpose-built with the latest multi-core technology, generous RAM provisioning and solid-state storage. This provides leading performance with scalability. You can view the throughput statistics here.

To be confident that your Sophos firewalls have the capacity to do what is now being asked of them, please contact Sophos or your Sophos Partner to discuss your requirements in more detail.

Further measures to keep your employees productive and safe while working remotely

The correct configuration of your VPN via your firewall is the first step in keeping your employees working remotely in a secure environment. It’s also imperative that your anti-malware and threat protection is up to date to stay on top of the new range of threats that are emerging daily – many even using the COID-19/coronavirus theme as hook playing on the uncertainty of these unprecedented times.

We've pulled together some additional tips to keep your business safe:

- **Make sure your defenses are patched and up to date**
  Your VPN should be configured correctly, hardened and patched. Follow this easy to follow video to **Configure Secure Remote VPN** for **Sophos XG firewall.**

- **Enable an encrypted tunnel**
  An encrypted tunnel provides secure remote connectivity to any location connecting to the corporate network. This is beneficial for your small offices or temporary pop up locations connecting back to the main office, where experienced network security or IT staff are not on hand.

  Activate your **Sophos SD RED – (Remote Ethernet Device)** to connect to your **Sophos XG Firewall**. This video shows you how.

- **Activate SSL/TSL inspection for greater visibility**
  There has been an increase of phishing and malware leveraging the heightened COVID-19 situation. You can read about it here. Phishing attacks and links also use secure HTTPS connections as these hide payloads from firewalls and appear legitimate.

  Leverage the latest **XGv18 Xstream SSL Inspection,** which provides visibility into your encrypted traffic flows, support for TLS 1.3 without downgrading, powerful policy tools, and performance.

  Configuring SSL/TLS inspection is demonstrated in this video. Scanning and securing all email against spam, email borne malware and phishing attacks elevates protection further. See how here.

- **Keep servers and endpoints in all locations up to date**
  All servers and endpoints in all locations should be updated with the latest threat prevention. **Sophos Intercept X Endpoint & Server advanced** will enable you to protect your endpoint devices from malware, ransomware and other malicious threats. It will also allow you to use web filtering to protect remote workers from potentially malicious websites. See more here.

- **Don't go it alone - leverage the strength and expertise of the experts**
  Few organisations have the people, tools and processes in house to effectively manage fluid and dynamic scenarios, which reduces their ability to effectively manage cybersecurity 24x7 across all locations. Focusing on monitoring and notifying is not enough. **Managed Threat Response (MTR)** from Sophos allows for targeted actions on your behalf to neutralise threats, with actionable intelligence across your network. Read more about Sophos MTR here.