

**Deliverable 3 – Purchase Recommendations**

**Group - 2  
Members:**

**Bhargav Gosai (100902330)**

**Shweta Kestwal (100900888)**

**Priyanshu Shah (100897637)**

**Manjot Kaur (100896951)**

**Course: INFT1100  
Professor: Chris Whidden**

**Purchase recommendation 1: VPN service**

In the post-Covid era, where remote work and working from home have become an essential part of arguably every corporation, the importance of VPN servers has increased drastically in order to provide secure and reliable connections for remote workers. Just like any other organization, Contoso also provides the facility to work remotely after the COVID era, and we have kept that factor in mind while designing the network. But just providing remote access may lead to many security issues, such as unauthorized access and data breaches, as intruders might try to break into the network and act as a remote worker, which might not only result in financial loss but may also damage the company’s reputation. Which is why we have decided to implement a trustworthy VPN provider to filter and monitor traffic coming from remote workers.

* **Software recommendation:**

We did some research on which products would be a perfect fit for the company and narrowed down our list to two that might be a good fit for the company network.

1. **Cisco AnyConnect**

Cisco AnyConnect is a VPN solution developed by Cisco that allows secure network connections to remote workers. It offers numerous features such as multifactor authentication, split tunnelling, network access control, threat protection, web security, and endpoint security.

1. **Fortinet FortiClient**

FortiClient is a free endpoint security service that offers VPN connections, web filtering, antivirus, and a firewall. FortiClient’s VPN offers multiple features, such as multifactor authentication, split tunnelling, and endpoint compliance checking.

While both of the software packages seemed to be a perfect match for the company infrastructure, we had to pick only one of them as, despite having enough budget to implement both software in the network, it might not be ideal to have two VPNs in a single network as it might lead to confusion among employees, which can lead to many more complications in the company.

After comparing both software side by side, we came to the conclusion that Cisco AnyConnect would in fact be the most suitable choice for the company due to the various reasons listed below.

* **Compatibility:** Cisco AnyConnect supports a wider range of operating systems compared to Fortinet FortiClient. While FortiClient does support all the commonly used operating systems, it does not offer as many operating system compatibilities as AnyConnect. For example, AnyConnect supports Blackberry, Solaris, Chrome OS, and Windows Phone, whereas FortiClient does not.
* **User-Friendliness:** Both the competitors are user-friendly, but while testing them, our team found the AnyConnect interface to be cleaner and easier to understand. But as user experience is a subjective thing, we cannot judge on the basis of the experience an individual user had. So, we also focused on different factors such as customization options, user guides, and tutorials, which give AnyConnect a slight edge over FortiClient.
* **Security:** Both software offers similar standards of security, which makes it harder to pick one over the other. To come to a conclusion, our team considered the implementation of this software as a factor of security, as almost all the security features are similar, but the functions of these features may vary according to how they are put to use. Having a lot of security features but not having a compatible way to put them to use might make them less effective. which brought us to our previous point of user friendliness. As the features are almost identical, the functions and implementation of these features are comparatively easier to understand and use in AnyConnect due to its user-friendly environment.
* **Additional features**: While there are a lot of similarities in both VPNs, there are some additional features that makes Cisco AnyConnect slightly superior to FortiClient. One biggest additional feature being allowing third party VPNs, AnyConnect allows third party VPNs which can allow the company to have multiple VPN providers at the same time.
* **Changes Required:**

Certain changes will be required in the company environment and network.

1. **Traffic flow:** VPN tends to increase the traffic flow in the network; we will have to make sure that the network can sustain this increase in traffic. If not, changes in the network will be required.
2. **Training and awareness:** The company will be required to provide training programs to employees to make sure the software is utilized correctly.
3. **Management: The** company should provide a dedicated management team to manage and monitor the VPN traffic and troubleshoot.

* **Negative Impact:**

There are a lot of benefits of using VPN for remote workers and it is ideal to use it so, but the one major downside of using VPN is increased traffic flow which might slow down the network’s performance and negatively impacts employee’s productivity and efficiency. as Contoso is expected to grow rapidly in next 16 months, the traffic flow will only increase rapidly and VPN will add more to it, this might slow down the network.

**Purchase Recommendation 2: Firewall Upgradation**

In the current period, businesses are experiencing more stress to strengthen their level of security due to the growing number of cyber threats, including malware, ransomware, and phishing attacks. Each and every type of safety architecture must have firewalls, and upgrading these firewalls can improve security from threats. In addition to secure confidential data and restricting cyber-attack, firewalls provide support in blocking unauthorized access to a company's system by filtering the traffic on the network. Sometimes it is impossible to identify the breach, which results in loss of sensitive data, financial loss, and damage to the company’s reputation. Thus, we made some improvements to the firewall by including certain advanced technologies like an intrusion prevention system and an intrusion detection system. This will help the company identify the threat, block the unnecessary traffic on the network, and secure it from malicious attack.

**Software recommendation:**

We conducted some research to see which product would be the ideal fit for the business and reduced our choice to two programs that would be suitable for the company network.

1. **CISCO ASA Firewall**

The Cisco ASA firewall is a network security device that provides firewall functionality with various security features such as intrusion prevention using signature-based and behaviour-based analysis, inspection of traffic flowing through the network, and access control.

1. **PF Sense Firewall**

PF Sense is an open-source firewall software. One advantage of the PF Sense firewall is that it can be modified to fit the organization according to its needs. It identifies and blocks or allows traffic based on IP addresses, protocols, and applications.

After analysing both Cisco ASA and PF Sense and having a deep discussion with the staff, we came to the conclusion that Cisco ASA would be ideal for the business. Though it is very expensive, Contoso is a large organization. It needs high-level support and advanced features. As with Cisco ASA, it would be beneficial for Contoso to have a tested and popular intrusion prevention system in their organization to get rid of future cybercrimes and malware attacks. The reason for selecting Cisco ASA is mentioned below:

* + **Security Features:** As we all know that CISCO ASA give more features like advanced threat detection, advanced access control policies, next generation firewall. This all features protects network from phishing, malware attacks, etc. whereas on the other side PF sense also provides advanced security features like threat detection but it is not as strong as CISCO ASA because installing new security features using CISCO ASA needs additional hardware or software license but PF sense is opensource and free to everyone.
  + **Scalability:** CISCO ASA is highly customizable and used for large organization as it provides multiple interfaces and higher bandwidth because it works on command line interface and it needs high level of understanding to operate it. On the other hand, PF sense is also scalable but it will not be able to handle the larger traffic because it is user-friendly and it is a web interface it can be easily configured and that will give advantage to the attacker to attack the system. For instance, Contoso is a large organization and is planning to expand and adding new 700 employees and also planning to open new branch so CISCO ASA is the best option rather than PF Sense.
  + **Integration:** CISCO ASA can easily integrate with other cisco products such as routers, switches and other security devices while it would be quite difficult for PF sense to integrate with the CISCO products. CISCO products can work easily with each other and are easy to maintain.
  + **Cost:** PF sense is free and open source used by anyone while CISCO ASA is expensive and needs license but benefit of CISCO ASA is it provides advanced security features, scalability, support and easy integration with other CISCO products.
* **Changes Required:**

Certain changes will be required in the company environment and network.

1. **The implementation of additional security technologies Upgrading the** firewall affects the data loss prevention techniques. So, we will have to plan for the changes that need to be made, and they should be compatible with the new firewall and enable new functions.
2. **Impact on Customers:** Upgrades to the firewall may have an effect on customers depending on the business's operations. The company should provide clients with alternate access methods and let them know in advance about any expected difficulties.
3. **Training Employees:** We should provide proper training to the IT staff and end users to make sure that they get completely used to the new functionalities and features of the upgraded firewall and also get used to the new policies and procedures.
4. **Network Topology:** When we upgrade the firewall, we have to change the configurations of the routers or add or remove network segments.

* **Negative impact:**

Even though firewall upgrades are beneficial for systems, upgrading a firewall might require additional education for IT personnel or end users in order to understand its new functions and features. These alteration procedures may take longer and cost more as a result. Company operations may be disrupted if a firewall upgrade requires leaving the system offline for a while.