ASSESS AND DESIGN FOR SECURITY

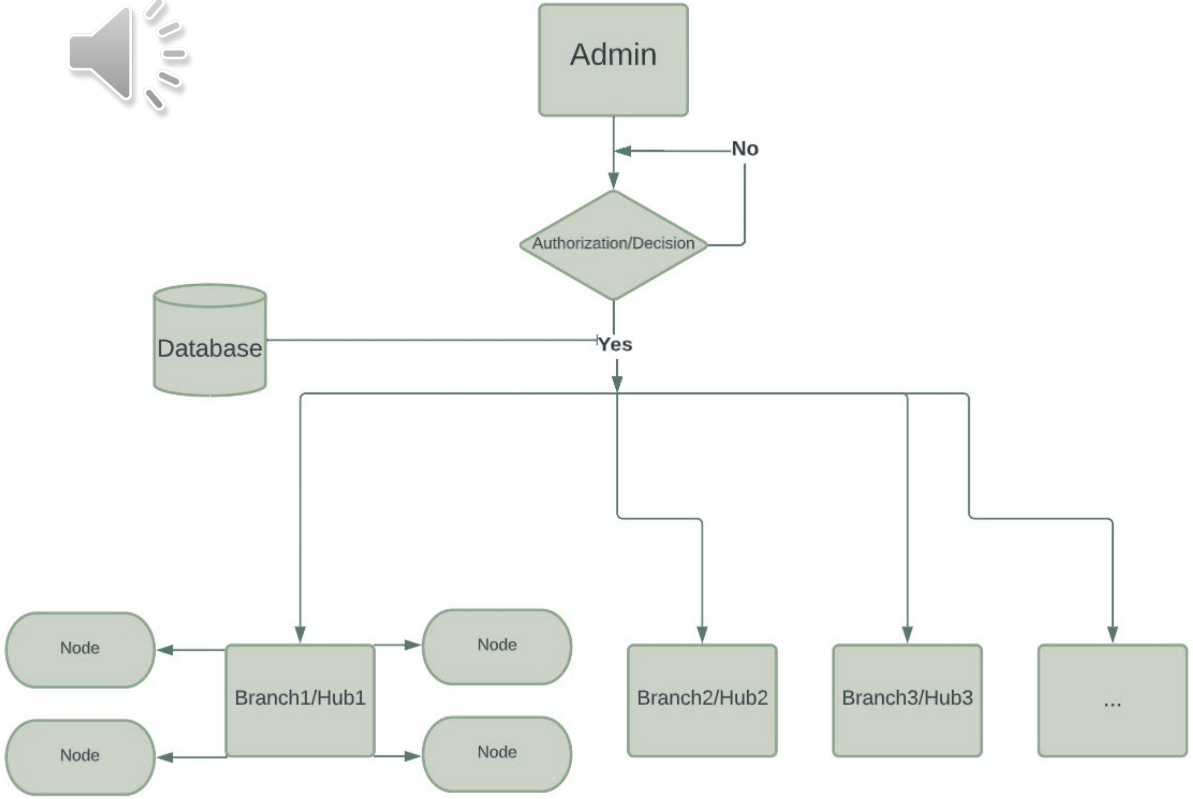
YIQIAO YIN | PHD CANDIDATE | HTTPS://WWW.YIQIAO-YIN.COM | HTTPS://WWW.YOUTUBE.COM/YIQIAOYIN

MOTIVATION AND CHALLENGE

The ensuring of network security is not always trivial. The process of implementing such a design to assist the CIO of a corporation is usually not that simple. Many scholars have investigated the possibility of "cloud first" policies (Alotaibi et. al. (2018), Cleveland (2005), Jaramillo et. al. (2013), Køien (2020), Seneviratne (2018), Stawowski (2018)).

Before we get started, let us recall the premise of this assignment:

- We are designing a network for a corporation that spans the entire northeastern region of the United States.
- The corporation will expand to 150 branches and will require WAN to provide secure internet connection.
- Previous assignments have proposed the right diagram for network topology.

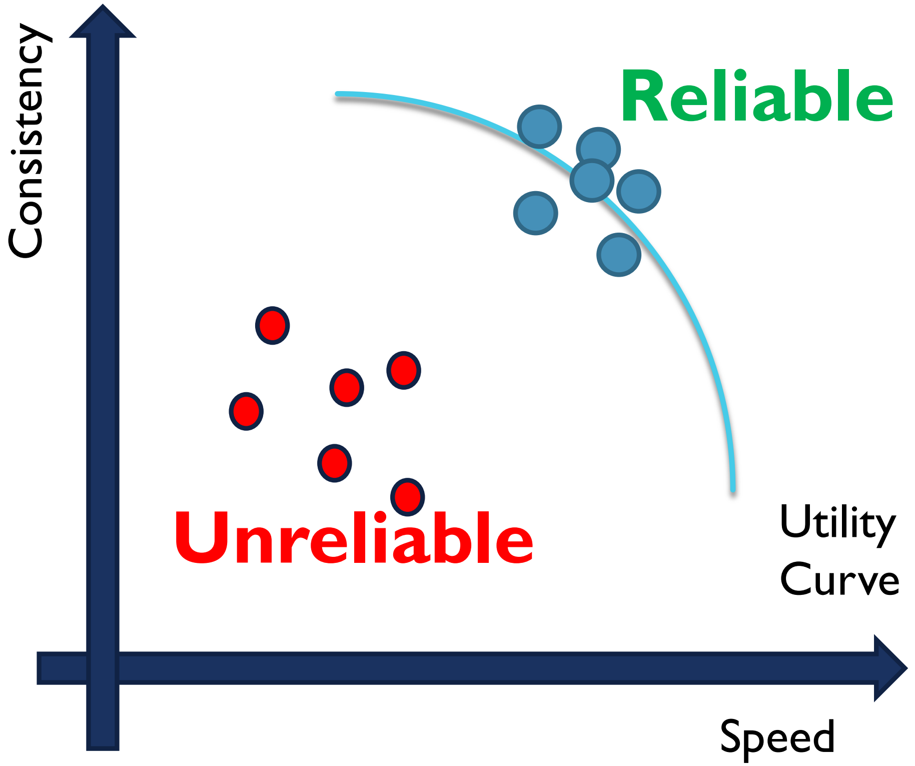


BRING YOUR OWN DEVICE (BYOD)

The guidance from the CIO is to provide critical solutions to the challenges when employees bring their own devices to work. Due to network safety and security, the company asks for segregation of employee-owned devices. This means the employee devices may not be allowed to access secured sites and may be registered as company blacklist. This is especially true when the employees desire to use a more "personalized" software space to do their work.

To tackle this problem, the CEO proposed the "Cloud First" policy.

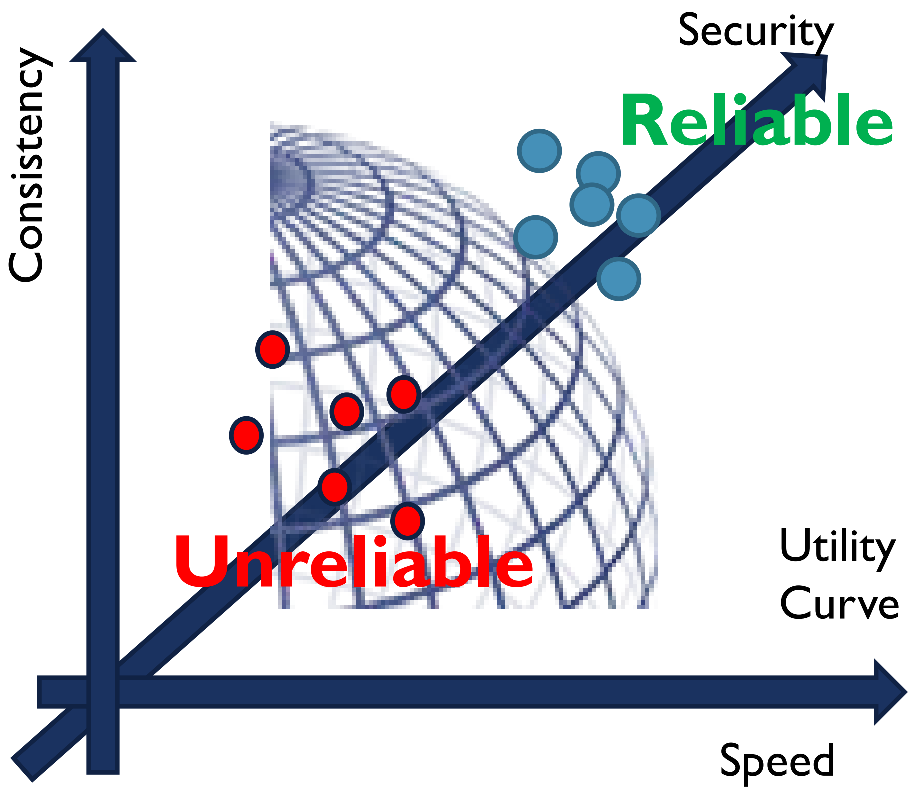
NETWORK CONNECTION RELIABILITY



In previous assignments, we have proposed this diagram as the main checkpoint to ensure optimality when designing new network. The proposal of the "cloud first" structure is no exception at all. We aim to design network connection that are both fast and consistent at the same time. In addition, the data transfer should not use "safety" as a compromise.

Image source: https://sites.google.com/site/itclasswebsite/home/it-systems/hardware-and-networks/networks

BRING YOUR OWN DEVICE (BYOD)



In previous assignments, we have proposed this diagram as the main checkpoint to ensure optimality when designing new network. The proposal of the "cloud first" structure is no exception at all. We aim to design network connection that are both fast and consistent at the same time. In addition, the data transfer should not use "safety" as a compromise.

A third-party software provider with virtual private networks (VPN) using encrypted path is an ideal solution.

In other words, we need implement a third axis, i.e. security. Based on this information, the utility curve became the utility surface and the dots scattered outside of the utility surface is the reliable samples.

Image source: https://sites.google.com/site/itclasswebsite/home/it-systems/hardware-and-networks/networks

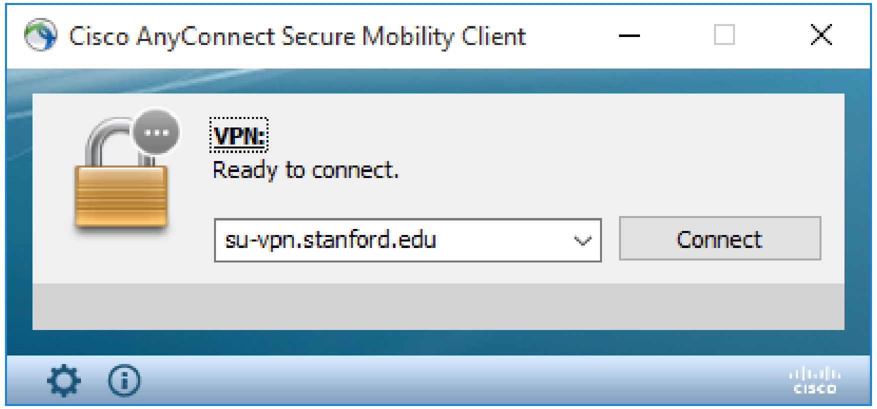
VIRTUAL PRIVATE NETWORK

The proposal is to use a third-party network encryption provider called Cisco AnyConnect. This assignment proposes the company offers Virtual Private Network to connect users with their account and ID numbers using the Cisco AnyConnect Secure Mobile Client. It is a mobile app that can be downloaded on a cell phone that relates to an individual phone number.

VIRTUAL PRIVATE NETWORK

The proposal is to use a third-party network encryption provider called Cisco AnyConnect. This assignment proposes the company offers Virtual Private Network to connect users with their account and ID numbers using the Cisco AnyConnect Secure Mobile Client. It is a mobile app that can be downloaded on a cell phone that relates to an individual phone number.

The setup of the proposed solution, Cisco AnyConnect Mobile Client, is easy to use. The user machine will be installed with this application. The mobile devices for each user can install this app called Cisco AnyConnect. Using the app, a user can login to the VPN which then can access company private network data.



Cisco AnyConnect Secure Mobility Client

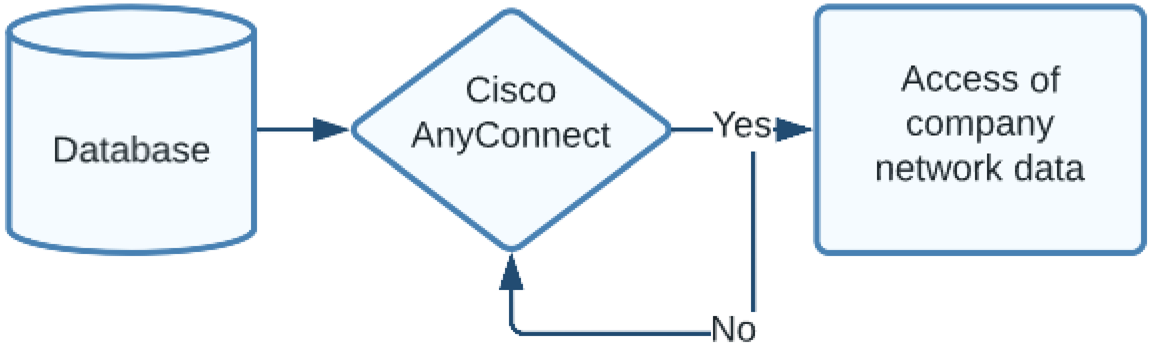
VPN:
Ready to connect.

su-vpn.stanford.edu

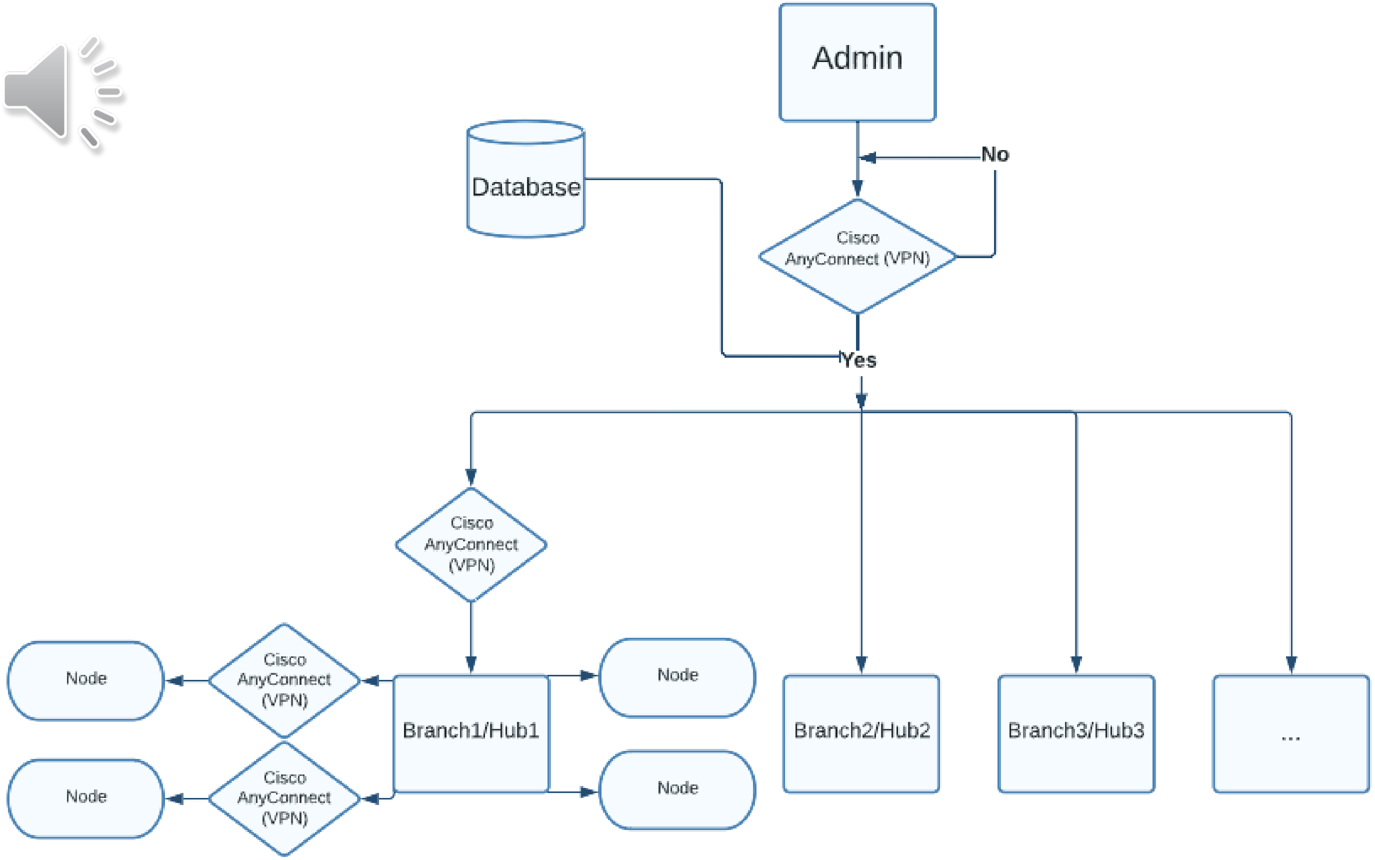
VIRTUAL PRIVATE NETWORK

The implementation is to set up a Cisco AnyConnect Client for each personal device. The company's database provider will require the access of Cisco AnyConnect to be approved with a secured password to be able to have access of the company's network data.

The password is required to be changed on a quarterly basis and cannot be allowed to have repeated password.



UPDATED CHANGES IN NETWORK TOPOLOGY

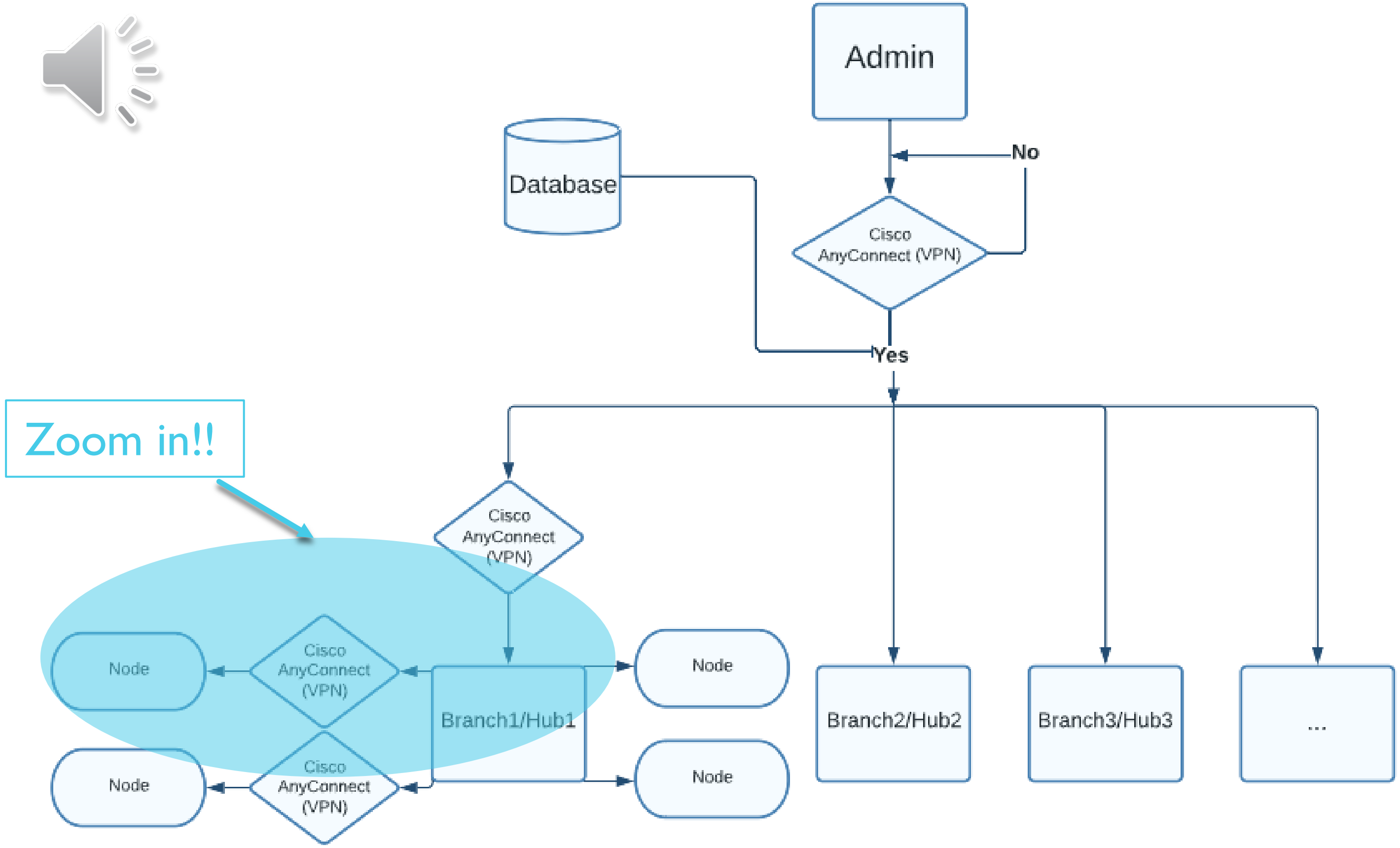


Upon the implementation of the Cisco AnyConnect Mobile Client, the network topology that was proposed from the previous assignments should also be updated.

The hierarchical topology will need to have Cisco AnyConnect initiated at each branch. This means the main branch on top, the branch/hub in the middle, and all the sub-nodes in the end.

Each of the branch/sub-branches will be equipped with Cisco AnyConnect.

UPDATED CHANGES IN NETWORK TOPOLOGY



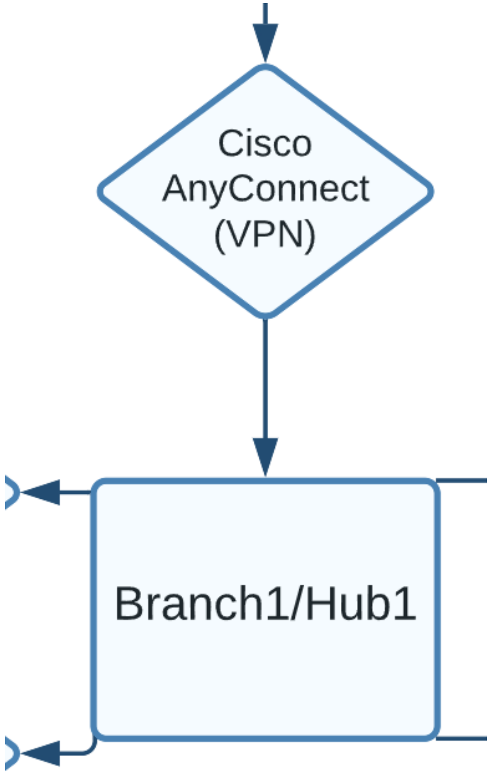
Zoom in!!

Upon the implementation of the Cisco AnyConnect Mobile Client, the network topology that was proposed from the previous assignments should also be updated.

The hierarchical topology will need to have Cisco AnyConnect initiated at each branch. This means the main branch on top, the branch/hub in the middle, and all the sub-nodes in the end.

Each of the branch/sub-branches will be equipped with Cisco AnyConnect.

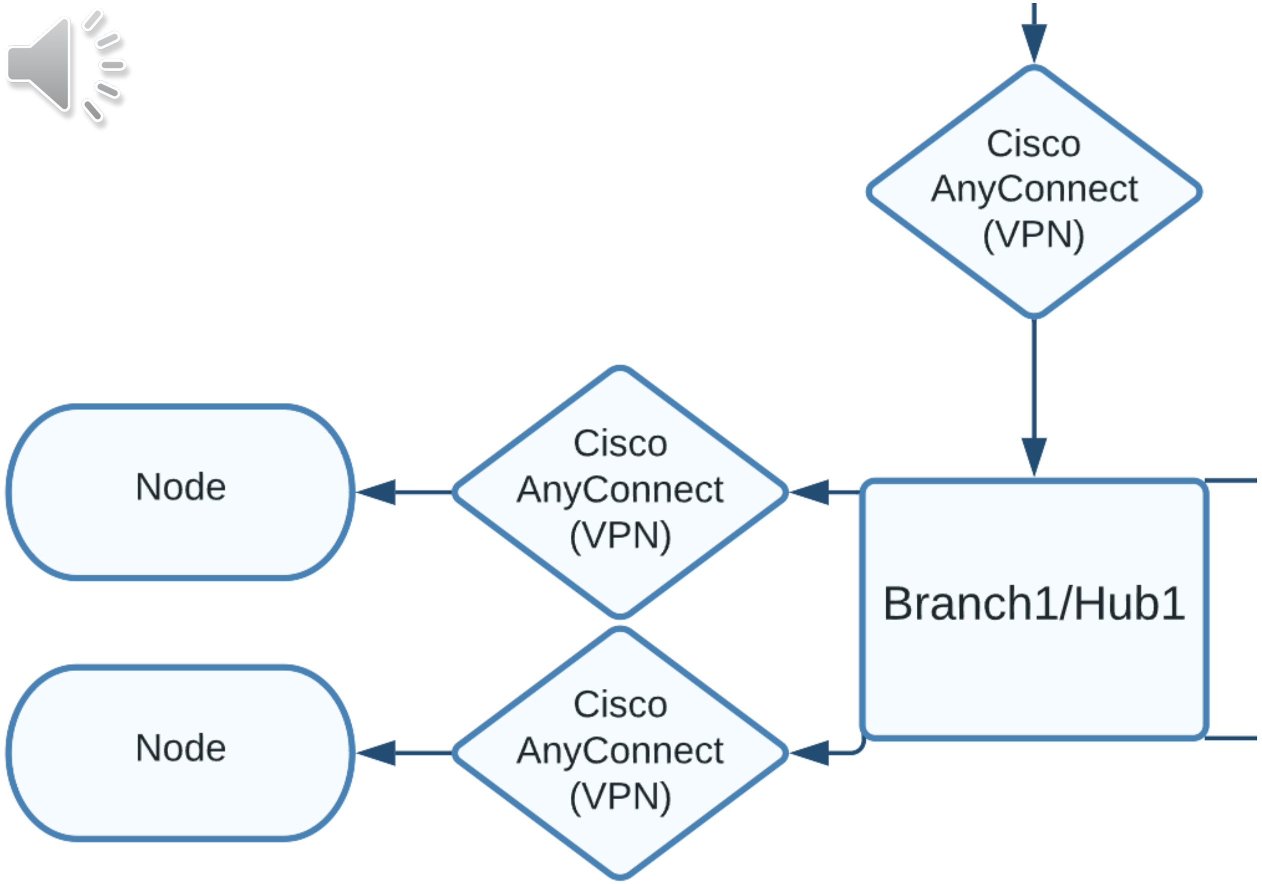
UPDATED CHANGES IN NETWORK TOPOLOGY



Let us use one branch as an example to further explain the architecture of this new implementation. For example, there could be a Branch1/Hub1 from the central hierarchical.

This branch/hub will need to be approved with Cisco AnyConnect to have data accessed at the branch level.

UPDATED CHANGES IN NETWORK TOPOLOGY



Let us use one branch as an example to further explain the architecture of this new implementation. For example, there could be a Branch1/Hub1 from the central hierarchical.

This branch/hub will need to be approved with Cisco AnyConnect to have data accessed at the branch level.

Then each employee may ask for Cisco AnyConnect for permission to log in to the branch's private network. Upon approval of this request, the employee may have access of the branch-level data. We used 2 nodes as an example, but, there can be multiple nodes in the endpoint.

References:

Alotaibi, B., & Almagwashi, H. (2018, April). A review of BYOD security challenges, solutions and policy best practices. In *2018 1st International Conference on Computer Applications & Information Security (ICCAIS)* (pp. 1-6). IEEE.

Cleveland, F. (2005, October). IEC TC57 security standards for the power system's information infrastructure–beyond simple encryption. In *Transmission and Distribution Conference and Exhibition* (Vol. 2006, pp. 1079-1087).

Jaramillo, D., Katz, N., Bodin, B., Tworek, W., Smart, R., & Cook, T. (2013). Cooperative solutions for bring your own device (BYOD). *IBM journal of research and development*, *57*(6), 5-1.

Køien, G. M. (2020). A philosophy of security architecture design. *Wireless Personal Communications*, *113*(3), 1615-1639.

Meersman, M. W. (2019). *Developing a Cloud Computing Risk Assessment Instrument for Small to Medium Sized Enterprises: A Qualitative Case Study Using a Delphi Technique* (Doctoral dissertation, Northcentral University).

Seneviratne, B. L. D., & Senaratne, S. A. (2018, December). Integrated Corporate Network Service Architecture for Bring Your Own Device (BYOD) Policy. In *2018 3rd International Conference on Information Technology Research (ICITR)* (pp. 1-6). IEEE.

Stawowski, M. (2018). Dilemmas of a security architect: How to protect critical systems without disrupting continuity of their services. *ISSA Journal*, *16*(3), 34-42.