Is you are in the right timeline.

Business, Accounting

Is your network AccessSecure? We live in a connected world that has embraced digitaltechnology enabled services and is like a small village.

We are alwaysconnected; checking our devices for a status update, or we are the ones postingan update or we are trying to send that status report or close a business dealonline. Our access to the internet as increased tenfold from theprevious years with many more plugging in to the World Wide Web every second, we like to call ourselves the . com generation or if you fancy the title" millennial" you are in the right timeline. But with such exposure, sometimes we just tend to forget thedangers lurking behind our use of the internet.

A few of us try to at leastensure we are using a secure connection. But many ignore it all and end-up in areally bad fix. Take for example the year 2017 as we knew it, every ITsecurity professional will tell you that it was a terrible year in the networksecurity home front especially in the malware category with Wannacry wreakinghavoc on company networks in a spat of ransomware attacks that led to losses inmillions of dollars. Such occurrences are a network security professional's worstnightmare. According to Forbes. com, as cyberattacks increase in frequency and sophistication, by the year 2020, the global security market is expected to be worth more $170billion, and is currently suffering from a dire skilled network security professional'sshortage. In many cases of cyber-attacks taking place, attackers can compromisean organization within minutes. The proportion of breaches discovered withindays always falls below that of time to resolve them and fix the threats.

The enterprise network today has rapidly changed, especiallyconcerning employee mobility and access to network facilities. Today’s employeesare not tied down to desktops and office desks, but alternatively are able to accessthe companies’ resources through a variety of devices such as smartphones, phablets, and personal laptops. The current norm is for a company’s employees to be able toaccess the companies resources from anywhere, this greatly increasesproductivity, but also exposes the company to the possibility of leakages inhighly confidential company data and increased cybersecurity threats, due tothe fact that you may not be able to track and control the security configurationof devices accessing the network from outside of the brick and mortar office setup. Controlling all the devices accessing the network is a great task in itself, which grows every day and is becoming more untenable as more devices getconnected and plugged into the company network. So, what can we do toget out of this fix? Fret not yourself, using a well configured identity serviceengine such as the Cisco ISE would greatly alleviate this challenges.

Accordingto CISCO, the CiscoIdentity Services Engine (ISE) 2. 0 is an identity-based network access controland policy enforcement system. It helps you take care of the time-intensiveday-to-day network administration tasks, allowing your IT staff to focus onother crucial tasks like keeping abreast with the current cyber threats and howto counteract them. According to CiscoISE product release notes, ISE will attach an identity to a device based ona user, function, or other character that allows it to do policy enforcementand security guidelines compliance before it is authorized to access thenetwork resources. Based on the results from different factors, a

device can beallowed access to the network based on specific set of access policies appliedto the interface it is connected to, or it can be explicitly denied or givenguest access privileges based on the specific company guidelines.

Cisco ISE is a context aware policy service, and it aims to control access and threats across wired, wireless and VPNnetworks. Security considerations The ISE platform inbriefFigure 1. 0 The ISE Platform ina nutshell – figure 1. 0 The ISE platform comes with a distributed deployment approachwith nodes handling three different roles: the Policy Administration Node(PAN), the Monitoring and Troubleshooting Node (MnT), and the Policy ServicesNode (PSN).

For ISE to function properly, all profiles are required. Let us briefly review each of this profiles and serviceentry points: Policy AdministrationNode (PAN)The PAN profile is the screen the administrator will loginto so they can configure policies to drive the ISE setup and configuration. It acts as the main control entry point for configuring and deploying the ISE. PANallows the admin to configure the ISE topology by making changes, with thischanges being send out from the administrator node to the Policy Services Node(PSN) in ISE.

Policy Services Node(PSN)The PSN profile allows for policy decisions to be made. Thenodes here allows the network service enforcement devices to send all networkmessaging. After processing the messages, the PSN will then give or deny accessto the network based on what was configured in PAN by the administrator. Monitoring andTroubleshooting Node (MnT)The MnT profile

will log all service reports, occurrencesand give you the access to generate reports as needed. All the logs will bereceived by MnT from other nodes in the ISE topology and sorted through, and compiledin a readable configuration for you. It gives you the ability to generate variousinformative and graphical reports that can aid you and the senior managementmake strategic decisions regarding your companies' network resources, as wellas notify you of any threats to ISE. Fundamentally, the CiscoISE offers a more holistic approach to network access security andprovides:? Accurate identification of everyuser and device.

? Easy onboarding and provisioningof all devices.? Centralized, context-aware policymanagement to control user access – whoever, wherever, and from whatever device.? Deeper contextual data aboutconnected users and devices to more rapidly identify, mitigate, and remediate threats. Security and PostureThe Cybersecurity landscape is changing very first andbecoming more complex and costly for organizations running legacy traditionalsecurity setups.

The cybersecurity demands have largely increased but thesecurity resources tend to remain the same. This increases the potential attacksurface greatly meaning the legacy security systems with a company's premisehas little to offer in terms of relevance and robustness to handle currentthreats. Employing the correct solution has become paramount and ashift from on premise, traditional security setups is inevitable with manyorganizations currently seeking to deploy a solution that will protect thecompany from within and without. Such solutions like the Cisco ISE have someinteresting

features that are likely to help organizations meet their securityneeds. According to the cisco ISEadministrator security guide , this are some of the security features thatcan be found within ISE: TACACS+ Device AdministrationCisco ISE supports device administration using the TerminalAccess Controller Access-Control System (TACACS+) security protocol to controland audit the configuration of network devices.

Devices are configured to queryISE for authentication and authorization of device user actions, and sendaccounting messages for ISE to log the actions. It offers granular control of who can access network devicesand change associated network configurations. An administrator can createpolicy sets that allow TACACS+ results, such as command sets and shellprofiles, to be selected in authorization policy rules in a deviceadministration access. The ISE Monitoring node provides enhanced reportsrelated to device administration. The Work Center menu will have all the deviceadministration pages, which is the single start point for ISE administratorswishing to configure the system. A Device Administration license is required inorder to use TACACS+.

Endpoints IdentitypageIt might look like seemingly irrelevant or less importantpage, as the single most frequently viewed page in of the ISE, it presented thegreatest pains in usability in previous versions of ISE. It has been revampedin ISE 2. 0, and in a great way. Useful functionalities have been appended to thepie charts at the top.

On clicking a pie chart slice, you will automatically beable to filter the table below it. The table itself is completely re-writtenand will take you to your last

selection since you clicked into an endpoint fordetails, as you go back to the table. Navigation FrameworkAs ISE is a complex system with great power to boot, you normallywould not expect it to come with a User Interface that is contained within onlya few pages. Most often a solution like this needs to have a menu system, andmany levels of navigation. It can be expected that ISE will certainly be afflictedwith a lot of navigation. However, ISE 2.

0 rips out the entire navigationalframework and replaces it with one that is modern and lightning fast. It’sobviously the start of a complete UI overhaul. The first time you log into ISE2. 0, you immediately see the difference with prominent menus and sidenavigation. Upgrade WizardThe upgrade process is usually a complex procedure in anylarge distributed system in any technological setup. Many solutions do awaywith the upgrade option all together and instead they require you to reinstalland restore the configuration from backup. ISE has always supported upgrade andhas made significant improvements with each release. ISE 2.

0 adds a newWizard-based GUI to handle the upgrades for you in an orderly manner. You canspecify which repository each node in the deployment should use, pre-stage theupgrade files, and control the order in which each node is upgraded. All withinthe GUI. Support TunnelsSupport tunnels have been added to ISE 2.

0. This feature allowsthe administrator to enable a secure tunnel for Cisco’s TAC to remotely accessthe appliance’s root operating system. Well, that’s to put it simply. This isfantastic tool, because it implies fewer WebEx sessions with Cisco TAC remotelyseeing the UI of a user’s ISE deployment – they can

see it directly if and onlyif the customer has enabled the support tunnel & provided the TAC engineerwith a unique access key needed to activate and authenticate the access. Stacking of CommandSetsISE 2. 0 allows for multiple command sets to be sent inresponse to an authorization request from any of the nodes.

This is done in a Brilliantway and it will allow command stacking, a permit statement shall alwaysoutweigh a deny statement – unless it is an explicit “ deny_always” statement. Network DeviceProfilesNetwork Device Profiles are completely brilliant and providesomething that many look for in ISE since the very beginning, the ability tocustomize the settings for network devices, including how it should handleChange of Authorizations, URL-Redirections and more. The implementation of NADprofiles gives a way to import and export so they can be shared. ISE 2. 0 comeswith an array of pre-built profiles for many network devices. Native EAP-TTLSSupportEAP-TTLS is a tunneled EAP protocol that is fairly popularwith universities that use eduroam applications. Certificate ProviderIn ISE 1.

3 the built-in Certificate Authority for bring yourown device (BYOD) endpoint certificates was added. It would help createendpoint certificates for devices that underwent the Cisco BYOD on-boardingprocess only. In ISE 1. 4 an API was added to aid and allow the creation ofpriv/pub certificate key-pairs that could be imported into devices that couldn’tgo through BYOD flows.

Now ISE 2. 0 there is a better, fully-blown customizableportal that allows the creation of individual certificate key-pairs, submittingand signing Certificate Signing Requests (CSRs), or even the bulk creation ofcertificates. This is a

gem for every network administrator out there. Kicking Endpoints offthe Network when Certificate is revokedISE issues a certificate to a device endpoint, and thatcertificate was revoked, it would naturally be denied access at the nextauthentication. However the endpoint would remain on the network. ISE 2. 0 hasimproved the process and adds ability to completely disconnect any endpointwith an active session whose certificate has been revoked, thereby immediatelykicking them off the network and reducing the clatter of endpoints you do notneed. Benefits of Using anIdentity Services EngineAccording to the research conducted by Forresteron having an Identity services Engine solution such as Cisco ISE deployedwithin an organization, it was found that an organization is likely to expectthe following benefits: Reduced infrastructure management and support costs for yourguest wireless access services.

Reduced infrastructure management and support costs for BYODsupportReduced help desk support costsReduced risk of security issues and major outbreaks. Reduce or eliminate IT management costs related to guestwireless access. Reduced OpEx/CapExdue to selection of the right solutionThe cost of securing an organizations IT infrastructure cango into billions of dollars. It is the intent of every organization to have themost robust and up to date security setup. With cloud security services, manyorganizations are moving from spending on their own premise security (CapEx) setupto a cloud solution which will only require operational expenditure (OpEx) andenjoys the facility of regular updates. The security products deployed within an organization willusually be funded out of the capital expenditure (CapEx) budget. The cost ofsuch hardware and software

(for example buying a full security setup at $ 200, 000)will require an upfront payment of the total amount amortized according to theaccounting cycle, in order for the organization to enjoy those services.

In contrast, if an organization chooses to employ a cloud solution (for example costing$100, 000 annually), which usually comes at a reduced price annually, and is fundedout of the operating expense budget (OpEx), it has an advantage. In accounting terms, it is more costly to take the first option(CapEx) as compared to the second option (OpEx). In this two options, the cloudservices make a better option for the employment of the organizations cash, since unlike the static hardware option that will require future replacementand another cash outlay of $200, 000, the cloud service enjoys a continualupdate with the latest technology and at a cheaper price for the organization. The question then arises, are their ways an organization canstill do an on premise cybersecurity solution deployment and enjoy a morerobust service? According to a research conducted by Forrester, regardingthe deployment of an onpremise Identity service engine such as the Cisco ISE within anorganization, a composite organization can incur risk adjusted costs, totalingabout $595, 000 in one-time, initial investment and implementation costs, plus$61, 00 administration and maintenance costs per year.

This costs relate to a deploymentof the Cisco ISE solution. Having an ISE solution on premise will help you greatlyreduce the OpEx for the organization by cutting down on help desk supportcosts, close major security holes avoiding major data breaches, and reduce ortotally eliminate IT

management costs associated with guest wireless accessamong others. ConclusionThis are just but a few of the many economic and securitybenefits to be derived from the use of Identity service engines such as CiscoISE 2.

0 in your organization. And according to a research carried out byForrester, CostSavings and Business Benefits Enabled by ISE, there is a huge incentive foryour organization to deploy an Identity service engine configuration and stayabreast of the cybersecurity needs of the modern digital organization.