Fast Lane
Consulting and Education Services Inc.

Enterprise Edge Security with Cisco ISE

May 2016

Background

Threats have never been more relevant than they are today. Nation states, adversaries, corporate and government espionage, hackers, disgruntled employees, Script Kiddies, Data Miners, etc. are all on the hunt for valuable information. The information they seek includes enterprise and individual details. Networks are only as secure as their weakest components. With the hyper-growth in connected devices including smart phones, tablets, wearables and Internet of Things (IoT) devices, networks have never been more vulnerable. Network professionals today must strike a balance between user's convenience, productivity and enterprise security.

Table of Contents

Chris Avants

White Paper

Introduction

When someone thinks of connecting their break room Smart TV to the Internet to watch Netflix, they don't think of it as a typical network device, and therefore not a high risk. In reality, hackers see these new devices as an easy target, typically designed with custom vendor OS, plug-n-play features enabled by default, software which is rarely updated and have weak security at best. If any device allows connectivity to the network/internet, there is a potential it could be compromised. This is especially true for consumer level devices like Smart TVs which were never designed for the Enterprise.

Even without the rise of IoT, enterprises are challenged with other megatrends like offering BYOD and Secure Guest Access services. These are excellent value-adds to employees and customers, but must be carefully planned and executed to mitigate potential vulnerabilities.

One problem with Enterprise Security is the requirement for a trust hierarchy which extends from Executives to Management through to employees. Standard network security policies assign levels of trust to each group within the enterprise. When a user is identified as belonging to one of these groups, they inherit the appropriate level of trust. For example, a Sales Manager would have network credentials that are assigned to all Sales Managers. As long as she uses these credentials, she inherits the trust assigned to the group when authenticating to the network. This typically translates into access to corporate resources that are deemed appropriate for that role in the organization and usually to any other organizational levels below. This type of mentality was okay when companies provided a single desktop or laptop which was 100% managed by Enterprise security software and simply prohibited any other device. But what happens when employees use their same credentials to connect their personal laptop, tablet, Smartphone, iWatch, etc.? The user can be trusted, but can the device? Without the technology to further identify and classify users and their devices, companies will continue to add network vulnerabilities.

The Basics of Securing the Network

Since the early days of Windows XP, NT 4.0 and even before, many network administrators have relied on Windows security to protect a company's digital assets. By implementing what is now known as Active Directory, users had to authenticate before being allowed access to their workstations or laptops or any shared network resource managed by AD. Windows and AD are used by the majority of enterprises for these services and offer administrators a simple GUI interface to manage these domain services. However, all of the security rights, permissions and resources AD provides is handled by the application. The ultimate problem with all security handled at the application level is that there are layers below in the process of network communication. Therefore, when a system compromises any of the layers below, the entirety could easily be compromised.

Lower Layer Threats

The first rule of any IT Security policy should always be protecting physical access to the network and network equipment. If an unauthorized user gets access to network equipment, it takes no time at all to gain full access to those devices thanks to password recovery features or small payloads delivered to the devices from a USB or any other physical access medium. In large enterprises, someone may not bother compromising a network device like your 25K firewall. With physical access they may simply leave a new network device in a secured area that could do a host of nefarious things even after the person is long gone. We are all familiar with the term “wiretap” where someone could eavesdrop on your phone calls without either party knowing. Now imagine the same concept but “listening” to all networked data. If a person was able to hack your network, they don’t just hear a single phone call, they “hear” everything transmitted through that network. This may include voice and video calls, as well as data traffic. The point is you’re now compromised. Again, if a hacker is able to compromise a lower layer, he can now elevate access to the other layers. And these tools and devices are more relevant and popular than ever before. For example, take a look at Hak5’s LAN Turtle, USB Rubber Ducky, or any number of micro computing devices built on a Raspberry PI. As you can see from Figure 1, these are small devices, not easily discernible from devices companies use every day. All an unauthorized user needs is physical access to unprotected network equipment or devices to cause great loss or damage.

Figure 1: SMALL ATTACK TOOLS Raspberry PI 2 | LAN Turtle | USB Rubber Ducky

The second part of any network security policy should be protecting access to the network itself. Let’s review the simple branch office topology shown in Figure 2. What do you think would happen if someone plugged in a private computer or other network device to the switch? If we were to plug another device in, including a switch, AP or client server operating systems have no way to inherently identify these devices. The point we have to realize and appreciate is that mainline Client/Server applications, like Windows Active Directory, are not natively network aware and have no way of securing the lower layers on their own. Securing access to the network requires the ability to identify and authenticate users and devices, starting with the physical connection itself before ever receiving an IP address. This requires a framework of devices and protocols commonly referred to as 802.1X.

802.1X

802.1X is a framework of devices and protocols which provides enterprise Authentication, Authorization and Accounting services collectively referred to as AAA or (triple A). There are three pillars of 802.1X, the Authentication Server, the Authentication Edge and the 802.1x Supplicant software (running on the client). The authentication edge is typically a switch on the wired LAN or Wireless LAN (WLAN) Controller. These devices essentially separate your network and any user or device and require proof of identity typically via a known form of identification (credentials/ certificate/key/card/etc.).

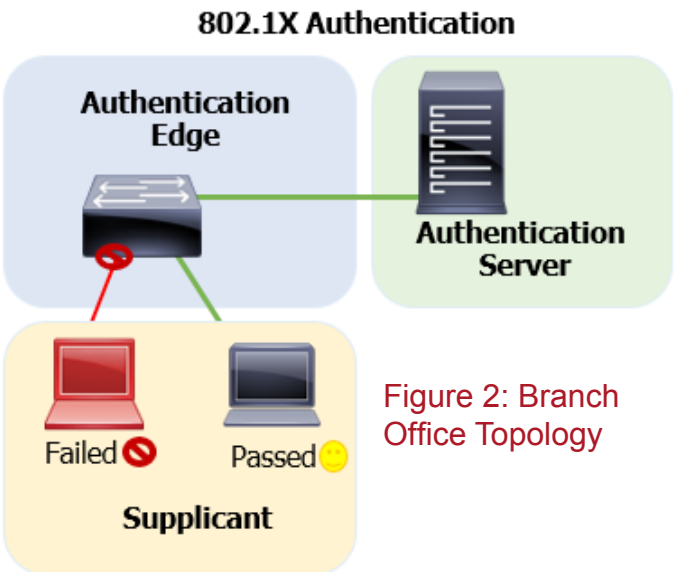


Figure 2: Branch Office Topology

When the authentication edge receives the ID it forwards it to the Authentication Server and waits for a response indicating acceptance or rejection. The great thing about this is it takes place before IP address authentication. This means, if any unauthorized user or device plugs into a switch port or attempts connecting to a WLAN, they would not be able to access any network resources, obtain an IP address, or even scan for network resources until authentication is complete. Using 802.1x you can authenticate a user, their device or both through any number of authentication types, which vary in their levels of security and complexity. This is one of the primary security mechanisms all enterprises should implement. Once authenticated, the next step is called Authorization. During the authorization phase access is granted to the user and privileges are derived based on the user and the device policies.

Network Access Control

We know we need users or devices to authenticate to the network, but we also must ensure these devices meet corporate polices and that is the function of Network Access Control (NAC). NAC is somewhat of an umbrella term that refers to additional services conducted on user devices as they authenticate to the network. For example, what good does it do to secure network access, if the person who authenticates legally does so from an infected computer, putting the Enterprise at risk? Allowing users to connect potentially infected devices to the enterprise network creates vulnerabilities. As more and more devices connect to the network, the potential for new vulnerabilities to be introduced increases significantly. Ideally both corporate and user-owned BYOD devices must meet corporate policies regarding OS Patches, software updates, AV updates, Anti-Malware updates, etc. A good NAC solution should be able to discriminate between different device types, even from the same vendor such as an iPhone or Android device.

Secure Guest Access

Another problem facing Enterprises today is how to provide network access to customers, visitors and contractors while keeping internal assets secure. This is commonly known as Guest Access. While this service is now a customer expectation for companies who have regular visitors like retail, travel, hospitality, food and entertainment industries, Enterprises must be careful to implement these services correctly or problems could follow. I have been called in on multiple occasions to diagnose network emergencies due to improper guest access configurations. Like any Enterprise network undertaking, guest access policies should be carefully planned and implemented before you make the service publicly available.

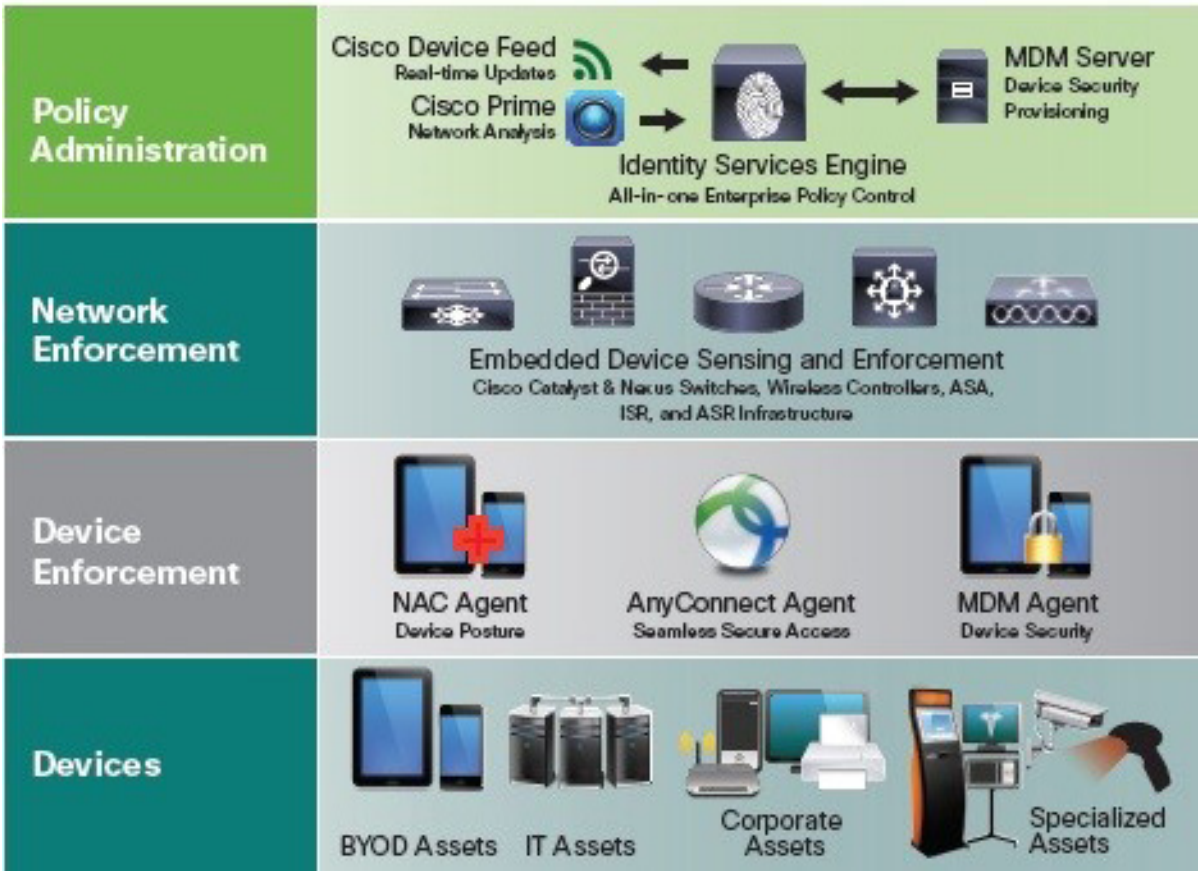
In an ideal scenario, all users should be fully secluded from secure enterprise assets by having to traverse some type of firewall or web/content filter while being separated from other guests. Additionally, Enterprise guest users should always be required to use a form of Enterprise-Level security when connecting to the network for security and privacy via VPN tunnels. Until recently providing guest users with Enterprise level security had an extremely high IT and/or receptionist burden. The main problem is how to generate credentials, certificates or tokens for guest users without requiring human intervention on the part of the Enterprise or requiring modifications to the device on the part of the guest.

Solving Network Security Challenges

The needs of today's Enterprise Security challenges typically require a number of different security solutions from a number of different vendors with lengthy and steep learning curves. Even then, vulnerabilities continue to exist.

Cisco Identity Services Engine (ISE) is an industry leading network policy server and is the sole product of Cisco's One Policy vision for Unified Access Architectures. ISE brings a wealth of security and policy features to solve the aforementioned challenges while mitigating future challenges.

Figure 2: Branch Office Topology



One Policy Features

1 One Policy

By centralizing, streamlining, and simplifying network access policy creation and management within ISE permits consistent secure network access for end-users, regardless of how they connect (e.g., wired, wireless, VPN). ISE is commonly used as the Authenticating Server for wired/wireless dot1x deployments. The release of ISE 1.3 includes a built in Certificate Authority feature which helps reduce administrative burden for dot1x client EAP methods which require client certificates. As the One Policy server, ISE is also the primary management application for Cisco TrustSec deployments. ISE 2.0 re-introduces TACACS+ as a more-secure feature-rich RADIUS alternative for network device administrative access. To achieve this ISE can integrate with several user repositories including AD, and LDAP compliant data sources essentially making ISE the central policy server and final decision maker for any user or device attempting to access the network.

2 Guest Self-Service

This gives trusted employees the ability to sponsor guests and also allow guests the ability to register themselves. Imagine your Enterprise Guest users connecting to a GUEST WLAN and being redirected to a Web-Authorization style page which lets them enroll to a service. After providing appropriate identification information, trusted employees or sponsors could authorize their account with a simple click in an email request that will result in an approval or denial of the user. Afterwards the user can download their user certificate or receive their password via SMS. Another option is to simply empower trusted employees to create guest accounts as needed via a simple web portal. This gives Enterprises the ability to provide a Secure Guest Access service to improve customer/contractor appreciation and productivity without any day-to-day administrative burden.

3 Device Onboarding

When Enterprises are making the critical decision to support a BYOD strategy a common question is who would be responsible for onboarding the influx of user devices to ensure they meet corporate security policies? ISE device onboarding empowers employees to enroll new devices via a network-provisioning portal that can simplify the process and reduce administrative burden at the same time. ISE work flow allows an employee to connect to a provisioning network and authenticate with Web-Auth using their network credentials. They are then redirected to a provisioning page where they add the details of their device. After that, the appropriate network profiles, user certificates, etc. can be downloaded. This process could, of course be customized to meet the specific needs of an Enterprise but this gives you an example of the power of device onboarding through ISE.

4 Device Profiling

This is an often-overlooked feature but can be very important for Enterprise security. The ability to make one device look like another to the network has become much easier than ever before. Even novice users can spoof MAC addresses and change their user-agent settings on devices pretending to be something they are not. Many times this is not for intentionally malicious reasons, i.e. iPads are not supported on a network but someone figured out how to make his iPad look like a laptop on the network so he could use his device for work. However, the fact remains that your company decided this should not be allowed and the security policy should be enforced. Device profiling gives us the ability to identify a device based on several criteria and establish a trust probability. For example, if the MAC address is from “APPLE”, and the host name contains “IPAD”, and UA contains OSX/iPad, then there is a pretty good certainty the device is an iPad. Device profiling is completely adjustable and can be used for tasks other than policy enforcement such as profiling a device to offer the end-user the correct AV or AS software to install during onboarding.

5 Context-Sharing Platform

This involves collecting tons of contextual information from wide and varied sources (including, for example, MDM, SIEM, identity stores and device agents), that permit ISE to prevent inappropriate access and detect and minimize the spread of network threats across the network.

Client Software & Supplicants

Supplicants are used to help enforce corporate security policies on client devices and/or simplify network access. There are installable clients which can be deployed to Enterprise owned assets, as well as web-based client/agents that can be used for Guest/BYOD devices.

1 Cisco AnyConnect

This is a universal client that delivers a complete, secure and seamless experience for remote VPN users and can optionally manage client network connections via the Network Access Manger (NAM) module with Windows PCs. The Cisco Secure AnyConnect client is installable on Windows, Mac, iOS and Android devices and allows simplified secure remote access to Enterprise Networks via Cisco Adaptive Security Appliance products or Cisco router based IOS Firewalls with AnyConnect licensing. The Secure AnyConnect client is required before clients can install the NAM component (supplicant) which can simplify the creation and distribution of network profiles to end-users for Enterprise 802.1x/EAP based authentication. The Cisco AnyConnect secure mobility client and NAM are commonly used client supplicants in secure Enterprise networks.

2 Cisco NAC Agent

Cisco Network Access Control (NAC) software is software that enables ISE to validate that a device conforms to the corporate security policy with regards to Anti-Virus, Anti-Spyware, Operating System OS patches, etc. As discussed above, it's imperative to ensure clients connecting to the network meet corporate compliance policies and are up-to-date with security software. This is an automated way of enforcing these policies to devices as they connect to the network. During a posture assessment, (typically during authentication phases) ISE retrieves details from the connecting device identifying the OS and Patch level, as well as any Anti-Virus/Anti-Spyware and its patch level. If the device does not have the correct OS patches or AV/AS patches, the device can either be informed of its compliance failure and denied access or provided the required updates to bring the device to a compliant level. There is a lightweight, installable agent for corporate controlled assets which provides details to ISE during a posture assessment. As an alternative to the installable client, the NAC web agent utilizes ActiveX or Java to perform posture assessments without installing software. All of these methods allow the user to remedy many compliance issues and once compliance policies are met, users would be granted the appropriate level of access.

Key Takeaways

The "One Policy" vision of ISE is one that brings Enterprise Security services which typically require 5 different servers/applications under one unified solution. ISE provides administrators that "Single Pane of Glass" visibility and management that most of us have been looking for. Still it's important to remember there is no single product to protect an Enterprise network and network security must be looked at from a holistic standpoint. With that said Cisco ISE provides Enterprises with a wealth of features that is really unparalleled in the market today and can greatly reduce the administrative burdens of providing enterprise level security and policy compliance. With an increasing and more diverse threat landscape, after your corporate security policy is designed and enforced, I recommend putting it to the test by having a penetration test performed to identify any remaining vulnerabilities. This way the good hackers find any remaining vulnerabilities you may have before the bad hackers do.

For more information on Cisco ISE and Network Security practices you should consider attending:
SISE – Implementing and Configuring Cisco Identity Services Engine
SISAS – Implementing Secure Access Solutions, part of the CCNP Security Program
WISECURE– Securing Cisco Enterprise Wireless Networks, part of the new CCNP Wireless program

About the Author

Chris Avants has 20 years of experience with Cisco technologies and has spent the last 5 years as a Sr. Instructor and Author. Chris specializes in Wireless, Collaboration and Security technologies. He has earned 30+ certifications including multiple expert-level certifications from Cisco (CCIE) and CWNP (CWNE). Chris is one of 30 people worldwide to have two expert credentials in the wireless arena, and is currently writing the new CCIE Wireless v3 boot camp for Fast Lane, targeted for release in the fall of 2016.

Twitter @RockstarWiFi
Blog – ChrisAvants.com
LinkedIn https://www.linkedin.com/in/chrisavants

