Network Access Control and Dot1x

LoyCurtis Smith

East Carolina University

Abstract

As a network is expanded and more users are granted access to a company's resources, more extensive measures are required to protect an enterprise from someone obtaining unauthorized access to those resources as well as company secrets. One of the most important measures an entity can deploy to mitigate one's ability to gain unauthorized access is network access control. There are many different flavors and implementations of access control, whether it is role based, rule based, discretionary, mandatory, and etc. It can also be implemented at many different layers of the OSI model. Network access control can be managed through user name and password, biometrics, IP address, logical port, certificates, and even at the switch port. To better protect a network from rogue systems and/or users connecting wirelessly or through wired connections, access control is necessary on the switches at the access layer of the network in the form of port based authentication. Port based network access control or layer 2 access control is the first line of defense in protecting network users and network resources from rogue and potentially malicious users. A good port based control that can protect an organization by not granting access to network resources until a user is authenticated is 802.1x or dot1x as it is also called. As with anything else implementation is key with do1x and can prove to be troublesome if done incorrectly however, if properly deployed it can prove to be very capable of controlling network access in an enterprise.

Introduction

The typical enterprise level network has at least two types of users. The first type is a user that utilizes the company's network and accesses network resources from within the network. In other words the traffic originates in the building, so this user is classified as an internal or local user. The second type is a user who accesses the network and network resources from outside of the company walls and utilizes some application to connect (e.g. VPN) to the network over the Internet, which classifies the user as an external or remote user. The internal users, depending on the organization's network infrastructure, may have the ability to connect via a wireless or a wired connection. To know whether a local or a remote user should or should not have access to the company's network an access control mechanism is required. According to the late Shon Harris, access control is a broad term that covers several different types of mechanisms deployed by a company that enforces access control features on computer systems, networks, and information. Access control allows an organization to control, restrict, monitor, and protect resource availability, integrity, and confidentiality (Shon). The National Institute of Standards and Technology Interagency Report (NISTIR) 7316: Assessment of Access Control Systems states that access control is concerned with determining the allowed activities of legitimate users, mediating every attempt by a user to access a resource in the system (Hu, V., Ferraiolo, D., & Kuhn, D.). The type of access control that both entities are defining and that is of great importance is logical access control. Although physical access control is of great importance in itself, logical access control protects the company from both local and remote users opposed to physical access control which only protects an organization from unauthorized personnel within the building obtaining physical access to company assets. Since access control is such an encompassing term the more appropriate term for controlling access to an entity's network is network access control. The Department of Information Systems Agency (DISA) in its Standard Technical Implementation Guide (STIG) for Network Access Control (NAC) version 8 describes network access control as being a suite of collective technologies that consist of Device Authentication, Device Policy Assessment, and Device Policy Remediation. Its goal is to harden the network by checking if devices connecting to the network are authenticated and compliant with network policy prior to allowing access to network resources (Network Access Control). A NAC mechanism that has proven to be very helpful in ensuring that authorized local users are granted access is IEEE standard 802.1x. 802.1x is a port based network access control mechanism that has grown from just being ideal for authentication of hosts connecting wirelessly to also being an efficient way to authenticate hosts on the wired network as well. The following topics will be covered in this paper: what is IEEE 802.1x, 802.1x advantages, 802.1x disadvantages, deployment requirements for 802.1x, and how to ensure that dot1x is properly and securely deployed on a company's network, i.e., best practices.

What is 802.1x?

According to the Institute of Electrical and Electronics Engineers, port based network access control allows a network administrator to restrict use of IEEE 802 local area network (LAN) service access points (i.e. ports) to secure communication between authenticated and authorized devices. IEEE 802.1x specifies an architecture, functional elements, and protocols that support mutual authentication between the clients of ports attached to the same LAN and secure communication between the ports (Port). CISCO defines 802.1x as an IEEE media-level (layer 2) access control that uses authentication to permit or deny network connectivity to an end user or device (Wired).

802.1x Advantages

If implemented correctly dot1x can be a very useful network authentication mechanism. According to Mohammed Younus' SANS Institute paper he states that implementing 802.1x on the network will mitigate the chances of unauthorized devices obtaining DHCP leased IP addresses on the network or from utilizing ARP redirects to eavesdrop on a networking device since all clients will be required to authenticate before gaining any network access (Younus). From personal experience dot1x benefits are as follows:

- It only authenticates authorized devices.
- When used in conjunction with a Network Policy Server it ensure that devices requesting network access are network compliant before granting access.
- Denies access to unauthorized devices.
- Devices can authenticate anywhere on the network as long as switch port it connects to is configured for 802.1x and its object is associated to a VLAN in Active Directory.

According to CISCO's Wired 802.1X Deployment Guide, Layer 2 access control provides an organization the following benefits:

- Visibility – username can be linked with IP Address, MAC Address, switch, and port. Useful for auditing purposes, use statistics, and troubleshooting.
- Security – Strongest method of authentication. Since it is Layer 2 access control it controls access at the access layer of the network.
- Identity-based services – Enables the delivery of custom services based on identity.

- Transparency – transparent to end user.
- User and Device authentication – can authenticate devices and users.

It is a very beneficial mechanism (Wired). In Forescout's CounterACT: 802.1x and Network Access Control technical note some other advantages of this authentication method. Since it is an IEEE standard most devices should be able 802.1x capable. It is also beneficial that it is a Layer 2 approach. Since the authentication is at Layer 2 the device does not pull an IP address until it first authenticates. This will keep unauthenticated devices from gaining network access (Forescout).

Disadvantages

Disadvantages of utilizing 802.1x from personal experience are few. One of the main issues faced with 802.1x is the sensitivity that it seems to add to the Cat 5 Ethernet cable. Minor cabling issues can cause a device to go through the authentication process multiple times before it exceeds the limit of fails and is no longer seen on the network. Hewlett-Packard (HP) states the following disadvantages in its 802.1x Solutions guide for its ProCurve switches: the main issue will be the 802.1x software for the client and the second disadvantage would be the setting up of a RADIUS server to manage the end-user database (ProCurve). Forescout disagrees with the complexity of port-based authentication in wired LANS. The issues in wired LANS are based on the inconsistency in how different switches are inconsistent in their 802.1x support. Other disadvantages would be architectural limitations and lack of security posture validation (CounterACT). The last disadvantage that one would experience with 802.1x is delay. It does not gain network access immediately (Wired). If the cable becomes unplugged or anything happens to the network device the host is plugged into it will restart the authentication process.

Deployment Requirements

For an organization to correctly deploy 802.1x they must be aware of the 802.1x authentication process and the necessary components that will lead to a successful implementation and protect their network from unauthorized users. Key terms/components that are involved in the 802.1x deployment are: supplicant, authenticator, and authentication server. The supplicant is entity that is being authenticated by the authenticator, i.e., the client requesting network access (Congdon). It is either connected via wired or wirelessly. The authenticator is the entity requiring authentication from the supplicant. This is typically the network access device, whether it is a switch or a wireless access point, that the supplicant is connected to. The authentication server is an entity that provides an Authentication Service to an Authenticator. It verifies the identity of the Supplicant based on the sent (Congdon). In addition to the main three components, the following components are used frequently:

Backend identity databases – centralized identity stores queried by the authentication server to validate credentials.

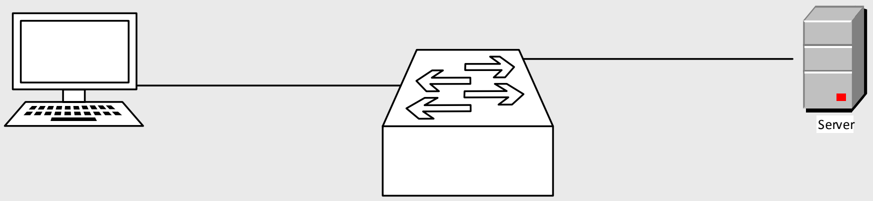
Public key infrastructure (PKI) – set of technologies and processes that enables the distribution and maintenance of digital certificates (Wired). The authentication process happens as follows:

1) Supplicant (Client) submits Extensible Authentication Protocol over LAN (EAPOL) message to the Authenticator (Switch).
2) The Authenticator then forwards the client’s request to the Authentication Server (RADIUS) without changing anything

3) The Authentication Server will verify the Supplicant’s credentials and transmit a response back to the Authenticator. Port state on switch is normally uncontrolled state, meaning no access granted. If the Authenticator Server approves the Supplicant’s request then the state is changed to controlled, which means access granted. Also depending on how it was deployed the Authenticator’s port can disable if the Supplicant fails the authorization process (Younus).

Figure 1 shows the 802.1x progress.

802.1x Authentication Process



EAPOL Start →		
← EAP-Request / Identity		
EAP-Response / Identity →		
	RADIUS-access-request →	
	← RADIUS-access-challenge	
← EAP-Request / Auth		
EAP-Response / Auth →		
	RADIUS-access-request →	
← EAP- success	← RADIUS-access-accept	Authentication Success
← EAP - failure	← RADIUS-access-reject	Authentication Failure

Figure 1

Cisco breaks down the message exchange into four stages:

1) Initialization
2) Authentication

3) Authorization
4) Accounting

These four stages are the same as the steps mentioned earlier (Wired).

To ensure that 802.1x is deployed correctly at a site the first priority would be ensuring that the three components are setup correctly. From experience 802.1x will need to be deployed in phases. Phase I would be prepare the network, Phase II would be to prepare end devices and policy servers, and the final phase is Phase III to enable dot1x.

Phase I: Preparing the Network:

1) The deployment of the Network Policy Server. The Network Policy can either be a virtual server or a physical server. It is ideal to at least run Windows Server 2008 R2. In the authentication process the Network Policy Server will consist of policies in regards to the different VLAN security groups in Active Directory. The rules will basically look into the object of the Supplicant in Active Directory to see if it meets the requirement. If the Supplicant does not have a VLAN security group it will fail authentication.
2) Create the Active Directory objects for all of the will be Supplicants on the network. For Printers and VOIP phones, Mac Address Bypass (MAB) objects can be created. A MAB object is an object created using a device's MAC Address and authenticated using the MAC as well.
3) Push new 802.1x printer setting to all network printers via the Group Policy Object per Organizational unit.

4) Configure Switches and Routers for dot1x authentication. Dot1x will only go on the ports that will connect to Supplicants and not on trunk ports. Until the deployment of 802.1x ensure that port is not set to authenticate automatically.

Phase II: Prepare End Devices and Policy Servers

1) Reconfigure end devices. This will requires the desktop support team of the organization or the workers if they are able. All of the end devices will have to be reconfigured. VOIP phones and network Printers will need passwords placed on the actual device.
2) Configure the Network Policy Server. Configuring the Network Policy Server will require the installation of a certificate on the Network Policy Server. It must also be checked that a policy is created for every VLAN on the network.

Phase III: Enable 802.1x

1) Create and Enforce the dot1x group policy
2) The Switches would now have 802.1x activated. The optimum deployment procedures for the switch would be a building or floor at a time depending n how the company is setup. This would take coordination throughout the week to ensure that the customers are aware of a major change taking place on the network.

According to a Network World article, the best practices for deploying 802.1x are:

1) Deploy a solution that supports the organization’s existing infrastructure and that works in a multivendor environment.

2) Find a solution that works with RADIUS or works easily with your existing RADIUS structure.
3) Use a solution that supports multiple operating systems for user configuration support.
4) Make sure the user configuration tool can create multiple preconfigured packages so that you can distribute different configuration options for your different type of onsite users depending on the type of business.
5) It is better to have an easy to use tool or wizards for the users that will be only a few clicks.
6) Make sure that the IT department can easily configure and distribute new packages when a configuration or policy change requires (Chen).

Conclusion

In conclusion, IEEE 802.1x is a port-based authentication protocol that if deployed correctly can have tremendous benefit for a company. It keeps unauthorized users from gaining any access to company assets or the network if the Supplicant is not first authenticated by the Authentication Server. Network Access Control is the first line of defense in protecting the network and it will work for both Wired and Wireless.

References

1. Chen, J., & Wang, Y. (2005). Extensible authentication protocol (EAP) and IEEE 802.1x: Tutorial and empirical experience. *Communications Magazine, IEEE, 43*(12), Pp.supl.26,supl.32,-Pp.supl.26,supl.32,. doi:10.1109/MCOM.2005.1561920
2. Congdon, P., Aboba, B., Smith, A., Zorn, G., & Roese, J. (2003, September 1). IEEE 802.1X Remote Authentication Dial In User Service (RADIUS) Useage Guidelines. Retrieved July 23, 2015, from http://tools.ietf.org/pdf/rfc3580.pdf
3. CounterACT: 802.1X and Network Access Control. (2013). Retrieved July 23, 2015, from http://www.forescout.com/wp-content/media/FS-8021X_and_NAC_Tech_Note.pdf
4. Hu, V., Ferraiolo, D., & Kuhn, D. (2006, September 1). Assessment of Access Control Systems (NISTIR 7316). Retrieved July 23, 2015, from http://csrc.nist.gov/publications/nistir/7316/NISTIR-7316.pdf
5. Musthaler, L. (2010). Best practices for rolling out 802.1X authentication. Network World (Online), Retrieved from http://search.proquest.com.jproxy.lib.ecu.edu/docview/758954821?accountid=10639
6. Network Access Control. (2010, March 24). Retrieved July 23, 2015, from http://iase.disa.mil/stigs/Documents/network_access_control_security_guidance_at-a-glance_v8r1.pdf
7. Port Based Network Access Control. (2010, February 5). Retrieved July 23, 2015, from http://standards.ieee.org/getieee802/download/802.1X-2010.pdf
8. ProCurve Network Security solutions. (2003). Retrieved July 23, 2015, from http://www.hp.com/rnd/pdf_html/guest_vlan_paper.htm

9. Shon, H. (2010). Access Control. In *All In One CISSP Exam Guide* (5th ed., p. 154). New York

10. Wired 802.1X Deployment Guide. (2011, September 6). Retrieved July 23, 2015, from http://www.cisco.com/c/en/us/td/docs/solutions/Enterprise/Security/TrustSec_1-99/Dot1X_Deployment/Dot1x_Dep_Guide.html#wp386670

11. Younus, M. (2006). Wired 802.1x Security. Retrieved July 23, 2015, from http://www.sans.org/reading-room/whitepapers/networkdevs/wired-8021x-security-1654