Cisco Secure Services Client: Enabling the Self-Defending Network

The Role of the Cisco Secure Services Client

Introduction

Today's threat environment requires that client devices and their associated users play a larger role in enterprise security. This challenge, however, is compounded by the growing population and diversity of such devices. To gain control of this situation, enterprises need a uniform approach for client management and security–one that accounts for the widest range of device types operating across both wired and wireless networks.

The Cisco® Secure Services Client is the cornerstone of the Cisco strategy for meeting this need. It is a full-featured, 802.1X software supplicant that:

- Enforces port-based access control while flexibly supporting a wide range of methods for user and device authentication
- Enables uniform applicability of client management and security across both wired and wireless networks
- Takes advantage of Cisco and other 802.1X-compliant infrastructures to deliver advanced security and management capabilities
- Establishes a foundation for rapid implementation of future intelligent network services developed by Cisco

Today's Security Challenges

Worms Expose Enterprise Network Weaknesses

Since their explosive emergence in the early 2000s, network worms have been a persistent feature of the threat landscape. Most organizations have implemented substantial perimeter-based defenses, but the current generation of worms is able to bypass such measures. The problem is not the failure of perimeter defenses, but rather worms attacking organizations from the inside after gaining entry via either unauthorized users plugging infected laptops directly into the local area network, or remote users that tunnel directly through the perimeter using virtual private network (VPN) connections.

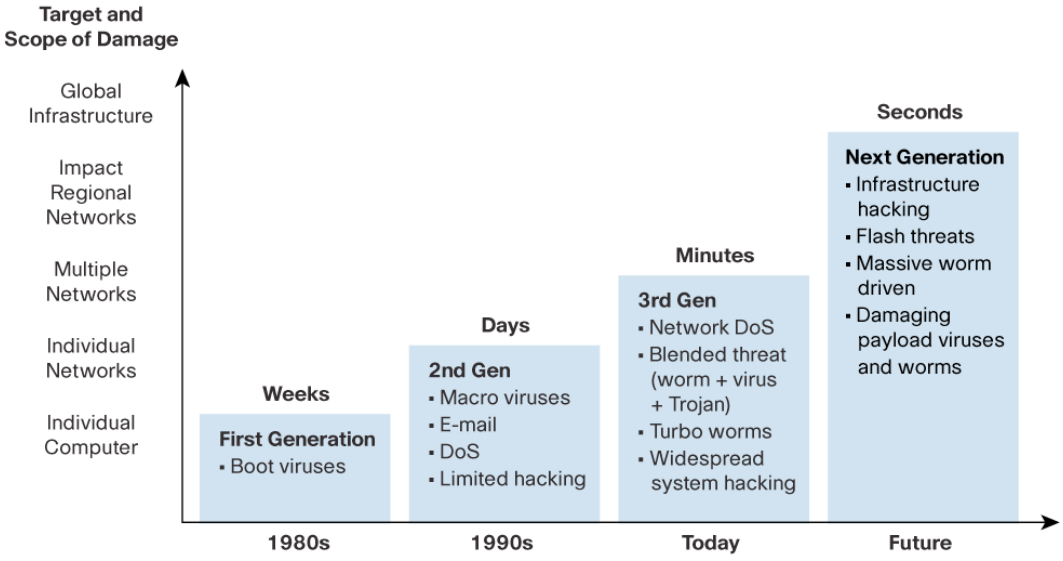
The result of this situation has been a growing recognition that organizations must better secure their internal networks. This includes being able to prevent the internal computing environment from being harmed by either managed or unmanaged endpoints. It also means providing better protection for endpoints that are under the organization's direct control.

Reactive Countermeasures Losing Ground

Another developing characteristic of the security landscape is the shrinking window of opportunity for enterprises to react to new threats. The widespread availability of exploit development toolkits now enables hackers–experts and novices alike–to create completely new attacks and variants in rapid-fire succession following the initial disclosure of any given vulnerability. The primary

implication is the diminishing effectiveness of virtually all reactive countermeasures, including patch management systems and the wide variety of products that rely on threat signatures (e.g., antivirus, anti-spyware, and intrusion detection software). Figure 1 illustrates this aspect of how threats have changed over the years.

Figure 1. Understanding Security Attacks—Past, Present, and Future



More Elusive Threats

A third concern is the change in hacker motivation, from gaining notoriety to making money. The result has been a shift in focus from quick, noticeable attacks that are easy to identify, to ones that are characterized as “low and slow”, and thus much more difficult to detect. This new subset of attacks is so highly targeted that even when one is discovered, the likelihood is low that an associated defensive capability will be generated.

One of the only defenses that holds much promise is to proactively reduce the surface area for attack. Any organization can achieve greater security by more tightly controlling who and what has access to its networked computing environment. The challenge then becomes one of identifying and implementing a solution that efficiently and cost-effectively yields a pervasively applicable capability for thorough admission and access control. In this regard, 802.1X technology is one of the primary keys to success.

An Introduction to 802.1X

The Basics

The IEEE 802.1X standard provides a definition for port-based network access control; it provides authenticated network access for Ethernet networks. Devices that are attached to an Ethernet switch port are granted the ability to send and receive frames if a pre-requisite authentication process is successful; this ability is denied if the process fails. Although the standard was originally intended for wired Ethernet networks, it has been adapted for use on IEEE 802.11 wireless LANs.

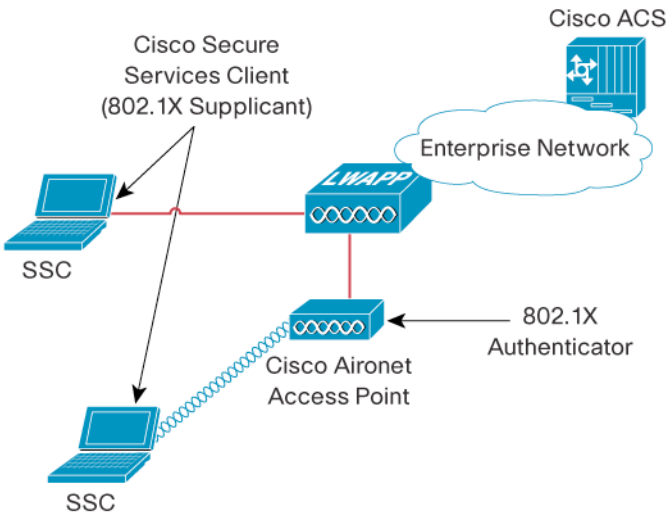
By definition, any 802.1X implementation will involve three primary components: an authenticator, a supplicant, and an authentication server.

The authenticator is a physical or logical LAN port on an infrastructure device that is responsible for facilitating and enforcing the authentication process after detecting the presence of a client device that is attempting to access services through it. Examples of devices that act as authenticators include Ethernet switches and wireless access points.

A supplicant is the corresponding software component on a client device that is requesting access. It is primarily responsible for obtaining and providing the authenticator with an appropriate credential. Supplicants for a wide variety of client platforms are available from several sources.

The authenticator subsequently forwards the credential to the authentication server, which establishes its validity and then informs the authenticator whether or not to grant the requesting device access. In most cases, the authentication server will be a RADIUS server–also referred to as an authentication, authorization, and accounting (AAA) server–such as the Cisco Secure Access Control Server (ACS). The relationship between these components is illustrated in Figure 2.

Figure 2. 802.1X Security Model



The Extensible Authentication Protocol

Another important characteristic of 802.1X is its use of the IETF standard (RFC 3748) Extensible Authentication Protocol (EAP), which handles the actual authentication process. EAP is essentially a framework that allows development and support for virtually any type of authentication, including passwords, challenge-response tokens, and public-key infrastructure certificates. However, this same flexibility is also the root of a significant challenge.

Numerous EAP types are currently available; choosing among them can be complicated. Each type has advantages and disadvantages, so organizations must evaluate the needs of their environment while examining tradeoffs in terms of the degree of security that is provided, solution manageability, the operating systems that are supported, the client devices that are supported, certificate requirements, user ease of use, messaging overhead, and the infrastructure devices that are supported.

A detailed evaluation of EAP types is beyond the scope of this paper; however, it is generally recognized that EAP types that provide strong mutual authentication are preferable, such as EAP-Flexible Authentication via Secure Tunneling (EAP-FAST), EAP-Transport Layer Security

(EAP-TLS), Protected Extensible Authentication Protocol (PEAP), and EAP-Tunneled TLS (EAP-TTLS).

In summary, 802.1X has several ideal capabilities for helping organizations secure their networks:

- As a Layer 2 solution, it confirms identity before providing any degree of access
- It supports a wide variety of authentication mechanisms
- It is applicable to both wired and wireless LAN environments

The Role of 802.1X in the Enterprise

802.1X for the Wireless LAN

802.11 wireless LANs have some inherent security issues. In contrast to wired networks, the media and the information that a wireless LAN is transporting is accessible without making a physical connection. This introduces a degree of uncertainty that is bi-directional in nature. Users need assurance that they are connecting to the organization, as opposed to a rogue access point. And organizations need assurance that only authorized users are able to “see” transported data and to access other networked resources.

The early developers of the 802.11 standard and related wireless technology addressed these uncertainties by incorporating some compensating features and security measures. However, the original WLAN security model–based on service set identifiers (SSIDs), open or shared-key authentication, and Wired Equivalent Privacy (WEP) for encryption–was proven to be ineffective against even moderately capable attackers. This stalled the enterprise adoption of this otherwise desirable technology.

The Wi-Fi Alliance created two specifications to remedy the security shortcomings exhibited by early wireless solutions: Wi-Fi Protected Access (WPA) and subsequently, Wi-Fi Protected Access 2 (WPA2). Both standards received widespread industry adoption and filled a much-needed gap as an intermediate solution, and as a fully compatible precursor to the eventually ratified 802.11i standard (Robust Security Network for WLANs). Today, WPA and WPA2/802.11i are recognized as definitive options enterprises can use to implement secure WLANs.

Using WPA or WPA2

The implementation of authentication and encryption capabilities specified by WPA and WPA2–for example, in solutions such as the Cisco Unified Wireless Network–eliminates the need for separate, overlay VPNs. VPNs are an important component of a security solution that involves remote-access scenarios; for example, when users associate with a public hotspot and then traverse the Internet before connecting to the enterprise network. For internal wireless deployments, however, VPNs provide no additional security benefit, and can adversely affect performance, limit roaming, and complicate the user experience.

Both WPA and WPA2 call for 802.1X/EAP as the authentication mechanism for enterprise mode operation. This has brought about nearly universal support for 802.1X in enterprise-class wireless access points and associated access point controllers, which has led to a proliferation of corresponding 802.1X supplicants. Basic supplicants can be found embedded in popular operating systems and many WLAN products; value-added versions are available as standalone products or components of broader networking and security solutions. This is positive in the sense that supplicants are a necessary pre-requisite for an 802.1X-based solution. However, it has the potential to increase complexity and cost of ownership. This is especially true if organizations must

use several different clients to establish comprehensive coverage–centralized management is much more difficult.

A universally applicable supplicant is a strong alternative.

802.1X for the Wired LAN

802.1X was first designed for wired networks, but its adoption within the wireless arena, in combination with the aforementioned security challenges, created a meaningful level of interest. A significant portion of the LAN infrastructure devices that are already deployed, as well as virtually all newly shipping ones, are now 802.1X-compliant. This gives organizations the means to begin securing their networks by enabling access to be restricted only to explicitly authorized and authenticated parties.

By itself this is a tremendous capability, but even greater degrees of protection can be achieved by further taking advantage of the 802.1X architecture. With an enhanced implementation, such as Cisco Identity-Based Network Services (IBNS), a properly configured authentication server can pass various identity-related attributes to the authenticator at the same time that it responds with a pass/fail signal for the authentication process. Intelligent authenticators (i.e., switches) can then apply those attributes not just to restrict access, but to control it more thoroughly. Unauthenticated users and devices can be routed to a “guest VLAN”, while authenticated users can be mapped to whichever VLAN corresponds to the resources they are authorized to access. User permissions can be delivered to any port on demand, eliminating the manual effort required to reconfigure ports as users move offices or other changes in location.

Even this is only small sample of what is ultimately possible with an enhanced 802.1X implementation. But once again, it is important to recognize that unlocking the potential of such solutions depends on the ability to cost-effectively implement and manage a pervasive population of 802.1X supplicants.

Cisco Secure Services Client

The Cisco Secure Services Client is an 802.1X supplicant that enables businesses of all sizes to deploy a single authentication framework across multiple device types, to both wired and wireless networks. By managing user and device identity and the network protocols required for secure access, the software client provides a robust first line of defense against unauthorized access and network intrusions. It delivers improved security, simplified management, and reduced total cost of ownership. Additionally, the Cisco Secure Services Client is the foundation for intelligent services that optimize the user experience when connecting to a Cisco Unified Wired and Wireless Network.

Improved Security

The Cisco Secure Services Client is a full-featured 802.1X supplicant that has been integrated with a range of Cisco solutions and infrastructure products. One of its greatest strengths is its capacity to help enterprises secure their networks.

- It provides an architectural extension of RADIUS solutions such as Cisco Secure Access Control Server (ACS), enabling a range of mechanisms to authenticate users and client devices, regardless of their method of network access. By taking advantage of RADIUS accounting functions, the client works with Cisco Secure ACS to support logging and reporting of detailed activity information on a per-user basis.

- It is fully supported in the Cisco Unified Wireless Network, an enterprise-ready, standards-based, wireless security solution that gives network administrators confidence that their data will remain private and secure when they use Cisco wireless products, Cisco Aironet® products, Cisco Compatible products, or Wi-Fi-certified WLAN client devices. It works with the complete Cisco portfolio of access points and wireless LAN controllers.
- It is a fully supported, instrumental component of Identity-Based Networking Services for Cisco Catalyst® switches, enabling extension of pre-access authentication, thorough access control, and a variety of other identity-related services to users and devices making wired connections.
- It positions the enterprise to take advantage of the Cisco Self-Defending Network by implementing Network Admission Control across wired and wireless networks.

Network Admission Control (NAC) is an important part of the Cisco Self-Defending Network initiative. Confirming user identity prior to granting access and then controlling the scope of that access, as is done with IBNS, are formidable security measures. NAC adds another dimension to the solution. With NAC, a “posture” check of the user’s device becomes another pre-requisite to granting admission. By checking for various client attributes, such as the presence and proper operation of antivirus software, personal firewalls, and certain patches, enterprises can obtain a greater degree of assurance that devices attempting to gain admission to their internal networks will not cause harm. The role of the Cisco Secure Services Client in this solution is that it offers a unified 802.1X client for organizations that have chosen 802.1X as their admission control technology.

Simplified Management

The Cisco Secure Services Client enables a rich and indispensable set of security capabilities, and does so without creating management challenges. Without a unified client, organizations must manage the numerous supplicants that are often found within their networks. At best, this results in a complicated makeshift solution with inconsistent policies and wholesale gaps in coverage. At worst, it dissuades the organization from taking advantage of the benefits of 802.1X technology.

The widespread applicability of the Cisco Secure Service Client across both wired and wireless networks ensures consistent function, capability, and coverage. Fully centralized management further eases the administrative burden, enabling straightforward deployment of multiple location-specific end-user profiles (different policies that apply when the user is in the office, on the road, or operating from home). Credential management capabilities include support for single sign-on and are fully compatible and nondisruptive to client-side scripting and other device startup processes that organizations may have implemented. Furthermore, by establishing a presence on client devices, the Cisco Secure Services Client provides a foothold for both current and future client management and security capabilities.

Reduced Total Cost of Ownership

The Cisco Secure Services Client also helps to reduce operational costs. Stronger security means fewer network intrusions, and therefore fewer incidents from which to recover. And simplified management means greater efficiency for time-challenged administrators. A unified user experience also comes with cost benefits: reduced training for users and, perhaps more importantly, reduced training costs for and reliance on help desk and related support staff.

The issue with using free supplicant software is not always one of compatibility. Of greater concern are the costs associated with overcoming the complexity of managing a diverse arrangement of client software, when organizations are already suffering from agent overload.

Foundation for Intelligent Services

The Cisco Secure Services Client establishes a foundation for both current and future intelligent network services. In addition to providing a uniform framework for obtaining and taking advantage of user and identity information–which itself has additional capacity for development–this flexible software client has the potential to support a wide variety of valuable capabilities, including:

- Secure and seamless wireless roaming
- Enhanced client protection
- Voice over WLAN
- User-centric performance management

Summary

Enterprises must continue to secure access to their networks. 802.1X technology holds promise for helping enterprises manage their security issues, but only a solution such as the Cisco Secure Services Client can fully address enterprise security needs. This flexible software supplicant enables an end-to-end Cisco security solution that is part of the Cisco Unified Wireless Network, Cisco Identity-Based Networking Services, and the Cisco Network Admission Control solution. By supporting multiple device types and access across both wired and wireless networks, the Cisco Security Services Client delivers stronger security, improved client management, and reduced cost of ownership.

Americas Headquarters
Cisco Systems, Inc.
170 West Tasman Drive
San Jose, CA 95134-1706
USA
www.cisco.com
Tel: 408 526-4000
800 553-NETS (6387)
Fax: 408 527-0883

Asia Pacific Headquarters
Cisco Systems, Inc.
168 Robinson Road
#28-01 Capital Tower
Singapore 068912
www.cisco.com
Tel: +65 6317 7777
Fax: +65 6317 7799

Europe Headquarters
Cisco Systems International BV
Haarlerbergpark
Haarlerbergweg 13-19
1101 CH Amsterdam
The Netherlands
www-europe.cisco.com
Tel: +31 0 800 020 0791
Fax: +31 0 20 357 1100

Printed in USA C11-389779-00 1/07

