802.1x Network Access Control
Introduction

Economic globalization has been the catalyst for businesses to extend the reach of their mobile workforce. Growing requirements for enabling remote employee access to company resources mandates the use of a solution that authenticates and connects. The IoT and BYOD phenomenon constitutes a significant percentage of network traffic originating from unmanaged personal devices, therefore stressing IT security and access control infrastructure. This consumerization of IT has raised end-user expectations for both performance and innovation.

Organizations of all sizes and verticals utilize a traditional Network Access Control (NAC) solution to discover and prevent rogue devices from connecting to the network. Devices are rejected unless complying with a predefined business security policy as enforced by a NAC solution.

About 802.1X

802.1X is an IEEE standard for port-based network access control. It provides an authentication mechanism for devices and users attempting to connect to wired and wireless LANs so that only authorized connections are allowed.

Key Elements

802.1X provides L2 access control by validating the user or device that is attempting to access a physical/virtual port, typically at a Switch or network edge device. As you can see in Figure 1, the basic 802.1X authentication mechanism consists of three components: endpoints (supplicant), authenticator, and authentication server.

![Figure 1: Key Elements](image-url)
• **Endpoints**: The endpoint is the device being authenticated. The supplicant is an agent running on the endpoint. For example, Pulse client, native supplicant, and non-Pulse Secure supplicant.

• **Authenticator/Switch**: The authenticator is a network device a managed Switch or wireless access point that facilitates authentication by relaying credentials between the supplicant and authentication server.

• **Authentication Server**: Pulse Policy Secure acts as an authentication server (typically a RADIUS server) and validates the credentials of the supplicant requesting access.

**Pulse Policy Secure**

Visibility and enforcement of users and endpoints is critical to guarding mission critical applications and sensitive data. Pulse Policy Secure (PPS) is a high-performance Network Access Control (NAC) policy server that leverages industry standards 802.1X and RADIUS. Designed to be scalable to companies of any size or vertical, PPS reduces cost and complexity, and addresses network access control challenges including insider threat, guest access control, and regulatory compliance.

**Authentication Protocols**

Authentication protocol is a method of defining how endpoints are authenticated through PPS. PPS supports a variety of Extensible Authentication Protocol (EAP) and non-EAP authentication methods that allow endpoints to authenticate.

**Radius Support**

802.1X requires an external RADIUS server that communicates with wireless access points and switches referred to as RADIUS clients. The PPS solution eliminates this need. The product includes a custom built-in RADIUS server that supports authentication, accounting, and authorization (AAA).

**Pulse Policy Secure Value**

**Host Checker**

Pulse Secure host checker performs a series of checks including patch assessment/remediation and malware detection. IT admins can be confident that an infected device has no connectivity to data center resources on the network prior to the completion of host check.

**Layer 2 and Layer 3 Access Control via SSO**

Enterprise users can deploy 802.1x based access control such as VLAN or filter assignments at Layer 2, along with Layer 3 access-control through next-generation firewalls (i.e., Checkpoint, Fortinet, and Palo Alto Networks Firewall). Once PPS authenticates the user, credentials are cached on the Pulse Secure client. Resource access policies for that user are pushed to the firewall and access is granted to the appropriate resource.
Conclusion

Pulse Policy Secure is a unicorn NAC solution in the networking and security industry. The PPS solution is based on open 802.1x standards and provides vendor-agnostic access-control and support for heterogeneous network environments. PPS utilizes pre-authentication host checks that deny network access to devices not in compliance with corporate security policies.

Integrations with industry leading next-generation firewalls (Fortinet, Palo Alto Networks, CheckPoint) and adds additional contextual intelligence about users that improve security effectiveness. PPS is compliant with popular standards such as Federal Information Processing Standard (FIPS), Defense DoD Unified Capabilities (UC), and Approved Products List (APL).

Pulse Secure’ unified security and policy control simply connects, protects, and manages users, their devices and access, from any device, anywhere.