Solution Overview

Pulse Secure®

Secure Access for the Federal Government

End-to-end Access Protection for Civilian, Intelligence, and Department of Defense Agencies

- Meet compliance mandates for 802.1x (IEEE), Layer 2 Switch STIGs, Comply to Connect, and NIST 800-53 AC Controls
- Secure the complex and expanding Internet of Things (IoT)
- Maximize ROI and lower TCO through interoperability with existing network and security infrastructure

A Robust Solution for NIST 800-53 Requirements

Government IT organizations must demonstrate and maintain compliance with a large and growing number of regulations and standards around network access control (NAC). For over a dozen years, Pulse Secure has been helping federal civilian, intelligence, and Department of Defense (DOD) agencies do exactly that – swiftly, seamlessly, and cost-effectively.

The Pulse Secure solution provides a holistic solution for local and remote access based on user and device identity. Administrators configure contextual access policies on Pulse Connect Secure to control VPN access to the data center based on devices, locations, resources, users and groups, or even endpoint profiling. Pulse Policy Secure with the Pulse Profiler extends policies to internal networks, allowing organization to identify, profile, secure and manage internal devices while also providing NAC policies for enforcement by a growing ecosystem of third-party security solutions. Pulse One provides centralized management and reporting to provide complete visibility and help meet the needs of the most stringent compliance environments.

Challenges

Compliance Pressure

Agencies are under pressure to comply with NIST 800-53 access control requirements

System Exposures

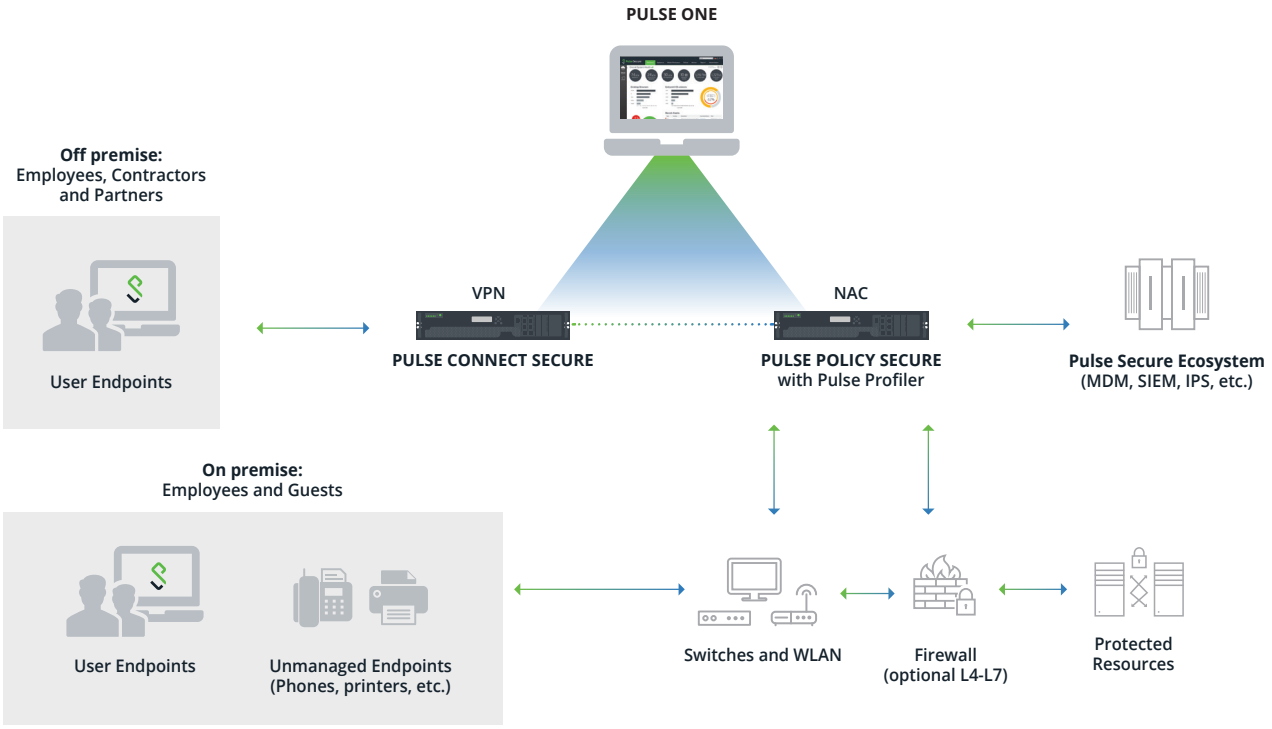
Existing safeguards, such as Cisco ACS, have entered end-of-life phases

Coordinated Action

Need to leverage existing infrastructure and systems to automate prevention and informed response

Limited Resources

Budgets are constrained, and experienced security personnel are scarce



Pulse Policy Secure, our high-performing and scalable NAC policy server, is founded on robust industry standards, including 802.1x and RADIUS. It secures your network by:

- Guarding mission-critical applications and sensitive data
- Providing user and device identity information for granular security enforcement by next-generation firewalls, access points, switches, and other interoperable platforms
- Delivering comprehensive NAC management, profiling, and monitoring for visibility of user and Internet of Things (IoT) devices
- Supplying granular, identity, and role-enabled access control from remote locations to the data center
- Addressing network access control challenges such as insider threats, guest access control, and regulatory compliance

DISA's STIGs (Layer 2 Switch, WLAN Authentication Server Security) and 802.1x Mandates

When it comes to meeting mandated authentication requirements such as DISA's Layer 2 Switch STIG, which mandates enabling 802.1x authentication, your agency may have faced the problem that most vendors want to sell a comprehensive – and expensive – solution that would entail replacing your existing systems and equipment: systems and equipment that involved a significant investment and which you do not want to retire at this time.

At Pulse Secure, we are vendor agnostic. Our AAA/RADIUS authentication server, which enables 802.1x authentication perfectly, integrates seamlessly with your existing infrastructure via open standards. This integration allows you to keep your current systems in place, accelerating your time to value by lowering your overall total cost of ownership (TCO) and maximizing your return on investment (ROI).

Additionally, with Pulse Secure's RADIUS solution, you don't have to enable 802.1x connectivity through complex, multi-tiered solutions requiring significant network redesign. Connectivity is enabled via existing capabilities on your endpoints, such as PCs, phones, and servers, in conjunction with settings enabled in your existing network switch or wireless access point. Everything then flows through the RADIUS server to ensure compliant authentication.

Internet of Things

IoT is here – and it is expanding at lightspeed. IoT devices require network access but have software updates and configuration settings established by the manufacturer that limit the ability to harden the device. The US Department of Homeland Security (DHS) has stated that IoT brings "multiple opportunities for malicious actors to manipulate the flow of information to and from network connected devices." DHS further advocates that agencies define network access controls to limit IoT devices to specific ports and to structure network permissions related to the IoT device's use.

Pulse Secure supports government IoT initiatives by combining device profiling with role-based access controls to define appropriate use polices. Pulse Profiler, founded on the RADIUS server, assesses each IoT device in terms of its role and rights: that is, what the device is, what it should be doing, and where it should be connecting. For example, a video camera should only connect to its video console. If it starts making connections elsewhere in the network, that raises a red flag. Profiling, therefore, provides network access control for IoT.

Additionally, Pulse Policy Secure automatically detects and classifies IoT devices and puts them into the administratively-defined IoT network. The solution also offers sponsor-based IoT device access where the sponsor can approve or deny IoT devices based on organizational policies. If Pulse Policy Secure detects a changed IoT profile or a compromised IoT device, it will automatically take enforcement actions to put devices into quarantine or into an isolated network.

Comply to Connect

Comply to Connect demands that any endpoint be vetted against established security requirements prior to connecting to your agency's network. Some vendors enable Comply to Connect in an agentless mode. At Pulse Secure, we recommend the implementation of a Pulse Secure agent for government agencies aligning with Comply to Connect directives. The following table shows the top three reasons for this recommendation.

Agentless Solution	Pulse Secure Agent Solution
Agentless solutions allow you to inspect endpoints from a distance before permitting or disallowing the device from connecting to the network. However, for the agentless solution to work, the device has to get Layer 3 access via an IP address. Therefore, you have given potentially non-compliant devices access to your network during the very process of vetting the device	With a Pulse Secure agent, an IP address is never given. The device never gets a full connection to the network during the validation cycle. Comply to Connect validations are performed at Layer 2 without requiring that the device access the network.
Agentless solutions poll the network on a regular cycle to check security measures. But, if someone starts disabling security protections at the beginning of a cycle, a lot of damage can be done before the next polling cycle begins and the danger is identified.	The Pulse Secure agent is always on and performs continuous monitoring. Any changes to security measures are caught in real-time, strengthening your network's security posture.
Agentless solutions can only inspect endpoints at a distance by using WMI protocols across the network. This is cause for concern, as WMI protocols can allow intruders to automate malicious activities – out of the question for high-security federal organizations.	The Pulse Secure agent eliminates the need for the potentially risky WMI protocol being used.

The Pulse Secure Access Advantage for Federal Civilian, Intelligence, and DOD Agencies

- Satisfy NIST 800-53 controls, including mandated requirements regarding 802.1x, Layer 2 Switch STIG, WLAN Authentication Server Security STIG, and Comply-to-Connect
- Gain cost-effective, easy-to-implement VPN and NAC/802.1x solutions with the fastest time-to-value in the industry
- Integrate Pulse Secure with existing infrastructure via open standards, removing the need to commit to a single route-switch vendor, load balancer, VDI provider, or client operating system
- Integrate with third-party next-generation firewalls (Palo Alto Networks, Juniper, Fortinet, Checkpoint), SIEM (IBM QRadar, HP ArcSight), Endpoint Security (OPSWAT, DUO, RSA, SecureAuth, Microsoft SCCM, etc.), MDM (MobileIron, Airwatch, Microsoft Intune, Pulse Workspace), Network switches, and WLC (Juniper, Cisco, HP Aruba, Ruckus, etc.).
- Establish unified access control for remote and internal end-points, as well as managed and unmanaged devices
- Provide an optimal and cost-effective Secure Access experience – including smartcards such as CAC and PIV – for workers who commute remote to onsite
- Gain extensive support for certificate handling, with features such as CRL, OCSP, and machine certificates
- Evaluate the compliance merits of endpoints without requiring authentication to the network, or a quarantine virtual local area network (VLAN)

Pulse Secure Federal Certifications and Accreditations

Pulse Secure provides a single security framework for VPN and NAC access that meets key certifications and accreditations for both.

Certifications and Accredidations	Pulse Connect Secure (VPN and Remote Access)	Pulse Policy Secure (Network Access Control: includes RADIUS and 802.1x)
UC-APL, JTIC	✓	✓
JTIC PKI-certified (Supports CAC and PIV)	✓	✓
FIPS 140-2 Level 1	✓	✓
Common Criteria (NDcPP)	✓	✓
STIG Compliant (Easy Setup Guides available)	✓	✓
Compliant with the latest Suite B and PFS standards required by JTIC	✓	N/A
Compliant with the latest TLS 1.2	✓	✓
Support for ECC certs	✓	✓
Supports 3K device certs	✓	✓