SOLUTION BRIEF

Pulse Secure®

Zero-Trust Secure Access Solutions for Government

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

Overview

Government IT organizations are tasked with demonstrating and maintaining compliance with a growing number of regulations and standards governing network access control (NAC) and secure remote access. For over a dozen years, Pulse Secure has been a leader in helping federal civilian, intelligence, and military agencies achieve full compliance.

For over a dozen years, Pulse Secure has helped government agencies address visibility, access, mobile, endpoint and IoT compliance challenges – efficiently, seamlessly and cost-effectively. By implementing Pulse Secure, federal civilian, defense and intelligence agencies can:

- Satisfy NIST 800-53 controls and specifications regarding 802.1x, Layer 2 Switch STIG, WLAN Authentication Server Security STIG, and Comply-to-Connect requisites
- Centrally manage an easy-to-use VPN and NAC/802.1x solution for wired, wireless and remote connections with flexibility for physical, virtual and cloud deployment
- Gain extensive user insight and unified access control for remote and internal endpoints, whether managed, uncatalogued, unsanctioned or unknown
- Automate endpoint and access situational awareness and security response through end-to-end visibility, policy-based controls, and infrastructure interoperability
- Validate device compliance pre-network connection and enable continuous remote and post-connection protection to efficiently find, assess and mitigate exposures
- Preserve remote and onsite user experience with context-aware access protection supporting a range of smartcards and certificate handling
- Integrate Pulse Secure via open standards that negates single vendor lock

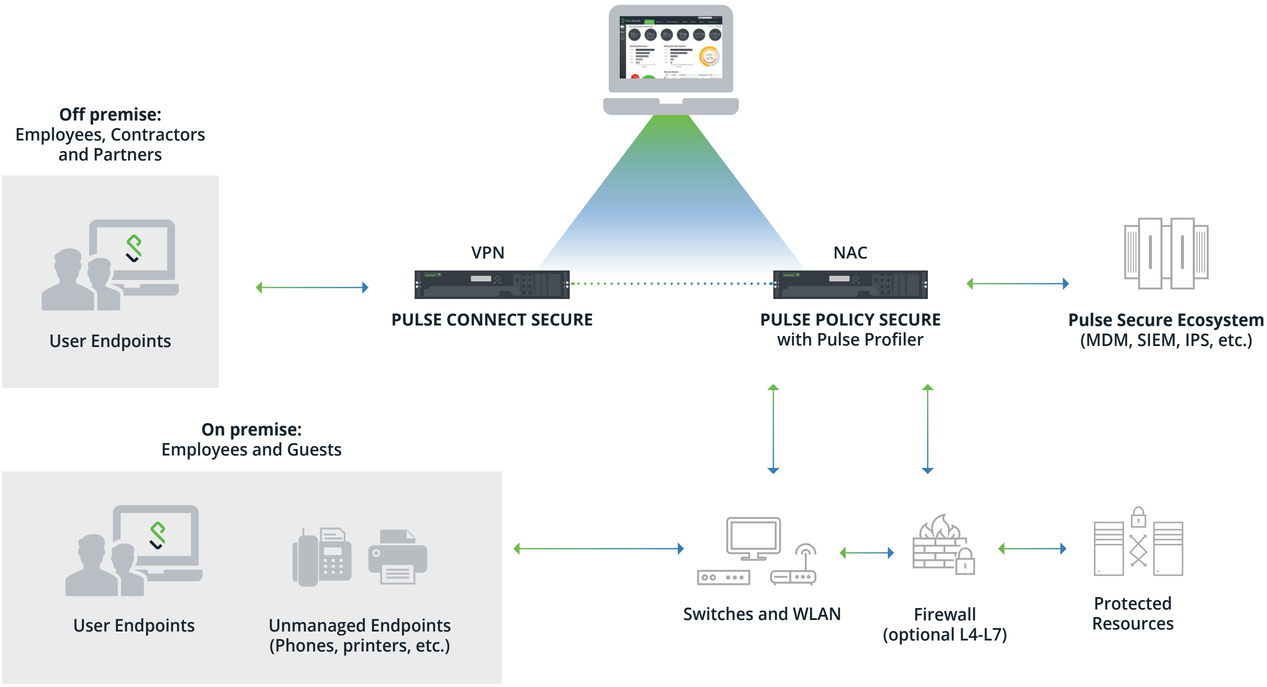
Additionally, with Pulse Secure's high performance on-board RADIUS solution, government enterprises don't have to enable 802.1x NAC connectivity through complex products. Instead, connectivity compliance can be achieved by simply leveraging existing endpoint and existing network switch and wireless access point infrastructure. Easily and cost-effectively deployed, the Pulse RADIUS server can manage access requests to ensure compliant network authentication.

Quotes

"While cyber security and data protection have been a natural focus of the federal government over the last decade, the recent wide-spread expansion into the world of IOT and enabling mobility, and the vulnerabilities that go with it have exponentially increased the burden of protecting federal networks against threat actors while introducing new, complex compliance requirements for our customers," said Sheryl Dunlap, CEO at Empower Solutions.

"The federal government is progressing towards a continuous and context-aware security agenda for network access control and endpoint security to address mobility, IOT threats, hybrid IT and broader military risks. This places a greater burden on agencies to assess their legacy systems, new initiatives and readiness capabilities to adhere to NIST guidelines," said Corey Solivan, director of strategic accounts at Consolidated Networks

PULSE ONE
Centralized Management, Visibility and Analytics


Off premise:
Employees, Contractors and Partners
User Endpoints
VPN
PULSE CONNECT SECURE
NAC
PULSE POLICY SECURE with Pulse Profiler
Pulse Secure Ecosystem (MDM, SIEM, IPS, etc.)
On premise:
Employees and Guests
User Endpoints
Unmanaged Endpoints (Phones, printers, etc.)
Switches and WLAN
Firewall (optional L4-L7)
Protected Resources

Pulse Policy Secure, our high-performing and scalable Network Access Control solution, 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 secure access control 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 Remote Access STIG and 802.1x Mandates

Standards outlining cybersecurity methodologies for remote access are written in the Remote Access Policy STIG (Security Technical Implementation Guide). DISA’s (Defense Systems Information Agency) Layer 2 Switch STIG clearly mandates the requirement of enabling 802.1x authentication. Pulse Secure RADIUS eliminates the need for complex connectivity solutions requiring significant network redesign. Pulse Secure AAA/RADIUS authentication server enables 802.1x authentication and integrates seamlessly with existing infrastructure via open standards. This modularity allows organizations to leverage their existing investment in current systems, accelerating time to value by lowering overall total cost of ownership (TCO).

Internet of Things (IoT)

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 agencies to define network access controls that limit IoT devices exposure 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 and apply segmentation. 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.

Comply to Connect

Comply to Connect demands that all endpoint devices be audited against an established security policy prior to admittance onto the network. Pulse Secure recommends an agent-based approach that aligns with Government Comply to Connect directives. The use of a device agent adds the benefits of always-on continuous monitoring, promotes a superior security posture through real-time security measure detection, and layer-2 security validation prior to establishing a full network connection.

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 endpoints, 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	✓	✓

Pulse Secure®

Corporate and Sales Headquarters
Pulse Secure LLC
2700 Zanker Rd. Suite 200
San Jose, CA 95134
www.pulsesecure.net

ABOUT PULSE SECURE

Pulse Secure provides easy, comprehensive software-driven Secure Access solutions for people, devices, things and services that improve visibility, protection and productivity for our customers. Our suites uniquely integrate cloud, mobile, application and network access to enable hybrid IT in a Zero Trust world. Over 20,000 enterprises and service providers across every vertical entrust Pulse Secure to empower their mobile workforce to securely access applications and information in the data center and cloud while ensuring business compliance. Learn more at www.pulsesecure.net.