Managed Network Access Control

Hughes delivers a robust Network Access Control (NAC) solution that allows you to confidently secure your network environment. Built with zero trust principles, Hughes provides the visibility, control, and automation that is required to effectively manage and secure every device that is seeking access.

Network Access Control and Security

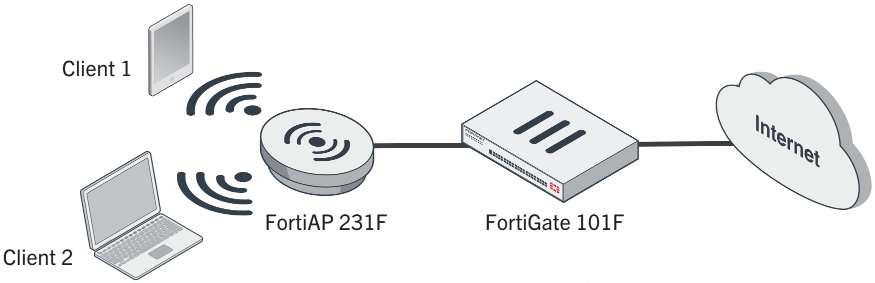
Hughes implements a comprehensive NAC solution that meticulously identifies, validates, and governs every connection attempting to access the network, whether it is a wired or wireless connection. This solution leverages a multifaceted approach, utilizing data from diverse sources and analyzing device behavior to achieve a granular understanding of all network participants. Additionally, Hughes identifies all of the devices attempting to connect to your network, and enforces granular, role-based access policies. This safeguards critical data and sensitive assets while ensuring adherence to all relevant industry regulations and established security standards.

NAC functionality ensures that only successfully authenticated endpoints are authorized in the production network, adhering to “need to know” and “separation of duties” security principles that are often found in zero trust policies.

- Devices connected to ports with the NAC function enabled are put into an onboarding VLAN.
- The onboarding VLAN has a restrictive security policy, enabled device identification, a DHCP server, and an enabled captive portal.
- The device identification feature collects device information. When the device matches the patterns that are defined in a NAC policy, an action is applied to the device, such as moving it to a specific VLAN or having a security policy applied.

The wireless controller supports NAC profiles that onboard wireless clients into the default VLAN. NAC policies match clients based on device properties, user groups, or EMS tags, and then assign the clients to specific VLANs. VLAN sub interfaces are based on the VAP interfaces that are used for the VLAN assignment.

When a wireless client first connects, it is assigned to the default VLAN per the NAC profile. After the client information is captured, if it matches a NAC policy, the client is disconnected, and when it reconnects, it is assigned to the VLAN that is specified by the SSID policy. The device properties that can be matched include a MAC address, hardware vendor, type, family, operating system, hardware version, software version, host, user, and source.



Pre-Connection Validation and Ongoing Monitoring

If a device attempts to join the network, Hughes rigorously validates its configuration against established compliance criteria. If discrepancies are detected, the connection is either denied outright or the device is isolated within a limited-access VLAN. Users are promptly notified of any non-compliance issues and the need for corrective action. Access is only granted once the device configuration has been successfully remediated. This multi-layered approach guarantees a secure and compliant network environment.

Incident Response

As a part of comprehensive Cyber Security strategy, the NAC function can be leveraged as an Incident Response function for the identified cyber threats in the production environment that warrant immediate attention.

Why Hughes?

Hughes goes beyond traditional NAC solutions, offering a feature-rich platform that delivers exceptional value:

- **Advanced Threat Detection with AI:** Leverage Hughes' industry-leading artificial intelligence (AI) to identify anomalous device behavior and potential threats that might slip past traditional NAC solutions.
- **Extensive Automation:** Simplify security operations with extensive automation capabilities. Hughes automates workflows for device onboarding, access control enforcement, and threat response—saving you valuable time and resources.
- **Deployment Flexibility:** Hughes caters to diverse network configurations. It offers centralized management for large deployments and flexible options for distributed networks, ensuring scalability for businesses of all sizes.

Hughes: Benefits at a Glance

- **Unmatched Visibility:** Gain comprehensive insights into all connected devices, including wired, wireless, IoT, and guest users. Hughes' asset inventory assists in identifying unknown devices and potential vulnerabilities.
- **Granular Access Control:** Implement role-based access controls to restrict or grant access based on device type, user identity, and security posture. This ensures that only authorized devices with appropriate security hygiene can access your network resources.
- **Automated Threat Response:** Hughes automates responses to security incidents. Isolate suspicious devices, block malware, and take swift action to minimize the impact of potential threats.
- **Simplified BYOD and Guest Management:** Hughes streamlines Bring Your Own Device (BYOD) and guest user management. The company also enforces security policies for BYOD devices and provides secure, controlled access for guest users.
- **Reduced Security Risks:** By proactively identifying and managing device vulnerabilities, Hughes helps you significantly reduce your network's exposure to security risks, such as malware attacks and data breaches.

Additional benefits include:

- Hughes SOC Support via a ticketing system that facilitates Customer Support
- Alerts and Reporting

Empower your security team and safeguard your network with Hughes.

Visit us at www.hughes.com/cybersecurity to learn more.

HUGHES
An EchoStar Company
11717 Exploration Lane Germantown, MD 20876 USA
www.hughes.com