# **Network Access Control**

**What is Network Access Control?  
 -**Network access control, or NAC, solutions support network visibility and access management through policy enforcement on devices and users of corporate networks.

**What is PacketFence?**An open-source NAC system which provides advance features such as: detection of abnormal network activities, proactive vulnerability scans, easy registration,isolation of problematic devices, remediation through a captive portal, 802.1X, wireless integration and User-Agent / DHCP fingerprinting etc.

**Few NAC solutions, their integration and comparision with PacketFence is detailed below:**

* **ARUBA CLEARPASS:**

**Functions:**

[Aruba ClearPass](http://www.arubanetworks.com/products/security/network-access-control/) is a policy management platform. It’s widely used by several businesses to onboard new devices, grant varying access levels, and keep their networks secure. ClearPass allows users to safely connect business and personal devices to their network in compliance with their security policies. It allows users to grant full or limited access to devices based on users’ roles, device type, and cybersecurity posture.  
The solution encompasses a three-step plan described below:

* **Identify**- ClearPass helps users identify valuable information about their systems such as: how many devices are connected to their networks, where are these devices connecting from, which devices are being used and which operating systems are supported.
* **Enforce**- ClearPass allows users to enforce policies during the onboarding of new devices without any involvement from the IT department thus reducing the effort and manpower.
* **Protect**- ClearPass offers a variety of third-party integrations which allows users to implement dynamic policy controls and threat remediation.

### 🡪Role-Based and Device-Based Access: ClearPass Policy Manager platform provides role-based and device-based NAC for contractors, employees, guests across any wireless or wired or VPN infrastructure. It can work with any multivendor network and can even be extended to IT systems and businesses.

🡪**Foundation for Network Security:** With a built-in context-based policy engine, support for multiple enforcement methods such as RADIUS, TACACS, SNMP, device fingerprinting and comprehensive posture assessment, onboarding and guest access options, ClearPass provides a foundation for network security.

### 🡪Self-Service Capabilities: With ClearPass, users can securely onboard their own devices for enterprise use or register AirPrint, AirPlay, DLNA and UPnP devices that are enabled for sharing, sponsor guest Wi-Fi access, and even set up sharing for Apple TV and Google Chromecast. Thus, ClearPass is said to deliver a wide range of unique self-service capabilities.

### 🡪Leveraging Contextual Data: ClearPass integrates ultra-scalable AAA (authentication, authorization, and accounting) with policy management, guest network access, device onboarding, and device health checks with a complete understanding of context. From this single ClearPass policy and AAA platform, contextual data is leveraged across the network to ensure that users and devices are granted the appropriate access privileges.

### 🡪Third-Party Security and IT Systems: ClearPass can be extended to third-party security and IT systems using REST-based APIs to automate work flows that previously required manual IT intervention. ClearPass integrates with mobile device management to leverage device inventory and posture information, which enables well-informed policy decisions.

**Integration:**

* Aruba ClearPass can easily integrate with third-party MDM to include mobile device posture validation before allowing access and for in-depth device assessments.
* It also Integrates with security and workflow systems and SIEM.
* Third party integration includes TippingPoint, Fortinet, ArcSight, Splunk, Brocade and IBM Radar.

**PacketFence vs Aruba ClearPass:**

* Both PacketFence and Aruba ClearPass support BYOD.
* Supported Authentication sources for PacketFence are: LDAP, RADIUS, Local user file (Apache htpasswd format) and OAuth2,SMAL. Whereas, Aruba ClearPass offers user and device authentication based on 802.1X, non-802.1X, and Web Portal access methods.
* ClearPass has a built-in Certificate Authority to support personal devices. On the other hand, for PacketFence, a PKI is used to generate a TLS certificate for each device/user.
* PacketFence supports the following operating systems on the x86\_64 architecture: Red Hat Enterprise Linux 7.x Server, CentOS 7.x and Debian 8.0 (Jessie). Whereas, Aruba ClearPass supports Windows 2003 64 bit, Windows 2008, Windows Vista, Wndows 7, Windows 8, Mac OS, and Ubuntu versions.
* PacketFence provides Single-Sign On features with many firewalls and supports firewall solutions such as: [Barracuda](http://www.barracuda.com/), [CheckPoint](http://www.checkpoint.com/), [Fortinet FortiGate](http://www.fortinet.com/), [iboss platform](http://www.iboss.com/) and [PaloAlo](http://www.paloaltonetworks.com/). On the other hand, in Aruba Clearpass, User-ID feature of the Palo Alto Networks firewall allows network administrators to configure and enforce firewall policies based on user and user groups.

* **Extreme Networks Network Access Control:**

**Functions:**

* It is a NAC solution used for wired and Wireless LAN and VPN users. It is integrated with Extreme Networks IPS and SIEM.
* Extreme Network NAC policies permit, deny, prioritize, rate-limit, tag, re-direct and auditing network traffic based on several environmental variables like time, location, device type, user identity.
* It supports RFC 3580 port and VLAN-based quarantine for Extreme Networks and third-party switches.
* It is is adaptable to any device using RADIUS for authorization with configurable attributes such as Login-LAT or Filter ID.
* It enables homogeneous configuration of policies across multiple wireless AP vendors and switches Thus, reducing the burden of policy lifecycle management and easing NAC deployment in wired and wireless heterogeneous infrastructures.

**Integration:**

* Extreme Networks NAC is tightly integrated with the Extreme Networks IPS and Extreme Networks SIEM and Extreme Networks NetSight Automated Security Manager to deliver best possible post-connect access control.
* OneFabric Connect API of Extreme Networks NAC provides a centrally managed, simple, open, programmable way to implement SDN for any network. Business applications can be directly controlled from OneFabric Control Center and managed by NetSight- a centralized set of rules for centralized controls.
* The result is an SDN solution including integrations with the NAC solution such as MDM integrations with vendors such as Airwatch, Mobile Iron, JAMF Software, and more.

**PacketFence vs Extreme Networks NAC:**

* Here as well, both PacketFence and Extreme Networks NAC support BYOD.
* Both PacketFence and Extreme Networks NAC support DHCP fingerprinting and MAC authentication mechanisms to block network access from unwanted devices.
* Authentication sources for PacketFence: LDAP, RADIUS, local user file, OAuth2 and SAML.   
  Authentication sources for Extreme Networks: LDAP and RADIUS.
* PacketFence supports firewall solutions such as: Barracuda, PaloAlto, CheckPoint, Fortinet Fortigate and iboss platform for firewall integration whereas Extreme Networks NAC supports Fortinet and Palo Alto NGFW. Here, Implementing single sign on features with PacketFence is easier as compared to Extreme Networks.
* One unique feature which of PacketFence which is not available with Extreme Networks NAC is that it supports bandwidth accounting which can automatically track the amount of bandwidth that the devices consume on the network. This helps it quarantine or change access level of devices that are consuming high level of bandwidth in a particular time frame.

**ForeScout CounterACT:**

**Functions:**

* Provides a way to enforce BYOD.
* It’s a visibility platform that provides insight into virtually any connected device across your extended enterprise and gives you a single-pane-of glass perspective.
* It can automate policy-based access control and enforcement, allowing users to perform a range of actions to limit access to appropriate resources.
* It’s Active scanning techniques are: NMAP, RPC, SSH, SMB and WMI.
* It automatically enforces actions for identified situations, reducing human interaction.
* It offers extensive guest registration options.
* It acts on vulnerabilities, IOCs, and other attributes provided by leading threat detection and SIEM vendors and orchestrates common, closed-loop processes with ITAM and other IT services.
* It performs passive discovery and profiling via SNMP traps, DHCP and TCP fingerprinting, NetFlow, HTTP user-agent, monitoring RADIUS requests, vSphere and EC2 integration.

**Integration:**

* ForeScout CounterAct can be easily integrated with switches, wireless infrastructure, VPNs and cloud-based network management systems such as Cisco Meraki.
* It can easily work with your existing infrastructure using the ControlFabric architecture.
* In private and public clouds, direct integration is possible with VMware and AWS.
* Integrates with Cisco PIX/ASA, Palo Alto Networks and provides extended module for Check Point firewall.

**PacketFence vs ForeScout CounterACT:**

* Both PacketFence and ForeScout CounterAct support BYOD.
* PacketFence supports the firewall solutions such as: Barracuda, CheckPoint, Fortigate, iboss platform and PaloAlto. CounterAct supports the firewall solutions such as: PaloAlto, Check Point, Fortinet, Juniper ARX, Forcepoint Stonesoft and Hirschmann EAGLE.
* PacketFence supports the concept of portal profiles which defines the registration workflow that will be used, together with registration and remediation pages. This is not available in ForeScout.
* PacketFence supports limited solutions for device management such as MobileIron, OPSWAT Metadefender and Symantec SEPM. Whereas, ForeScout CounterACT supports several service platforms including MobileIron, Airwatch, XenMobile, etc.
* PacketFence only support EAP-TLS for certificate-based authentication, whereas ForeScout CounterAct support PEAP-MSCHAPv2 along with EAP-TLS for authentication.
* In PacketFence, the access duration to the network can be controlled with configuration parameters for expiration. There is no such feature in ForeScout CounterAct.
* **Cisco NAC:**

**Functions:**

* protects information assets by preventing unauthorized network access to them.
* Helps in mitigating network threats such as worms, viruses, spyware.
* Provides clientless web authentication for guest users.
* Applies posture assessment and remediation services to a variety of devices, operating systems, and device access methods including LAN, WLAN, WAN, and VPN.
* Evaluates security policy compliance based on user type, device type, and OS.
* Recognizes and categorizes users and their devices before malicious code can cause damage.

**Integration:**

Cisco NAC works with existing authentication sources, natively integrating with Active Directory, LDAP, RADIUS, Kerberos, S/Ident, etc. It supports single sign-on for wireless clients, VPN clients and Windows Active Directory domains. With Cisco NAC, administrators get to maintain several user profiles with different permission levels through the use of role-based access control. The Cisco NAC in-band mode supports any network infrastructure. The out-of-band mode communicates with switches using SNMP. Cisco NAC Framework also facilitates broad integration with multivendor security and management software. Additionally, it enhances existing investments in network infrastructure and vendor software.

**PacketFence Vs Cisco NAC**

* In terms of OS support, PacketFence relies on Linux-specific features and hence, a direct port for Windows isn't available. However, PacketFence works on most of the current Linux versions. Whereas, Cisco NAC supports Windows Vista Business, Windows Vista Ultimate, Windows Vista Enterprise, Windows Vista Home, Windows 7, Windows XP Professional, Windows XP Home, Windows XP Media Center Edition, Windows XP Tablet PC, Windows 2000, Windows 98, Windows SE, Windows ME, Mac OS X (v10.5.x, v10.6.x).
* PacketFence does support EAP-TLS protocol for certificate-based authentication. It also provides a small PKI solution which is used to generate TLS certificates for users and devices. On the other hand, Cisco NAC supports Cisco NAC supports various protocols such as: EAP including MSCHAPv2, certificate based authentication, and PKI, EAP-TLV, EAP-UDP, EAP- Fast, Host, HCAP, GAME.
* PacketFence supports a guest VLAN or role out of the box for easy and secure guest access. Additionally, it integrates with online billing solutions such as [Authorize.net](http://www.authorize.net/), [PayPal](http://www.paypal.com/), [Stripe](http://www.stripe.com/) etc using which one can securely handle online payments. Whereas, in case of Cisco NAC, it’s guest server provides internet access to visiting customers, contractors, and partners without having to expose a company's internal infrastructure.
* PacketFence uses detection mechanisms such as Snort, Suricata, OpenVAS, DHCP Fingerprint, UserAgent, MAC addresses, Nessus to effectively block network access from unwanted devices. On the other hand, Cisco NAC network scanner uses customizable Nessus plugins to check and rule out any security vulnerabilities.
* **Pulse Policy Secure:**

**Functions:**

* Provides visibility into the network by detecting and continuously monitoring the network.
* Can be enabled at Layer 2 leveraging 802.1X/RADIUS.
* Supports device visibility and policy enforcement on switches using SNMP.
* Provides guest access support and dynamic authentication policy
* Provides an easy-to-use BYOD ready granular access control.
* Provides visibility for on-site and remote endpoints/users connecting through VPN.
* Uses SNMP v1/v2/v3 to discover L2/L3 switches and discover endpoints using SNMP traps.

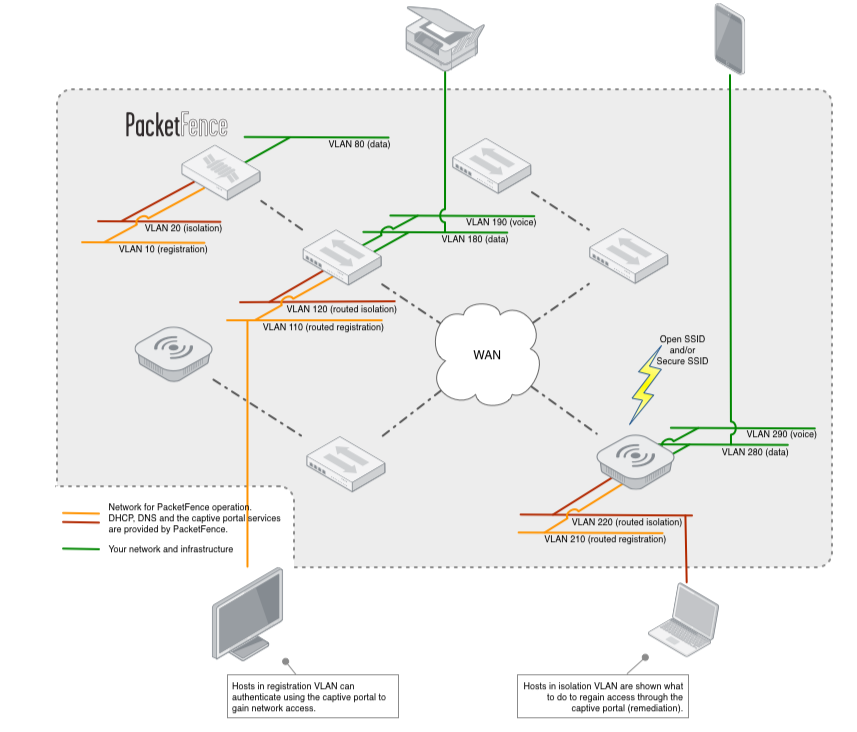
**Integration:**

* It fully integrates with any vendor’s 802.1X/RADIUS;-enabled wireless access points, such as Cisco, HP/Aruba Wireless, Brocade/ Ruckus Wireless.
* Integrates with any vendor’s 802.1X-enabled switches, such as Juniper Networks EX Series Ethernet Switches.
* Integrates with IPS capabilities of the SRX series gateways for both data center and branch, as well as standalone Juniper Networks IDP Series Intrusion Detection and Prevention Appliances.
* Integrates with layer 2 through layer 7 policy enforcement with Juniper SRX series firewalls.
* Integrates with MDM systems to execute health check and set policy based on a wider set of attributes for iOS and Android based devices.
* Adopts the TNC’s open standard IF-MAP, enabling integration with third party network and security devices.

**PacketFence vs Pulse Policy Secure:**

* Both PacketFence and Pulse Policy Secure support BYOD.
* Both PacketFence and Pulse Policy Secure integrate well with Microsoft Active Directory.
* Pulse Policy Secure provides ease of integration with Palo Alto and Check Point firewalls, whereas PacketFence doesn’t.
* Supported device management solutions for Pulse Policy Secure: Airwatch, Airwatch and Microsoft Intune, MobileIron, Whereas, PacketFence supports OPSWAT and Symantec SEPM.
* On-box Pulse Secure Profiler supports various fingerprinting methods for Pulse Policy Secure such as DHCP fingerprinting, MAC OUI, HTTP User Agent. Similarly, PacketFence supports detection mechanisms such as: DHCP, UserAgent, MAC addresses.
* EAP-TLS allows non-pulse secure 802.1X supplicants to authenticate through certificate authentication server. For the EAP-TLS protocol, the CA certificate must be configured along with the client certificate on Samsung devices for authentication, which is a much more tedious process as compared with EAP-TLS approach for PacketFence.

**Network Diagram and integration Requirements to show how PacketFence is inserted into the infrastructure:**



**Subnet Requirement:**

* Subnet for VLAN registration: 192.168.2.0/24
* Subnet for VLAN isolation: 192.168.3.0/24
* Subnet for normal VLAN: 192.168.1.0/24

**VLAN Requirement:**

* VLAN 20: isolation of VLAN.
* VLAN 10: registration
* VLAN 80, 180, 280: Data
* VLAN 120, 220: Routed isolation
* VLAN 110, 210: Routed registration
* VLAN 190, 290: Voice

**Services Requirement:**

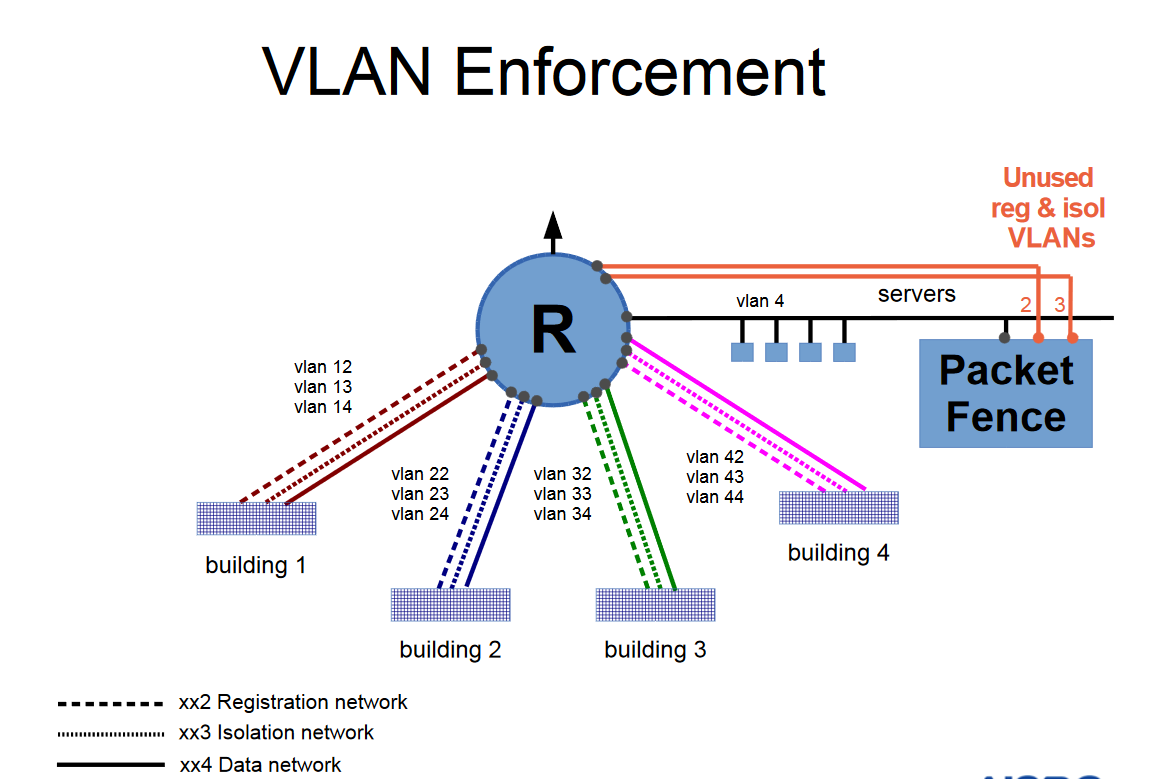
* DHCP server
* DNS
* Database server (MySQL or MariaDB)
* Captive portal services using RADIUS
* Web server (Apache)
* Firewall (iptables)

**Minimum Configuration Requirement:**

**Supported Linux OS:**

* CentOS/RedHat 6 (used to be only option)
* Debian 7 (Wheezy)
* Ubuntu 12.04 LTS
* Intel or AMD CPU 3 GHz
* 8GB RAM
* 100GB disk (RAID-1 recommended)
* 1 NIC (+1 for IDS, +1 for high availability)

**VLAN Enforcement diagram for PacketFence in Campus Network:**



**Summary:** By controlling access to the network with NAC solutions, businesses or organizations control their exposure to several emerging digital business risks, keeping their organizational network healthy and secure.

**References:**

* [**https://packetfence.org/**](https://packetfence.org/)
* [**https://www.secureaccessworks.com/Pulse-Policy-Secure.asp**](https://www.secureaccessworks.com/Pulse-Policy-Secure.asp)
* [**https://www.arubanetworks.com/products/security/network-access-control/**](https://www.arubanetworks.com/products/security/network-access-control/)
* [**https://www.cisco.com/c/en/us/products/collateral/security/nac-appliance-clean-access/product\_data\_sheet0900aecd802da1b5.html**](https://www.cisco.com/c/en/us/products/collateral/security/nac-appliance-clean-access/product_data_sheet0900aecd802da1b5.html)
* [**https://www.secureaccessworks.com/Pulse-Policy-Secure.asp**](https://www.secureaccessworks.com/Pulse-Policy-Secure.asp)
* [**https://packetfence.org/about.html**](https://packetfence.org/about.html)