

ClearPass – Welcome Home!

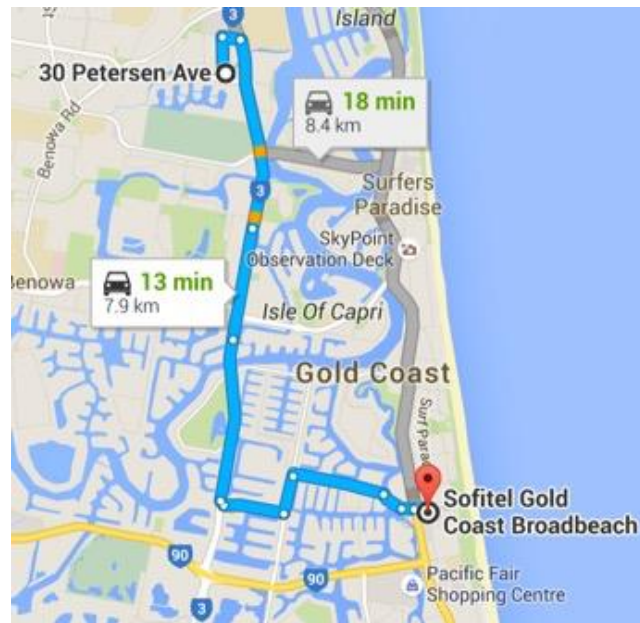
Carlos Gómez Gallego

Nov 18, 2015

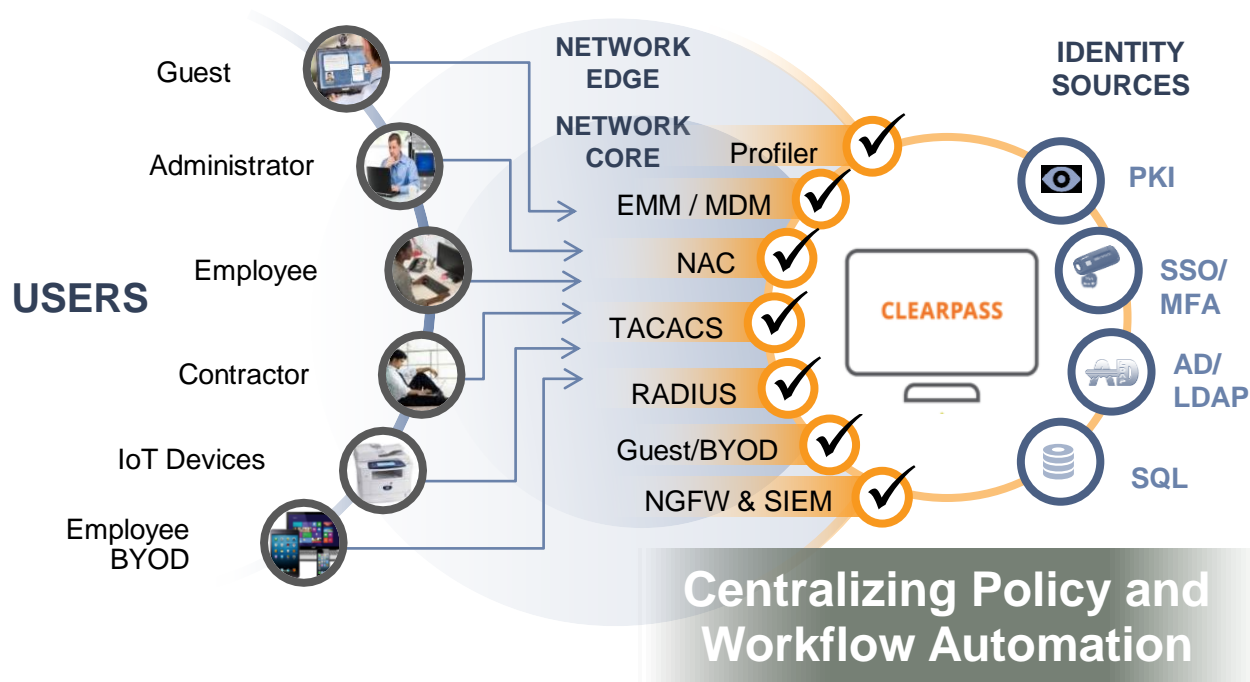
- **3 minute overview**
- **Beyond Authentication**
- **ClearPass Exchange**
- **Demo Time!**

ClearPass Overview

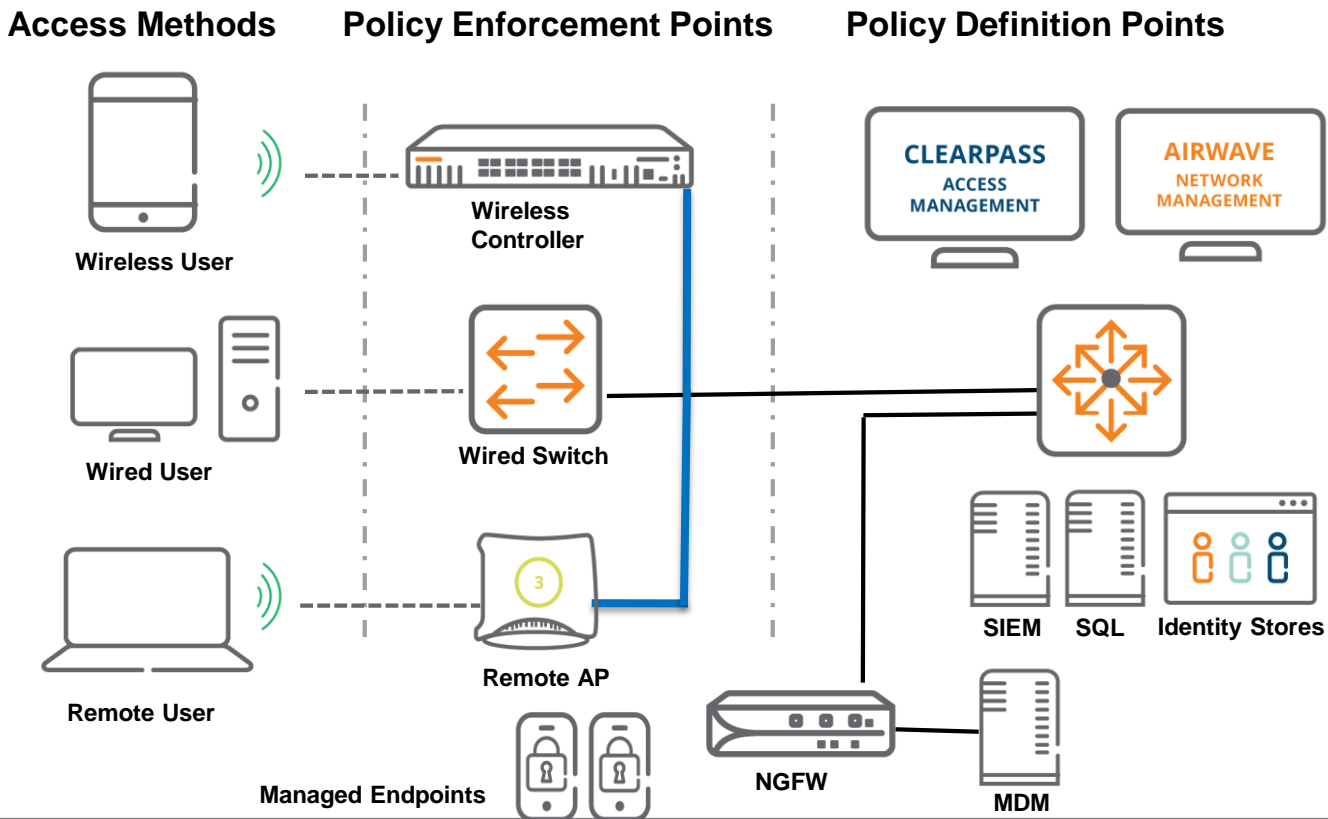
The amigopod Garage...



ClearPass Security Platform



Network Architecture



Beyond Authentication

AAA Framework Overview



1. **Compares** credentials versus those stored in a database.
2. **Enforces** privileges or services that a user can perform.
3. **Measures** usage for authz control, billing, analysis.
4. Usually uses RADIUS to perform authentication

Authentication alone doesn't provide context

Corporate Tablet



Internet
and Corporate Apps



BYOD Tablet



Internet Only



Sources of Usable Context



Device Profiling

- Samsung SM-G900
- Android
- “Jons-Galaxy”

EMM/MDM



- Personal owned
- Registered
- OS up-to-date



- Hansen, Jon [Sales]
- MDM enabled = true
- In-compliance = true



- Hansen, Jon [Sales]
- Title – COO
- Dept – Executive office
- City – London

Identity Stores



Network Devices

- Location – Bldg 10
- Floor – 3
- Bandwidth – 10Mbps



Sources of Usable Context



EMM/MDM



Device
Profiling



Adaptive Trust Identity

- Hansen, Jon [Sales]
- Title – COO
- Dept – Executive of
- City – London

- Hansen, Jon [Sales]
- COO, Executive Office
- London
- Personal Owned
- Samsung SM-G900
- Android 4.4, Knox

- MDM enabled = true
- In-compliance = true
- At Bldg 10, floor 3
- 21:22GMT, 21/12/14

h [Sales]
ed = true
ce = true

Identity
Stores

MySQL



- Location – Bldg 10
- Floor – 3
- Bandwidth – 10Mbps



ClearPass Policy Model – AuthN vs AuthZ



ClearPass Policy Manager

Username = Bob
Mac Address = XYZ
SSID = Secure
Location = Building 1
Request = Radius

Service Matching

Authentication

Authorization

Role Mapping

Enforcement

Added Context:
MDM Enrolled = True
Device Type = iPad
Owner = Bob
Required Apps = True
Active Sessions = 2
AD Group = Exec
Corp Asset = True

Guest

Insight

Endpoint

Onboard

AD/LDAP

SQL

MDM

HTTP

Response = Radius
- Accept
- Reject
- Attributes

Sample Role Mapping

Conditions	Role Name
1. (Authorization:[Local User Repository]:Category EQUALS SmartDevice)	Smart Device
2. (Authorization:[Onboard Devices Repository]:ON EXISTS)	[Employee]
3. (Authorization:[Local User Repository]:Category EQUALS Computer)	Computer
4. (Authentication:AuthMethod EQUALS EAP-TLS)	Onboarded
OR (Authorization:[Onboard Devices Repository]:Owner EXISTS)	
5. (Endpoint:Ownership CONTAINS Corporate)	Corp-Device
AND (Endpoint:MDM Enabled EQUALS true)	
6. (Authorization:Blue Skies DC:Email EXISTS)	Partner
7. (Authorization:SEEL AD:memberOf CONTAINS OnBoard)	OnBoard-Users
OR (Authorization:OpenLDAP:UserDN EXISTS)	
8. (Authorization:Corp AD:Groups CONTAINS Global Enablement)	Lab-Admin
9. (Authorization:Corp AD:Groups CONTAINS dl-channel-se)	Lab-Admin
10. (Authorization:Corp AD:Groups CONTAINS dl-cse)	CSE
11. (Authorization:Corp AD:memberOf EXISTS)	ArubaSE
12. (Authorization:SEEL AD:memberOf CONTAINS Aruba Employees)	ArubaSE
13. (Authorization:SEEL AD:memberOf CONTAINS Student)	Sales
14. (Authorization:SEEL AD:memberOf CONTAINS Lync Bypass)	Lync Bypass
15. (Authorization:[Local User Repository]:Role_Name EQUALS Student)	Student
16. (Authorization:[Local User Repository]:Role_Name EQUALS Teacher)	Teacher
17. (Radius:IETF-User-Name EQUALS 10.79.100.100)	AirGroup-Only-Demo-Controller
18. (Certificate:Subject-DirName-OnboardMACAddress EQUALS_IGNORE_CASE % {Connection:Client-Mac-Address-Colon})	Device-Cert-Match
19. (Endpoint:MDM Enabled EQUALS false)	EMM Profile Removed
AND (Endpoint:Ownership CONTAINS Corporate)	

Device
Context

Onboard
Context

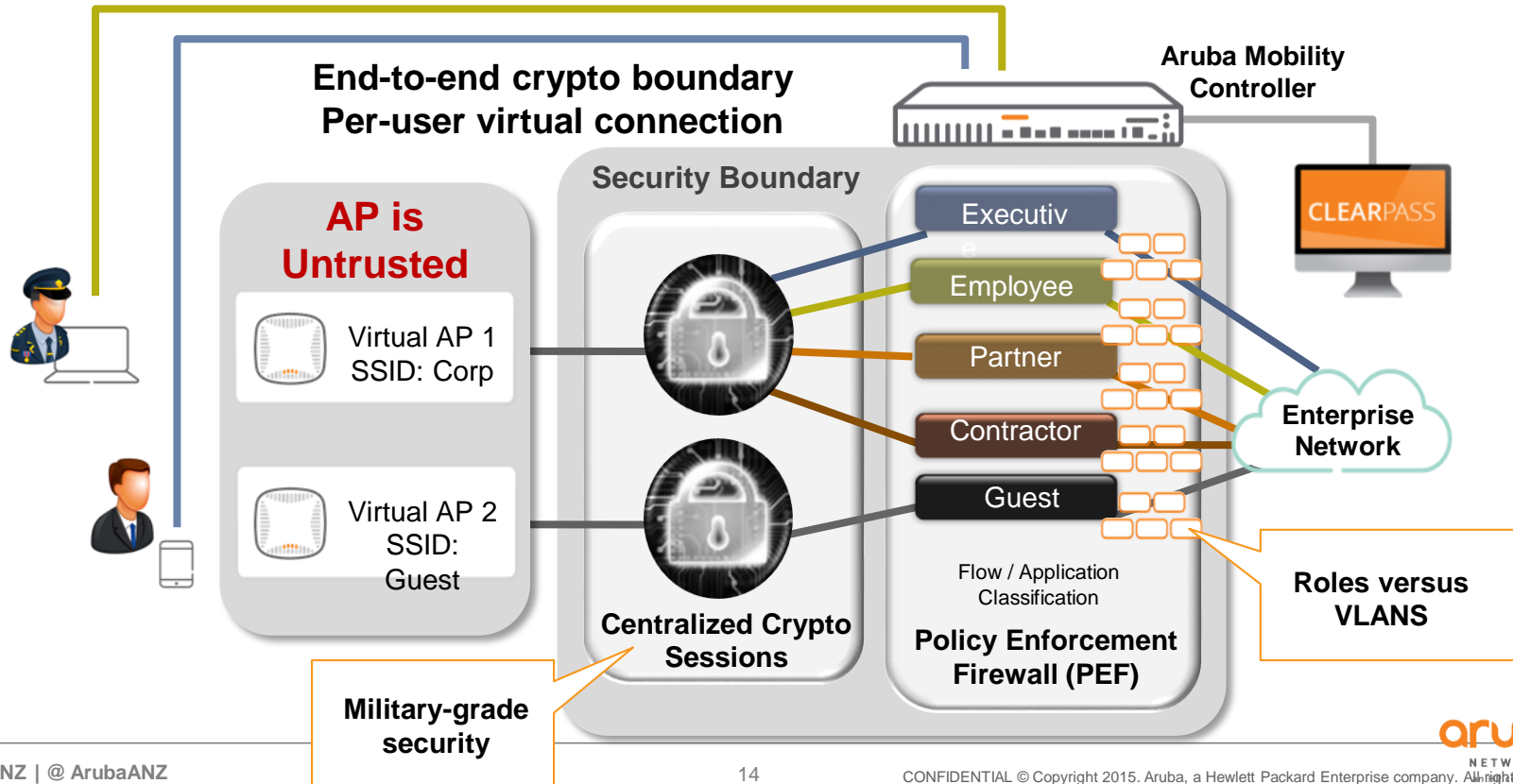
Auth
Context

User
Context

MDM
Context

Cert
Context

Role-based Access Control



ClearPass Exchange










What is ClearPass Exchange?

ClearPass Exchange provides context-sharing and integration of ClearPass services with many third-party devices and applications. This enables the coordination of security, operational or HR workflows based on policies defined in ClearPass

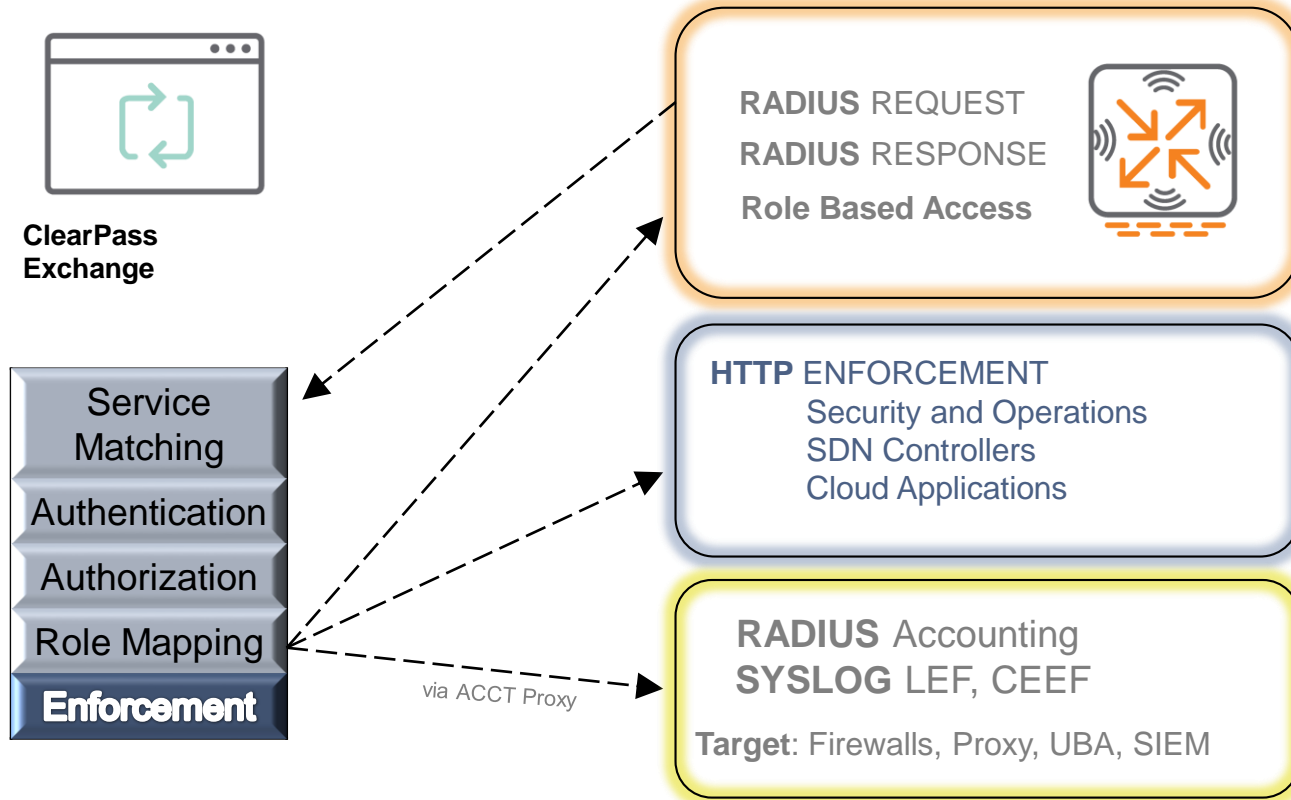
Customers can build their own integrations or choose from a series of pre-integrated solutions from Aruba.



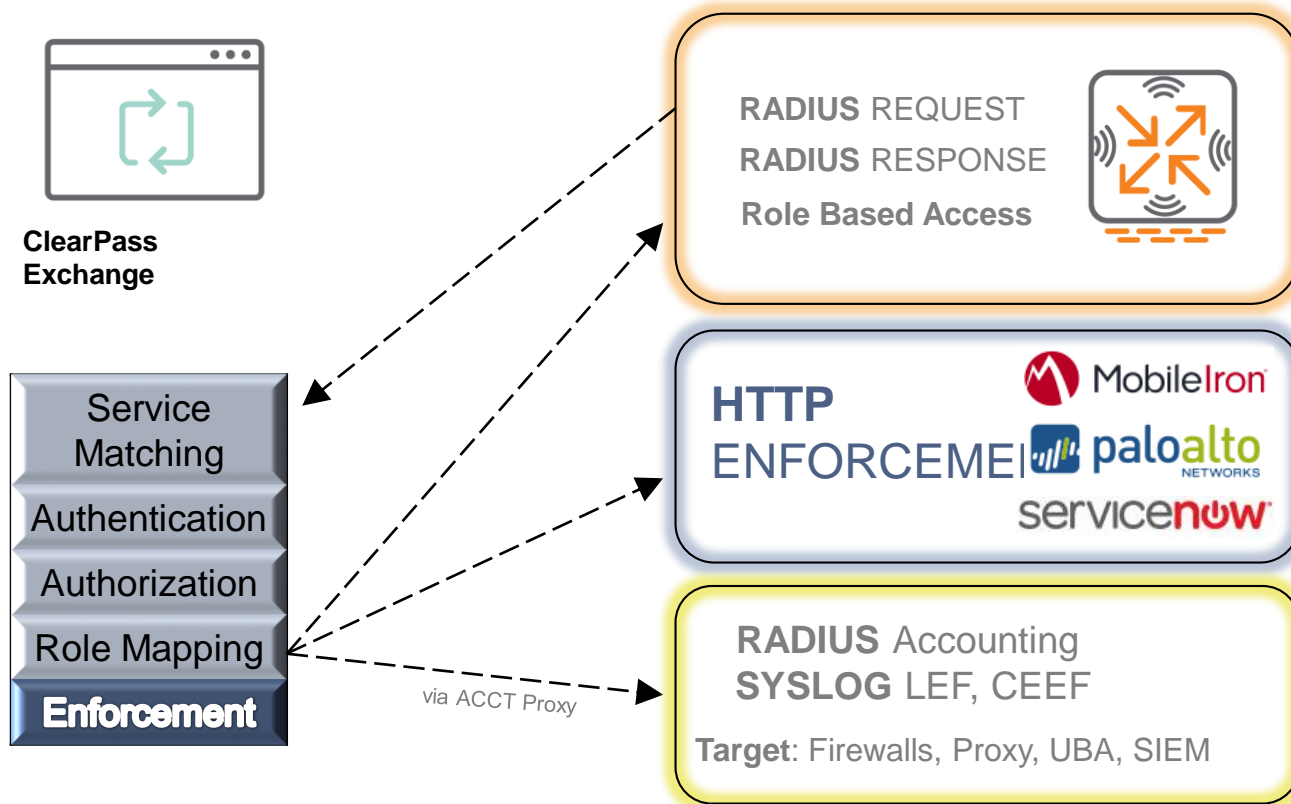
Featured Recipes

 ServiceNow Trouble Ticketing 16 Kudos	 PagerDuty 8 Kudos	 Philips HUE Light Shutoff/on 10 Kudos
 SendGrid Email Notification 8 Kudos	 Loggly Event Integration 4 Kudos	 Fortinet Forti Authenticator 3 Kudos
 Infoblox IPAM Username Update 4 Kudos	 Blacklist a user on an Aruba C... 7 Kudos	 Boxcar 6 Kudos

Enforcement Options



Enforcement Options



Streamlined Access Control

SELF-SERVICE Employee Driven Provisioning



Managed or
personal devices



Guest Devices
IoT Devices



Enforcement
Captive Portal
SDN

Multivendor Networks Enterprise AAA, CoA, TACACS+

Access Switches



WLAN Controllers



Autonomous APs



VPN



ClearPass Exchange Components

External 'Context Servers'

- The server or application you are connecting to
- Requires URL and Authentication credentials

Context Server 'Actions'

- The custom payload to send
- Content Types: HTTP, PLAIN, XML, JSON
- HTTP Methods: GET, PUT, POST
- Include any stored attributes e.g.. User name, device type, location, etc.

Enforcement Profile and Policy

- ClearPass policy configuration
- Sets condition for when to trigger Action
- Multiple actions to multiple servers supported

Add Endpoint Context Server

Server

Select Server Type:

Generic HTTP

Server Name:

www.application.com

Server Base URL:

https://www.application.com

Username:

admin

Password:

Verify:

Validate Server:

☐ Enable to validate the server certificate

Bypass Proxy:

☐ Enable to bypass proxy server

Endpoint Context Server Details

Action**Header****Content****Attributes**

Content-Type:

JSON

Content:

```
{ "shared_secret": "%{shared_secret}", "request":  
  [ { "command": "add_user", "username": "%{name}", "ip": "%{ip}",  
    "machine_name": "%{machine}", "domain": "%  
    {domain}", "identity_source": "Aruba ClearPass Policy  
    Manager", "timeout": "%{timeout}", "fetch_roles": 1, "fetch_groups": 1 } ] }
```

Summary**Profile****Attributes**

Profile:

Name:

Send Info to Loggly Server

Description:

Type:

HTTP

Action:

Accept

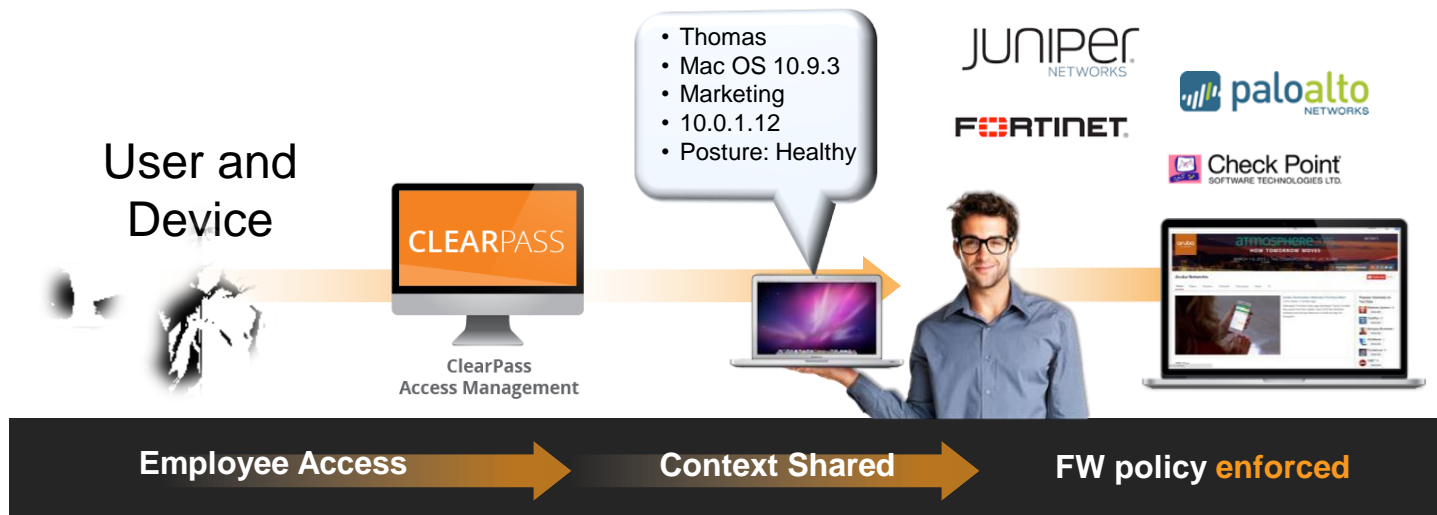
Device Group List:

-

Attributes:

Attribute Name	Attribute Value
1. Target Server	= logs-01.loggly.com
2. Action	= Send Social Auth data to Loggly Dashboard

Example: Share context with Firewall



- Network, Data Center and Internet Firewalls
- No agents/clients required
- Dynamic User, Device and Posture visibility
- Applies similarly to Proxy Servers, SDN Controllers, etc

Example: Help Desk tickets with Context

Endpoint Context Server Details

Action

Header

Content

Attributes

Server Type: Generic HTTP

Name: Create ServiceNow Ticket

Description: contextServerAction.CreateTicket

HTTP Method: POST

URL: /problem.do?JSON&sysparm_action=insert

Endpoint Context Server Details

Action

Header

Content

Attributes

Specify the key-value pairs to be included in the HTTP Header -

#	Header Name	Header Value
1.	Content-Type	= application/json
2.	Click to add...	

Endpoint Context Server Details

Action

Header

Content

Attributes

Content-Type: JSON

Content: {"short_description":"Compromised Device WiFi Connection Attempt","priority":"3","description":"The following compromised device has attempted to connect to the cp-secure WiFi network:\nMac Address: %(Connection:Client-Mac-Address)\nEnrolled User: %(Authentication:Full-Username)\nDevice Serial: %(Endpoint:Serial Number)\nMobile: %(Endpoint:Model)\nOS Version: %(Endpoint:OS Version)\nLocation: %(Radius:Aruba:Aruba-Location-Id)*,"u_category":"71feaf0f8c00d100a4e1ee6a09f9bc72","u_subcategory":"02feaf0f8c00d100a4e1ee6a09f9bc29":"assigned_to":"mobileadmin"}

Save Cancel

Welcome: WSDL Test

Application: -- None --

Update Set: Default

Time zone: US/Pacific

Login Logout

Type filter text

Analytics

Incident

Problem

Create New

Assigned to me

Known Errors

Open

Pending

All

Overview

Change

Release v2

SDLC

SDLC (scrum)

Project

Problem = Required field

Update Save

Number: PRB0000503

Priority: 3 - Moderate

Known error: ☐

Category: BYOD Policy

Subcategory: Compromised Device

Short description: Compromised Device WiFi Connection Attempt

Description: The following compromised device has attempted to connect to the cp-secure WiFi network:
Mac Address: E806889CA350
Enrolled User: cam
Device Serial: GB0216XVA90
Mobile: iPad
OS Version: iOS 5.1
Location: ap-1344-ebc-05

Opened by: WSDL Test

Problem state: New

Assignment group: Service Desk

Assigned to:

Automate Security Policy

SELF-SERVICE

Employee Driven
Provisioning



Managed or
personal devices



Guest Devices



ClearPass Exchange

AUTOMATE SECURITY

Tickets, Notifications &
Enforcement

Endpoint Security



Next Generation Firewalls



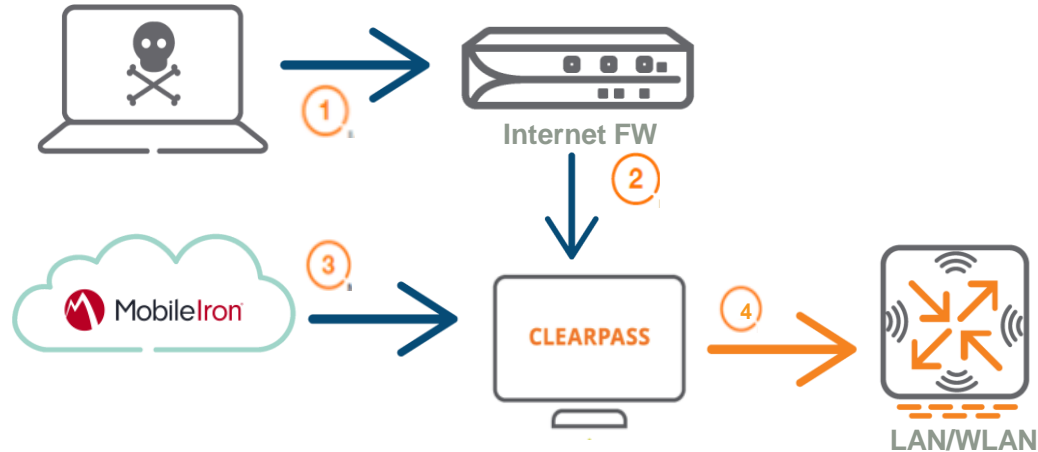
SIEM/Helpdesk



Mobile Device Management



Adaptive Network Access based on Threat level

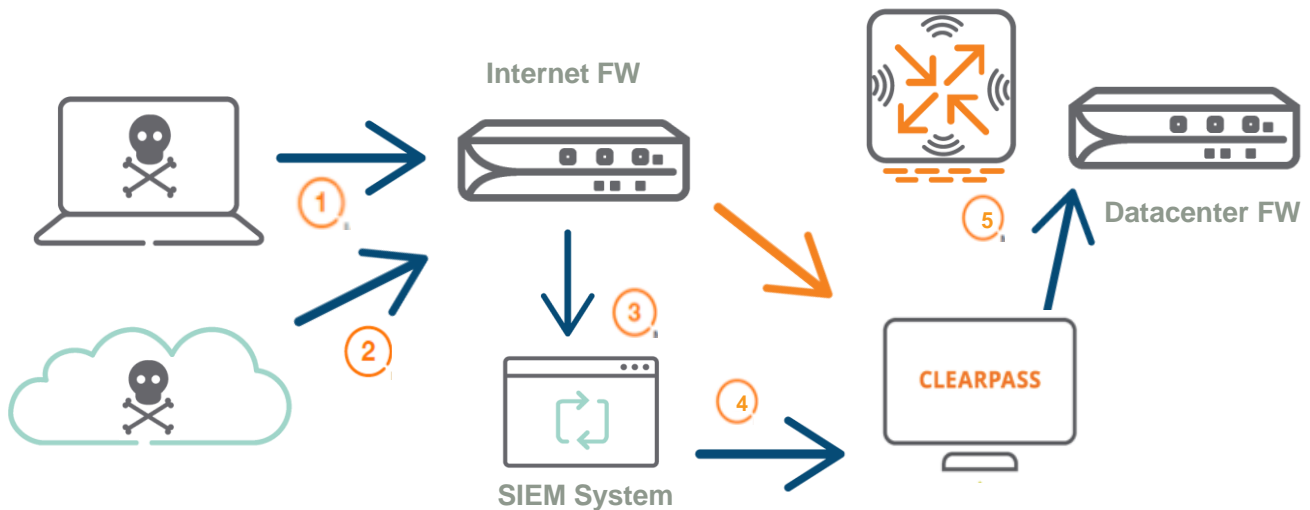


1. User connects and downloads threat
2. NGFW/IPS generates event to ClearPass
3. Or EMM generates security event to ClearPass

4. ClearPass isolates client on network; informs other enforcement points, triggers additional scans and notifies helpdesk

Leverage SIEM to alert on Threats

Adaptive Network Access based on Threat level



1. User connects and downloads threat
2. NGFW/IPS intercepts file and identifies threat type

3. NGFW/IPS generates event to SIEM system
4. SIEM system sends threat details to CPPM
5. ClearPass isolates client on network; informs other enforcement points, triggers additional scans and notifies helpdesk

SELF-SERVICE Uses Existing Identity

Managed or
personal devices

Guest Devices



Public WiFi
Education
Government
Enterprise



SAML 2.0
Oauth2
HTTPS

Identity Stores Public or Private Providers

Social Networks



Office Collaboration



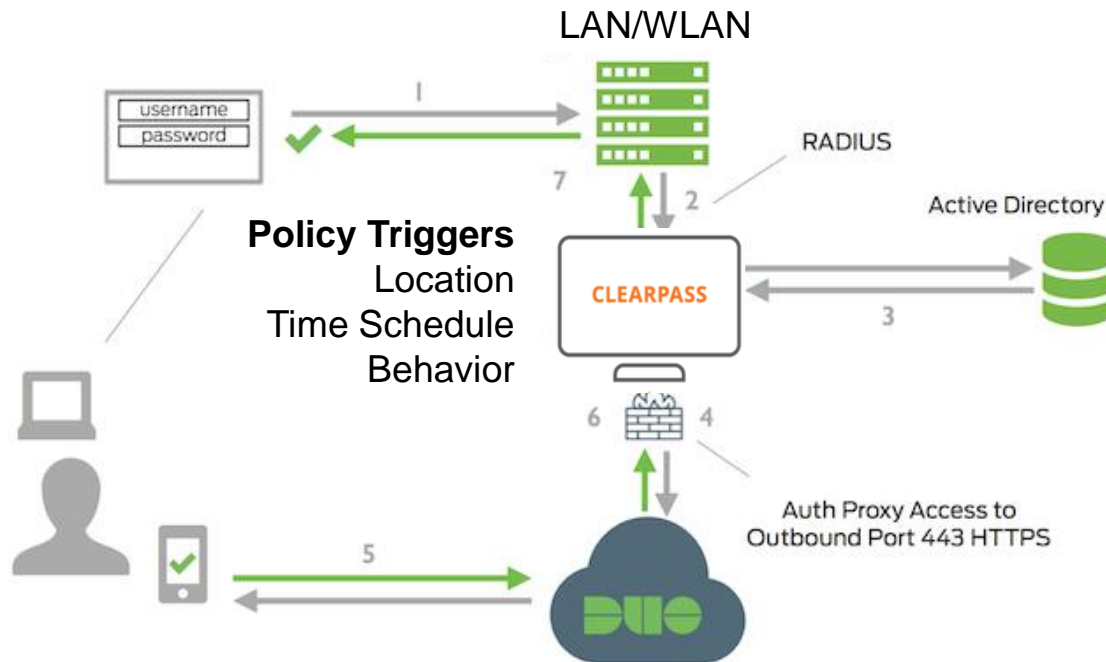
Identity SSO and MFA



Payment Management



Policy Based Multi Factor Authentication



Orchestrating Multiple Actions

Request Details

Summary | **Input** | **Output**

Session Identifier:	
Date and Time:	
End-Host Identifier:	
User:	
Address:	10.79.1... 04:0
System:	UNKNOWN (100)

Policies Used -

Service:	Ethersp...-Aruba-Policy
Authentication Method:	EAP-PE... EAP-MSCHAPv2
Radius Action to force notification page	AD:sjc...-05.arubanetworks.com
Enforcement Profiles:	Endpoints Repository], Corp AD
	ArubaS..., EMM Profile Removed, Smart Device, [Employee], [User Authenticated]
	Send M... Force Enrollment Message, EMM Not Enrolled Admin Alert Email, Open Help Desk Ticket - Device Need Enrollment, Turn on the Hue light, Update SEEL AD Display Name, Update Partner AD Display Name, Update Corp AD Display Name, PANW_Trigger_Profile, Clear MAC Caching, Update Aruba Wireless Endpoint Location, Force MDM Enrollment

Showing 2 of 1-100 records

Change Status | **Export** | **Show Logs** | **Close**

Update Palo Alto Firewall

Send user SMS/Push notification

Radius Action to force notification page

Send Email to security team

Sound the alarm!

Open Help Desk Ticket

Developer friendly REST API framework

API Explorer – Identity-v1

[Back to API Explorer](#)

Authorization:

Endpoint : Operations for Endpoint

[Show/Hide](#) [List Operations](#) [Expand Operations](#)

GET	/endpoint
POST	/endpoint
GET	/endpoint/{endpoint_id}
PATCH	/endpoint/{endpoint_id}
PUT	/endpoint/{endpoint_id}
DELETE	/endpoint/{endpoint_id}

LocalUser : Operations for LocalUser

[Show/Hide](#) [List Operations](#) [Expand Operations](#)

Role : Operations for Role

[Show/Hide](#) [List Operations](#) [Expand Operations](#)

StaticHostList : Operations for StaticHostList

[Show/Hide](#) [List Operations](#) [Expand Operations](#)

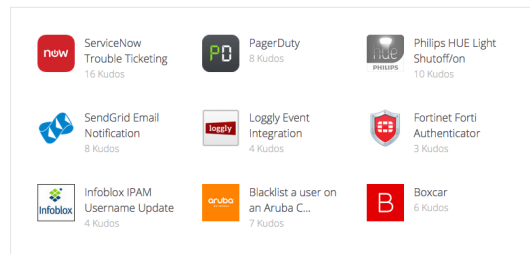
- OAuth2 based client authorization
- Built in API Explorer
- Ability to run inline tests

ClearPass Exchange Recipes

Recipe site and tech note available to help with your integrations:

- Site:
 - <http://community.arubanetworks.com/t5/ClearPass-Exchange-Recipes/tkbc-p/clearpass-recipes>
- TechNotes:
 - http://support.arubanetworks.com/Documentation/tabid/77/DMXModule/512/Command/Core_Download/Default.aspx?EntryId=15508
- Not to be confused with Aruba Solution Exchange
 - <http://ase.arubanetworks.com>

Featured Recipes



```
{ "short_description": "Compromised Device WiFi Connection Attempt", "priority": "3", "description": "The following compromised device has attempted to connect to the cp-secure WiFi network:\nMac Address: ${Connection:Client-Mac-Address}\nEnrolled User: ${Authentication:Full-Username}\nDevice Serial: ${Endpoint:Serial Number}\nMobile: ${Endpoint:Model}\nOS Version: ${Endpoint:OS Version}\nLocation: ${Radius:Aruba:Aruba-Location-Id}", "u_category": "${u_category}", "u_subcategory": "${u_subcategory}", "assigned_to": "mobileadmin" }
```



ANZ atmosPHeRe 2015

HOW TOMORROW MOVES



THANK YOU