Accessing IT Resources Securely, with Single Sign On

okta

Accessing IT resources securely, whether it be user or device driven, continues to be challenging. The number and type of endpoints have grown exponentially, as well as the location and number of IT assets in which to authenticate with. In comparison to 10 years ago, where IT was challenged with BYOD (bring your own device initiatives), IT now has to deal with IOT devices, a rapidly broadening of cloud driven productivity applications (G-suite etc), social media controls, microservices, and video streaming.

Point solution approaches for authenticating and accessing resources for any device, anywhere is an IT troubleticketing nightmare on steroids; the average user cannot easily remember, update and/or protect a multiplicity of user ID's and passwords. They view password management as a nuisance and a productivity blocker.

This new enterprise landscape requires an integrated access management approach where all of the infrastructure and application authentication and authorization elements are managed together as a single sign on workflow, by all different types of endpoints (user and devices). While this is an obvious value proposition, there are many components that require integration, especially between the application and infrastructure layers.

There are a rich number of infrastructure protocols, API's, encryption algorithms, policies, security partitions, and techniques for securing access onto the network (Network Access Control). This nets to SSID's, VLANS, Firewall rules, tunnels with packet encryptions, IP addresses, and port filters. Similarly there are a rich number of application calls for securing access into databases, documents, files, web sites, collaboration tools. These include authentication at a user ID level, where restriction is driven by application ports, sockets, URL's and other layer-7 attributes.

Given these two worlds above, most enterprises use a separate authentication mechanism for Network Access Control (NAC). This mechanism involves a AAA (Authentication, Authorization, and Accounting) server, using RADIUS, to authorize access to resources that are contained/secure within a network construct (VLAN, VXLAN, IP Subnet etc). Admission into a specific network, typically permits reachability to all of the applications that are allowed to communicate within this network. Reachability however does not mean that the user can actually interact within the application as application interactions require another authentication action.

And this is further complicated with the growing number of Cloud hosted applications, and the tunnels required to reach these from within the network. These SaaS offerings require additional network, cloud provider, and application sign ins.

Over the past five years new approaches have been put forward where there is a single sign on (SSO) to access corporate IT resources; several new vendors including Okta are driving a more integrated, end user friendly approach. Rather than authenticating to each individual resource, a single sign-on is leveraged, with one set of credentials (not many). Vendors like Okta handle the authentication to each individual IT resource on the back-end, where as a broker, handle one to many authentication transactions. This significantly reduces account, password, and multi-factor authentications by the end user. Moreover this reduces multiple logins per day, with multiple different ID's and passwords.

These brokers are integrating with both on premise and cloud based infrastructures (networks and applications). For more information regarding Okta's Single Sign On applications please refer to their web site.

Network Access Control Frustration

What has been overlooked by many of these SSO approaches is the integration of NAC with application and web service authentications. For most enterprises, the user, as well as the device they are using, needs to first be authenticated onto the network, and placed into "trust zones" such as a VLAN, or an SSID, before authenticating at the application level with an SSO service. While the network authentication request can leverage the same authorization server, with well-known tunneling protocols such as SAML (Security Assertion Mark-Up Language), the workflow is multi-step as the user needs to authenticate several times, which again is frustrating and error prone.

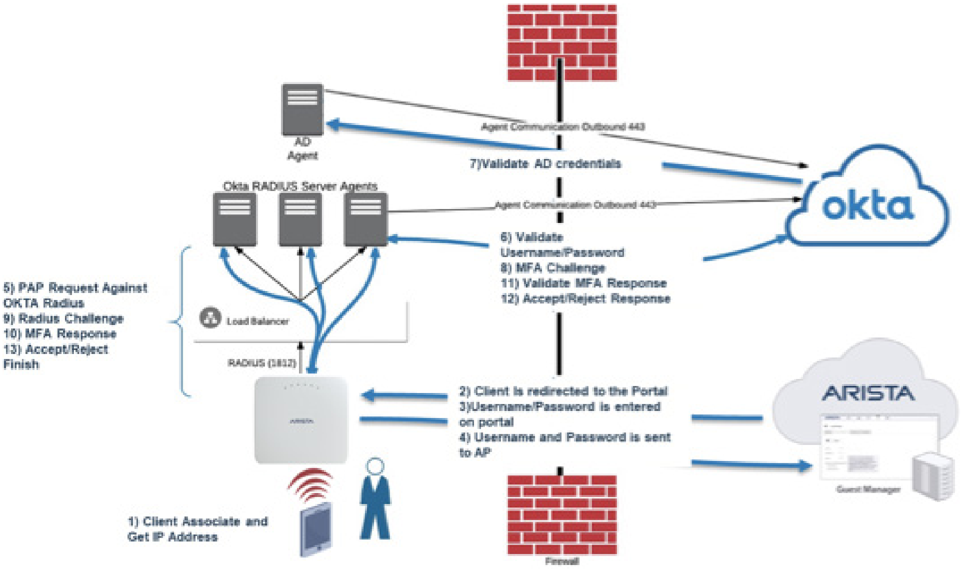
Arista NAC Integration with Okta

Arista has collaborated with Okta in addressing the above where a single set of credentials, can be leveraged concurrently for both being admitted onto the network and their assigned trust zone, as well as authorizing the device/user at the web services and application level. Moreover, Arista has architected this with Okta where the radius services can reside locally, on premise, and or can implemented as full cloud service where both Arista's admission control and Okta's SSO services are hosted within a 3rd party cloud infrastructure.

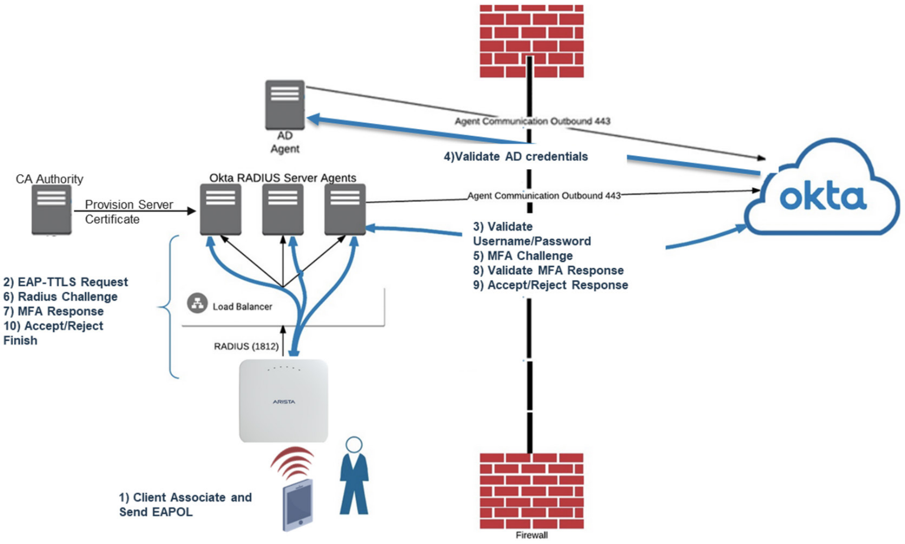
Per the diagrams and workflows below, Arista Cognitive Campus devices (switches and access points) intercept a login request from the end user, and perform a redirect of the client to a Okta provided web based authentication page. Upon credential validation, Okta tells the Arista AP, or Arista switch which network construct to assign this user to, and whether to internet access, while also authorizing access to specific applications and other IT resources. This offers an integrated user experience, with one login action by the end user, typically only once a day (depending on the time out policies configured by the Okta admin).

Currently two client driven approaches are supported with Okta, the first where the IT organization has deployed a clear text PAP (Password Authentication Protocol) based authentication approach, and the second where the IT organization is using a tunnel based encryption, EAP-TTLS (Extensible Authentication Protocol) approach. The integration with Arista WLAN products support both approaches.

PaP Authentication Flow


AD
Agent
Agent Communication Outbound 443
7)Validate AD credentials
Okta RADIUS Server Agents
Agent Communication Outbound 443
okta
6) Validate
Username/Password
8) MFA Challenge
11) Validate MFA Response
12) Accept/Reject Response
5) PAP Request Against
OKTA Radius
9) Radius Challenge
10) MFA Response
13) Accept/Reject
Finish
Load Balancer
RADIUS (1812)
ARISTA
2) Client is redirected to the Portal
3)Username/Password is entered
on portal
4) Username and Password is sent
to AP
ARISTA
Guest Manager
1) Client Associate and
Get IP Address
Firewall

EAP-TTLS Authentication Flow



Conclusion

User simplicity while maintaining trusted security, via single login integration across all infrastructure layers, is essential for enterprises today. Together Arista and Okta offer this solution, leveraging industry standard protocols and open API's. Customers have several different options they can choose based on their authentication framework deployments.

Santa Clara—Corporate Headquarters
5453 Great America Parkway,
Santa Clara, CA 95054

Phone: +1-408-547-5500
Fax: +1-408-538-8920
Email: info@arista.com

Ireland—International Headquarters
3130 Atlantic Avenue
Westpark Business Campus
Shannon, Co. Clare
Ireland

Vancouver—R&D Office
9200 Glenlyon Pkwy, Unit 300
Burnaby, British Columbia
Canada V5J 5J8

San Francisco—R&D and Sales Office 1390
Market Street, Suite 800
San Francisco, CA 94102

India—R&D Office
Global Tech Park, Tower A & B, 11th Floor
Marathahalli Outer Ring Road
Devarabeesanahalli Village, Varthur Hobli
Bangalore, India 560103

Singapore—APAC Administrative Office
9 Temasek Boulevard
#29-01, Suntec Tower Two
Singapore 038989

Nashua—R&D Office
10 Tara Boulevard
Nashua, NH 03062