Technology Partner Program

Use Case Documentation

Author: Okta

Revision History	
May 5, 2020	Initial deployment guide

Table 1: Partner Information	
Date	May 5, 2020
Partner Name	Okta
Website	www.okta.com
Product Name	Okta Identity Cloud – SSO and MFA
Partner Contact	Alex Rich, Sr. Manager – Strategic Alliances, arich@okta.com, 415-683-5478
Support Contact	support@okta.com
Partner Product for Integration	Okta SSO and MFA
Product Description	The Okta Identity Cloud makes it easy for organizations to securely connect their users with the resources they need to do their job, seamlessly and securely. Okta centralizes access to SaaS apps, WAM and custom web apps, APIs and infrastructure all in one unified interface, making it easy for end users to sign in with one set of credentials to access all of the resources they need to be productive, wherever and on whatever device they choose. Administrators can assign resources relevant only to that user's role and set access policies based on role, the resource he/she is trying to access as well as risk signals from the device, network, geography, etc. to prompt for a second factor or, if risk is determined to be low, allow for a passwordless experience. Finally, Okta can centralize user stores from on-prem systems like AD or LDAP and HR systems like Workday and automate on/offboarding of applications—saving admins time and reducing the risk of manual provisioning and deprovisioning processes.

Table 2: Palo Alto Networks Products for Integration			
Palo Alto Networks Product	**Integration Status**	**Palo Alto Networks Versions Tested**	**Okta Versions Tested**
AutoFocus			
Cortex Data Lake			
Cortex XDR			
GlobalProtect	Validated	PAN-OS 9.0	SSO and MFA – August 2019
IoT Security			
Prisma Access	Validated	Prisma Access 1.5 (March 2020)	SSO and MFA – August 2019
Prisma Cloud			
MineMeld			
Next-Generation Firewall	Validated	PAN-OS 9.0	SSO and MFA – August 2019
Panorama	Validated	PAN-OS 9.0	SSO and MFA – August 2019
VM-Series			
WildFire			
Other			

Use Cases for Integration with the Palo Alto Networks

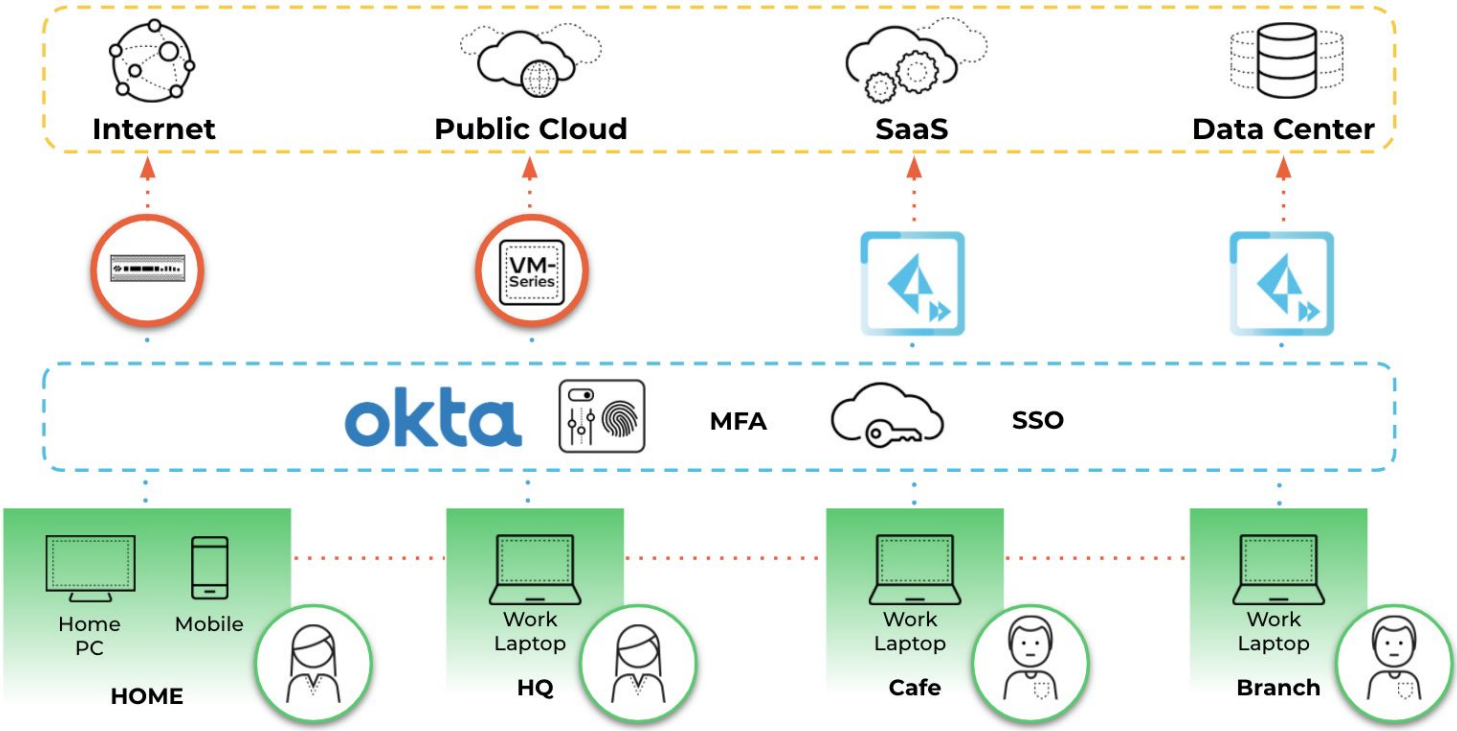
- Deep integration between Okta and Palo Alto Networks for robust, user-centric security across your hybrid IT environment for all users, including partners and contractors
- Strong authentication for additional access security across hybrid IT environments through Okta Adaptive Multi-Factor Authentication (MFA)
- Seamless authorized access to cloud assets through Okta Identity Cloud and on-prem assets through Palo Alto Networks GlobalProtect™ VPN
- Simple and intuitive authentication for all users everywhere with Okta Single Sign-On (SSO)

Integration Benefits

- Okta + Palo Alto Networks provides a complex, multilayered defense against credential-based attacks.
- Remote users enjoy seamless Okta SSO for cloud apps as well as on-prem resources thanks to Palo Alto Networks Prisma™ Access.

  IT can further secure access through Okta Adaptive MFA, easily meeting compliance requirements and security best practices.
- Administrators can easily and securely access the Palo Alto Networks admin console.
- Integration is easily deployed, using SAML, RADIUS, or APIs, for Palo Alto Networks Prisma SaaS, Captive Portal, and admin UI.

Integration Diagram



Before You Begin

- Customers must have an Okta tenant and be on PAN-OS® 8.1 or later.

Palo Alto Networks and Okta Configuration by Use Case

Prisma Access and GlobalProtect

Prisma Access SAML Authentication Using Okta as IdP for Mobile Users
https://docs.paloaltonetworks.com/prisma/prisma-access/prisma-access-panorama-integration/authenticate-mobile-users/saml-authentication-using-okta-as-idp-for-users

SAML Integration with GlobalProtect
https://saml-doc.okta.com/SAML_Docs/How-to-Configure-SAML-2.0-for-Palo-Alto-Networks-GlobalProtect.html

RADIUS Integration with GlobalProtect
https://help.okta.com/en/prod/Content/Topics/integrations/palo-alto-radius-intg.htm

- Note: MFA can be enforced via SAML or RADIUS for this use case.

Authentication Policy

Using SAML

https://docs.paloaltonetworks.com/pan-os/9-1/pan-os-admin/authentication/configure-saml-authentication.html

Using RADIUS

https://docs.paloaltonetworks.com/pan-os/9-1/pan-os-admin/authentication/configure-radius-authentication.html

https://help.okta.com/en/prod/Content/Topics/integrations/palo-alto-radius-intg.htm

Using API Integration (MFA Server Profile)

https://docs.paloaltonetworks.com/pan-os/9-1/pan-os-admin/authentication/configure-multi-factor-authentication/configure-mfa-between-okta-and-the-firewall.html#id185NH00C0GA_id185NH030I4I

Creating Authentication Policy

https://docs.paloaltonetworks.com/pan-os/9-1/pan-os-admin/authentication/authentication-policy/configure-authentication-policy.html#id0ff4d899-df86-4f6f-905e-e7b86c938203

- Note: MFA can be enforced via SAML, RADIUS or Okta API for this integration use case.

Administrator Authentication to NGFW and Panorama

Using SAML (UI Only)

https://saml-doc.okta.com/SAML_Docs/How-to-Configure-SAML-2.0-for-Palo-Alto-Networks-Admin-UI.htm

https://docs.paloaltonetworks.com/pan-os/9-1/pan-os-admin/authentication/configure-saml-authentication.html

Using RADIUS (UI and CLI)

https://docs.paloaltonetworks.com/pan-os/9-1/pan-os-admin/authentication/configure-radius-authentication.html

https://help.okta.com/en/prod/Content/Topics/integrations/palo-alto-radius-intg.htm

- Note: MFA can be enforced via SAML or RADIUS for this use case.

Troubleshooting

Common troubleshooting steps

- Troubleshooting documentation: https://help.okta.com/en/prod/Content/index.htm

Contact Information for Support

- https://support.okta.com/help/s/