Case Study

Symantec
A Division of Broadcom

IAM and IdP for Zero Trust Network Access to Corporate Applications

Introduction

An international enterprise communications technology vendor, headquartered in New York and running operations in eight offices across USA, EMEA, and APAC, is working in a hybrid data center environment.

The company is adopting Software-as-a-Service (SaaS) solutions for various business applications, while also investing in mission critical control, automation, and analytics systems that are hosted on-premises and in their Identity-as-a-Service (IaaS), cloud-based data centers.

Corporate employees, regardless of their department, need to use both SaaS and self-hosted tools during their daily tasks.

The tools must be accessible both from corporate offices and to remote employees in a seamless manner, allowing the employees to continue working from managed devices without compromising their mobility.

Duplicate Access Policies

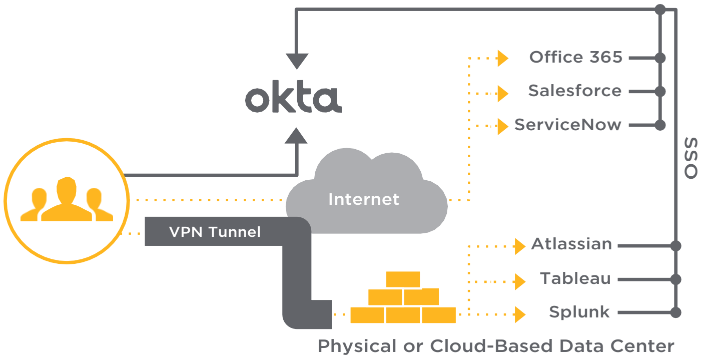
The corporate IT security department was using Okta's IaaS solution to control access to their SaaS resources, but when it came to resources hosted in the corporate data centers or in IaaS, they needed to rely on VPN for connectivity. The users had to be aware of where each application is hosted and then manage their access accordingly.

While some of the internal, self-hosted applications were also integrated with Okta, accessing them from outside the corporate offices required using a traditional Remote Access VPN. The result was a cumbersome access mechanism and poor user experience for the users, driving inefficiency in daily operation.

The IT security department needed to maintain VPN/Firewall policies that duplicate the logical access defined in Okta for the network-level access provided by the Remote Access VPN solution.

The Challenge

Onboarding of new services required updates to both policies, adding costs and extending time-to-market of the daily IT and security operation. All corporate applications were configured for single sign-on with Okta, including both the SaaS and the self-hosted ones.



The schema above shows the previously deployed access control mechanism. The identity and access policy in Okta was arranged similar to the following:

- User Group 1: Office 365, SalesForce, Tableau
- User Group 2: Office 365, ServiceNow, Atlassian, Splunk
- User Group 3: Office 365, Atlassian, Splunk
- User Group 4: Application

Naturally, this is a simplified schema of the company's architecture, as it was deploying close to 100 SaaS and self-hosted applications and numerous organizational groups through their IdP.

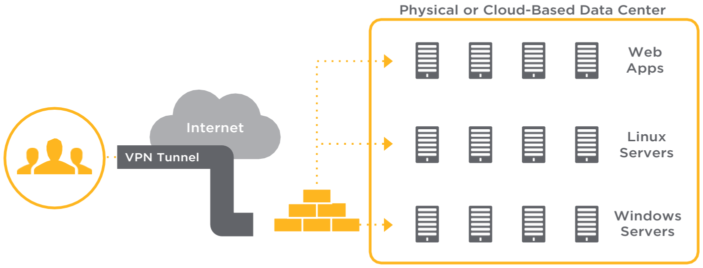
Providing connectivity to the self-hosted applications, the Firewall Policy on the Remote Access VPN solution looked like the following:

- Group 1: Subnet of Tableau Servers
- Group 2: Subnet of Atlassian Servers, Subnet of Splunk Servers
- Group 3: Office 365, Atlassian, Splunk
- Group 4: Application

The company also had self-hosted resources that were not integrated with Okta SSO, such as the following:

- Web Applications
- Linux Servers (SSH access)
- Windows Servers (RDP access)

To provide access to these resources, the IT and Security operations department managed dedicated access policies at the Remote Access VPN level for the relevant parties, as shown in the following figure:



To allow such access while not compromising on the security of corporate resources, only managed devices with endpoint agents could access the applications. As a result, the IT operations department, and particularly the user help desk, spent a lot of time deploying and maintaining VPN agents on endpoint devices.

Exposing the Corporate Data Center to a Range of Network Attack Risks

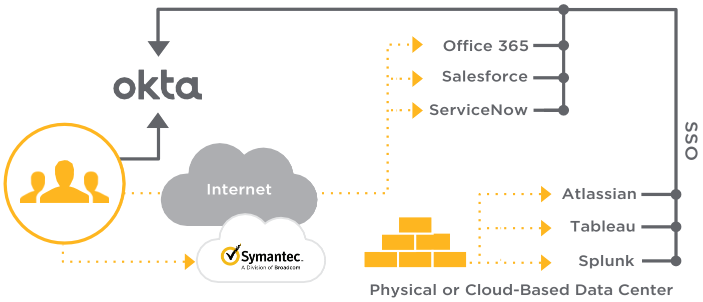
While the IT and Security operations department wished to maintain tight control over access policies and practices, the DevOps and R&D teams continued deploying new services that were needed for their daily operation.

As a result, the IT and Security department was always challenged with the need to grant secure access to the new applications in a timely manner, in order not to slow down the business or risk exposing the network by the quick-to-deploy DevOps team.

Over time, due to the overhead of managing a tight, per-resource access policy, and as the network topology and infrastructure grew and expanded, the access policy turned into network-level access, based on complete subnets/data centers rather than resources-based.

The Symantec® ZTNA Solution

To solve both the department challenges and the user experience, the company choose Symantec Secure Access Cloud™ to replace their Remote Access solution for the self-hosted resources, both in their physical data centers and the IaaS VPCs. The deployment took less than a week. The resulting architecture looked like the following:

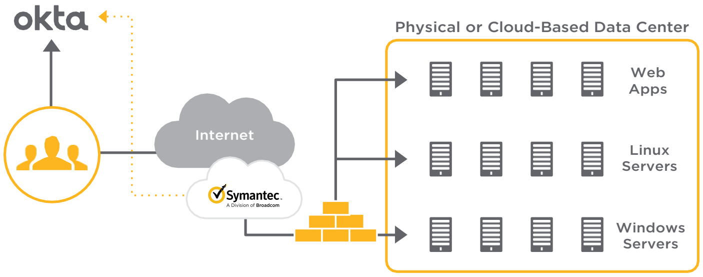


By integrating Symantec Secure Access Cloud with the corporate Identity and Access Management (in this case, Okta), the IT and Security operations could now manage all their access policies with a single point of control.

The firewall's function changed from being the complex and expensive access management solution, on the network topology level, to a data center security component. It's only responsible for blocking inbound traffic into corporate networks with a simple static policy that doesn't change every time new applications or services are being deployed in one of the corporate data center locations.

Symantec Secure Access Cloud does not require any inbound communications to be accepted by the data center firewalls. In fact, all the communication is done with a reverse proxy, connecting the applications to the trusted users instead of allowing inbound communication from the users to the applications. In order to broker connectivity to self-hosted resources, the platform requires lightweight cloud-native connectors to be deployed in every subnet hosting the corporate resources (or in utility subnets that have routing to other subnets).

The administrators could now also provide access to resources that were previously controlled only on the network level, managing the access policy on the logical "Role Resource" level in the Okta IAM policy:



With the above configuration, the Okta IAM policy has been extended to provide access to resources that were previously governed by VPN/Firewall:

- **Windows Server Administrators:** Windows Domain Servers, Windows SQL Server
- **DevOps for Project X:** Linux Servers of Project X
- **RND for Project Y:** Linux Servers of a Staging environment for Project Y

Summary and Benefits

Okta Identity and Access Management has turned into the authoritative policy for accessing all of the company's IT resources. The efforts associated with maintaining access policy on the network level with the Firewall/VPN solutions were made redundant, saving on many man-hours in the process. It also made auditing on corporate access policies into a very straightforward and easy process.

The direct outcome of integrating Symantec secure access with the Okta's single point of control is a full Zero Trust Access to the company's data centers:

- **Cloaking:** No network-level exposure of the data center and its networks to unauthorized parties
- **Authentication and validation:** Before gaining access, the user must be authenticated, the device posture must be checked, and the application must be confirmed
- **Identity-based access:** All access is managed with Okta-governed Identity and Access Policies, regardless of the type of resource and its location
- **Least-privileged access:** Access is given on application-level functionality, with no privileges in the data center networks
- **Always verify:** Every step performed by an accessing party (URI in HTTPS request, SSH command, and so on) gets logged and can be audited and governed on the application level (and not on the network level)

Symantec, a division of Broadcom, enables security and IT teams to create Zero Trust Application Access architecture without traditional VPN appliances. Symantec Secure Access Cloud securely connects any user from any device, anywhere in the world to corporate on-premises and cloud-hosted applications while all other corporate resources are cloaked. No network access is ever granted to prevent any lateral movements to other network resources while eliminating the risk of network-based attacks. The platform is agentless and can be deployed in less than five minutes, without forcing a disruptive change in the organization's existing architecture, user permissions, and applications. Symantec Secure Access Cloud provides full governance and real- time enforcement of users' actions in each corporate application.

Symantec™
A Division of Broadcom

For more product information: broadcom.com

Copyright © 2021 Broadcom. All Rights Reserved. The term "Broadcom" refers to Broadcom Inc. and/or its subsidiaries. All trademarks, trade names, service marks, and logos referenced herein belong to their respective companies.

SYM-ZT-IAM-IdP-CS100 November 10, 2021