Extend IdP/IAM to Provide ZTNA to Hosted Resources

Having an organizational Identity and Access Management (IAM) solution is a critical first step in creating Zero Trust Network Access (ZTNA) to all corporate applications, services, and workloads. The next step would be to use an Identity Provider (IdP) to replace network firewalls, VPNs, and DMZs providing secure access to various resources hosted in corporate on-premises data centers, as well as in co-location, IaaS, and PaaS.

Overview

The Zero Trust model for access is based on the following principles:

- **All resources are cloaked:** There is no mechanism that allows discovery and it is not possible to connect to a resource prior to authentication and authorization. This assumes that no public IP addresses or open ports will accept connections.
- **Authentication and authorization prior to connection:** IT resources will not accept network connections and then try to authenticate the connecting parties. Instead, only relevant, approved connections will reach the protected resources.
- **Security posture of all accessing parties' devices:** The system assesses the accessing party's device before allowing or withholding access to the system.
- **Application-level connectivity:** Network connectivity should never be provided. Accessing parties will only be allowed to use the required functionality and will not be able to leverage any other resource on the network level.
- **Trust no one:** Even after providing the application-level access to relevant resources for authenticated and authorized parties using devices compliant with the corporate policy, the connections should not be trusted. Every action performed by the accessing party must be analyzed, audited, and, if it's considered risky or dangerous, it should be subjected to a granular contextual security policy.

A Clear Path to Zero Trust Practice

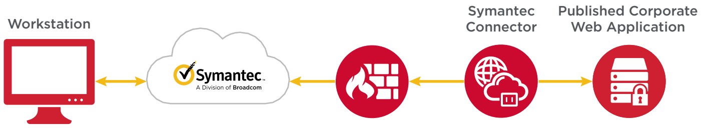
Symantec® Secure Access Cloud collaborates with any Identity Provider solution to create the next-generation access fabric. By sticking to the following six steps, you can implement Zero Trust Network Access on all servers, applications, and workloads—hosted in the cloud and on-premises.

Step 1: Deploy Secure Access Cloud Connectors in Locations Hosting Your Resources

Symantec Secure Access Cloud provides brokered access to corporate resources by proxying all access sessions. The brokered access is carried out through cloud-based points of delivery, as well as through locally deployed Symantec connectors.

The connector is a lightweight software agent that can run as a Docker container. It can be deployed on Linux or Windows servers supporting Docker Engine, or in various container orchestration environments, such as Kubernetes, Elastic Container Service, Mesosphere, and more.

The basic architecture would look like this:



The connection between the user's device and the published IT assets works in the following way:

1. The Connector, deployed at the same location as the asset, is capable of accessing the assets via IP Routing. It initiates the connection to Secure Access Cloud over standard TCP Port 443.
2. The user accesses the asset's external address, for example, https://mybusinessapp.mycompany.com or https://mybusinessapp.mycompany.luminatesec.com
3. Symantec Secure Access Cloud uses the IdP to perform authentication, verification of device security posture, and authorization, and then brokers the authorized connections via the connector to the relevant assets.

Step 2: Prevent Unauthorized Network Access to Your Resources

All resources should be cloaked and network access to relevant exposed services (HTTP/HTTPS, SSH, RDP, and so on) should be allowed only from the Symantec Connectors.

The environment security structure will not be considered a Zero Trust one until this step is completed.

The restriction of access could be achieved either by traditional network firewalls, or by specialized virtual firewalls in software-defined data centers, such as VMWare or OpenStack (on-premises), or Amazon Web Services, Microsoft Azure, or Google Cloud. Alternatively, host-based firewalls, such as IPTables or Uncomplicated Firewall on Linux Servers or Windows Firewall on Windows Servers.

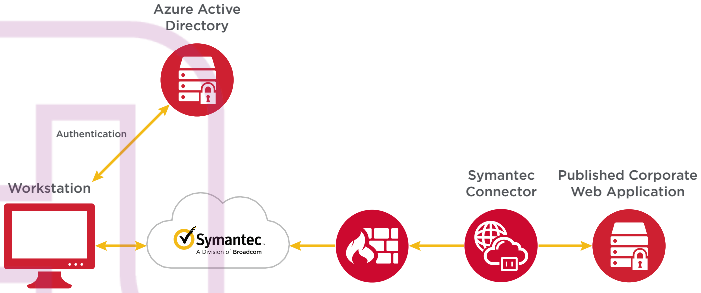
Ensuring that only Symantec Connectors can open network connectivity to the IT assets will guarantee access is governed by identity-centric Zero Trust Network Access policy.

Step 3: Connect Symantec Secure Access Cloud to Your IdP

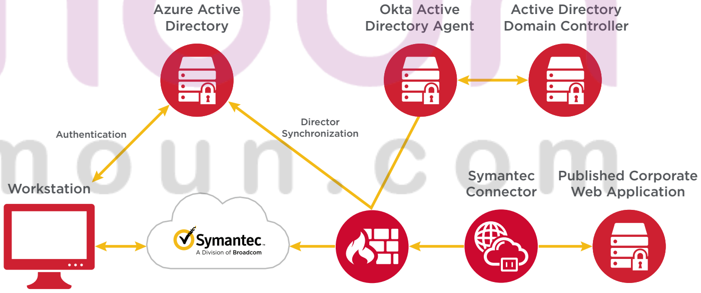
Symantec Secure Access Cloud integrates with Identity Management solutions, providing the following capabilities:

- Authenticate users attempting to access IT resources via Symantec
- Enforce multi-factor authentication (MFA), conditional access policy, and device security posture, per IdP definitions for all access cases
- List the users and groups that are defined in the IdP and build Zero Trust access policies using these
- Audit all actions performed by users while accessing corporate resources, tying the operations to the unique user identity in the IdP

A sample architecture with Symantec using cloud-based IDaaS service (such as Okta, Ping Identity, Microsoft Azure Active Directory, and so on) would look like this:



Symantec can also work in hybrid environments with on-premises-based Identity Providers, either partially synchronized to IDaaS or offering local authentication proxies:



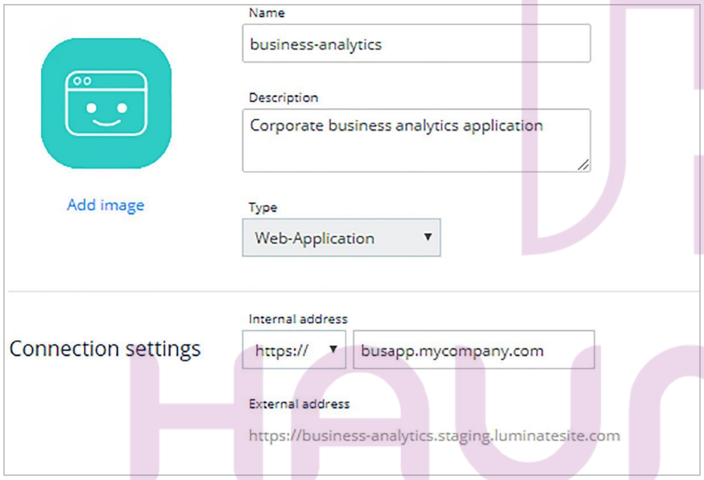
The on-premises Active Directory IdP can synchronize with a cloud-based IDaaS using a local agent. It is also possible to use an on-premises proxy (such as Microsoft Active Directory Federation Services) that provides federated authentication capabilities. The integration between Symantec Secure Access Cloud and various IdP solutions is a straightforward configuration task that can be completed within minutes.

Step 4: Define Your Resources with Symantec Secure Access Cloud

Configuring various resources for access via Symantec is a straightforward task that requires the following:

- Internal address: A DNS address that can be resolved by the Symantec connector or a routable IP address and accessible port that can be used by the Symantec connector to reach the selected resource that is being defined.
- External address: A DNS address for users to access the resources from anywhere. The external address can be allocated under the company's domain or under a different domain.

See the following definition of an internal business intelligence portal/ application:



Name: business-analytics

Description: Corporate business analytics application

Type: Web-Application

Connection settings

Internal address: https:// busapp.mycompany.com

External address: https://business-analytics.staging.luminatesite.com

Step 5: Define Your Access Policy

The access policy should be defined on high-level terms. There are no networks, IP addresses, or ports involved in the policy. It is just a logical mapping of the following:

users/groups > access governance rules > resources/resource groups

The notion of Zero Trust implies that any access should always follow the principle of least privilege. A user should get access only to resources that are absolutely necessary for performing one's duties and nothing more. The user should also have the ability to perform operations that are necessary for their job and no more. In advanced access solutions, such as Symantec, such policies can be governed by the access governance rules.

This applies to a wider range of access scenarios than the traditional Privileged Access Management/Privilege Session Management products, where all operations of the accessing party are monitored and controlled.

The access governance rules can define the following:

- A user can download large chunks of data (and under what conditions), or only access certain portions
- A user can perform specific wide-impact operations
- A user can change certain configuration properties

The conditional access policies that are defined on the IdP level can outline the following authorization factors for various users/groups:

- The types of devices that can be used for accessing the resources
- Geographical locations/networks that the accessing party can reside in
- The days and hours when access is allowed

A combination of conditional access, user/group assignment to resources, and access governance rules provides organizations with the ability to express the Zero Trust access requirements to all IT resources.

Step 6: Audit and Govern Activities on the Identity Level

Once the ZTNA solution is deployed, and the access policy is set, the user's activity when accessing corporate resources should be audited and the access governance should be validated as the mechanism that provides the correct access level to the relevant role players. Periodic review of access/security events should lead to further tightening of the access policies, targeting even better focused access.

The following are events that should require attention:

- Users who are assigned access to certain resources, but don't access them
- Users who sign in after a long absence
- Devices that have been used by certain users and are now being used by other users
- Consequent failed login attempts
- Attempts to perform operations not allowed by the access governance rules

Advanced access solutions allow configuring automated responses for such events, simplifying the governance. Such systems could either respond to the events internally or trigger orchestrated processes, using either next-generation SIEM solutions or security automation and orchestration solutions.

Summary and Benefits

Deploying Zero Trust Network Access instead of using traditional access and control solutions, such as network firewalls and VPNs, will have the following benefits:

- Simplification and better audit-ability of organizational access policy
- Reduction of network attack surface in the IT infrastructure
- Improvement of effectiveness in IT and security operations processes

Identity and Access Management is an important foundation for Zero Trust in the organization. Combining an existing IdP/IAM solution with a Zero Trust Network Access solution can be deployed gradually through six simple steps and can lead to a much simpler and more secure access architecture.

Symantec Secure Access Cloud

Symantec 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 direct 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