

# CHECK POINT IDENTITY AWARENESS APPLICATION AND ACCESS CONTROL



## Maintain Control through Accurate, Identity-Based Policies

### Benefits

- Dynamic user-based policy simplifies security administration
- User to IP mapping augments traffic monitoring
- Multiple identity connectors facilitate deployment in large and small customer environments
- Increased visibility of user activities with a dynamic user-based policy
- Prevents unauthorized access, while still allowing legitimate user access
- Easy to deploy on any Check Point gateway and integrates with leading identity vendors

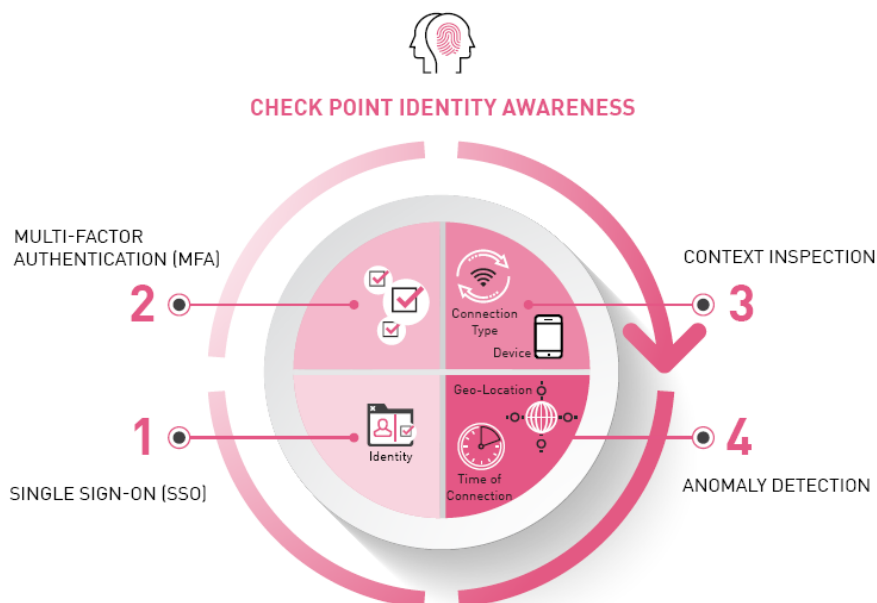
## THE IMPORTANCE OF ACCESS ROLES

Role-based access control (RBAC) authorizes requests for network access based on an individual's defined role. Practicing RBAC results in employees only having access to the information they need to perform their job duties. For example, access to sensitive data is only granted to employees in an organization who require this information in order to perform their specific job duties.

Employing RBAC improves operational efficiency and compliance. When an employee changes job positions, their access to data can be changed with a simple role switch. With clear roles defined, the IT department can clearly see and ensure that only approved roles are accessing sensitive data. Unfortunately, identities and devices are easily compromised. According to Verizon DBIR, 81% of data breaches involve stolen credentials. Security professionals are responding to these threats by shifting to a zero trust security approach where no device, user, workload, or system is trusted by default.

## TRUST NO USER OR DEVICE

Check Point Identity Awareness seamlessly integrates with leading IAM (Identity and Access Management) vendors to ensure access is only granted to authorized users from devices verified to be secure using anomaly detection and context-aware policies. Multi-factor authentication, identity agents and user to IP address mapping from trusted third parties verify the identity of the user and add context to verify the user is connecting from a trusted device.

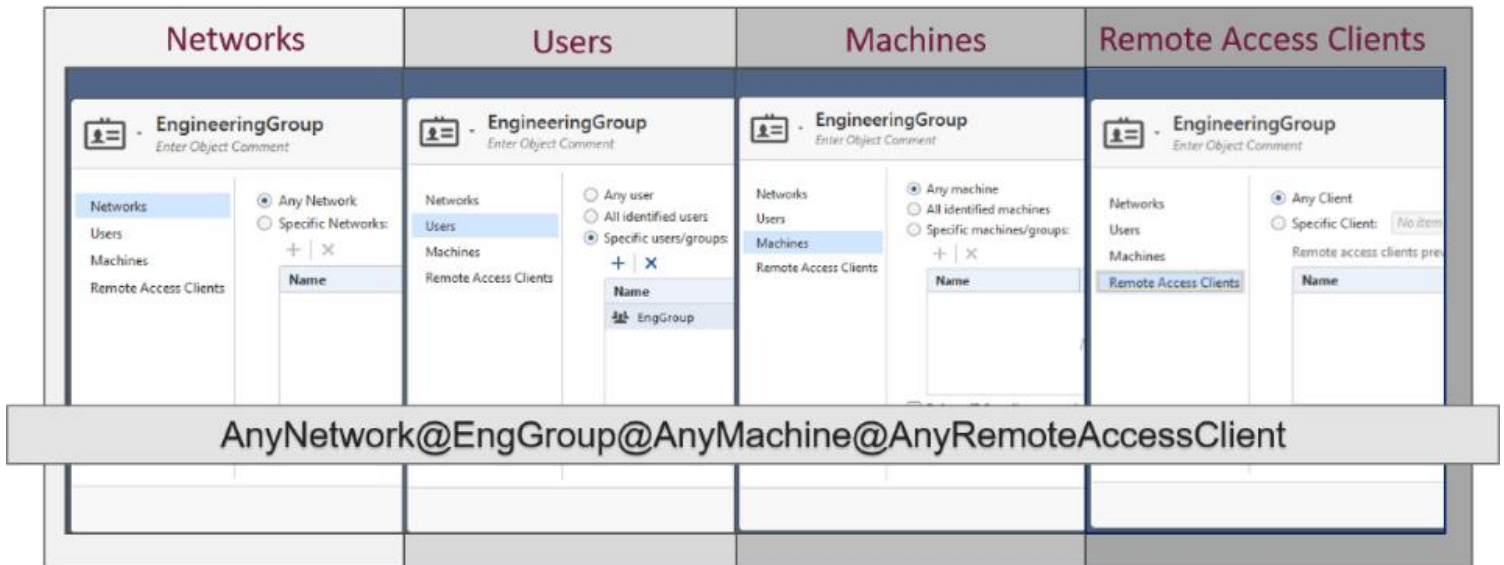


## Dynamic, User-based Policy

Dynamic, identity-based policy provides granular visibility and control of users, groups and machines and is easier to manage than static, IP-based policy. In a single, unified console administrators define the objects once. When gateways see a connection for the first time, the IP is mapped to the user and group by querying the third party user directory. This dynamic user to IP mapping frees administrators from constantly updating the Check Point policy.

## Configurable Access Roles

With Identity Awareness, you can easily add users, user groups, and machine identity intelligence to your security defenses. Unlike traditional firewalls that only use IP addresses to monitor traffic, Identity Awareness monitors traffic while giving your organization insight into user and computer identities. Access Role objects can include networks, users and user groups, machines and machine groups, as well as remote access clients.



The screenshot shows the configuration interface for an 'EngineeringGroup' object. It is divided into four columns: Networks, Users, Machines, and Remote Access Clients. Each column has a 'Name' field and a list of objects. The 'Users' column has a 'Name' field containing 'EngGroup'. A central banner displays the resulting policy expression: **AnyNetwork@EngGroup@AnyMachine@AnyRemoteAccessClient**.

## Multiple User Identification Sources

Identity Awareness is comprised of multiple identity connectors that obtain identity from a variety of sources.



Terminal Servers	Identities are acquired using agents installed on a Windows-based application server that hosts Terminal Servers, Citrix XenApp, and Citrix Xen Desktop services. These agents identify individual user traffic coming from Terminal Servers.
Identity Agents	Identities are acquired using agents that are installed on the Endpoint computers.
Active Directory Query	Identities are acquired seamlessly from Microsoft Active Directory WMI API.
RADIUS Accounting	Identities are acquired from a RADIUS accounting client.
Identity Collector	Identities are acquired using a multi-purpose agent installed on a Windows host. The agent uses APIs to connect to Microsoft Active Directory Domain Controllers, Cisco ISE servers, and NetIQ eDirectory LDAP servers. The agent can also parse syslog messages to extract identities from a syslog message.
Identity Web API	Gives you a flexible method for creating identities and easily perform third party integrations.

## Identity Collector

Identity Awareness maps users and computer identities, allowing you to enforce access and audit data based on identity. The Check Point Identity Collector agent installed on a Windows host acquires identities from: Microsoft Active Directory Domain Controllers via the Windows Event Log API, Cisco Identity Services Engine (ISE) servers via the pxGrid API, and can parse identities from syslog and integrates with NetIQ eDirectory.

## Browser-Based Authentication

Another feature of Identity Awareness is the use of browser-based authentication. Identities from unidentified users can be acquired through Captive Portal and Transparent Kerberos Authentication. Captive Portal is a simple method that attempts authentication through a web interface before granting a user access to Intranet resources. Transparent Kerberos Authentication is when a browser attempts to authenticate users transparently by retrieving identity information before a Captive Portal sign-on page pops up. When Transparent Kerberos Authentication is enabled, Captive Portal requests authentication data from the browser itself. If this transparent method is unable to authenticate, then a user must enter their credentials in the Captive Portal sign-on before accessing the resources.

## Identity Sharing

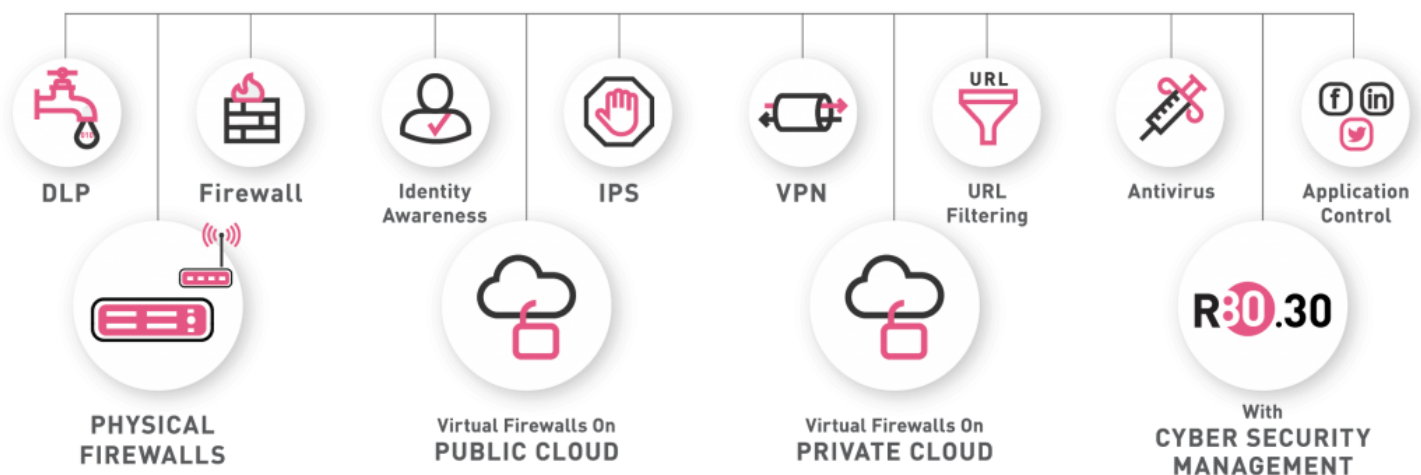
Identity Aware Security Gateways can share the identity information that they acquire with other Identity Aware Security Gateways. Users who need to pass through many Security Gateways are only identified once, without creating additional load on the identity sources or interfering with a streamlined end-user experience.

## Data Center Integrations

Check Point CloudGuard Controller, Identity Awareness and Check Point security gateways integrate seamlessly within the following virtual cloud environments: Amazon Web Services (AWS), Microsoft Azure, Cisco ACI, Cisco ISE, Google Cloud Platform (GCP), Nuage Networks VSP, OpenStack, VMware vCenter and VMware NSX. CloudGuard Controller scanner periodically polls objects in the data center. The scanner then updates the management server data center objects and Identity Awareness enabled gateways to enforce the security policy.

## Tightly Integrated Security Ecosystem

Identity Awareness is integrated into the consolidated Check Point Infinity Architecture that protects customers from sophisticated Gen V mega-cyber-attacks. It can be easily and rapidly deployed on existing Check Point Security Gateways and seamlessly integrates with multiple identity sources.



### CONTACT US

**Worldwide Headquarters** | 5 Shlomo Kaplan Street, Tel Aviv 67897, Israel | Tel: 972-3-753-4555 | Fax: 972-3-624-1100 | Email: [info@checkpoint.com](mailto:info@checkpoint.com)  
**U.S. Headquarters** | 959 Skyway Road, Suite 300, San Carlos, CA 94070 | Tel: 800-429-4391; 650-628-2000 | Fax: 650-628-2117 | [www.checkpoint.com](http://www.checkpoint.com)