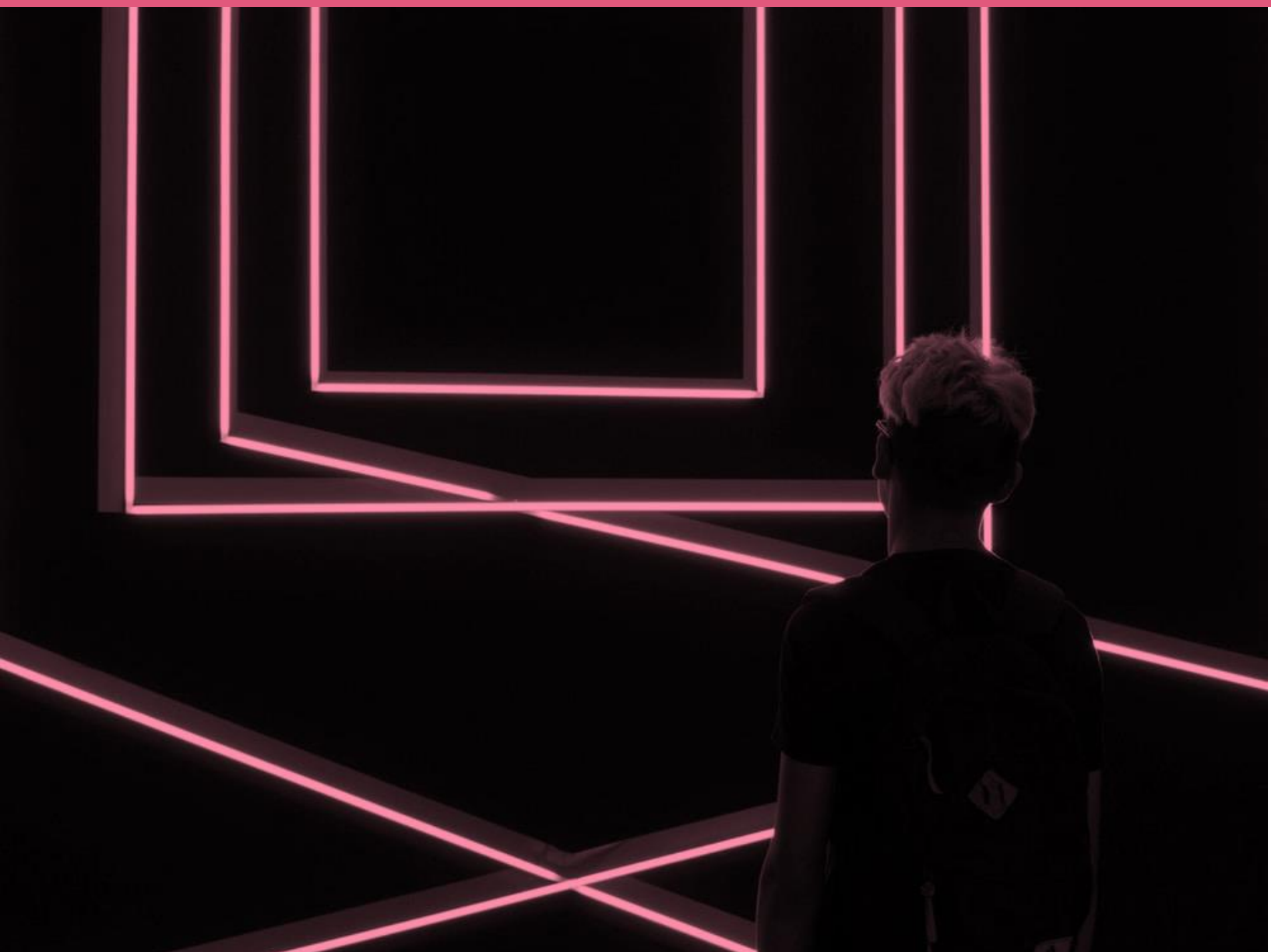
Check Point
SOFTWARE TECHNOLOGIES LTD

Identity Awareness in Multi-Domain environment for R80.30 and early versions

Best Practices



THE SCOPE OF THIS DOCUMENT

This document is focused on a scenario of enforcing identity-based policies on security gateways running version R80.30 and earlier in a Multi-Domain environment.

It specifically provides recommendations and describes procedures how to enforce identity-based policies for users from other Management Domains.

To learn more about Identity Awareness see the *Configuring Identity Awareness* https://sc1.checkpoint.com/documents/R80.30/WebAdminGuides/EN/CP_R80.30_IdentityAwareness_AdminGuide/62050.htm and other related materials.

CHALLENGES OF USING IDENTITY AWARENESS IN A MULTI-DOMAIN ENVIRONMENT

Security gateways managed by a single Management Server can easily share users' identities with each other. However, in a Multi-Domain environment every Domain Server has its own Internal Certificate Authority. Security gateways from different Management Domains cannot establish Secure Internal Communication by default. Therefore, they fail to communicate each other and share identities.

Establishing Trust in a Multi-SIC Environment is possible but the procedure is complex and scales poorly.

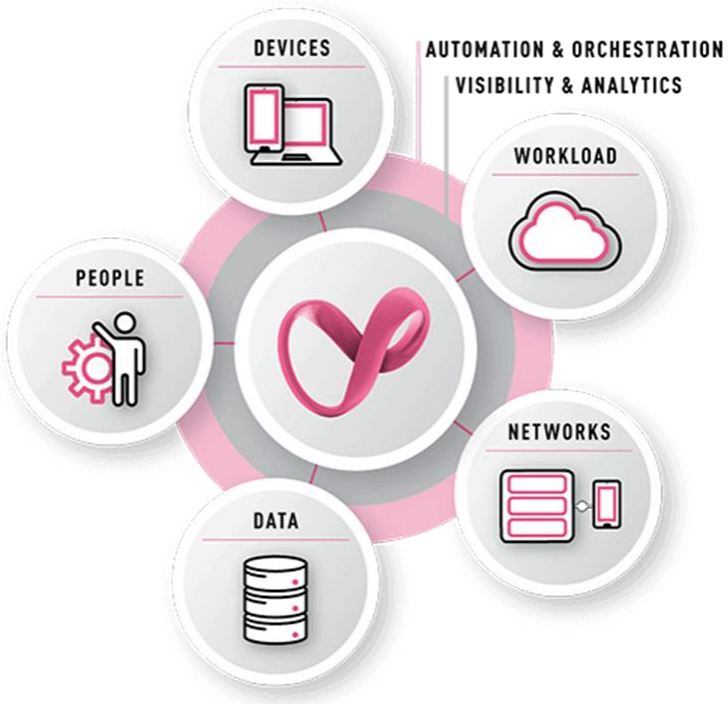
Another challenge is SMB appliances with R77.20 version, which require special efforts to process identities acquired by Identity Collector.

IDENTITY IN ZERO-TRUST ENVIRONMENTS

Cyber threats exist within and outside of the traditional secure enterprise perimeter. In 2018, 34% of cyber-attacks were perpetrated by insiders. In the face of this reality, legacy perimeter-focused security approaches have become ineffective. The outdated assumption that everything inside the security perimeter can be trusted leaves organizations exposed.

A new security paradigm closes these security gaps. Across the industry, security professionals are shifting to a Zero Trust Security state-of-mind: no device, user, workload or system should be trusted by default, regardless of the location in which it operates from, neither inside or outside of the security perimeter.

Verifying users (people) is one of the five pillars of the Zero Trust model. With 81% of data breaches involving stolen credentials, it is clear that username and passwords no longer prove the identity of a user. Identities are easily compromised, so access control to a business's valuable assets must be strengthened.

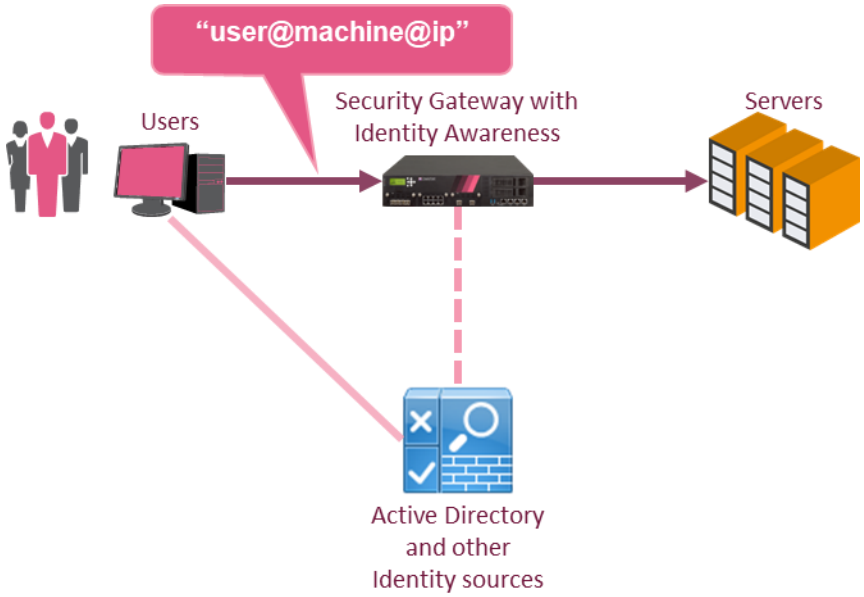


The Forrester Zero Trust Extended Security Model

IDENTITY AWARENESS OVERVIEW

Traditionally, firewalls use IP addresses to monitor traffic and are unaware of the user and computer identities behind those IP addresses. Identity Awareness removes this notion of anonymity since it maps users and computer identities. This lets the administrator enforce access and audit data based on identity.

Critically, Identity Awareness is an easy to deploy and a scalable solution. It is applicable for both Active Directory and non-Active Directory based networks, as well as for employees and guest users.



Identity Awareness illustration: AD Query

Furthermore, Identity Awareness uses the Source and Destination IP addresses of network traffic to identity users and computers. These elements can be used as matching criteria in the Source and Destination fields of a policy's rules:

- The identity of users or user groups
- The identity of computers or computer groups

Identity Awareness lets the administrator define policy rules for specified users, who send traffic from specified computers or from any computer. In addition, policy rules can be created for any user on specified computers, i.e. access roles combines Network, User group, Machine ID (OU).

Source	Destination	Services & Applications	Content	Action	Track
Any	Internet	Critical Risk	Any	Drop	Log
Any	Internet	Any	Any	Drop	None
roleMarketing	Internet	Media Streams	Any	Accept (display captiv	Log Accounting
roleCorpUsers	Internet	Violence Games	Any	Drop	Log
roleCorpUsers	Internet	Any	Any	Accept	Log Accounting
roleTechSupport	Any	Remote Administration	Any	Accept	Log

Rule base example

Logs can be seen based on user and computer name, and not just IP addresses.

Every Check Point Security Gateway need to know identities (users) and their associated IP addresses for identity enforcement. Identity Awareness gets identities from the configured identity sources.

Identity sources options

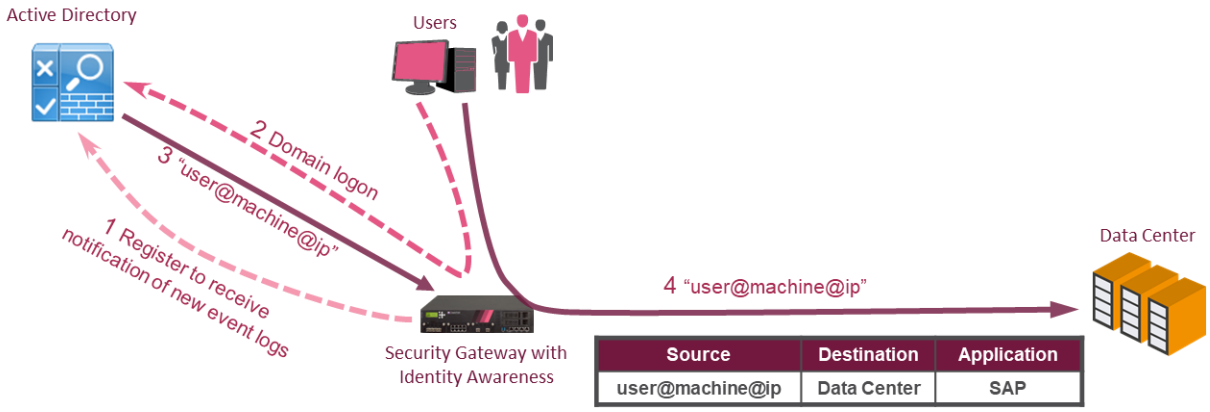
AD Query identity source example

AD Query is an easy to deploy, clientless identity acquisition tool. It is based on Active Directory integration, and it is completely transparent to the user.

AD Query works when:

- An identified user or computer tries to access a resource that creates an authentication request. For example, when a user logs in, unlocks a screen, shares a network drive, reads emails through Exchange, or uses an Intranet portal.
- AD Query is selected as a way to acquire identities.

The technology is based on querying the Active Directory Security Event Logs and extracting the user and computer mapping to the network address from them. It is based on Windows Management Instrumentation (WMI), a standard Microsoft protocol. The Identity Awareness Gateway communicates directly with the Active Directory domain controllers and does not require a separate server.



AD Query flow

No installation is necessary on the clients, or on the Active Directory server.

Identity Source	Description
Browser-Based Authentication	Identities are acquired through an authentication web portal on Identity Awareness. Gateway (Captive Portal), or Transparent Kerberos Authentication.
Active Directory Query (AD Query)	Identities are acquired seamlessly from Microsoft Active Directory. This is a clientless identity acquisition tool.
Identity Agents	Identities are acquired using agents that are installed on user endpoint computers.
Terminal Servers	Identities are acquired using agents that are installed on a Windows-based application server that hosts Terminal Servers, Citrix XenApp, and Citrix XenDesktop services. These agents are used to identify individual user traffic coming from Terminal Servers.
RADIUS Accounting	Identities are acquired using RADIUS Accounting directly from a RADIUS accounting client.
Identity Collector	Identities are acquired using agents that are installed on Microsoft Active Directory Domain Controllers, Cisco Identity Services Engine (ISE) Servers, or NetIQ eDirectory Servers.

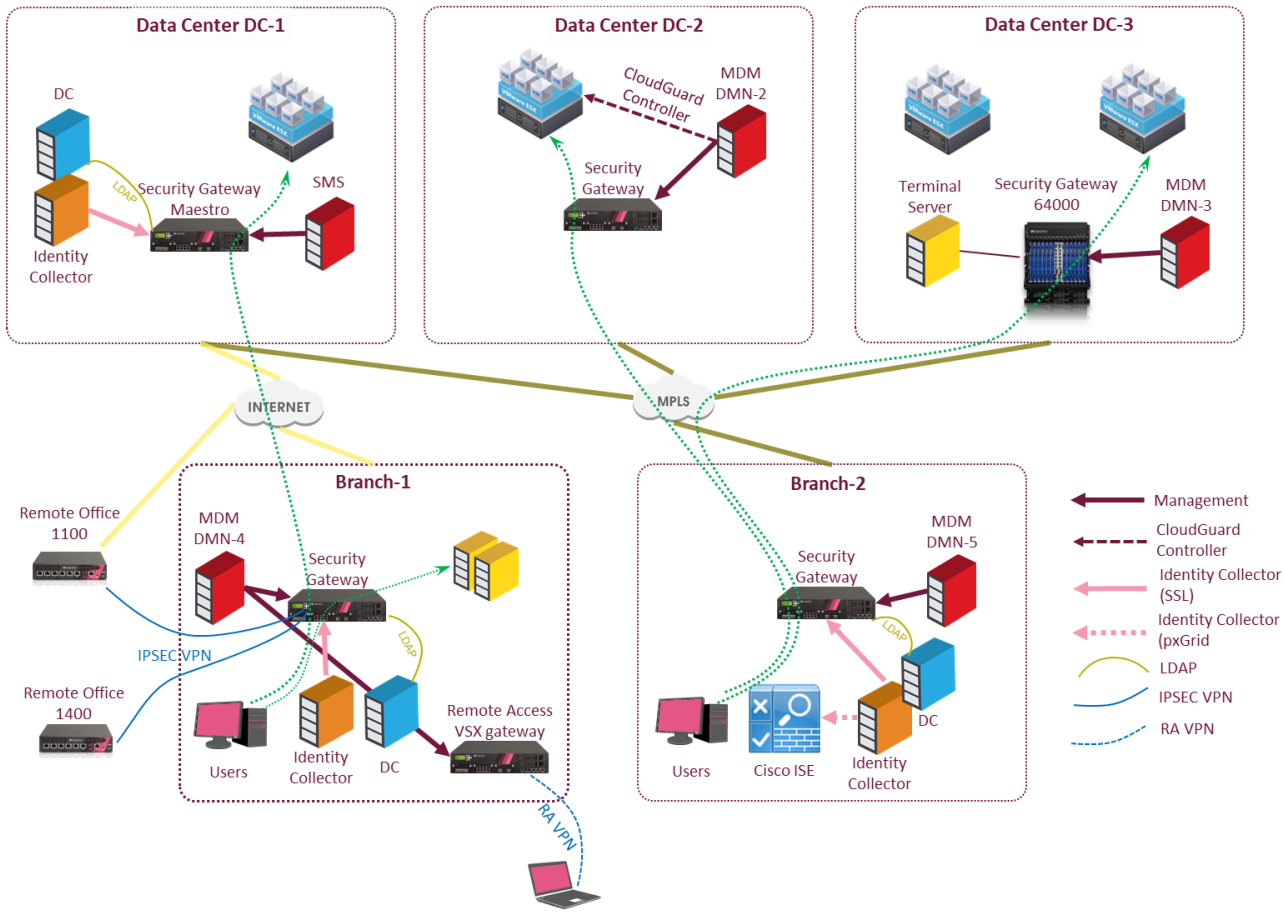
Identity Web API	Provides a flexible method for creating identities.
Remote Access	Identities are acquired for Mobile Access clients and IPsec VPN clients configured to work in Office Mode, when they connect to the Security Gateway.

Identity sources supported by Check Point Identity Awareness

CASE STUDY: THE CHALLENGE OF COMPLEX ENVIRONMENTS

Let's consider a typical enterprise wanting to implement identity-based policies. It has a very complex environment with a mix of gateway types and versions, from Embedded Gaia to Scalable appliances. It is managed by Multi-Domain Management (MDM) and may have additional Security Management Servers (SMS) for specific tasks. An integration with third party user stores such as Cisco ISE and/or Microsoft Active Directory is typical.

How is Identity Awareness implemented in this complex environment? Which features will be used? How will they work together?



Complex Multi-site Enterprise Architecture

Environment specifications

DC-1

– Maestro Hyperscale Solution (R80SP20) managed by a standalone Security Management Server.

- Security Management Server (R80.20, note Maestro is managed from R80.20 and above).
- Domain Controller sends identities to Identity Collector, which provides them to a Maestro security gateway.

DC-2

- Security Gateways (R80.10), managed by MDM DMN-2.
- MDM DMN-2 (R80.10) with specific custom fixes.
- CloudGuard Controller on MDM collects VMware objects used in Check Point policy.

DC-3

- 64000 security appliances (R76SP50).
- MDM DMN-3.
- Terminal Server with MUH agent sends identities to the 64000 security appliance.

Branch-1

- Security Gateways (R77.30).
- MDM DMN-4.
- Local Domain Controller that is a part of the corporate domain sends identities to Identity Collector.
- VSX for Remote Access (split 20,000 remote users per 4 Virtual Systems for better performance and stability).
- Local users (some of them also use Remote Access inside the LAN to access confidential data).
- Hundreds of small offices with 5 to 20 users and gas stations with 1100 and 1400 security appliances in a site-to-site VPN mesh.

Branch-2

- Security Gateways (R80.10).
- MDM DMN-5 (R80.10).
- Identity Collector acquires user identities from the Cisco ISE as well as from the Active Directory.

Environment Issues and limitations

- Security Gateways versions R80.10, and sometimes R77.30, are widely used due to compliance restriction and custom fixes. Only some gateways can be upgraded.
- Check Point Security Gateways 1100 and 1400 SMB appliances protect small networks, i.e. there are multiple segments, including restricted segments, which require user authentication. Unfortunately, Embedded Gaia appliances do not support the Identity Collector.
- Only authenticated users from remote branches should be able to access Data Center resources. It is complicated to configure shared trust to allow Identity Sharing between gateways managed by different Managed Domains and separate Security Management Servers, which are the trust authority for the gateways they manage.

HOW TO SOLVE THIS PUZZLE?

The key component for this solution is a PDP Broker.

The PDP Broker functionality resolves the challenge of sharing identities in large-scale environments. With the PDP Broker, Identity Sharing can be easily achieved across management domains and across geographical or organizational realms.

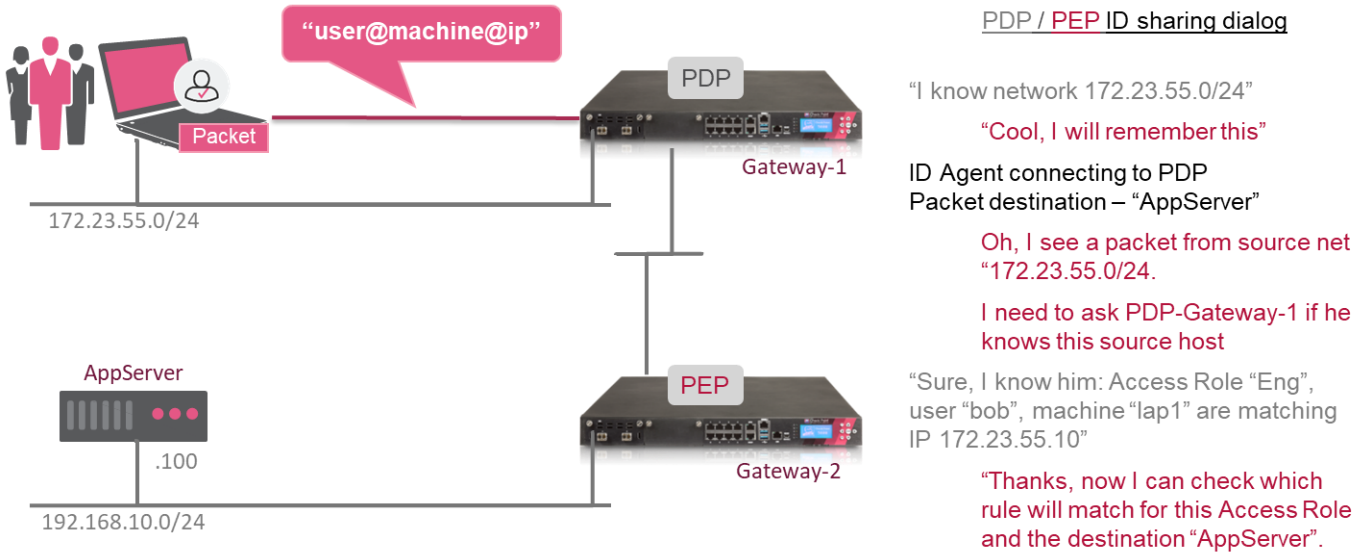
Identity Sharing Details

There are two components of Identity Awareness: Policy Decision Point (PDP) and Policy Enforcement Point (PEP).

The PEP gateway registers on the PDP gateway asking for the list of networks that this PDP may have identities for. The PDP then sends a list of networks to the PEP gateway in the registration process. The PDP gateway will consequently perform a group membership query once a login event is observed and will calculate the Access Role object matching. It will then create an Identity Awareness Session related to the Source IP address.

In case a packet sourced by one of the networks learned from the PDP will arrive on the PEP gateway, the PEP gateway will query the PDP for the current identities related to this source IP address.

The PDP will provide the relevant Access Role and the PEP will perform the rule base matching, allowing or blocking the packet accordingly.



1) The PEP is learning about networks the PDP knows
2) The PEP is querying the PDP for a host from the learned network when seeing packets

PDP / PEP Identity Sharing

Please refer to sk149255 [Advanced Access] for more details.

Initially the PDP Broker was developed as a special hotfix on top of R80.10 + JHF 112. It has been a part of the main train since R80.40[1].

The PDP Broker includes two functionalities: Publisher and Subscriber. The PDP Broker Publisher is the instance initiating an HTTPS connection to the PDP Broker Subscriber using the Identity Awareness API as an underlying

[1] R80.40 Early Availability phase – Q3 2019

infrastructure. The functionality has been created in addition to the so-called "Multi-SIC" function documented in SK65404 [Advanced Access], allowing the sharing identities across management domains from PDP to PEP instances.

Users and machines are represented as Access Role objects in the security policy. Once users have logged on to the network, the login event is learned by the PDP and the matching Access Role is calculated and an identity session is created. This identity session is shared with peering PDP Broker nodes and security gateways running the identity based enforcement instance, PEP. The user will get access to the applications based on these identity sessions.

Establishing Trust in a Multi-SIC Environment (sk65404)

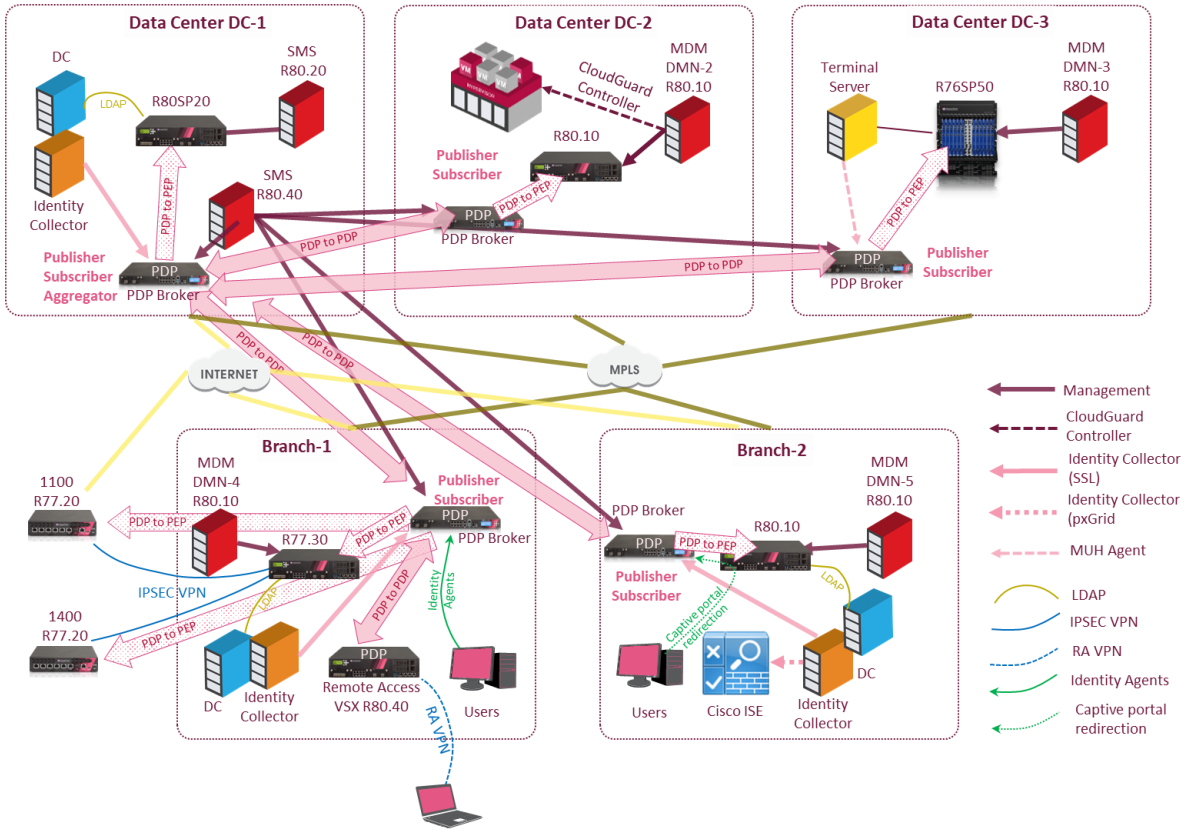
The following is a step-by-step procedure of establishing SIC trust between Identity Awareness entities managed by ***different*** Security Management Servers / Domain Management Servers (this procedure is not required when entities are managed by the same Management Servers). As an example, consider this environment:

- ***PDP_gw*** – The PDP gateway
- ***PDP_mgmt*** – The Security Management Server that manages ***PDP_gw***
- ***PEP_gw*** – The PEP gateway
- ***PEP_mgmt*** – The Security Management Server that manages ***PEP_gw***

To establish communication between the ***PEP_gw*** and the ***PDP_gw***, a certificate must be created of each side signed by the Security Management Server / Domain Management Server they trust. Thus, for ***PDP_gw*** to communicate with ***PEP_gw***, the ***PDP_gw*** will be required to present a certificate that the ***PEP_gw*** can trust, namely a certificate signed by ***PEP_mgmt***. As both sides require establishing communication between them, each side must have a certificate to be trusted by the other side.

On the other hand, the PDP Broker does not rely on SIC. It is less complicated to configure identity sharing between management domains and has additional features.

RECOMMENDED DESIGN

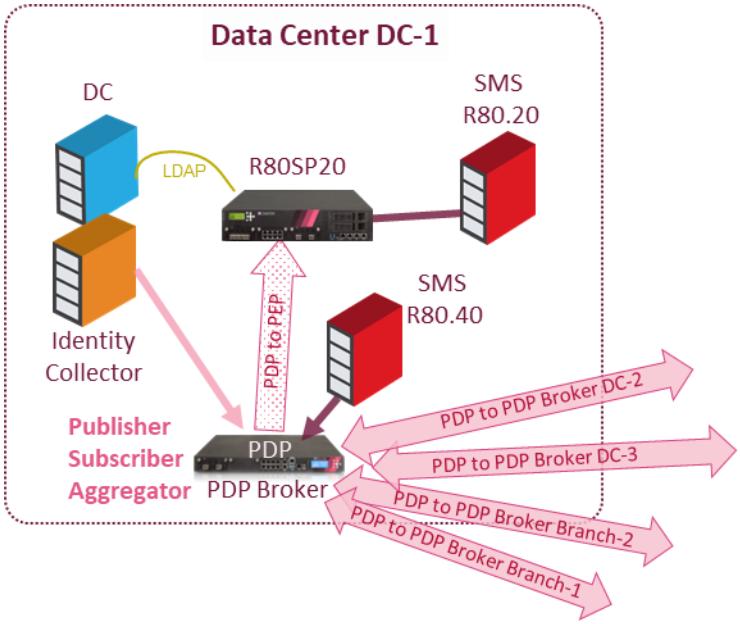


Identity Awareness flow

How does the PDP Broker work?

Although there is a version of the PDP Broker based on R80.10, it is a special build. It does not support any other hotfixes, Jumbo hotfixes, etc. It is thus preferable to use the latest R80.40 (main train) version for the PDP Broker and therefore, we add a dedicated R80.40 Security Management Server to manage all PDP Brokers.

DC-1



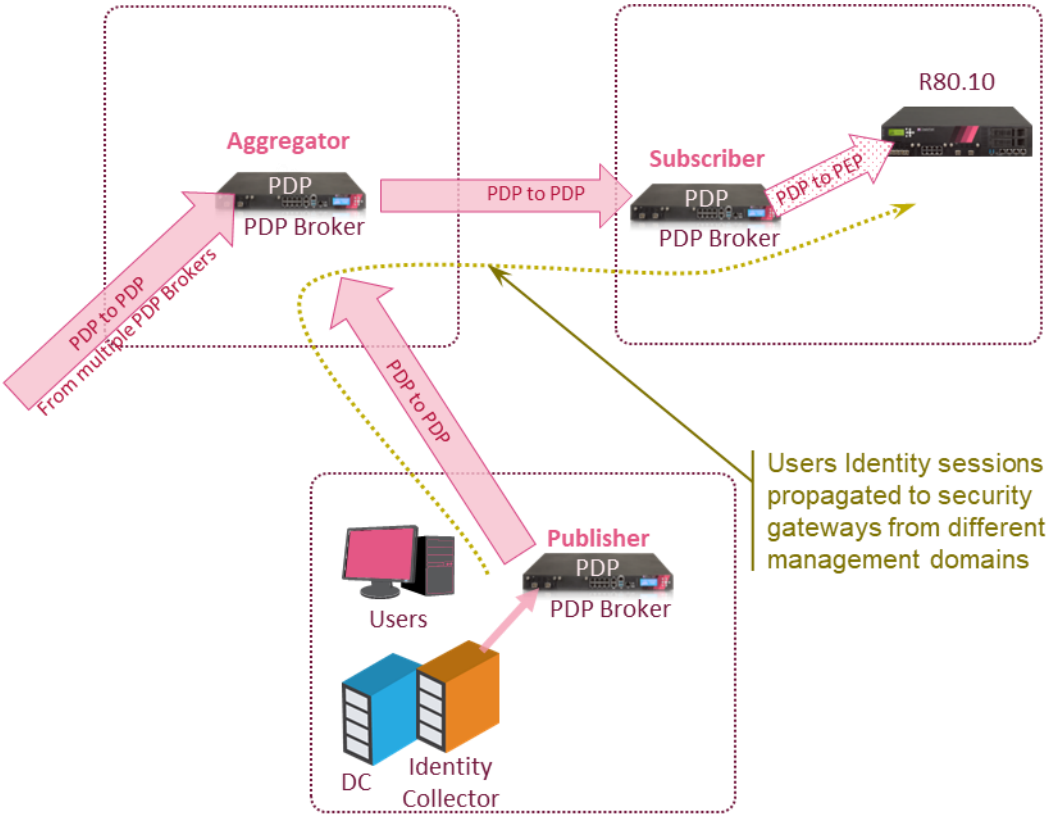
In the above illustration, the term “PDP Broker” refers to gateways running as a dedicated PDP instance with the PDP Broker functionality enabled. PDP Brokers do not enforce security policies in this case.

The PDP Broker in the DC-1 is a Subscriber (receives identities from other sources including PDP brokers in other geographical locations and organizational units) and shares identities with gateways in the DC-1 (PDP to PEP).

Therefore, these Maestro gateways with the R80SP20 version can properly apply role-based policies to users authenticated on the local Domain Controllers (via Identity Collector in the DC-1) as well as for users from Remote Branches (identities learned from the PDP Brokers in those Remote Branches).

This PDP Broker is also a Publisher and shares identities with other PDP Brokers (PDP to PDP).

It is also an Aggregator, i.e it aggregates all identities across the organization and propagates them to other PDP Brokers. It acts like a center of the “Star” topology to avoid excessive configuration of the “Full mesh” PDP Brokers connections.

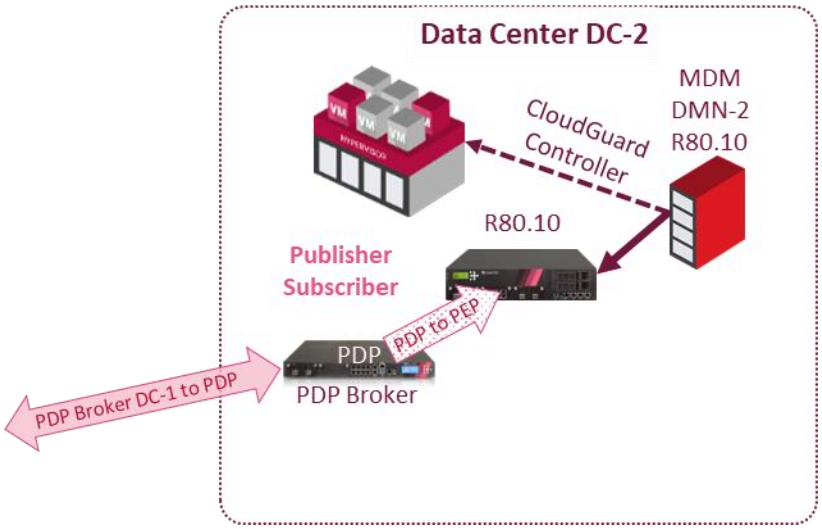


PDP Broker roles

It is important to understand that the Access Role matching the learned identities is calculated before the information is shared with PDP Broker peers, just in the same way as they are calculated before being shared with PEP instances running on gateways. Operating a network by following this principle requires **Access Role objects to be consistent (i.e. they need to have the same names) across management domains**. The security rule base is required using the same Access Role objects (with the same names) on the relevant gateways.

Alternatively, the PDP Broker Subscriber can be configured to re-calculate the Access Role object once it has received the identity. This method allows using Access Role objects with different names in each management domain.

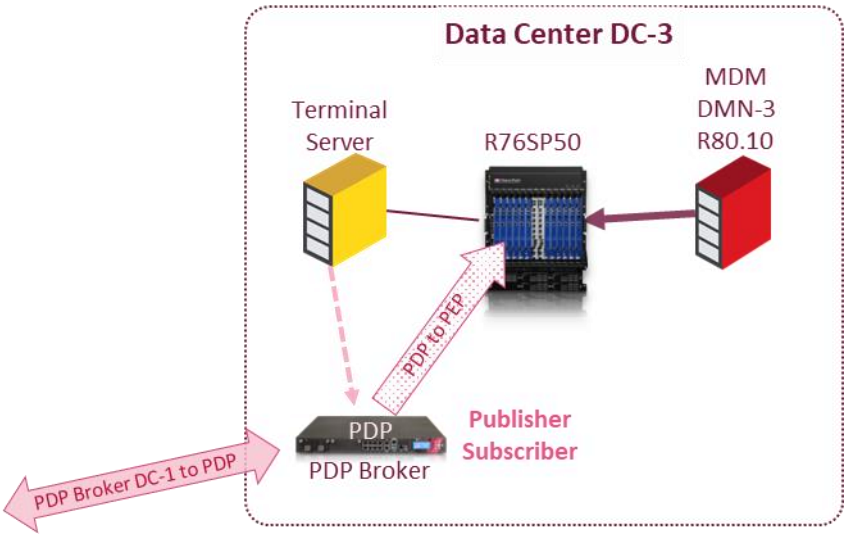
DC-2



There is a PDP Broker in the DC-2 subscribed to the PDP Broker in the DC-1. It receives identity sessions from the Aggregator PDP Broker in the DC-1 and updates R80.10 security gateways with the Remote Branches users' identities.

The security gateway also uses objects from the VMware when enforcing security policies. This information is provided by the CloudGuard Controller component activated on the Multi-Domain Management server.

DC-3

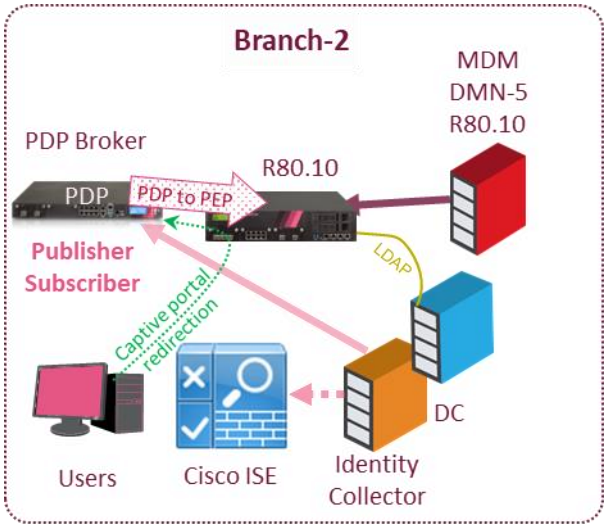


The Identity Awareness Terminal Servers solution lets the system enforce Identity Awareness policies on multiple users that connect from one IP address. This functionality is necessary when an administrator must control traffic created by users of application servers that host Microsoft Terminal Servers, Citrix XenApp, and Citrix XenDesktop.

The Terminal Servers solution is based on reserving a set of TCP/UDP ports for each user. The Terminal Server Multi-User Host Agent (TS MUH Agent) notifies the PDP process (PDP Broker it is connecting to) about users' sessions.

Most customers are using Check Point 64000 Scalable Platform only as Policy Enforcement Point learning Identity Sessions from PDP gateways. In this way, the Check Point 64000 Scalable Platform is best used to enforce security on high traffic volume and the compute intense work of creating Identity Sessions to PDP instances running on dedicated gateways.

Branch-2



Identity Collector receives the identity information from the Domain Controller as well as from the Cisco ISE (pxGrid integration) and provides it to the PDP Broker.

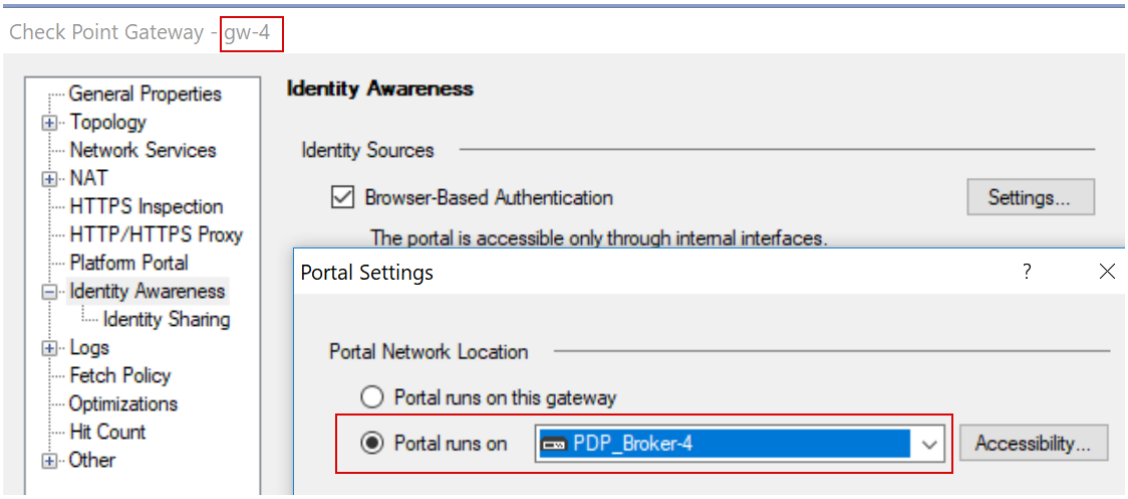
PDP Broker updates R80.10 gateway with this information. It allows this gateway to apply identity-based policies using roles based on SGTs assigned by the Cisco ISE.

Captive portal redirection

There are also users, which are not a part of the Active Directory domain (i.e. using personal laptops, MacBook, tablets). In order to authenticate them individually, a Captive Portal is used by the gateway.

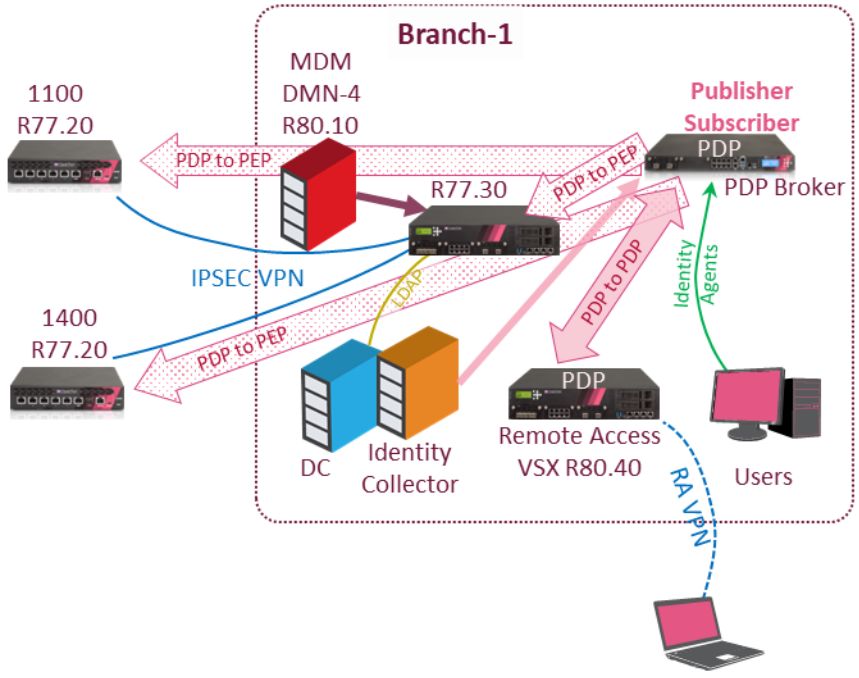
The gateway receiving the authentication request from these endpoints not integrated into the corporate Active Directory will forward them to a Captive Portal to authenticate. Once the user has been authenticated, an Identity Session is created, which can be shared across the organization using PDP to PDP sharing and/or PDP to PEP sharing.

The simplest way to achieve this is to redirect an unauthenticated user to the Captive Portal running on the PDP Broker. After successful user authentication, the PDP Broker calculates their role and updates the gateway (PDP to PEP) as well as an Aggregator PDP Broker (PDP to PDP). All gateways will now be able to enforce a proper policy according to this user's role.



gw-4 redirects users to the PDP_Broker-4

Branch-1



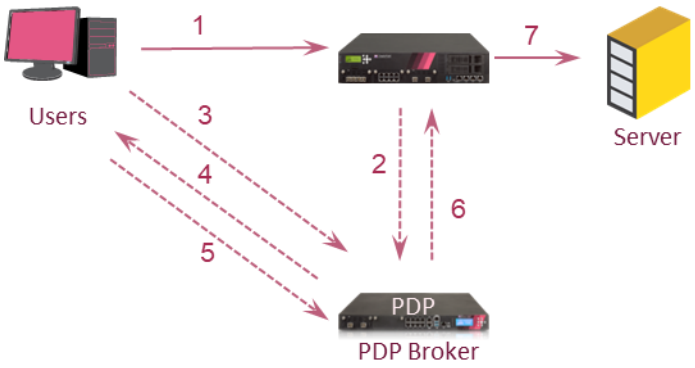
1100/1400 appliances

Identity Collector provides user identities to the PDP Broker. Then the PDP Broker updates SMB appliances (1100/1400 models) via supported PDP to PEP mechanism.

Limitation: DAIP gateways are not supported. In most cases this is not important as either a static IP is available or Identity Awareness is not required because the protected network is too small.

Identity Agents

Besides using Captive Portal (as for the Branch-2) non-domain endpoints can be authenticated using Identity Agents. These agents should connect to the PDP-Broker of the Branch-1, which will update the gateway itself and propagate these identities to the Aggregator PDP Broker and other gateways (PDP to PDP).



Flow with Identity Agents

Item	Description
1	A user logs into a computer with their credentials and tries to access the Server.
2	The Security Gateway with Identity Awareness does not recognize the user and redirects them to the Captive Portal on the PDP Broker.
3	The user sees the Portal page, with a link to download the Endpoint Identity Agent*.
4	The user downloads the Endpoint Identity Agent from the Captive Portal and installs it.
5	The Endpoint Identity Agent client connects to the PDP Broker.
6	PDP Broker propagates the user's identity to the gateway (PDP to PEP).
7	The user is authenticated and the Security Gateway sends the connection to its destination according to the Firewall Rule Base.

* Users can download and install Endpoint Identity Agents from the Captive Portal or the administrator can distribute MSI/DMG files to computers with the distribution software or any other method (such as advising them where to download the client from).

Remote Access Gateway

All previous gateways were used only as Policy Enforcement Points (PEPs). They received identities from the PDP Broker (PDP to PEP) and never shared identities to the PDP Broker.

The Remote Access Gateway is different: identities can be acquired for Mobile Access clients and IPSec VPN clients configured to work in Office Mode when they connect to the Remote Access Security Gateway.

Although it is possible to rely on policies defined on the Remote Access gateway, in complex environments it is preferable to define policies on the gateway protecting its segment rather than on the Remote Access gateway managed by administrators in another management domain.

As remotely connected users receive individual private IP addresses, the Remote Access gateway can associate their IP addresses received from the Office Mode IP Pool with their roles and share them with other gateways. In order to

propagate their identities across the organization, this Remote Access gateway must update the PDP Broker (PDP to PDP). This is possible only if the PDP Broker component is activated on the security gateway. Thus, this Remote Access gateway must be upgraded to either R80.10 + JHF 112 + PDP Broker HF (fixed version, other fixes are not supported) or (recommended) to the latest version of R80.40, supporting this feature natively. An upgrade to R80.40 will require a separate Security Management Server of R80.40 version.

SUMMARY

For effective use of identity-based policies in complex environments, the following considerations are recommended:

- Use PDP Broker to share identities across different management domains (different DMNs in the Multi-Domain Management or event separate Security Management Servers).
- PDP Broker per every management domain is recommended. Can run as a virtual machine.
- Old versions of gateways are supported in most cases (PDP Broker shares identities with them via PDP to PEP mechanism).
- All identity sources are supported (including AD Query, Identity Collector, Captive Portal, Identity Agents, Multi-User Homed terminal servers, Cisco ISE and others).
- SMB appliances can learn identities from the PDP Broker, which receives them from the Identity Collector.
- It is recommended to keep 1 publisher for up to 10 subscribers, ratio.

ADDITIONAL MATERIALS

sk86441 Advanced Technical Reference Guide: Identity Awareness

sk88520 Best Practices – Identity Awareness Large Scale Deployment

PDP Broker: Getting Started Guide

Understanding Identity Sharing