Check Point
SOFTWARE TECHNOLOGIES LTD

CHECK POINT REMOTE ACCESS VPN CLIENT USING SAML

Design Diagram and Notes

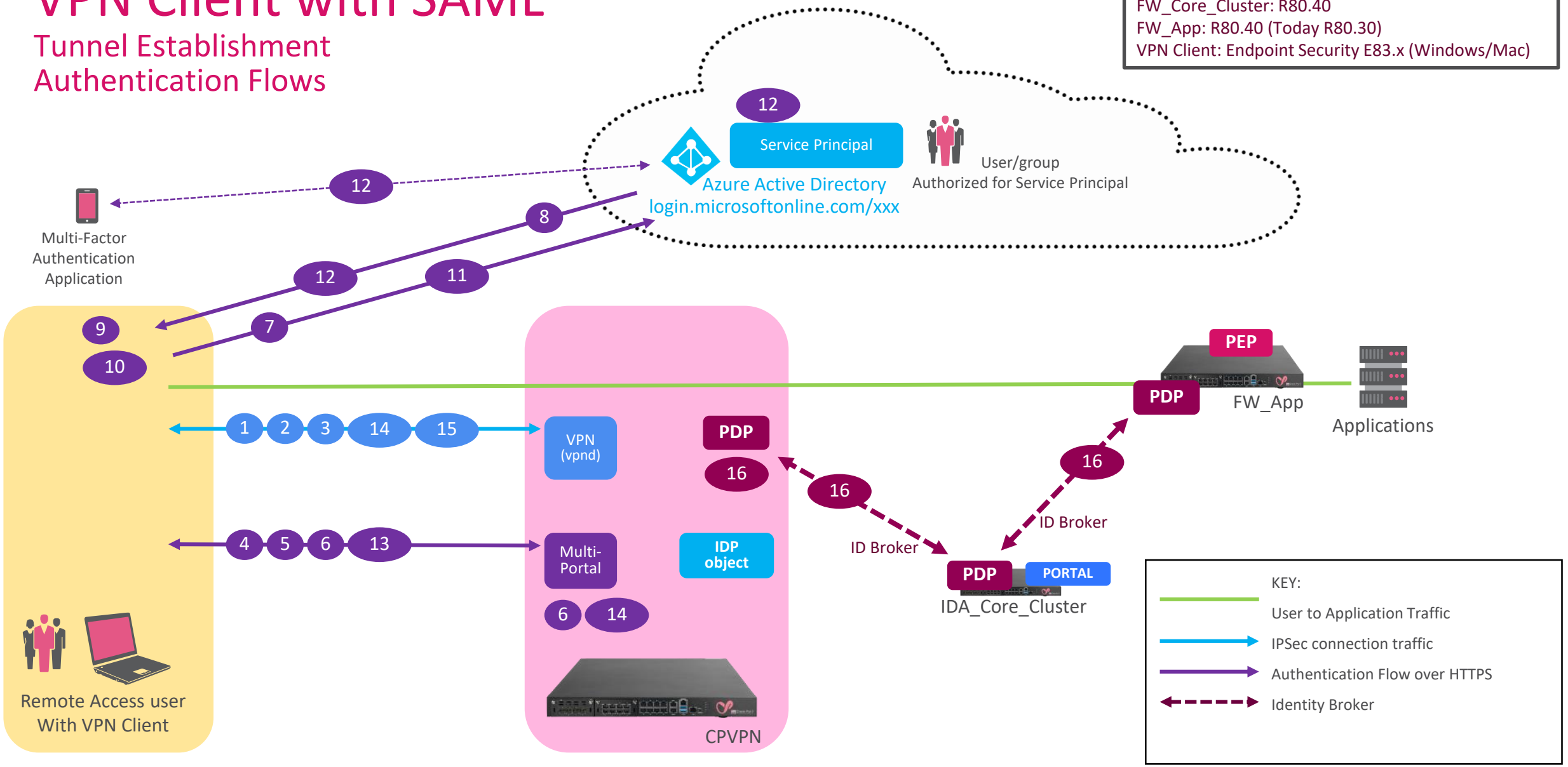
Andy Nicholson | Security Expert EMEA

Version 3 – September 2021

VPN Client with SAML

Tunnel Establishment
Authentication Flows

Version information
Windows 10 clients
VPN gw: R80.40
FW_Core_Cluster: R80.40
FW_App: R80.40 (Today R80.30)
VPN Client: Endpoint Security E83.x (Windows/Mac)



Overview of authentication and creation of VPN connection

1. VPN client opens IPSec connection to VPN gateway (IKE Phase 1 Initiator packet)
2. VPN Gateway responds to IKE phase1 initiator packet
3. Gateway challenges VPN client for authentication - instructing the VPN client to use SAML token based authentication
4. VPN client uses internal browser (or operating system browser if configured) to connect to the gateway's multi-portal infrastructure
5. The multi-portal infrastructure performs TLS handshake and presents multi-portal certificate to the client. The user on the VPN client computer may need to accept this certificate if the multi-portal is using a self-signed certificate.
6. Multi-portal reads the configuration of Identity Provider object and sends HTTP Redirect with the URL of the authentication infrastructure configured in Azure for the authentication service related to this gateway. This is the URL of an IDP in Microsoft Azure Active Directory configured on the Enterprise Application (called 'Service Principal'). The Check Point IDP must be correctly configured with these details.
7. VPN client browser instance connects to URL received in the HTTP Redirect from the VPN gateway (i.e. Login.microsoftonline.com/xxx).
8. Identity Provider challenges the browser for SAML authentication.
9. VPN client browser checks for a cached SAML token in the cache of Internet Explorer of Windows operating system.
10. If no valid SAML token is found, user needs to perform authentication based on the configured authentication scheme in Azure for this IDP.
11. User supplies credentials.
12. IDP verifies credentials and …
    - …if configured – initiates additional authentication challenges such as SmartPhone based biometrical methods
    - …verifies if user is member of a group defined as authorized in the Enterprise Application/Service Principal
    - …issues a SAML token
13. VPN client reconnects to the Gateway's multi-portal infrastructure and presents the SAML token.
14. Gateway verifies the validity of the SAML token using IDP object configuration, and if successful, completes IKE Phase1.
15. IKE Phase2 starts with IPSec SA setup (standard adherence IPSec connection establishment).
16. PDP on the VPN gateway creates the Identity Session then, if sharing is configures, shares it according to the Identity Awareness configuration.

Notes and References

- This solution requires specific minimum versions of the Check Point Security Manager, Security Gateway and Endpoint Security client

- See sk172909 for details of these minimum versions and configuration instructions:
  https://supportcenter.checkpoint.com/supportcenter/portal?eventSubmit_doGoviewsolutiondetails=&solutionid=sk172909

- See also the Remote Access VPN R81 Administration guide:
  https://sc1.checkpoint.com/documents/R81/WebAdminGuides/EN/CP_R81_RemoteAccessVPN_AdminGuide/Topics-VPNRG/Check-Point-VPN.htm

- Identity Awareness Administration Guide - SAML Authentication Flow
  https://sc1.checkpoint.com/documents/R81.10/WebAdminGuides/EN/CP_R81.10_IdentityAwareness_AdminGuide/Topics-IDAG/SAML-Identity-Provider-Configuration.htm?Highlight=saml