Peter Elmer, 24 October 2018

About Office 365 Tenant Support on Check Point Security Gateways

About Office 365 Tenant Restrictions

Source https://docs.microsoft.com/en-us/azure/active-directory/manage-apps/tenant-restrictions

> "Tenant Restrictions gives organizations the ability to specify the list of tenants that their users are permitted to access. Azure AD then only grants access to these permitted tenants."

Learning: It is the **Azure AD environment enforcing the access control** on the incoming data traffic sourced by the Enterprise network.

Functionalities of RFE# WYE-300-20810 as documented in the release notes

This HF requires R80.10 JHF 121 being installed on the gateways and management server. In addition a dedicated SmartConsole version is required. Once this HF is installed no other JHF can be installed. If an update is required Solution Center must be consulted.

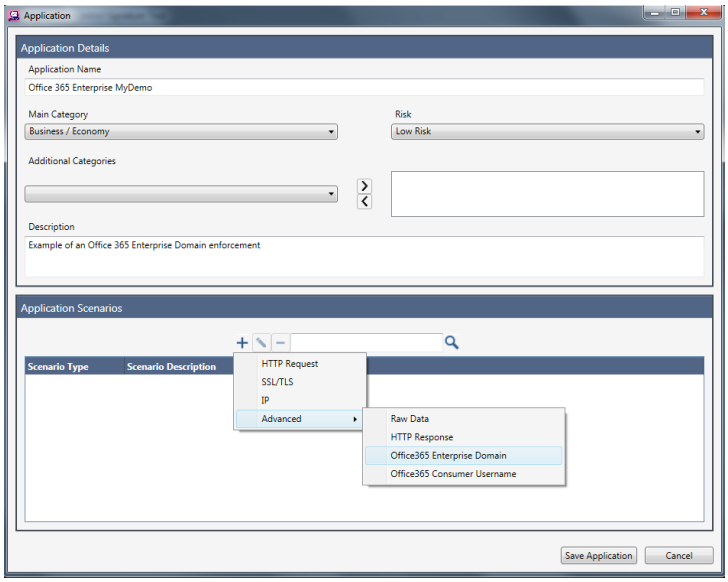
The HF allows configuring additional HTTP headers being injected into the outgoing traffic targeted the Office 365 cloud hosted service. The headers injected contain the tenant identification assigned to the customers Office 365 domain.

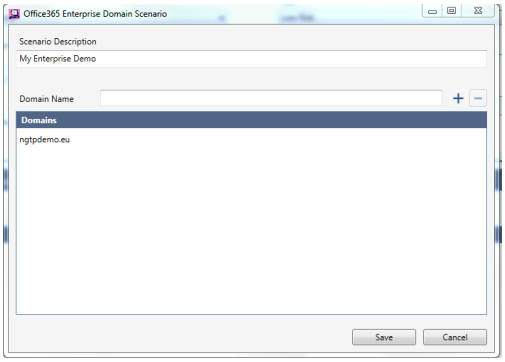
Important: Injecting the header requires outbound HTTPS inspection being active on the gateway.

Functionality of Application Control custom APCL signature for Office 365 Enterprise Domains

The Check Point tool allowing generating custom specific application signatures (link) can be used to generate an APP signature matching on outgoing traffic targeted for an Office 365 Enterprise Domain or Consumer Username.

This function **enforces security on the perimeter gateway** securing the traffic from the Enterprise users in the direction of the Office 365 cloud hosted environment.





The gateway will require outgoing HTTPS inspection in order to read the Enterprise domain specific information inserted into the http headers send by the client to the Office 365 cloud.

