MS-SEC

Identity security

Bastion Tier 0

Mise en œuvre de Royal Server 5

Auteur Loic VEIRMAN

MS*Sec* – 7 rue Denis Papin – 78190 Trappes

Table des matières

Présentation

Objectif

La protection des identités à privilèges est aujourd'hui devenue une nécessité absolue pour toutes les entreprises. Malheureusement, les solutions du marché représentent un budget conséquent et une complexité certaine dans la mise en œuvre, freinant de nombreux services informatiques dans son déploiement. Ce document présente une solution abordable et simple à maitriser pour protéger les comptes à haut privilège de votre domaine Active Directory.

Cahier des charges

L'architecture proposée doit permettre de protéger les comptes du tier 0 contre le vol d'identité ; pour ce faire, le modèle devra s'affranchir de l'utilisation de mot de passe (pas de saisie au clavier) et utiliser une solution moderne d'authentification pour accéder aux ressources sensible (TOTP, SAML, …). La solution devra s'intégrer dans un modèle de silo d'identité et être en mesure de distribuer les droits via Active Directory.

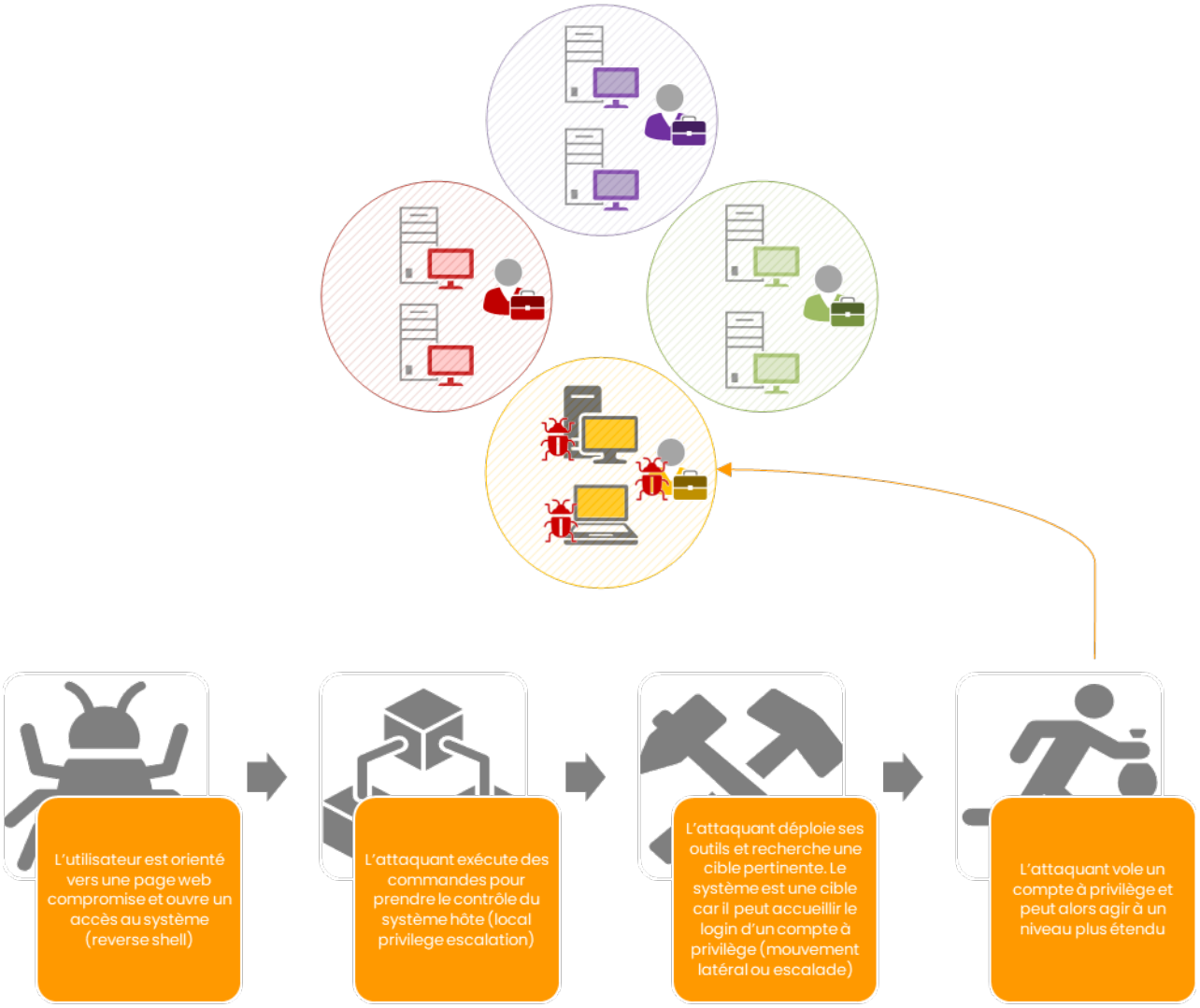
Le modèle de silo d'identité

Présentation

Le modèle de Silo d'identité permet de limiter le mouvement d'un attaquant lorsqu'un compte est compromis. Il se base sur la ségrégation des ressources par Tier :

- Le *Tier 0* regroupe les éléments les plus sensibles du SI en charge de la gestion des identités. On y trouve tout naturellement les contrôleurs de domaine, les serveurs principaux de l'infrastructure de PKI, les serveurs méta-annuaire (azure AD Connect, Okta, …) et les hyperviseurs.
- Le *Tier 1* regroupe les serveurs hébergeant les applications ou les services nécessaires au fonctionnement du SI. Ces derniers sont challengés au regard du risque qu'ils représentent pour le Tier 0 : si un service requiert des droits élevés sur les objets du domaine, le serveur devra être considéré comme de Tier 0 – tous les autres seront de Tier 1 – on y trouve donc les services de base de données, les serveurs web, les serveurs applicatifs ou les serveurs de fichiers.
- Le *Tier 2* regroupe les équipements directement utilisé par l'utilisateur : poste de travail, imprimante, copieur, badgeuse, …

Le schéma ci-dessous illustre le principe de protection apportée par une combinaison des tiers et des silos d'identités dans le cas d'une attaque réussie :

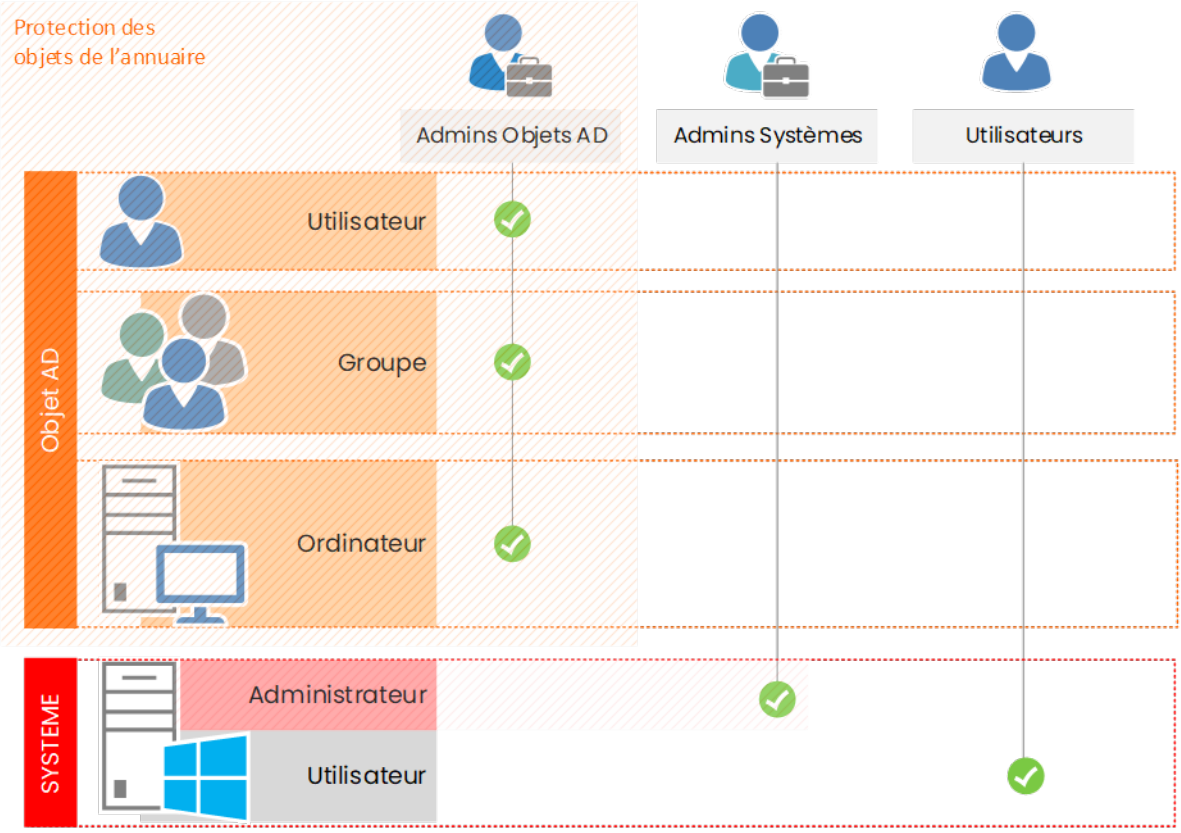


Comptes et périmètres opérationnels

Pour le bon fonctionnement de chaque Tier, vous devrez définir des comptes d'administration dédiés à chacun d'eux – ces derniers ne doivent en aucun cas être utilisé sur un autre Tier : un compte de Tier 0 ne doit donc pas se connecter sur un serveur de Tier 1 ou un poste de Travail (dans l'illustration précédente, les deux tiers seraient compromis).

Pour simplifier l'explication, vous pouvez considérer que le Tier 0 regroupe les comptes administrateurs du domaine (ci-après désigné sous la terminologie de *compte Gestionnaire*) et les comptes de gestion des serveurs du Tier (ci-après désigné sous la terminologie de *compte opérateur*).

D'autre part, deux périmètres doivent être séparés : les comptes en charge de l'administration des systèmes, et donc les plus vulnérable au vol d'identité, ne peuvent pas être les comptes en charge de l'administration des objets de l'annuaire Active Directory. Ainsi, le modèle de Silo des identités doit être construit avec ce type d'approche :



Dans le cadre du bastion de Tier 0, nous aurons à prendre en compte les éléments factuels suivant :

- Le compte d'origine, qui se présentera au bastion, sera un compte utilisateur classique (dans le cas où vous disposez d'un réseau d'administration, il s'agira de votre compte de login) ;
- Les permissions du bastion devront être gérés par un administrateur des objets AD, ces derniers donnant l'accès au bastion par l'appartenance à des groupes ;
- Le compte qui se connectera au système cible ne pourra pas être administrateur des objets AD ;
- Seul le mot de passe du compte d'origine pourra être utilisé.

Les bases étant maintenant définies, regardons comment implémenter la solution de Tier 0.

Royal TS, Royal Server et Yubikey

Royal Apps

Il s'agit d'un éditeur de logiciel spécialisé dans les outils d'administration pour les équipes informatiques. La société existe depuis plus de 10 ans et est basée en Autriche. Il s'agit d'un éditeur très actif avec un catalogue de produits à un produit abordable, ce qui en fait un candidat idéal naturel pour cette étude.

Site web : https://royalapps.com

Royal TS

Ce produit a été spécifiquement conçue a des fins de gestion centralisée d'une infrastructure informatique et adresse tout autant les machines *Linux* que *Microsoft* ou *vmWare*. Ce produit ne se limite pas à la prise en main à distance (ssh, rdp) mais offre également des solutions très poussées pour gérer un système sans avoir à s'y connecter (supervision, redémarrage de service, script, …).

Dans le cas particulier du bastion, ce produit nous intéresse car il permet de travailler avec des fichiers de travail qui regroupe les informations de connexion – ce fichier est chiffré en SHA256 afin de réduire le risque de vol des informations qu'il contient - à ce jour, il n'est pas possible de casser la clé mais le brute force reste possible, aussi l'utilisation d'un mot de passe force et non devinable est-il recommandé (*Keepass* offre une solution pertinente pour stocker le mot de passe).

Royal Server

En complément de Royal TS, Royal Apps a produit un serveur d'administration qui peut tout à la fois jouer le rôle de point central d'administration et de passerelle d'accès à distance. Toutefois, ce produit souffre d'un défaut sur son service de passerelle, ce dernier requérant de pouvoir faire de la délégation contrainte avec le compte d'un utilisateur le traversant, ce qui en exclu d'office les comptes protégés par le groupe *protected users* (ce qui est en réalité un plus, cela nous obligeant à accéder au Tier 0 avec un compte sans privilège sur le domaine !).

Le serveur permet également de stocker les fichiers des clients Royal TS dans un magasin central sur le serveur lui-même et de protéger ces derniers en interdisant l'export de l'information. Lorsqu'un fichier est géré par le serveur, ce dernier permet également de gérer l'accès (ou de le

refuser), le niveau de l'accès (lecture, modification) et d'interdire certaines actions (export/lecture du mot de passe par exemple). Enfin, Royal Server est compatible avec les le protocole DUO, les services TOTP de Microsoft et Google et le service TOTP de Yubico (la version 5, dans sa version bêta, y a ajouter l'utilisation des clés Yubikey et de son API publique pour l'authentification).

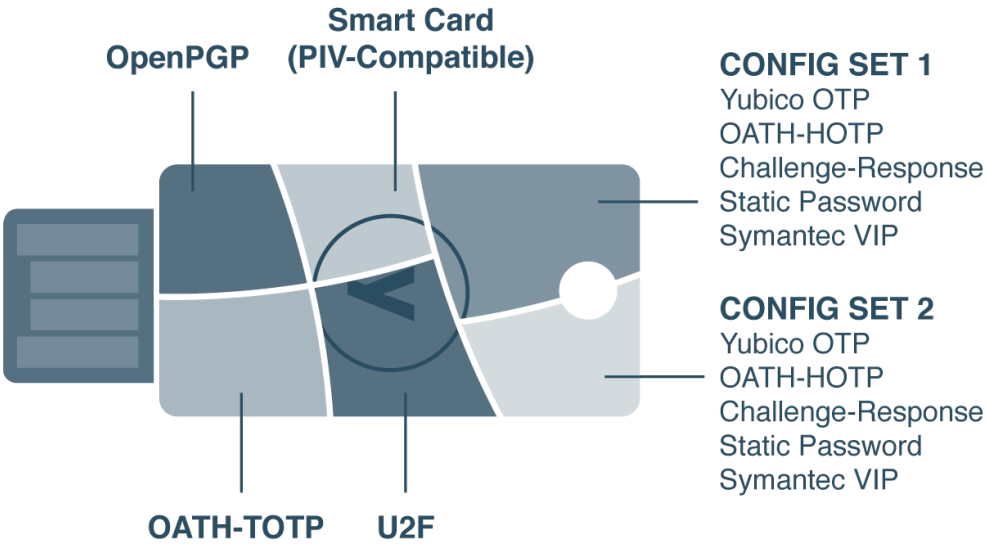
Pour le bastion, Royal Server sera le point d'accès unique vers les systèmes du Tier 0 (le firewall bloquant tous les flux d'administration provenant des Tier 1 et 2) et assurera le contrôle des identités qui l'accède.

Yubico et sa Yubikey

Dans l'univers de la sécurisation de l'accès client, l'utilisation de clé de sécurité est un élément essentiel au renforcement de la protection des identités numériques. Yubico propose une clé permettant de combiner nos besoins dans un seul et même périphérique :

- Disposer d'une solution de TOTP simple et abordable,
- Disposer d'une solution évolutive vers de futurs besoins (Smart Card Logon, MFA, Windows Hello for Business, clé SSH, …)

La clé retenue est une Yubikey série 5, qui offre toutes les fonctions présentées dans ce schéma :



La clé se décline en plusieurs modèles : USB-A, USB-C, Lightening, NFC, … et sous plusieurs dimensions, ce qui permet d'adresser tous les cas d'usages et toutes les populations.

Ci-dessous la gamme série 5 au complète (hors clé Biométrique) :

Dans le cadre du bastion, la clé retenue devra disposer d'un contacteur pour détecter une pression courte.

Pour certaines actions de configuration, vous devrez avoir installé l'application Yubikey Manager (https://www.yubico.com/support/download/yubikey-manager/) et/ou Yubico Authenticator (https://www.yubico.com/products/yubico-authenticator/).

Plus d'informations sur le site du fabricant : https://www.yubico.com/la-cle-yubikey/yubikey-5-series/?lang=fr

Un petit mot pour les puristes du bastion…

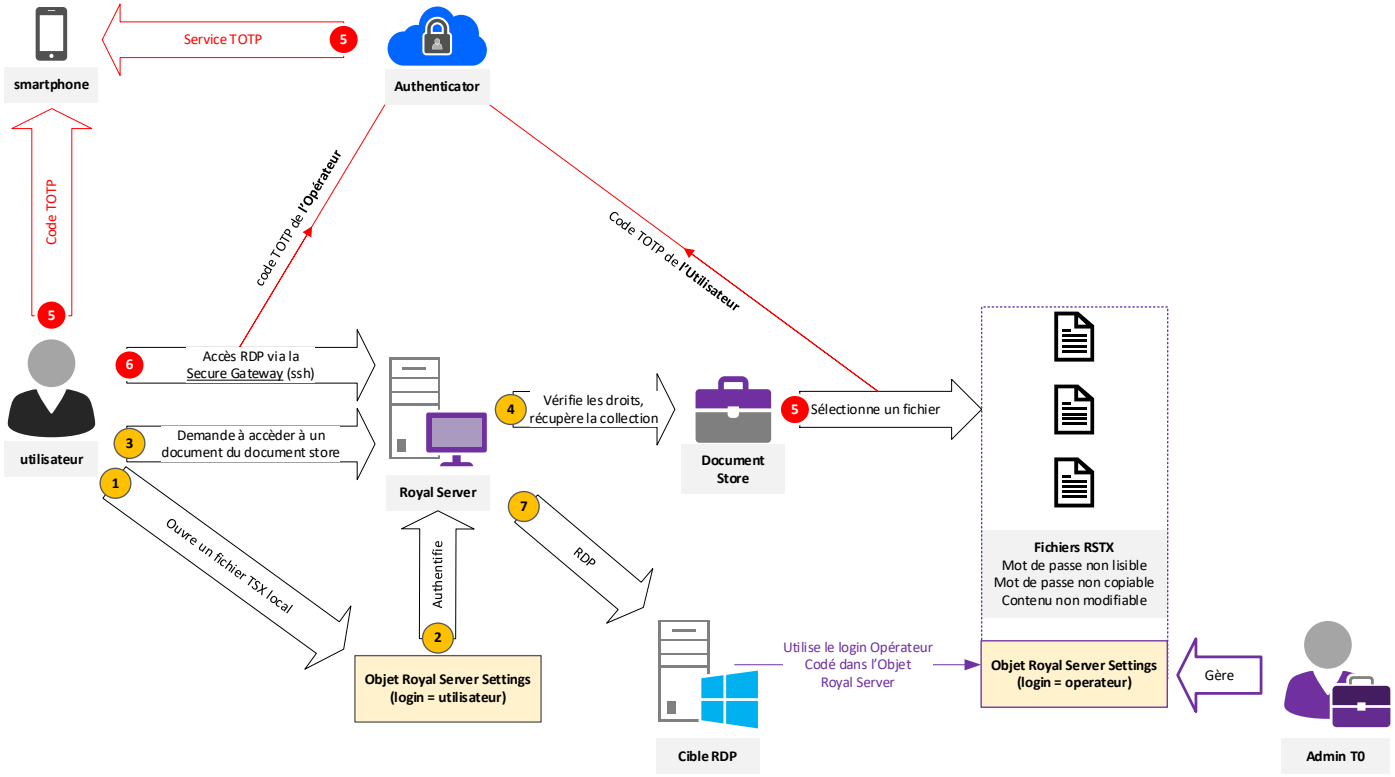
Soyons honnête : si l'on compare Royal Server aux références du marché, nous ne sommes pas au même niveau de sécurité et de fonctionnalité. Pourtant, s'il est bien configuré, il est possible d'assurer les missions de base que sont les ruptures d'identités et de protocoles entre la source et la cible à administrer. Il y a aura nécessairement une limite fonctionnelle quant à son exploitation, qui sera directement liée à la taille de l'équipe – cela dit, la plupart des entreprises n'atteindront pas ce seuil et trouveront dans ce « bastion » une approche sécurisante pour leur travail quotidien.

Ami puriste, ne soit pas trop dur avec la solution !

Bastion avec Royal TS et Royal Server

Schéma de principe

Le schéma ci-dessous représente le principe mis en œuvre d'une connexion au travers du bastion, étape par étape :



1. L'utilisateur dispose d'un document Royal TS sur son poste de travail ou un partage réseau accessible – le document contient un objet de configuration Royal Server qui contient son login (si le mot de passe y est stocké, un mot de passe sera demandé)
2. L'objet de configuration Royal Server est déverrouillé et sera présenté auprès du serveur Royal Serveur pour les étapes 3, 4 et 5
3. L'utilisateur demande à parcourir la liste des documents présent dans le Document Store de Royal Server
4. Royal Server vérifie les permissions de l'utilisateur
5. L'utilisateur sélectionne un document : avant de pouvoir le lire, un code TOTP sera demandé à l'utilisateur pour le compte *utilisateur*

6. L'utilisateur lance une connexion vers un serveur cible : pour établir le tunnel SSH avec Royal Server, un code TOTP pour le compte *opérateur* est demandé préalablement.
7. Une fois le tunnel établi, une connexion RDP est ouverte entre Royal Server et le serveur ciblé avec le compte *opérateur*.

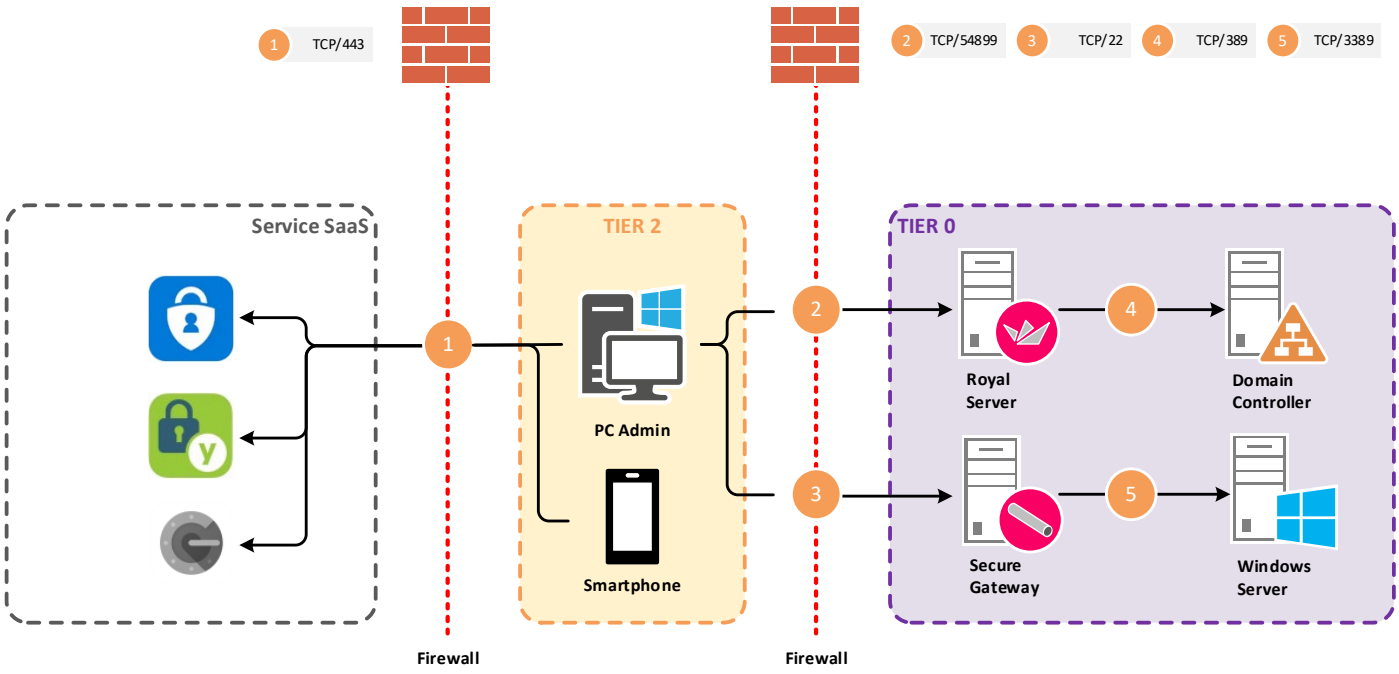
Pour plus de sécurité, l'utilisateur ne peut pas lire ou copier les mots de passe contenus dans le document Royal TS fournit par Royal Server (ces informations sont saisies et maintenues par l'administrateur).

Le fichier est également protégé par un mot de passe, connu de l'utilisateur, afin de lui permettre de modifier les connexions existantes ou d'en ajouter. Le mot de passe peut être simple, le document ne pouvant être exfiltrer de Royal Server et l'accès primaire étant conditionner à une authentification forte.

L'administrateur du bastion (par défaut un administrateur du domaine) est le seul a pouvoir gérer le document – ce dernier définie l'exigence de TOTP, configure les comptes utilisateurs et assure le pairing du téléphone.

Enfin, pour renforcer la sécurité des comptes, deux systèmes de TOTP différents sur deux périphériques différents seront nécessaires : le compte *utilisateur* s'appuie sur le TOTP de Yubikey et le TOTP du compte *opérateur* sur celui de Microsoft via le téléphone professionnel de l'utilisateur.

Intégration réseau



Flux Tier 2 vers Service SaaS

Lors de l'authentification forte, un accès au service SaaS sera nécessaire sur le port TCP/443. Ce service sera accédé par le smartphone de l'utilisateur ou une application installée sur le PC (Yubico Authenticator).

Ce flux n'est donc nécessaire que lorsque l'équipement en charge de la récupération du code TOTP est connecté au réseau de l'entreprise.

Flux Tier 2 vers Tier 0

Le poste utilisé pour la connexion n'établit de connexion que vers le serveur RS et le serveur Secure Gateway (ce peut-être le même serveur ou deux serveurs différents). Seul les flux TCP/54899 et TCP/22 sont requis ; le serveur RS est le point d'entré indispensable pour l'accès au Document Store. Le serveur Secure Gateway vous permet de fermer les flux d'administration entre les tiers

Flux interne Tier 0

En dehors des flux habituel de production, le serveur RS aura besoin de réaliser des requêtes LDAP auprès des contrôleurs de domaine (TCP/389) et le serveur Secure Gateway d'établir une connexion en RDP avec la cible (TCP/389) ou en SSH pour les serveurs Linux (TCP/22).

Considération relative à la sécurité

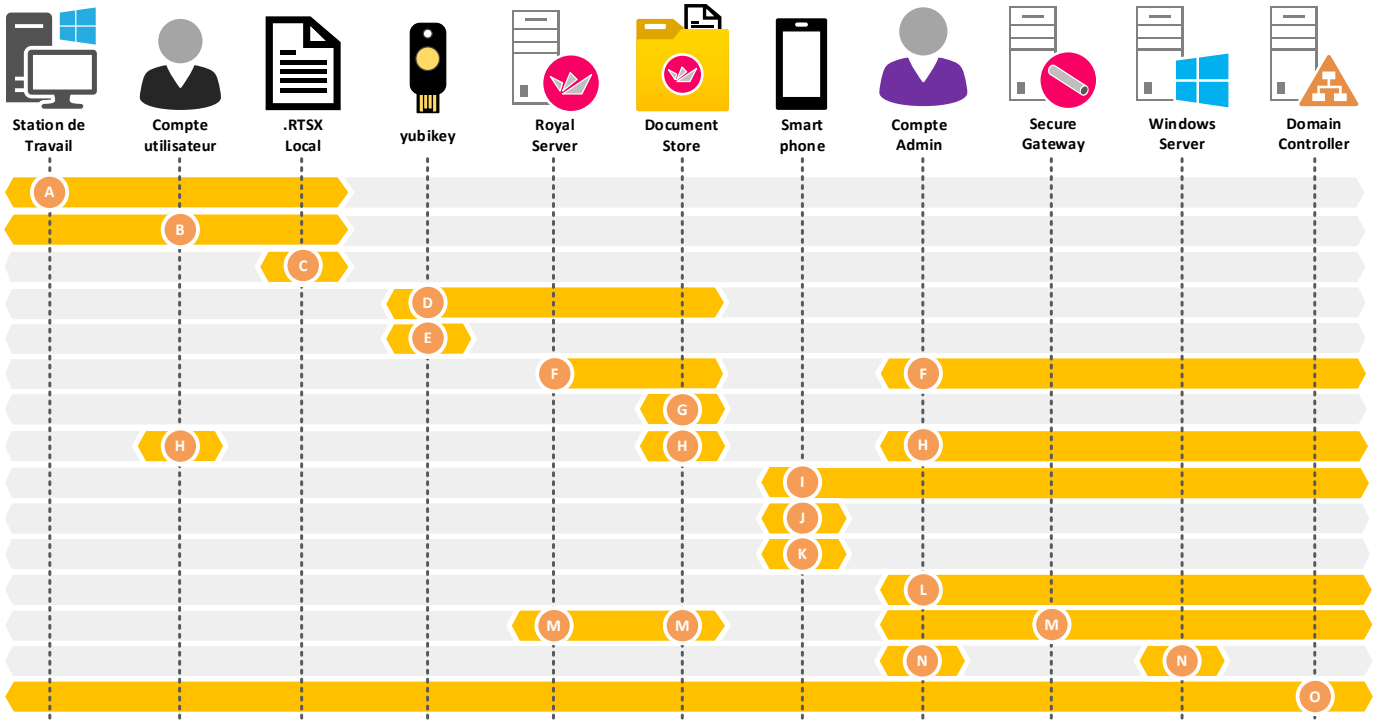
Puisque le point d'initialisation de l'accès est en Tier 2, ce dernier est le plus susceptible d'être compromis : il est donc essentiel de respecter les règles suivantes :

- Le compte établissant la connexion vers le bastion pour atteindre le Document Store doit appartenir au Tier 2.
- Le compte accédant au serveur RS doit être de même nature que le compte de login sur la station hébergeant Royal TS (i.e. *utilisateur* pour un PC bureautique, *opérateur* pour un PC dans un réseau d'administration Tier 2), afin d'éviter une escalade de privilège dans le Tier.
- Les mots de passe des comptes de Tier 0 ne doivent pas être accessible depuis l'environnement de Tier 2 (saisie, récupération par copier/coller ou affichage).
- L'accès au Document Store doit être protégé à deux niveaux : l'ouverture doit être conditionné par une authentification unique (MFA) et le contenu sensible du document ne doit pas pouvoir être modifié par l'utilisateur Tier 2.

- Seul un accès RDP est permis au travers de la Secure Gateway. Idéalement, cet accès devrait permettre une connexion sur un serveur d'administration central pour réaliser tout autre opération de maintenance.
- Les accès type WinRM, remoteShell, … ne sont pas permis vers les systèmes du Tier 0 (ces accès doivent être fait depuis un serveur du Tier 0 exclusivement).

Scénarios d'attaques et contre-mesures

Pour qu'un bastion soit efficace, il est nécessaire de se positionner dans un contexte de compromission pour essayer d'évaluer sa robustesse. La chaine de risque serait la suivante :



A	Le poste est compromis	B	Le compte utilisateur est volé
C	Le fichier de royal TS local est volé	D	La Yubikey est volée ou perdue
E	La Yubikey est oubliée	F	Le serveur Royal Server est compromis
G	Le Document Store est compromis à distance	H	Le Document Store est compromis localement
I	Le Smartphone est compromis	J	Le Smartphone est volée ou perdu
K	Le Smartphone est oublié	L	Le compte Admin est volé
M	La Secure Gateway est compromise	N	Le serveur cible est compromis
O	LE contrôleur de domaine est compromis		

Vous trouverez ci-après les différentes analyses sur le modèle présenté et les contre-mesures misent en œuvre.

Cas A : compromission du poste de l'utilisateur

Risque	Le poste de l'utilisateur est sous le contrôle de l'attaquant. Dans ce scénario, l'attaquant a la capacité d'installer ses outils, de maintenir sa présence dans le SI de manière persistante et de voler tout compte qui se connecte à la machine. Il peut également faire une analyse du réseau pour détecter des cibles potentielles ou capturer le flux réseau.
Conséquences	Le compte utilisateur est compromis et pourrait permettre un accès au serveur Royal Server (1), au Document Store (2) et au fichier Royal TS local qui contient les informations de connexion au serveur Royal Server (3).
Contre-mesure	(1) La mise en place du MFA rendra le compte inutilisable (2) La mise en place d'un second MFA rendra l'accès impossible (3) Le chiffrement du fichier empêchera son exploitation. Le mot de passe doit être suffisamment complexe pour éviter que ce dernier soit cassé. Note : le MFA ne doit pas être un code OTP sur le poste du client (accessible).

Cas B : le compte utilisateur a été volé

Risque	Le compte de l'utilisateur est sous le contrôle de l'attaquant. Dans ce scénario, l'attaquant a un accès sur le système et peut arriver à compromettre tout le poste de travail (voir cas A). Les fichiers accessibles par l'utilisateur le sont également pour l'attaquant.
Conséquences	Le compte utilisateur est compromis et pourrait permettre un accès au serveur Royal Server (1), au Document Store (2) et au fichier Royal TS local qui contient les informations de connexion au serveur Royal Server (3).
Contre-mesure	(1) La mise en place du MFA rendra l'accès impossible (2) La mise en place d'un second MFA rendra l'accès impossible (3) Le chiffrement du fichier empêchera son exploitation. Le mot de passe doit être suffisamment complexe pour éviter que ce dernier soit cassé.

Cas C : le fichier Royal TS local est volé

Risque	Le fichier peut être utilisé depuis un poste inconnu.
Conséquences	Le compte utilisateur est inclus dans le fichier et pourrait permettre un accès au serveur Royal Server (1), au Document Store (2) et aux informations de connexion au serveur Royal Server (3).
Contre-mesure	(1) La mise en place du MFA rendra l'accès impossible (2) La mise en place d'un second MFA rendra l'accès impossible (3) Le chiffrement du fichier empêchera son exploitation. Le mot de passe doit être suffisamment complexe pour éviter que ce dernier soit cassé.

Cas D : la clé Yubikey a été perdue ou volée

Risque	La clé peut être utilisée par l'attaquant.
Conséquences	L'accès au server Royal Server (1) devient possible ainsi que l'accès au Document Store (2). La clé peut être utilisé (3).
Contre-mesure	(1) Le compte doit également avoir été volé, ou le fichier local. (2) La mise en place d'un second MFA rendra l'accès impossible. (3) Utiliser un code OTP avec un smartphone en NFC ou USB.

Cas E : la clé Yubikey a été oubliée

Risque	Aucun.
Conséquences	L'administrateur ne peut plus se connecter au serveur Royal Server (1).
Contre-mesure	(1) L'administrateur peut reconfigurer le compte pour utiliser un autre accès MFA.

Cas F : Le serveur Royal Server est compromis

Risque	Compromission du Tier 0.
Conséquences	L'accès à la configuration de Royal Server est possible pour l'attaquant. De ce fait, ce dernier peut créer un compte et déjouer toutes les sécurités pour obtenir un accès permanent depuis l'extérieur du Tier 0 (1). D'autre part, l'attaquant peut voler des comptes (2) qui se connecteraient sur le système et réaliser des mouvements latéraux (pass-the-hash ou rejeu d'identité). Si un compte à privilège se connecte sur le serveur, l'attaquant peut compromettre le domaine en entier (3).
Contre-mesure	(1) Superviser régulièrement la configuration du serveur et mettre ne place une politique de contrôle de l'accès. Durcir le système avec des règles strictes. Interdire l'accès en RDP et utiliser un serveur physique. (2) Limiter les comptes ayant le droit de se connecter au serveur. Considérer le serveur comme aussi sensible qu'un contrôleur de domaine. (3) Interdire la connexion de comptes ayant des privilèges Active Directory sur le serveur.

Cas G : le Document Store est compromis à distance

Risque	Récupération des accès aux serveurs du Tier 0.
Conséquences	L'attaquant peut récupérer les comptes déclarés dans les fichiers de connexion (1).
Contre-mesure	(1) L'ouverture du fichier doit être protéger par un code MFA. Le cache de code doit être réduit au minimum.

Cas H : Le Document Store est compromis localement

Risque	Récupération des accès aux serveurs du Tier 0.
Conséquences	L'attaquant peut récupérer les comptes déclarés dans les fichiers de connexion (1). L'attaquant peut récupérer les fichiers modèles (2).
Contre-mesure	(1) L'ouverture du fichier doit être protéger par un code MFA. Le cache de code doit être réduit au minimum. Les fichiers doivent être chiffrés intégralement. (2) Les fichiers modèles ne doivent pas contenir d'information d'authentification.

Cas I : Le smartphone est compromis

Risque	Accès au code TOTP de l'authenticator.
Conséquences	L'attaquant peut s'identifier en lieu et place de l'administrateur (1).
Contre-mesure	(1) Ce risque est conditionné à la compromission de l'accès primaire au serveur Royal Server.

Cas J : Le smartphone est volé ou perdu

Risque	Accès au code TOTP de l'authenticator.
Conséquences	L'attaquant peut s'identifier en lieu et place de l'administrateur (1).
Contre-mesure	(1) Ce risque est conditionné à la compromission de l'accès primaire au serveur Royal Server.

Cas K : Le smartphone est oublié

Risque	Aucun.
Conséquences	L'administrateur ne peut plus se connecter au serveur Royal Server (1).
Contre-mesure	(1) L'administrateur peut reconfigurer le compte pour utiliser un autre accès MFA.

Cas L : Le compte administrateur est volé (non-administrateur de Royal Server)

Risque	Compromission du Tier 0.
Conséquences	L'attaquant peut se connecter au système du Tier 0 (1) s'il obtient un accès à ces derniers (2).
Contre-mesure	(1) Surveiller l'activité des comptes. (2) Interdire l'accès distance depuis un serveur autre que la Secure Gateway.

Cas L : Le compte administrateur est volé (administrateur de Royal Server)

Risque	Compromission du Tier 0 et du serveur Royal Server.
Conséquences	L'attaquant peut se connecter au système du Tier 0 (1) s'il obtient un accès à ces derniers (2). L'attaquant peut prendre le contrôleur de Royal Server (voir les cas F, G et H) (3).
Contre-mesure	(1) Surveiller l'activité des comptes. (2) Interdire l'accès distance depuis un serveur autre que la Secure Gateway. (3) Avoir mis en place les contre-mesures des cas F, G et H.

Cas M : La Secure Gateway est compromise

Risque	Compromission du Tier 0.
Conséquences	L'attaquant peut se connecter au système du Tier 0 (1) s'il obtient un accès valide à ces derniers (2).
Contre-mesure	(1) Surveiller l'activité des comptes. (2) Utiliser le Smart-Card-Logon ou une solution de MFA.

Cas N : Un serveur du Tier 0 est compromis

Risque	Compromission du Tier 0.
Conséquences	L'attaquant peut se connecter au système du Tier 0 (1) et voler les comptes qui se connecte au système compromis (2).
Contre-mesure	(1) Surveiller l'activité des comptes. (2) Utiliser le Smart-Card-Logon ou une solution de MFA.

Cas O : Le contrôleur de domaine est compromis

Risque	Compromission du domaine.
Conséquences	Perte de contrôle complète du SI (1).
Contre-mesure	(1) Interdire l'administration des Contrôleurs de domaine Directement depuis Royal Server. Mettre les comptes administrateurs du domaine dans le groupe *Protected Users* afin de bloquer leur utilisation au travers de la Secure Gateway. Utiliser un serveur de rebond au travers de Royal Server pour se connecter aux contrôleurs de domaine. Mettre en place le Smart-Card-Logon pour les comptes d'administration du domaine.

Mise en œuvre

Serveur Royal Server

Installation

Un serveur physique a été dédié à l'hébergement du serveur Royal Server (*Serveur RS* pour la suite de ce document). Ce prérequis est nécessaire pour permettre l'accès aux hyperviseurs en cas de problème ne permettant pas aux machines virtuelles d'être jointes. A noter que ce principe n'est valable que si au moins l'un de vos DC n'est pas hébergé sur le cluster…

L'installation est assez classique : vous devez disposer d'un compte administrateur local pour réaliser l'installation et disposer d'une licence valide pour terminer l'installation.

Une fois l'installation terminée, un service nommé *Royal Server* sera installé et configuré avec le compte *Local System*.

Prérequis à la configuration

Avant de configurer le serveur, vous devrez vérifier que le compte *authenticated users* soit bien membre du groupe *Accès compatible pré-Windows 2000* – cela est malheureusement requis pour que l'authentification fonctionne correctement.

Note : vous pouvez remplacer le groupe *authenticated users* par le Server RS mais faites attention aux effets de bords pour certaines applications ou services (ADFS, RODC, …)

Pour son fonctionnement avec Active Directory, un compte de service sera utilisé pour interroger les groupes de l'annuaire (simple utilisateur suffit) et si vous envisagez également d'utiliser les autres fonctionnalités de Royal Server (remote script, relancer un service, …), ce même compte sera utilisé. Ce compte est appelé *Worker Account* – ce dernier devra disposer des droits adéquates sur le système cible et s'appuiera sur un compte Active Directory (non-compatible avec les gMSA) :

Type de compte	Descrption	SamAccountName
Objet Utilisateur	Worker Account	SVC.RoyalServer

Trois groupes seront également créés localement pour définir les privilèges d'accès et d'administration, ces groupes devront avoir pour membre des groupes du domaine :

Type de Groupe	Portée	Nom
Objet Utilisateur	Domaine Local	L-S-RoyalServer-Users
Objet Utilisateur	Domaine Local	L-S-RoyalServer-GwayUsers
Objet Utilisateur	Domaine Local	L-S-RoyalServer-Admins
Objet Utilisateur	Global	G-S-RoyalServer-Users
Objet Utilisateur	Global	G-S-RoyalServer-GwayUsers
Objet Utilisateur	Global	G-S-RoyalServer-Admins

Les groupes de type *domaine local* permettent d'appliquer le droit sur le serveur, alors que les groupes de type *global* permettent de gérer les comptes par adhérence. Chaque groupe global doit être membre de son binôme domaine local (ex. : *G-S-RoyalServe-Users* est membre de *L-S-RoyalServe-Users*).

Une fois les prérequis créés, vous pouvez commencer la configuration du serveur.

Royal Server

Configuration initiale

Lors de son lancement initial, Royal Server vous demandera de procéder à l'enregistrement de votre licence, puis de créer un *Worker Account* : ce compte permet à l'application d'interagir auprès de vos serveurs pour effectuer les opérations à distance ainsi que d'interroger l'annuaire.

Insérez ici le compte de service *SVC.RoyalServer* précédemment créé.

Configuration du service

Rendez-vous ensuite dans le menu *Service Configuration* et faite pointer le service sur l'adresse d'écoute du bastion – vous pouvez également changer le port par défaut et activer la compression des données pour optimiser la bande passante de votre réseau (au détriment de la mémoire et du processeur). Par défaut, Royal Server est configuré pour fonctionner avec un

certificat auto-signé en SHA256, mais vous pouvez y ajouter votre propre certificat (attention, la clé privée est nécessaire).

Configuration de la sécurité

Rendez-vous dans le menu *Security Configuration* et activer l'option *Require Authentification*. Cette option force le client à présenter un couple « utilisateur/mot de passe » lorsqu'il tente d'accéder au serveur RS – ce compte peut-être enregistrer dans un fichier de configuration Royal Server (ce qui sera utile pour ne pas dévoiler le mot de passe du compte opérateur).

Si vous le souhaitez, vous pouvez également bloquer automatiquement les adresses IP qui tente de s'authentifier sans succès avec l'option *block IPs after unsuccessfull login attempts*. Vous pouvez définir la durée du blocage en minute (*Blocking time*), le nombre d'échec autorisé avant le déclenchement (*number of attempts*) et la période d'observation avant la réinitialisation du compteur d'échec (*time frame*).

Permissions

Les permissions octroient un accès pour un utilisateur à un certains niveau de droits sur l'application et ses données. Il existe trois niveaux de permission :

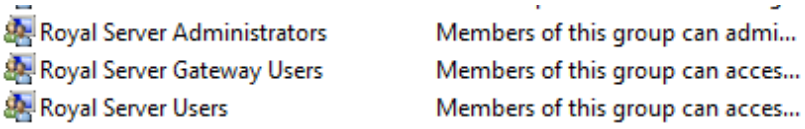
1. Le niveau *Users* :
   Donne un accès au serveur RS et à ses services. C'est le niveau requis pour un simple utilisateur qui souhaite accéder au Document Store par exemple, ou s'appuyer sur le *worker Account* pour faire effectuer des opérations à distance par le serveur RS.

2. Le niveau *Gateway Users* :
   Permet d'utiliser le service de passerelle pour forcer le flux à transiter via la Secure Gateway dans un flux SSH.

3. Le niveau *Administrators* :
   Permet d'administrer tout le serveur et ses services.

Chacun de ses niveaux de permissions est contrôler par un groupe local sur le système. Ce groupe devra contenir les groupes de domaine que nous avons pré-créés.

Pour configurer les permissions d'accès, allez dans le menu *Permissions* puis sélectionnez l'onglet *Users*. Cliquez sur *Configure…* pour ouvrir la console d'accès. A son premier lancement, trois nouveaux groupes locaux seront ajoutés dans votre base SAM :



Vous devrez ajouter, pour chacun, son pendant « domaine local » dans l'AD :

Groupe local	Groupe de domaine membre
Royal Server Administrators	L-S-RoyalServer-Admins
Royal Server Gateway Users	L-S-RoyalServer-GwayUsers
Royal Server Users	L-S-RoyalServer-Users

Une fois fait, fermez la console *Local User Manager* et redémarrez le service (bouton en haut à gauche de la console).

Enfin, l'onglet *Effective Permissions* vous permet de contrôler que le serveur récupère correctement les permissions d'un compte utilisateur.

Authentification multi-facteur

Sélectionnez le menu *Multi-Factor Authentication* puis cliquez sur l'onglet *Providers*. Cochez l'option *Enable Multi-Factor Authentication* puis sélectionnez les services à activer (Authenticator, DUO ou Yubikey).

Secure Gateway

Gateway Configuration

Sélectionner le menu *Secure Gateway* puis *Gateway Configuration* : définissez l'adresse d'écoute du service. Vous pouvez également modifier le port d'écoute du service SSH, la durée d'inactivité avant fermeture du tunnel et le nombre de connexion maximale autorisée.

Gateway Security Configuration

Pour augmenter la sécurité, sélectionnez *Gateway Security Configuration* puis cocher la case *Only Allow Royal TS/X as client.* Cela forcera la passerelle à n'accepter que les clients Royal TS et bloquera toute tentative de compromission du tunnel SSH depuis l'extérieur.

Permissions

L'utilisation de la passerelle requiert que les utilisateurs soient membre du groupe Royal *Server Gateway Users* – ce groupe a normalement déjà été configuré à l'étape précédente.

Document Store

Configuration

Sélectionnez *Document Store* puis *Configuration* dans le menu puis activez l'option *Enable Document Store*. Précisez l'emplacement par défaut de vos documents et le nombre de sauvegarde souhaité. Cochez l'option *Access Rules enabled* pour permettre d'ajouter un niveau de droit additionnel sur le document.

Chaque document se verra allouer une stratégie d'accès par utilisateur : lecture ou modification, accès autorisé ou interdit. Cette stratégie est l'une des clés de la sécurisation.

Documents

Cet emplacement permet de gérer les documents et les permissions d'accès en lecture ou modification (ou d'interdire l'accès à un document). Pour le moment, ce dernier reste vide.

Permissions

L'accès au Document Store est possible dès lors que le compte est membre du groupe *Royal Server Users*. L'onglet *Effective Permissions* permet de vérifier les droits d'accès d'un utilisateur ; l'onglet *Users* permet de gérer les permissions d'accès via le groupe local.

Le serveur est maintenant configuré avec les options de bases qui nous permettrons d'ajouter les utilisateurs et les documents de configuration. La sécurisation des comptes par MFA sera abordée plus tard, au travers du modus operandi de l'ajout d'un compte.

Royal TS

Récupération du binaire

Le binaire est téléchargeable à l'adresse suivante :

https://www.royalapps.com/ts/win/features

Installation

L'installation requiert un privilège d'administrateur local sur le système cible. Les instructions d'installation sont disponibles à cette adresse :

https://support.royalapps.com/support/solutions/articles/17000027816-install-and-uninstall-instructions

Scénario d'utilisation

Le document fera référence à l'utilisateur *Jetro ANVIDYALER* avec les informations suivantes :

Compte Utilisateur	Jetro.Anvidyaler
Compte Administrateur	Adm001.T0-ope
Serveur Royal Server et Secure Gateway	SRV016.LAB.MSSEC.FR

Configuration du MFA avec Yubikey

La configuration du MFA avec une Yubikey nécessite de créer au préalable une clé de connexion à l'API public de Yubico. Cette clé est nécessaire pour le service TOTP et vous génèrera un secret symétrique à échanger avec le service SaaS.

Configuration d'une Yubikey

- Récupérer l'une de vos clés Yubikey (n'importe laquelle)
- Lancez le *Yubikey Manager* puis sélectionnez *Applications* | *OTP*

- Sélectionnez *Configure* sous *Short Touch (Slot 1)*
- Sélectionnez *Yubico OTP* puis cliquez sur *next*
- Cochez la case *Use Serial* pour le champ *Public ID* – sauvez la valeur dans coffre-fort numérique (elle sera nécessaire pour la configuration de l'utilisateur)
- Cliquez sur le bouton *Generate* pour le champ *Private ID*
- Cliquez sur le bouton *Generate* pour le champ *Secret Key*
- Cochez la case *Upload* puis cliquez sur *Finish*

Configuration du serveur SaaS Yubico

- Rendez-vous sur le site web https://upgrade.yubico.com/getapikey/
- Dans le champ *email address*, saisissez une adresse mail servant de référence

- Positionnez votre curseur dans le champ *Yubico OTP*, puis appuyer brièvement sur le capteur de la Yubikey
- Cochez la case *I have read the term and condition*
- Cliquez sur *Get API*
- Sauvegarder dans un coffre-fort numérique le *client ID* et la *Secret Key* qui s'affiche (vous en aurez besoin pour configurez le service Yubikey sur le serveur RS)

Configuration du service Yubikey

- Lancez la console Royal Server
- Sélectionnez la section *royal Server* en bas à gauche puis *Multi-Factor Authentication*
- Sélectionnez *Providers* puis Cochez l'option option *Yubikey*
- Cliquez sur le bouton *Configure…* en face de *Yubikey*
- En face de *Client ID*, saisir le Client ID obtenu précédemment
- En face de *Secret Key*, saisir la Secret Key générée précédemment
- Cliquez sur *OK*
- Sauvez la configuration puis redémarrer le service Royal Server

Récupérer le Public ID d'une Yubikey

- Connectez la clé à votre système
- Lancez notepad, positionnez le curseur dans la zone de saisie puis appuyez brièvement sur le capteur de la Yubikey
- Récupérer les 12 premiers caractères de la chaine – ils sont identiques au *Public ID* configuré précédemment lors de la configuration de la Yubikey.

Configuration d'un utilisateur avec le MFA Yubikey

- Lancez la console Royal Server
- Sélectionnez la section *royal Server* en bas à gauche puis *Multi-Factor Authentication*
- Cliquez sur *Add…* pour ajouter un nouvel utilisateur
- Configurer l'utilisateur à associer à un code MFA depuis l'annuaire AD
- En face de *Provider*, sélectionnez *Yubikey*
- Sélectionnez l'accès à protéger (Document Store)
- Ajouter un commentaire si nécessaire dans le champ *Comment*
- Positionner le *Caching Time* à 1 minute
- Saisissez le *Public ID* de la clé associée à l'utilisateur dans le champ *Token ID*
- Cliquez sur *OK*

Créer un modèle de document Royal TS

Le modèle de document vous permettra de gagner du temps dans la création d'un nouvel utilisateur : en effet, pour protéger l'identifiant de Tier 0 utilisé par l'opérateur, ce dernier doit être déclaré dans un objet de connexion (Royal Server Object) et dans les paramètres de configuration du document – une fois fait, le document peut être verrouillé et le compte ainsi protégé.

Les documents présents dans le Document Store ne peuvent pas être modifié directement sur le serveur, ni exporté ; seul un administrateur du document sera alors en mesure de le modifier, depuis une station de travail (idéalement, depuis le serveur bastion lui-même). Le document est protégé contre la modification par un mot de passe que seul l'administrateur devra connaitre (l'utilisation de KeePass est recommandée).

Pour que l'authentification soit possible, vous devrez configurer la chaine de dossier jusqu'à la racine avec les mêmes paramètres d'authentification (*Use Credential From the Parent Folder*) de sorte que l'arborescence aboutisse à la racine du document, qui contient le login.

> **Note : le principe de connexion retenu ici implique que l'utilisateur ne soit pas obligé de se réauthentifier sur le serveur cible. Si vous souhaitez activer cette sécurité, il ne sera pas nécessaire d'enregistrer le login de l'utilisateur à la racine. Toutefois, dans ce contexte, une telle option exposerait l'authentification à un vol de mot de passe, ce dernier étant en présent en mémoire sur la station de connexion Tier 2 pendant un laps de temps donné, à moins d'utiliser la connexion par certificat (Smart Card Logon).**

Pour créer un modèle, qui contiendra toutes les connexions qu'un utilisateur devrait avoir, procédez comme suis :

Création du modèle

- Connectez sur le serveur d'administration de Tier 0, sur lequel le client Royal TS est installé (aucune licence n'est nécessaire)
- Lancez le client Royal TS
- Sélectionnez *New* en haut à droite
- Nommez le document selon vos souhaits et laissez le type de document sur *Shared*
- Sélectionnez *Security* et cochez l'option *Enable Encryption*
- Définissez un mot de passe pour l'accès au document – ce mot de passe sera saisie par l'utilisateur qui voudra modifier le document (ce mode ne donnera pas accès au mot de passe des comptes).
- Cliquez sur *OK*
- Faites un clic-droit sur le document nouvellement créé et sélectionnez *Properties*
- Saisissez le mot de passe précédemment créés
- Dans la section *Common*, cliquez sur *Credentials*

- Dans le menu déroulant, sélectionnez *Spécify Username and Password*
- Dans le champ *Username*, saisir le nom du compte de tier 0 sous la forme NetBIOS (*MSSEC\ADM001.T0-OPE*)
- Saisissez le mot de passe du compte dans le champ *Password*
- Cliquez sur OK

Une fois le fichier préparer, deux actions restent à faire : configurer un objet de connexion Secure Gateway et ajouter toutes les connexions de votre environnement (dans cet exemple, nous n'ajouterons qu'une connexion RDP).

Ajouter l'objet de connexion Secure Gateway

- Positionnez-vous à la racine du document
- Sélectionnez *Add* puis *Secure Gateway* (par clic-droit ou via le bandeau supérieur)
- Dans le champ *Display Name*, indiquer un nom décrivant le serveur de passerelle (*SG Tier 0* par exemple)
- Dans le champ *Computer Name*, indiquer le nom pleinement qualifié du serveur de passerelle (*srv016.LAB.MSSEC.FR*)
- Si besoin, adaptez le Port SSH à vote configuration et indiquez une description
- Dans la section *Common*, sélectionnez *Credentials*
- Modifiez le champ *Configuration* pour la valeur *Specify Username and Password*
- Dans le champ *Username*, saisir le nom du compte de tier 0 sous la forme NetBIOS (*MSSEC\ADM001.T0-OPE*)
- Saisissez le mot de passe du compte dans le champ *Password*
- Cliquez sur OK

Ajouter un nouveau dossier d'organisation

- Positionnez-vous à la racine du document
- Cliquez sur *Add* puis sélectionnez *Folder*
- Dans le champ *Display Name*, indiquez le nom du dossier (DEMO)
- Dans le champ *Description*, indiquez un commentaire explication
- Dans la section *Common*, sélectionnez *Credentials*
- Dans le champ *Configuration*, sélectionnez *Use Credential From the Parent Folder*

Configurer un dossier préexistant

- Faites un clic-droit sur le dossier existant et sélectionnez *Properties*
- Dans la section *Common*, sélectionnez *Credentials*
- Dans le champ *Configuration*, sélectionnez *Use Credential From the Parent Folder*

Ajouter une connexion RDP

- Cliquez sur *Add* puis sélectionnez *Remote Desktop Protocole Connection*
- Dans le champ *Display Name*, saisir le nom NetBIOS de la cible (SRV001 – Demo Server)

- Dans le champ *Computer Name*, saisir le nom pleinement qualifié de la cible (SRV001.LAB.MSSEC.FR)
- Ajouter une description pour aider à identifier le rôle du serveur
- Dans la section *Common*, sélectionnez *Credentials*
- Dans le champ *Configuration*, sélectionnez *Use Credential From the Parent Folder*

Note : puisque le document contient un compte utilisateur unique, chaque utilisateur devra avoir son document propre et aura la charge de son évolution (hors mot de passe, qui est sous la responsabilité de l'administrateur en cas de changement).

Une fois le document terminé, vous devez protéger les secrets de connexion contre l'exfiltration : cela est possible en activant les options de verrouillage du fichier. Une fois activé, la lecture ou la modification du compte passeront nécessairement par ce mot de passe (il est donc important de le conserver dans un coffre-fort numérique). Notez également que ce mot de passe ne peut pas être changé plus tard (il faudra créer un nouveau document).

Verrouillage des informations sensibles

- Faites un clic-droit sur le nom du document et sélectionnez *Properties*
- Saisissez le mot de passe de protection du document
- Sélectionnez *Security* dans le menu de gauche
- Sélectionnez l'onglet *Lockdown*
- Cochez l'option *Encrypt Complete File*
- Appuez sur le bouton *Set Lockdown Password…*
- Définissez un mot de passe fort et complexe puis cliquez sur *Apply*
- Cochez l'option *Do not allow to reveal passwords in this document*
- Cliquez sur *OK*
- Faites un clic-droit sur le nom du document et sélectionnez *Merge and Save*
- Enregistrer le fichier dans un endroit protégé (il ne doit être accessible qu'aux administrateurs)
- Fermez le document et Royal TS

Modifier un modèle de document

Avant d'importer un modèle de document dans le Document Store, vous pourriez avoir besoin de modifier une ou plusieurs données de celui-ci (par exemple, le nom de l'utilisateur de Tier 0 et son mot de passe).

Modification d'un modèle de document

- Allez à l'emplacement sécurisé où son enregistrés les fichiers modèles
- Copier le modèle de document à modifier et donnez-lui un nouveau nom
- Editez le fichier avec Royal TS

Modifier une connexion (utilisateur et administrateur)

- Sélectionnez la connexion à modifier
- Faites-un clic-droit dessus et sélectionnez *Properties*
- Modifiez les informations souhaitez
- Cliquez sur *OK.*

Modifier le compte de Tier 0 (administrateur uniquement)

- Faites un clic-droit sur le document et sélectionnez *Unlock Document*
- Saisissez le mot de passe de *lockdown* du document
- Pour modifier le compte pour toutes les connexions, modifier les informations directement dans les propriétés du fichier après avoir saisie le mot de passe de protection
- Pour modifier le compte de connexion à la Secure Gateway, modifiez l'objet Secure Gateway directement
- Cliquez sur *OK*
- Faites ensuite un clic-droit sur le document et sélectionnez *Merge and Save* puis *Lock*

Modifier le mot de passe de LockDown (administrateur uniquement)

- Faites-un clic-droit sur le document et sélectionnez *Unlock Document*
- Saisissez le mot de passe de *lockdown* du document
- Faites-un clic-droit sur le document et sélectionnez *Properties*
- Saisissez le mot de passe de protection du document
- Sélectionnez *Security* dans le menu de gauche
- Sélectionnez l'onglet *Lockdown*
- Appuez sur le bouton *Set Lockdown Password…*
- Définissez un mot de passe fort et complexe puis cliquez sur *Apply*
- Cliquez sur *OK*
- Faites ensuite un clic-droit sur le document et sélectionnez *Merge and Save* puis *Lock*

Importer un modèle dans le Document Store

Une fois le document prêt, vous devrez le mettre à disposition des utilisateurs dans le Document Store. Cette étape permet de publier le document et d'attribuer des droits d'accès à ce dernier.

Import d'un document

- Lancez la console Royal Server
- Sélectionnez la section *document Store* en bas à gauche de la fenêtre
- Sélectionnez *Document* dans la partie supérieur du menu de gauche
- Cliquez sur le bouton *Add…* et sélectionnez *Existing…*
- Dans le champ File *to import*, Indiquez le chemin vers le fichier modèle à utiliser (ou utilisez l'assistant en cliquant sur … à droite du champ de saisie)

- Au besoin, renommez le document : ce nom sera affiché dans la liste des documents que verra l'utilisateur
- Ajouter un commentaire si besoin
- Spécifier le mot de passe de protection du document pour que Royal Server puisse l'accéder
- Cochez l'option *Document can only be opened via Royal Server* (l'option va chiffrer tous les éléments du fichier et les stockés dans sa base documentaire)
- Cliquez sur OK

Une fois importer, le document doit être sécurisé pour l'accès :

Autorisation d'accès sur un document

- Lancez la console Royal Server
- Sélectionnez la section *document Store* en bas à gauche de la fenêtre
- Sélectionnez *Document* dans la partie supérieur du menu de gauche
- Sélectionnez le document à protéger
- Cliquez sur le bouton *Edit…* à droite de la fenêtre et sélectionnez *Edit Access Rules…*
- Cliquez sur *Add…* en bas de la fenêtre
- Définissez le niveau d'accès sur *Modify* et *Grant*
- Cliquez sur *Add…*
- Ajouter l'utilisateur Tier (Jetro.Envidyaler)
- Cliquez sur *Close*

Ajout d'un utilisateur

Les opérations décrites ci-dessous doivent être réalisées dans cet ordre pour ajouter un nouvel utilisateur au bastion. Le document Royal TS, hébergé dans le Document Store, doit avoir été créé au préalable.

Autoriser la connexion au Bastion

Pour permettre à l'utilisateur de se connecter au bastion, ajouter le compte *Jetro.Anvidyaler* au groupe Active Directory suivant :

- G-S-T0-RoyalServer-Users

L'accès octroyé permet également de parcourir le Document Store.

Autoriser la connexion à la Secure Gateway

La connexion au Secure Gateway n'est permise qu'au compte de Tier 0.

Pour autoriser *adm001.T0-ope* à accéder à la Secure Gateway et ainsi se connecter aux systèmes cibles, ajoutez le compte dans le groupe Active Directory suivant :

- G-S-T0-RoyalServer-Users
- G-S-T0-RoyalServer-GwayUsers

Configurer l'accès MFA

L'accès MFA doit être activé pour l'accès au Document Store et la connexion à un système.

Pour sécuriser l'accès, connectez-vous sur le serveur Royal Server puis, Dans le menu de gauche, sélectionnez *Royal Server* et *Multi-Factor Authentication*. Positionnez-vous sur l'onglet *Users*.

Enrôlement du compte Tier 0 (Secure Gateway + Authenticator)

- Cliquez sur *Add…*
- Depuis la fenêtre *Enroll User for MFA*, cliquez sur *Select User…*
- Saisir le compte de Tier 0 *adm001.T0-ope* et cliquez sur *OK*
- Dans le champ *Provider*, sélectionnez *Generic TOTP*
- Cochez l'option *Secure Gateway*
- Ajouter un commentaire dans le champ description (*MFA for Jetro ANVIDYALER (Tier 0 Opérateur)* par exemple)
- Définissez le temps de cache de session à *1 minute*, afin d'obliger l'utilisateur à se connecter au MFA pour chaque connexion (une session en cache pouvant être exploitée par n'importe-qui sans plus de contrôle)
- Dans le champ *Issuer*, indiquez *Royal Server Tier 0*
- Dans le champ *Label*, indiquez le login de connexion *ADM001.T0-OPE*
- Cliquez sur *OK*
- Le QR-Code s'affiche à l'écran : scannez-le avec votre application d'authentification
- Cliquez sur *close*

Enrôlement du compte Tier 2 (Document Store + Yubikey)

- Cliquez à nouveau sur *Add…*
- Depuis la fenêtre *Enroll User for MFA*, cliquez sur *Select User…*
- Saisir le compte de Tier 2 *Jetro.Anvidyaler* et cliquez sur *OK*
- Dans le champ *Provider*, sélectionnez *Yubikey*
- Cochez l'option *Document Store*
- Ajouter un commentaire dans le champ description (*MFA for Jetro ANVIDYALER (Tier 2)* par exemple)

- Définissez le temps de cache de session à *1 minute*, afin d'obliger l'utilisateur à se connecter au MFA pour chaque connexion (une session en cache pouvant être exploitée par n'importe-qui sans plus de contrôle)
- Dans le champ *Yubikey ID*, indiquez le numéro de série de la Yubikey
- Cliquez sur *OK*
- Le QR-Code s'affiche à l'écran : scannez-le avec votre application d'authentification
- Cliquez sur *close*

Configurer le poste client

Le client doit être équipé de Royal TS et pouvoir accéder aux serveurs Royal Server et Secure Gateway. La configuration est ensuite limitée à l'ajout d'un objet Royal Server dans un document Royal TS.

Création du document

- Lancez le client Royal TS
- Sélectionnez *New* en haut à droite
- Nommez le document selon vos souhaits et laissez le type de document sur *Personal (Overwrite File)*
- Sélectionnez *Security* et cochez l'option *Enable Encryption*
- Définissez un mot de passe pour l'accès au document
- Cliquez sur *OK*
- Positionnez-vous à l'endroit ou vous souhaitez stocker l'objet
- Faites *Add…* puis sélectionnez *Royal Server*
- Donnez un nom d'affichage (par exemple *Bastion Tier 0*)
- Saisissez le nom pleinement qualifié dur serveur RS (Srv016.LAB.MSSEC.FR)
- Sélectionnez *Royal Server Credentials* dans le menu de gauche
- Saisissez votre nom d'utilisateur (Jetro.Anvidyaler) et votre mot de passe
- Cliquez sur *OK*
- Faites ensuite un clic-droit sur le document et sélectionnez *Merge and Save* puis *Lock*

Accéder au Document Store

L'accès au Document Store permet à l'utilisateur de se connecter aux ressources anonymement.

Accès à Document du Document Store

- Lancez le client Royal TS
- Ouvrez le document contenant votre objet Royal Server pour la connexion au Tier 0
- Saisissez le mot de passe de protection du fichier Royal TS

- Depuis le bandeau supérieur, cliquez sur *Open* puis sélectionnez votre objet Royal Server
- Une fenêtre s'affiche avec les documents contenus dans le Document Store pour lequel vous disposez d'un droit d'accès : sélectionnez le document à ouvrir et cliquez sur *OK*
- Saisissez le code TOTP demandé en appuyant brièvement sur le capteur de la Yubikey

Seules les informations sensibles et les propriétés du document sont protégées par le mot de passe du document : l'utilisateur peut librement modifier le document pour ajouter des dossiers, des connexions, … Pour déverrouiller le document, vous devrez saisir d'abord le mot de passe de lockdown puis le mot de passe du document.

Le mot de la fin…

Nous espérons sincèrement que cette documentation vous sera utile et aidera à mieux protéger les identités sensibles de vos annuaires Active Directory.

Nos équipes se tiennent à votre disposition pour vous aider à implémenter le modèle, n'hésitez pas à nous contacter :

- Sur LinkedIN : https://www.linkedin.com/company/mssec/
- Sur Discord : https://discord.gg/HJsaaPYn
- Sur notre site web : https://mssec.fr

MS-SEC

Identity security