Understand Terminal Services, Citrix and Umbrella Integration with Active Directory

Contents

Introduction

This document describes Terminal Services, Citrix, and Umbrella integrarion with Active Directory.

Overview

Applies to: Windows Terminal Services and Remote Desktop Services, Windows 10 Enterprise multi-session, Citrix XenApp and XenDesktop

Terminal Services and Citrix servers provide the ability for multiple, simultaneous client sessions to be hosted on a single server. There are two distinct configurations:

- **Remote Desktop Service (RDS)**. Multiple users run a session on a single virtual machine on the same server. These sessions all share the same OS and IP address. This is commonly referred to as Terminal Services.
- **Virtual Desktop Infrastructure (VDI)**. The server runs a pool of virtual machines and each user connects to a unique VM, with its own Operating System and IP address

Web Policy: Applicable to RDS and VDI

Secure Web Gateway with SAML cookies based authentication via PAC file, CDFW Tunnel and Proxy Chain support multiple users to a single IP address. It means virtual desktops (Citrix/TS) is supported per user Web Policy enforcement.

DNS Policy: RDS with AD integration

We do not support RDS / Remote Desktop Session Host / Terminal servers for per-user identification. This includes the Azure only Windows 10 Enterprise multi-session OS.

The client sessions hosted on these servers share a single IP address: the one belonging to the host machine. Umbrella Active Directory (AD) integration with virtual appliances (VAs) rely on unique user-to-IP address mappings in order to work correctly. *In short this means that per-user identification is not possible in any situation where users share the same source IP address.*

When multiple logged-in users are sharing the same IP this adversely affects policy application and

reporting. All users receive the same policy and the identified user can continuously change based on the last logged on user.

DNS Policy: Solution - RDS with AD integration

The best way to tackle this problem is to configure a unique policy for the **IP address** of your Terminal Server or Citrix server. This means that all users of the Terminal Server receive the same, consistent policy.

1. Create an **Internal Network** in 'Deployments > Internal Networks'. This covers the /32 IP address of your Terminal Server. Assign the network to the same Umbrella site as the applicable Virtual Appliance(s).
2. Navigate to the Policy Wizard and create a new **Policy**.
3. In the **Select Identities** section, select click on 'Sites' and then open the relevant Umbrella site.
4. Select the **Internal Network** identity you created previously
5. Configure the policy as you normally would
6. After you have created the policy for your Terminal server, be sure to order this policy at the top of the list of policies so it takes precedence over any user-based policies.

Alternatively, it is possible to create a policy for the Terminal Server based on the **AD Computer** identity. This method operates in the same way; all users of the server are identified as the Terminal Server computer name. However, for this to work consistently the VA must be configured in a way that optimizes the host-to-IP mappings. Please see the **AD Host GUID Timeout instructions** for more details, or contact Umbrella support for assistance.

DNS Policy: Using VDI with AD integration

VDI-type deployments - where there is a unique virtual machine running for each user - can still receive per-user identities. The requirements are as follows:

- **Virtual Appliance** - Each user must have a unique source IP which is visible to the Virtual Appliance. The source IP must not be subject to "Source NATing" before it reaches the appliance.
- **Roaming Client** - AD integration in the Roaming Client is possible when the Roaming Client is installed on each Virtual Machine. Deployment in this manner is more feasible when each user has a persistent (eg. personal) virtual machine.