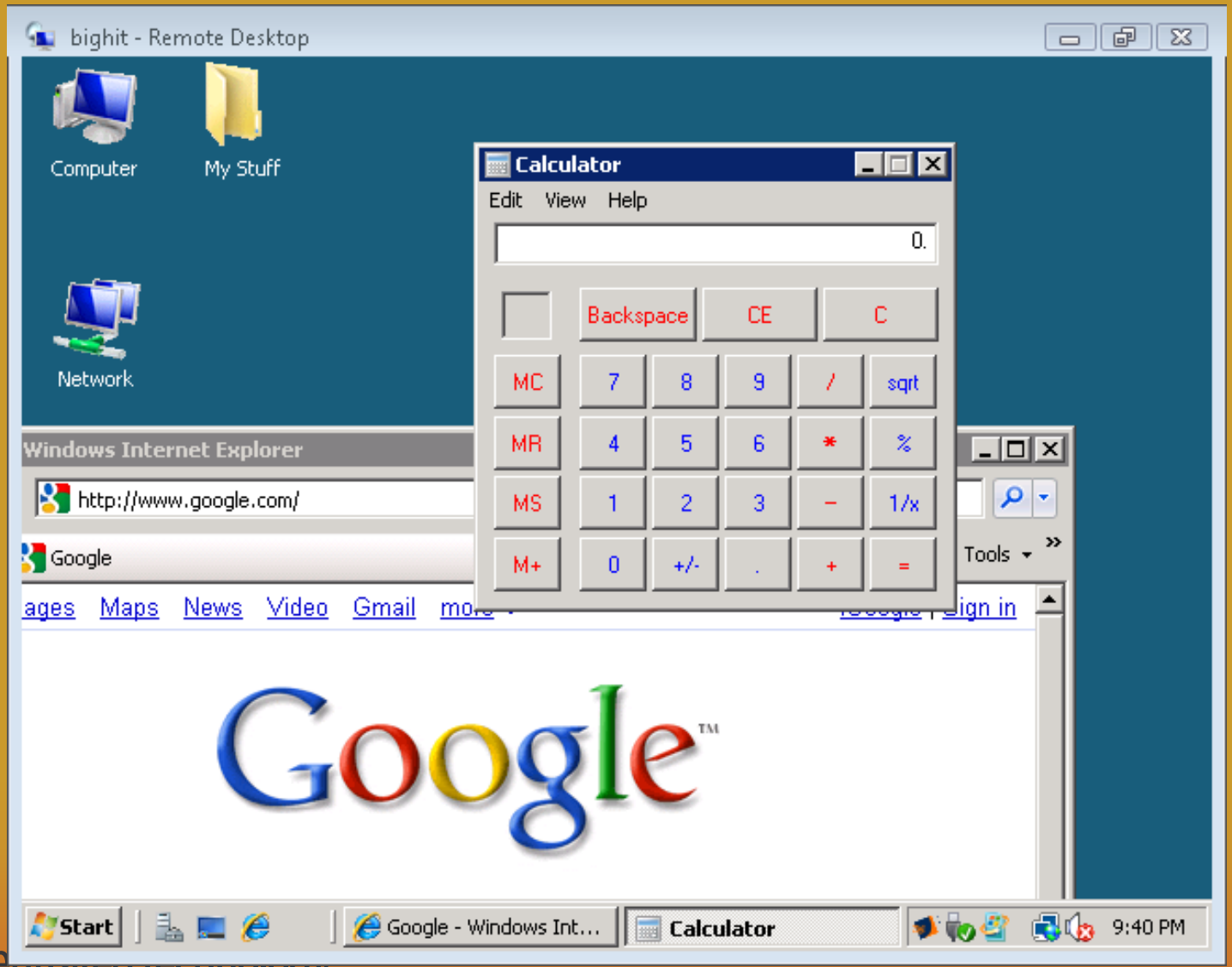
Extending Applications to…Everywhere!

Your Guide to Internet-enabling Remote Desktop Services

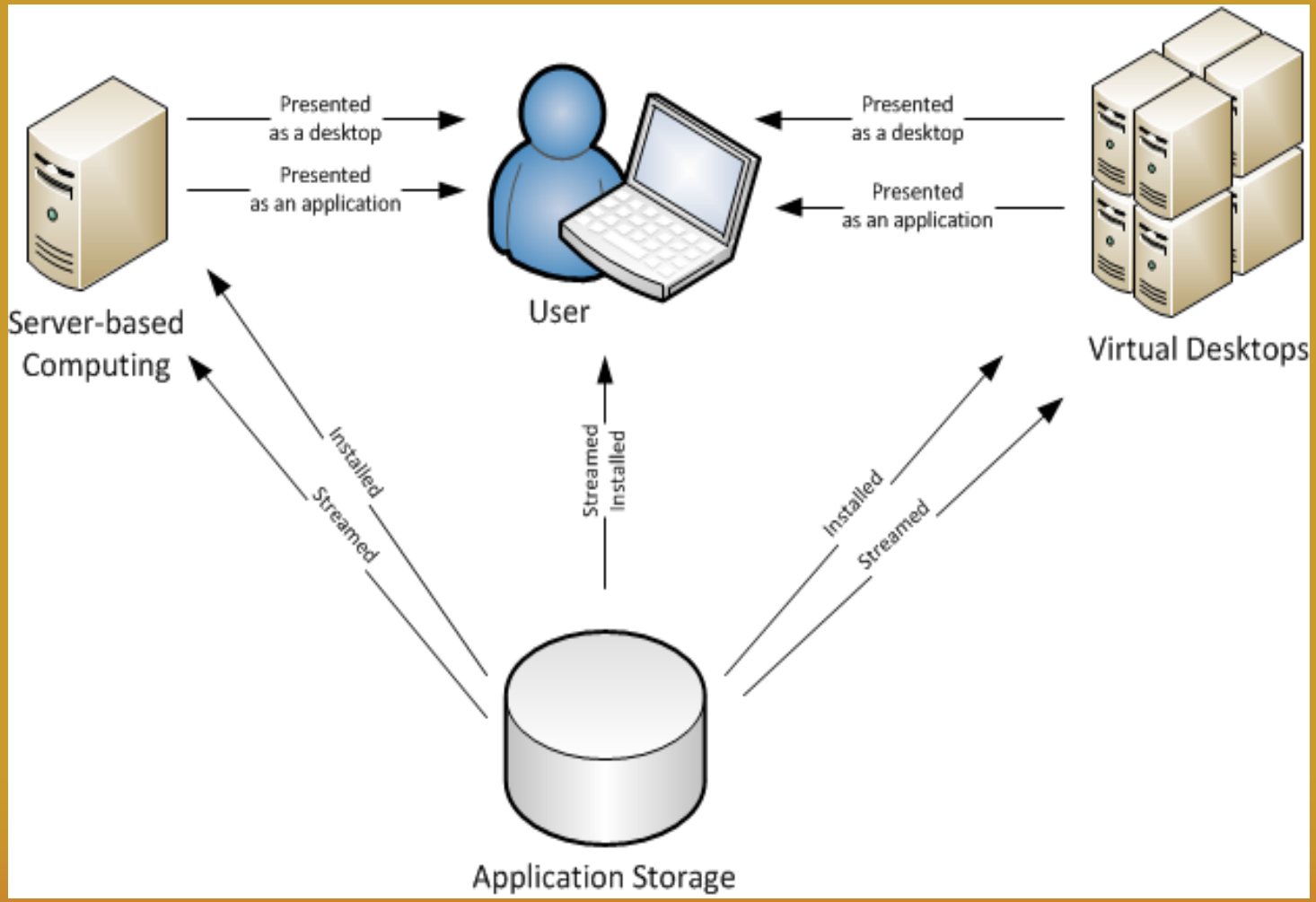
Greg Shields
Senior Partner and Principal Technologist,
Concentrated Technology, LLC
http://ConcentratedTech.com

concentrated technology

Not Just About Desktops Any More!



Not Just About Sessions Either!



concentrated technology

New Realization:

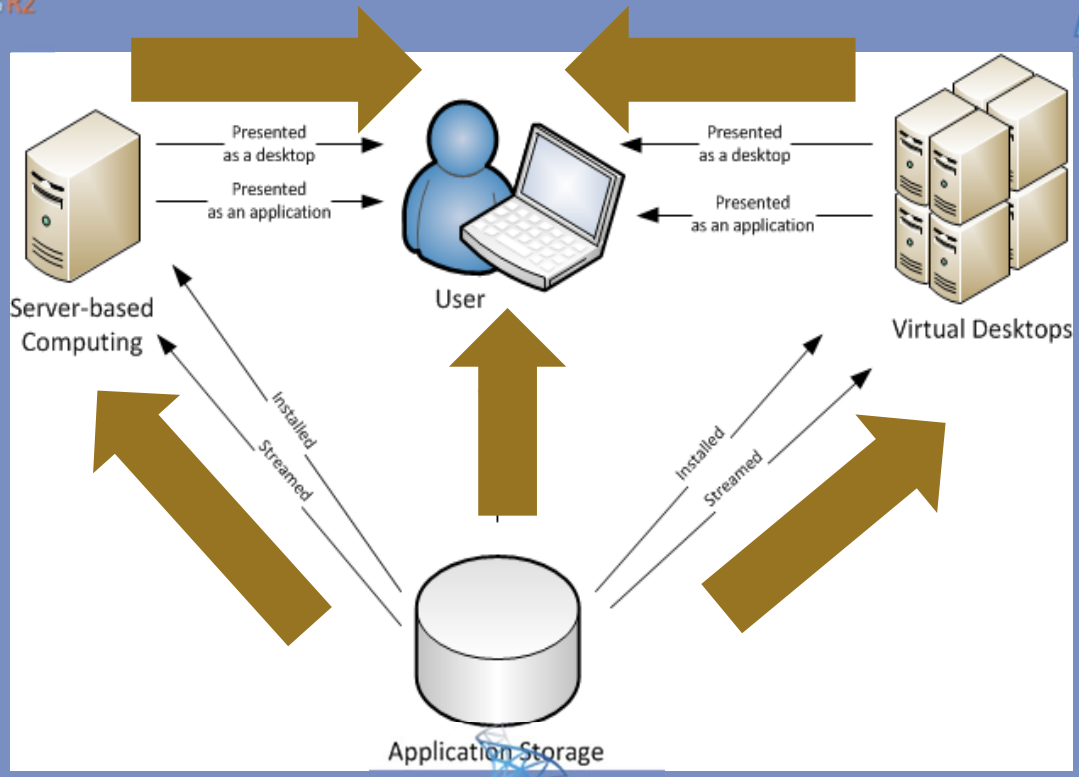
RDS is a Key App Delivery Mechanism

Microsoft Virtual Desktop Infrastructure

Windows Server 2008 R2 Remote Desktop Services

Windows Server 2008 R2 Remote Desktop Services

Microsoft Hyper-V

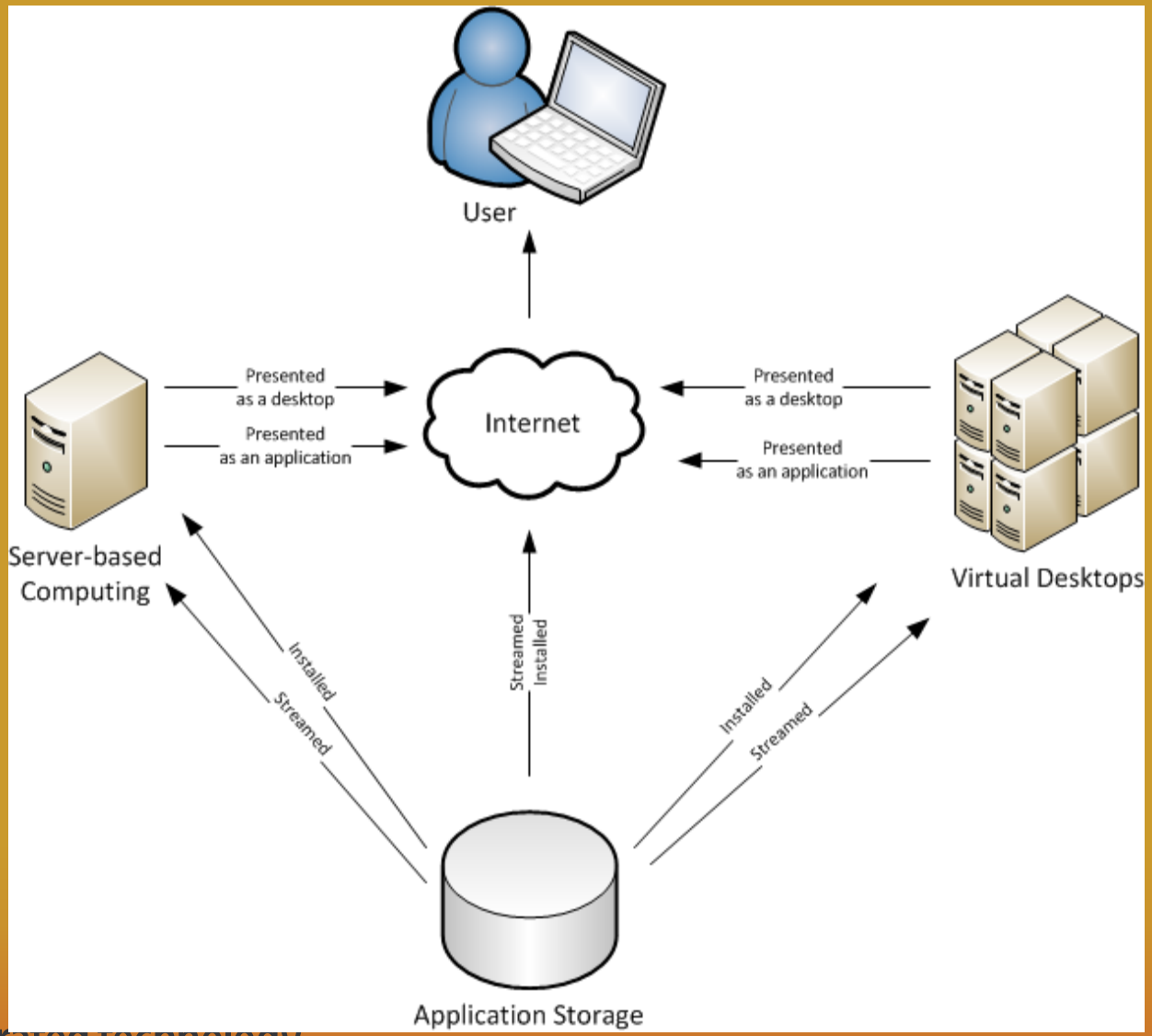


Microsoft System Center

Microsoft Application Virtualization

concentrated technology

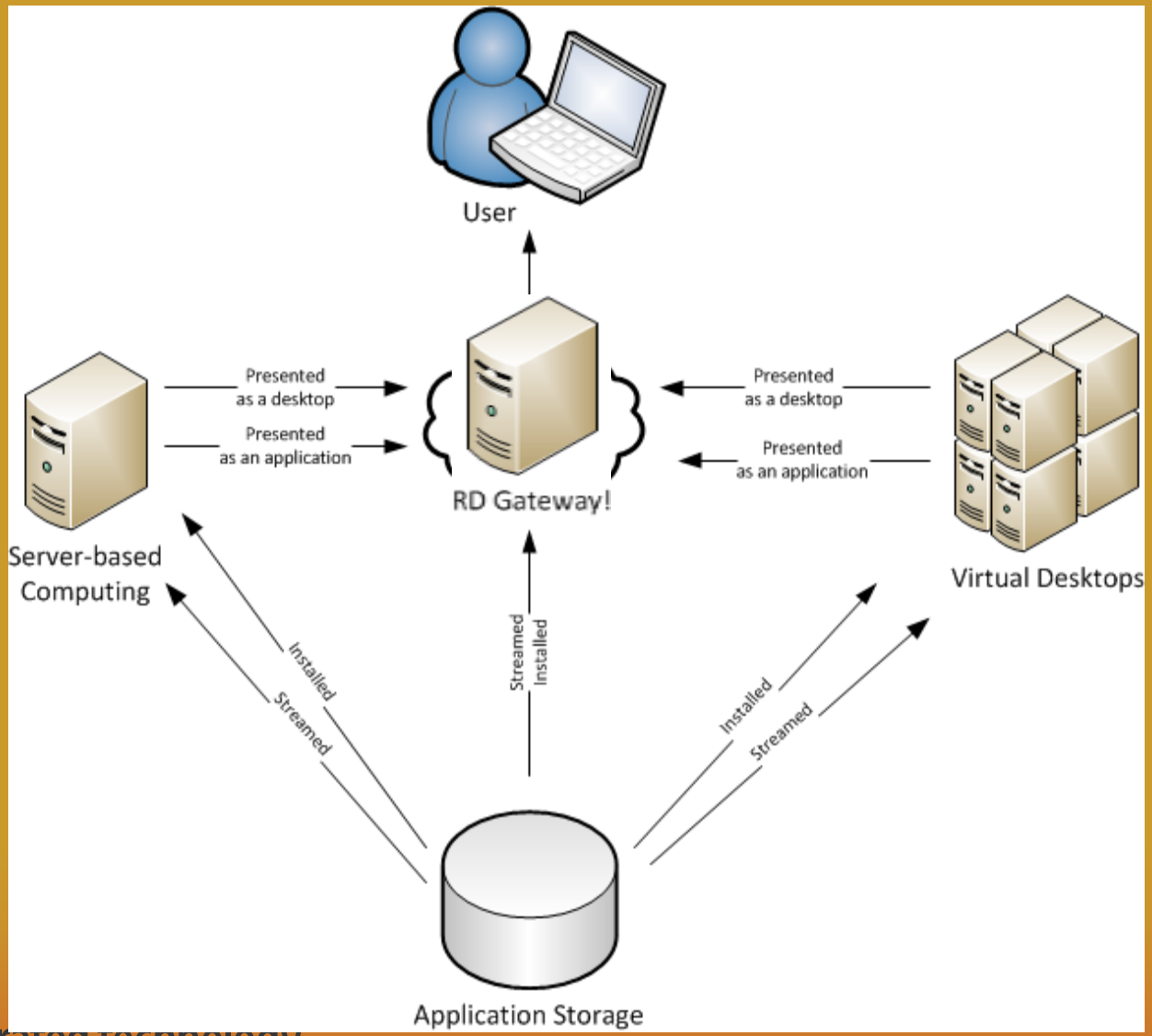
What about Users Outside the Office?



concentrated technology

Session, Meet the RD Gateway!

All Together Now: "Hi, RD Gateway."



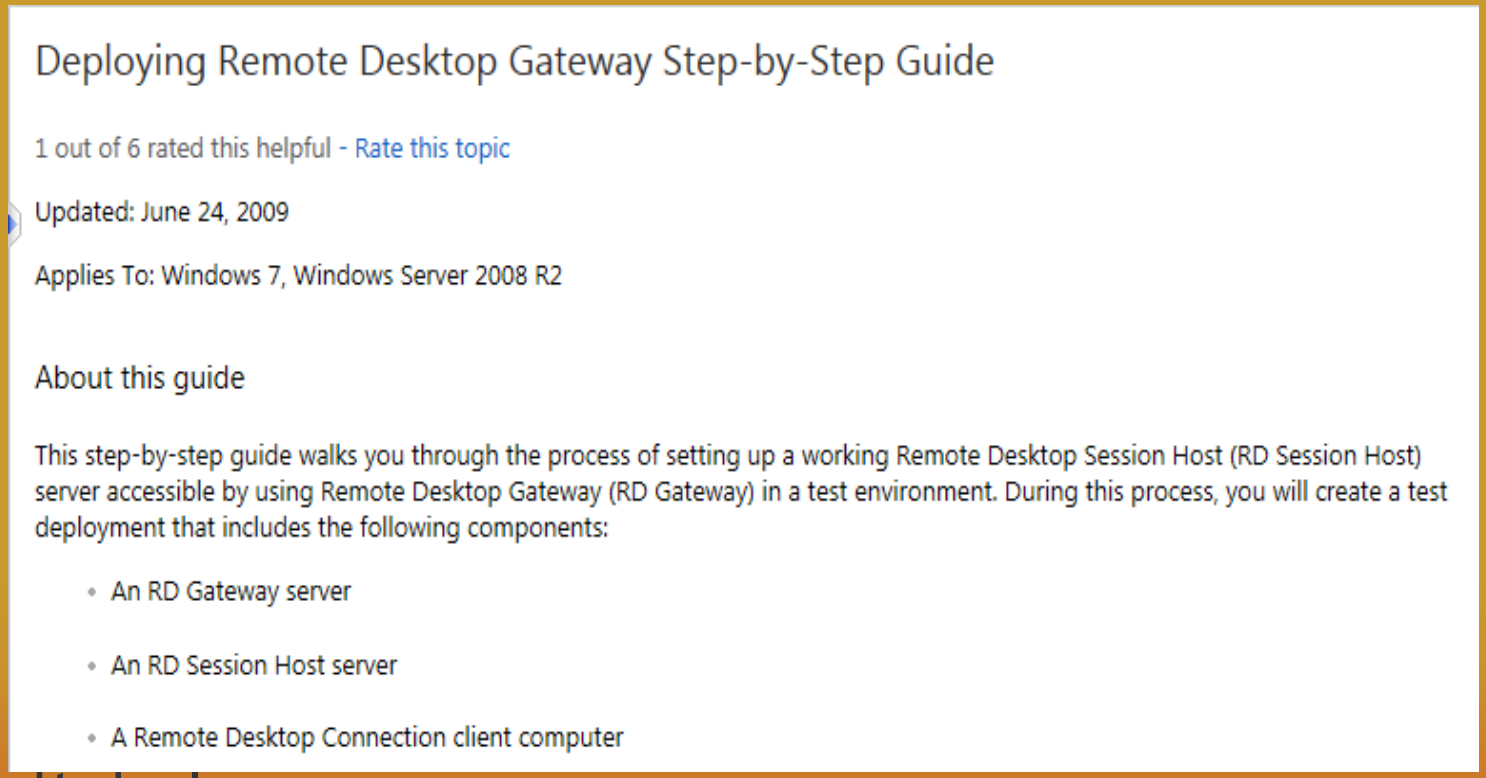
concentrated technology

A RemoteApp! Live! Over the Internet! Big Wow!

dramatic demo
to keep people awake

RDS' Most Misunderstood Role Service

- Doesn't TechNet's documentation just drive you nuts sometimes?



Deploying Remote Desktop Gateway Step-by-Step Guide

1 out of 6 rated this helpful - Rate this topic

Updated: June 24, 2009

Applies To: Windows 7, Windows Server 2008 R2

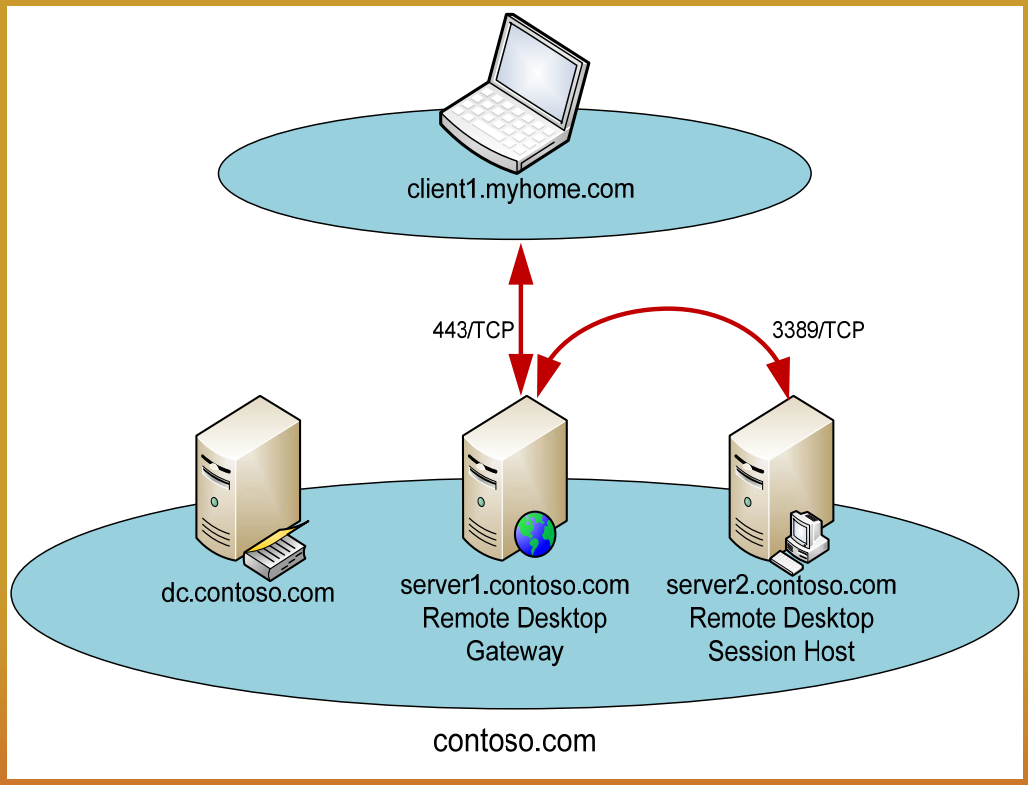
About this guide

This step-by-step guide walks you through the process of setting up a working Remote Desktop Session Host (RD Session Host) server accessible by using Remote Desktop Gateway (RD Gateway) in a test environment. During this process, you will create a test deployment that includes the following components:

- An RD Gateway server
- An RD Session Host server
- A Remote Desktop Connection client computer

RDS' Most Misunderstood Role Service

- Doesn't TechNet's documentation just drive you nuts sometimes?
  - This is what it suggests…

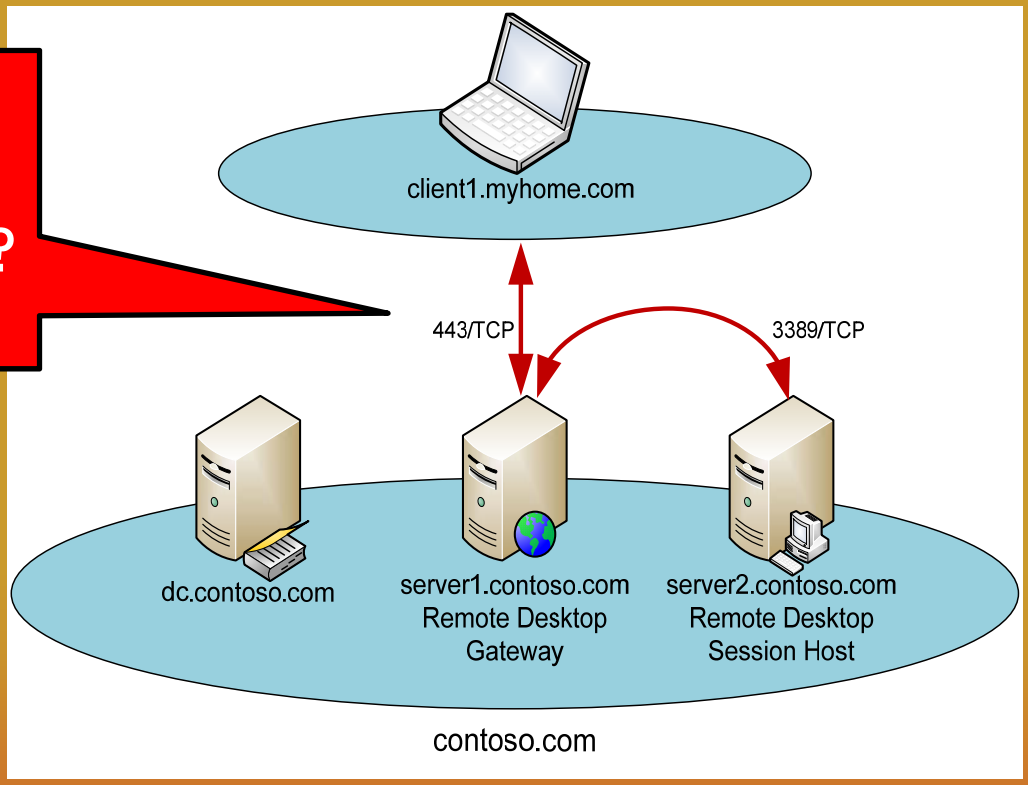


concentrated technology

RDS' Most Misunderstood Role Service

- Doesn't TechNet's documentation just drive you nuts sometimes?

…but wait a minute!
Anyone see an issue here?



concentrated technology

The Hard-to-Glean-from-TechNet Part:

There are Four RDG Architectures

concentrated technology

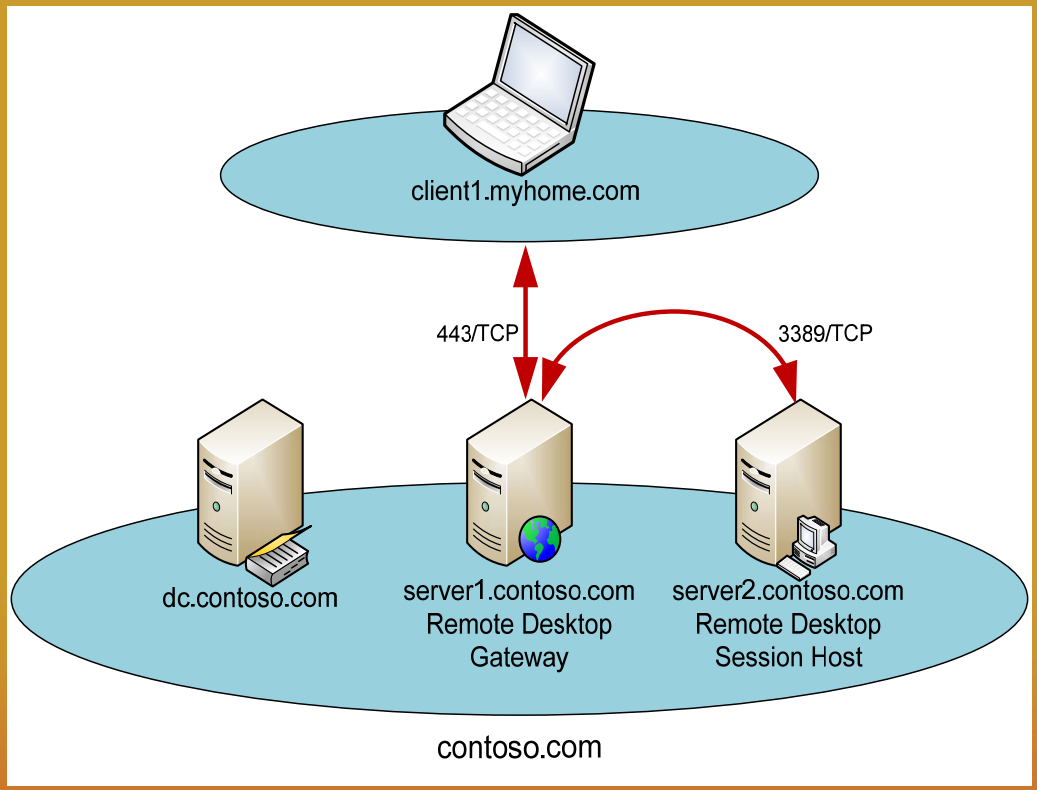
The Hard-to-Glean-from-TechNet Part:

There are Four RDG Architectures

- Option #1: No DMZ. RDG in the LAN.

#1: No DMZ. RDG in LAN.

- Totally doable.
  - Makes Security people squirm.



concentrated technology

The Hard-to-Glean-from-TechNet Part:

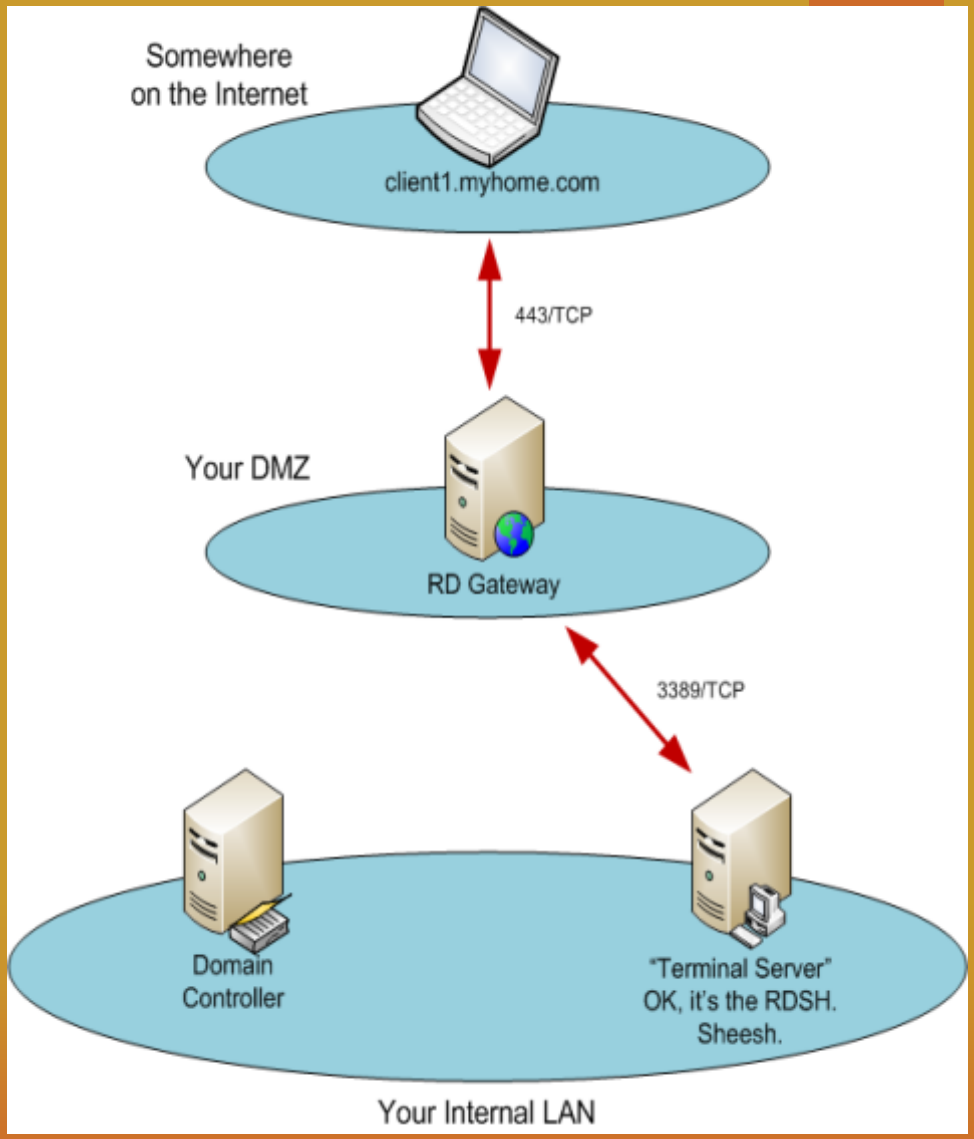
There are Four RDG Architectures

- Option #1: No DMZ. RDG in the LAN.
- Option #2: RDG in DMZ. No internal AD for RDG.

concentrated technology

#2: RDG in DMZ. Internal AD.

- Also relatively simple.
  - Security folks likey.
  - Users don't: No SSO.
- Management headache.
  - RDG in Workgroup.
  - One set of credentials for RDG, another set for internal AD.
  - Oy.



concentrated technology

The Hard-to-Glean-from-TechNet Part:

There are Four RDG Architectures

- Option #1: No DMZ. RDG in the LAN.
- Option #2: RDG in DMZ. No internal AD for RDG.
- Option #3: RDG in the DMZ. Internal AD for RDG!

OK, I lied.

There are SIX RDG Architectures

- Option #1: No DMZ. RDG in the LAN.
- Option #2: RDG in DMZ. No internal AD for RDG.
- Option #3: RDG in the DMZ. Internal AD for RDG!
  - Option #3a: Use internal DC. Open lots of ports.
  - Option #3b: Internal RODC in the DMZ. Open lots of ports.
  - Option #3c: Forest trust to DC in the DMZ.

Humorous Aside:

Who has Read this TechNet Article?

Article ID: 179442 - Last Review: March 19, 2012 - Revision: 16.0

How to configure a firewall for domains and trusts

View products that this article applies to.

This article was previously published under Q179442

Humorous Aside:

Who has Read this TechNet Article?

Article ID: 179442 - Last Review: March 19, 2012 - Revision: 16.0

How to configure a firewall for domains and trusts

View products that this article applies to.

This article was previously published under Q179442

- Is this not the most ridiculous TechNet article ever?

Humorous Aside:

Who has Read this TechNet Article?

- Is this not the most ridiculous TechNet article ever?
  - Not to mention, its in Revision 16.

Humorous Aside:

Who has Read this TechNet Article?

Article ID: 179442 - Last Review: March 19, 2012 - Revision: 16.0

How to configure a firewall for domains and trusts

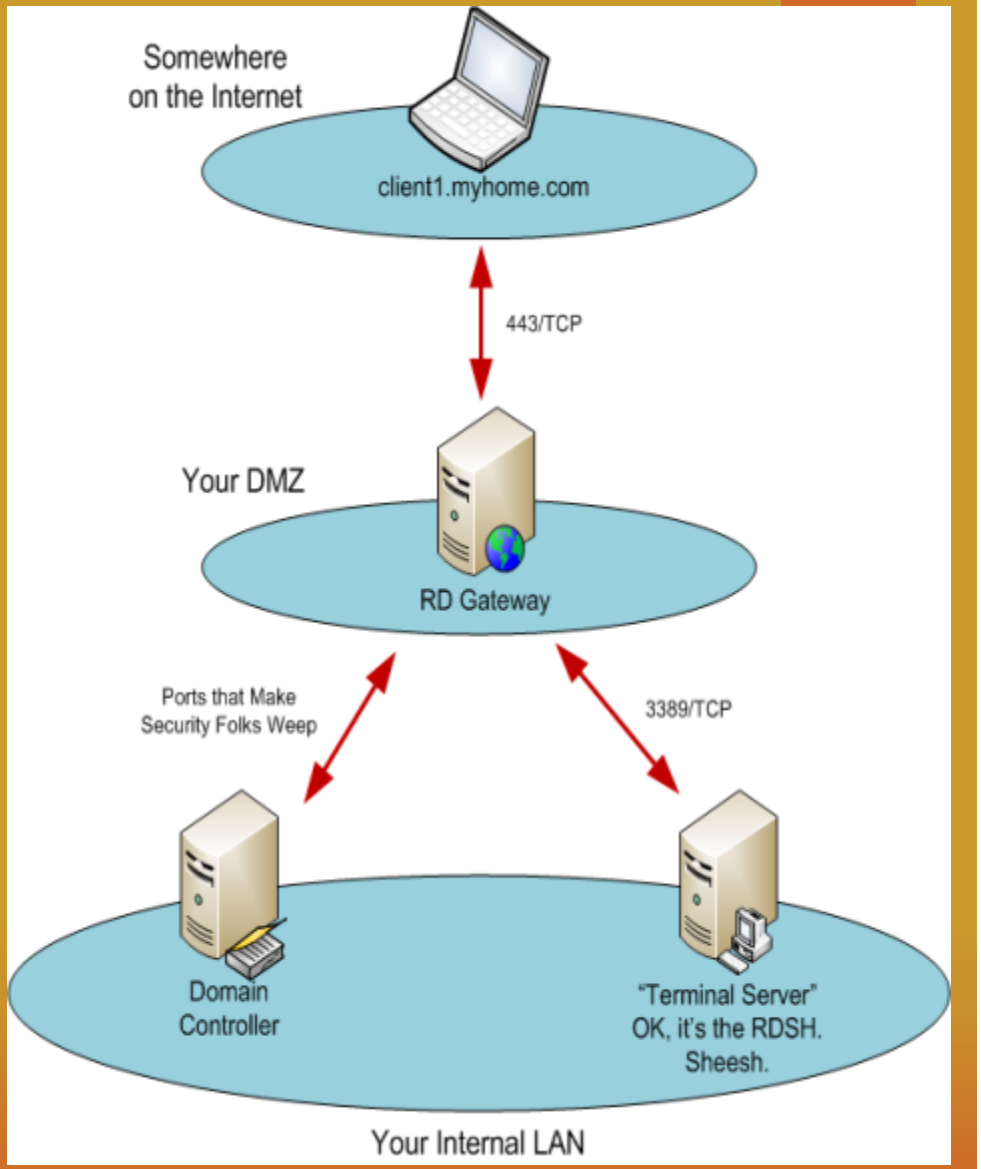
View products that this article applies to.

This article was previously published under Q179442

- Is this not the most ridiculous TechNet article ever?
  - Not to mention, its in Revision 16.
- Little Known Fact:
  Every time you read Q179442, a kitten dies.

#3: RDG in DMZ. Internal AD!

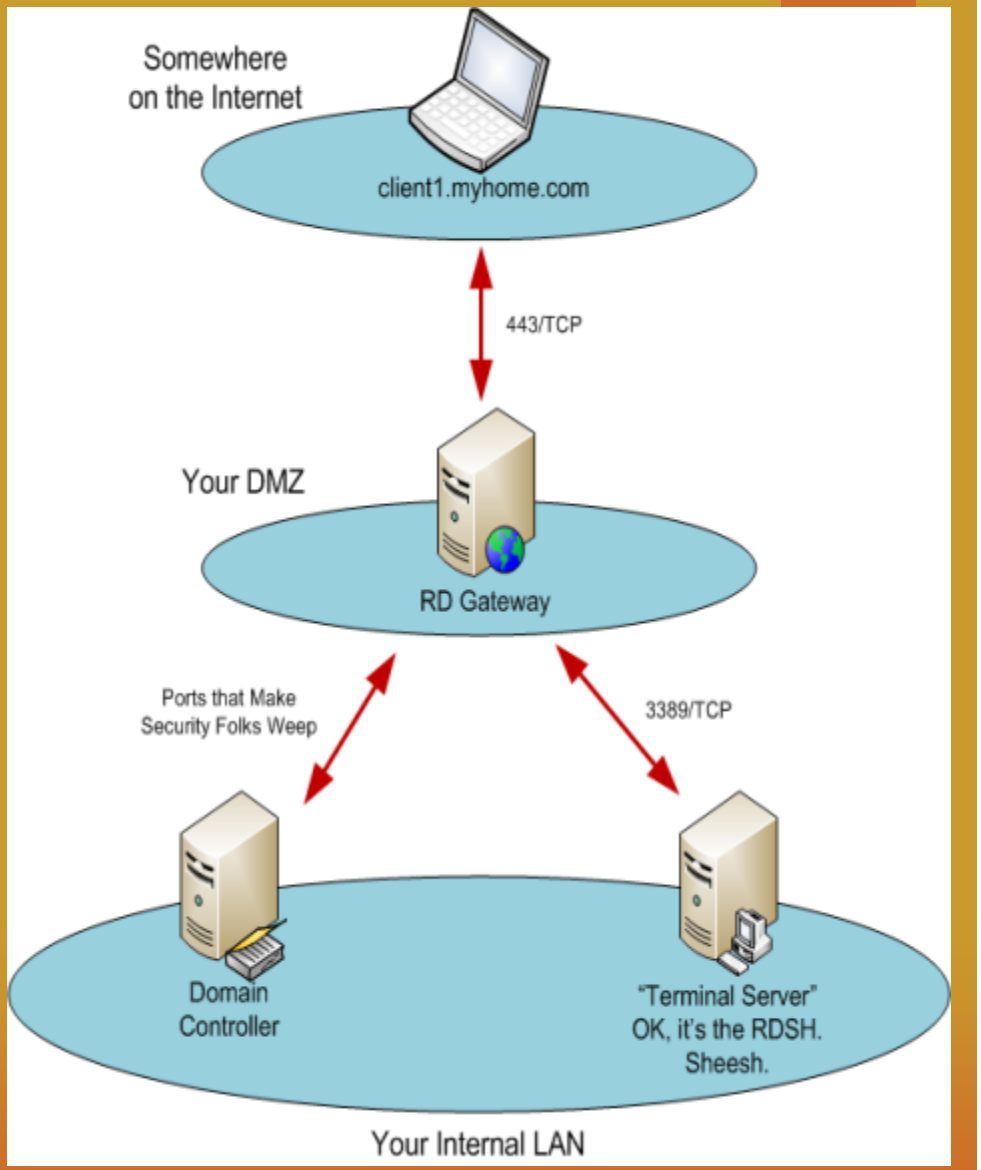
- Fairly Not Doable.
  - Option #3a
    - Use internal DC.
    - Open lots of ports.
  - Option #3b
    - Internal RODC in the DMZ.
    - Open lots of ports.
  - Option #3c
    - Forest trust to DC in the DMZ.
    - Open slightly fewer ports.



concentrated technology

#3: RDG in DMZ. Internal AD!

- Fairly Not Doable.
  - Option #3a
    - Use internal DC.
    - Open lots of ports.
  - Option #3b
    - Internal RODC in the DMZ.
    - Open lots of ports.
  - Option #3c
    - Forest trust to DC in the DMZ.
    - Open slightly fewer ports.
- If you're doing this, see me after class.
  I have very reasonable consulting rates. ☺



concentrated technology

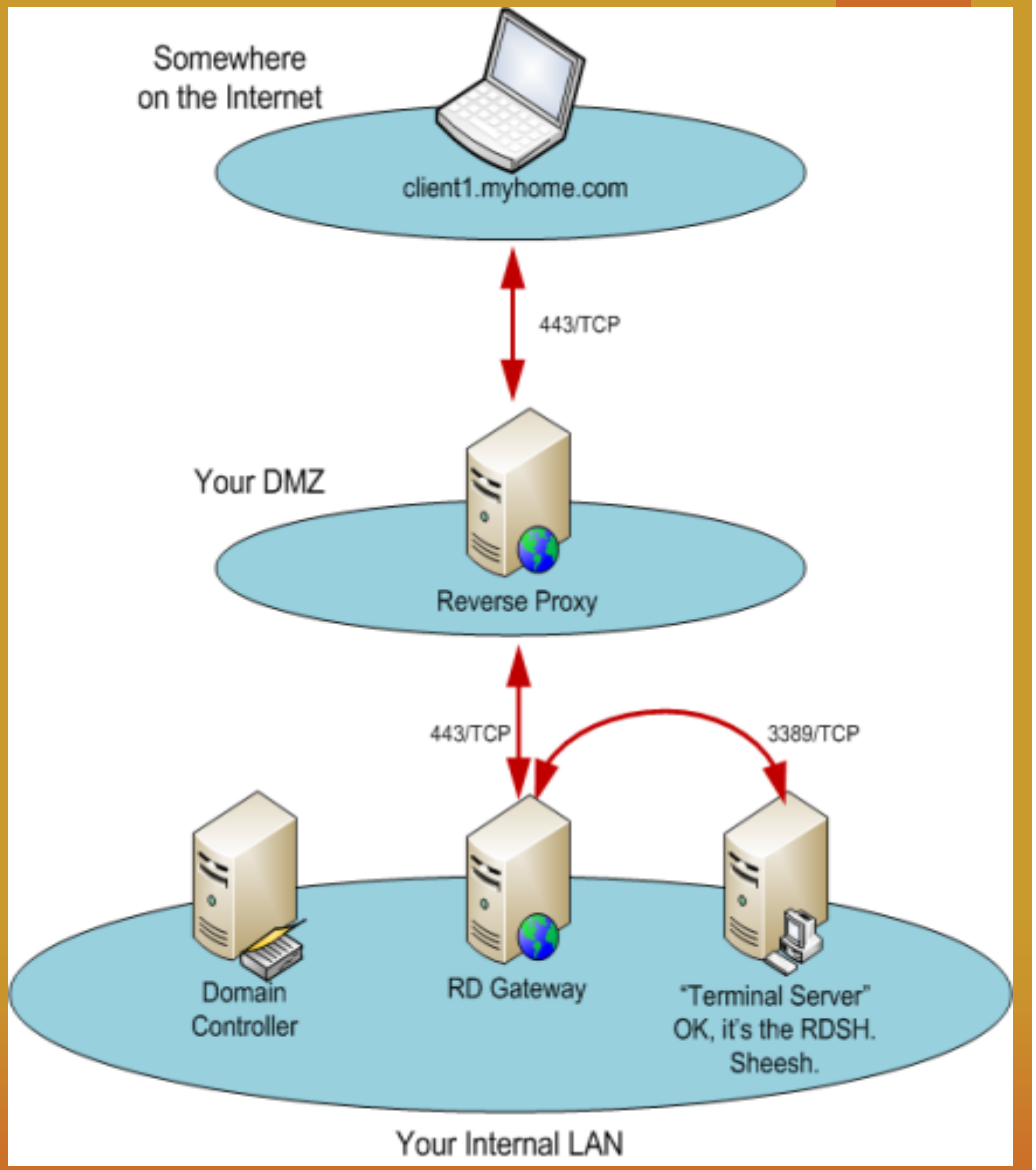
OK, I lied.

There are SIX RDG Architectures

- Option #1: No DMZ. RDG in the LAN.
- Option #2: RDG in DMZ. No internal AD for RDG.
- Option #3: RDG in the DMZ. Internal AD for RDG!
  - Option #3a: Use internal DC. Open lots of ports.
  - Option #3b: Internal RODC in the DMZ. Open lots of ports.
  - Option #3c: Forest trust to DC in the DMZ.
- Option #4: Reverse Proxy in the DMZ. RDG in the LAN.
  - Four out of Five Security Admins Agree, this is the recommended practice.

#4: Reverse Proxy in DMZ. RDG in LAN.

- Suddenly, everything makes sense.
  - Security people get what they want.
  - Users get what they want.
  - Dogs and cats living together in peace and harmony.



concentrated technology

I Summon the Vast Power of Reverse Proxying!

- An SSL Reverse Proxy is a device used to bridge external SSL connections to the inside.
  - Inbound SSL connections are terminated at the proxy.
  - Decrypts SSL communication.
  - Inspects them for malicious code.
  - (Optionally) Reconstructs them into a new SSL connection and forwards traffic inside.

- Microsoft Examples: ISA Server, Threat Management Gateway, Unified Access Gateway.

Things to Gather, Before you Start

- A Server Certificate.
- An RDG.
- A TS CAP and a RS RAP.
- A Reverse Proxy Server.
- Your RemoteApps.

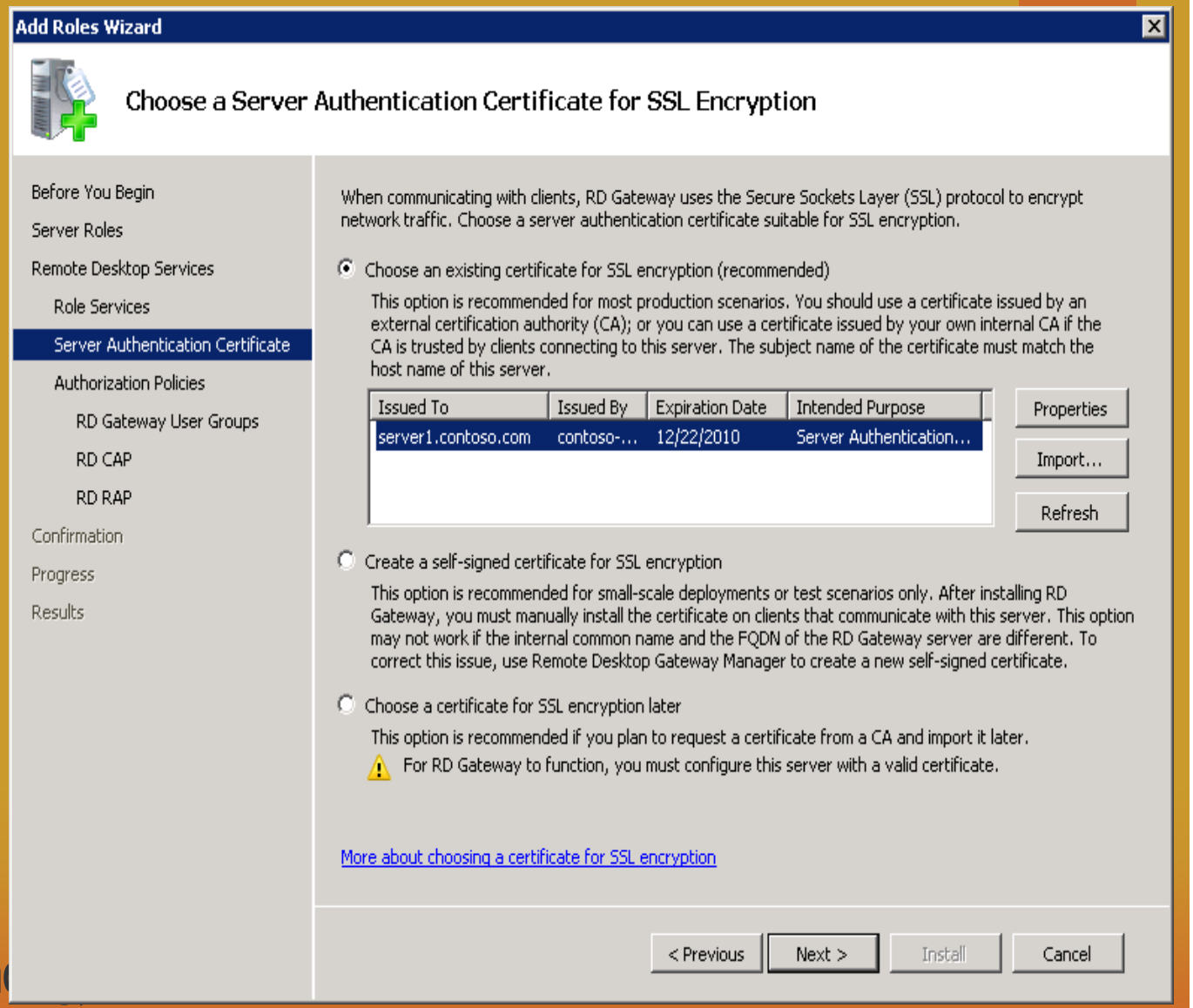
- Note: In the case of Microsoft's Unified Access Gateway, the RDG and the Reverse Proxy are the same.

Thing #1: A Server Certificate

- Server certificate attributes
  - Must be a computer certificate
  - Extended key usage must be for Server Authentication (OID 1.3.6.1.5.5.7.3.1)
  - Subject Name must exactly match the RDG's external FQDN, must also match internal FQDN if used internally.
  - Must be installed to the local computer's Personal Store and not the current user's Personal Store

Thing #1: A Server Certificate

- You'll know you've done it right if your certificate appears here.



Thing #2: An RDG.

- Four questions asked during installation.
  - Server authentication certificate. If you've correctly installed your certificate to the local computer's Personal Store, you will see that certificate listed in the box.
  - RD Gateway User Groups. Groups which are allowed to connect to internal resources through this RDG server.
  - RD CAP. Identifies mechanisms used for authenticating users to the RD Gateway server: Password or smart card.
  - RD RAP. Identifies internal computers which can be accessed by users who enter through the RDG.

Thing #3: A TS CAP and a TS RAP.

RD CAP

The "Who"

RD RAP

The "What"

RDG: Initial Configuration

another demo!

Thing #4: A Reverse Proxy Server.

- Option #4a (UAG):
  - RDG and UAG are integrated. Configure one, and done.

- Option #4b (Everything Else):
  - Create an SSL Listener.
  - Select the Certificate.
  - Create a Publishing Rule.

this demo intentionally left blank

Concerned about RDG Performance?

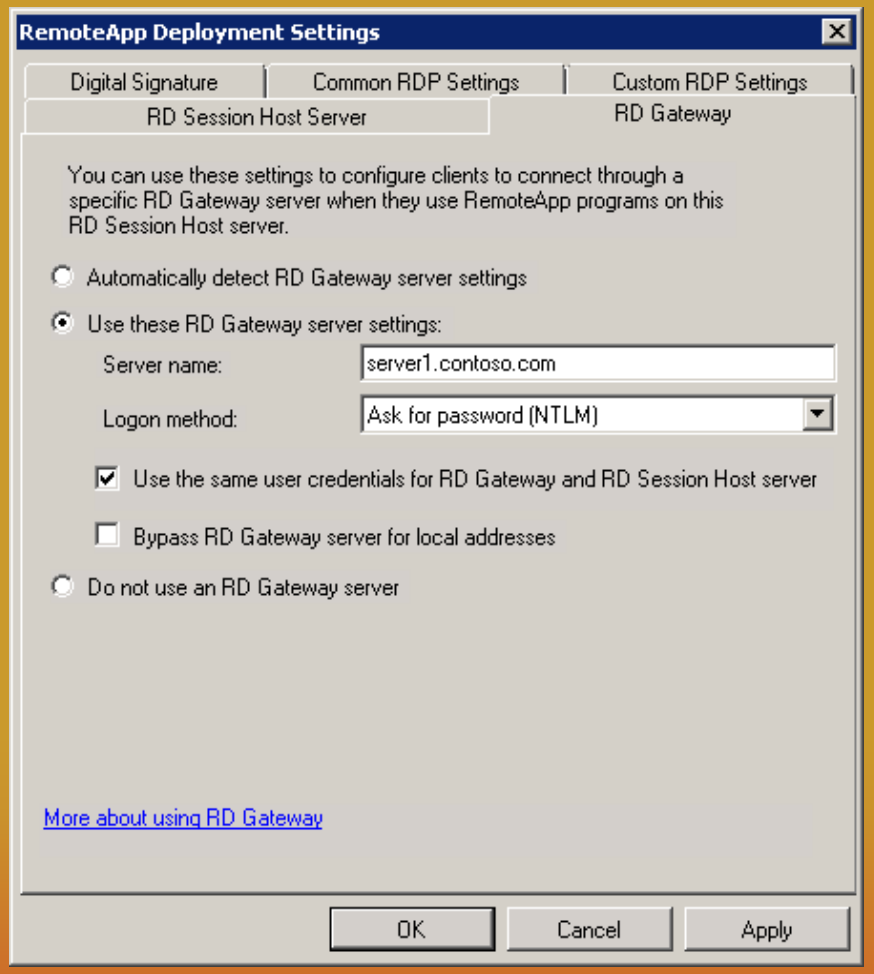
- Don't be.

- Microsoft asserts a single RDG can support up to 1200 concurrent connections.
  - Dual-processor server with 4GB of RAM.
  - Virtualizing RDG is suggested.
  - Important Note:
    - Standard Edition has a hard limit of 256 concurrent connections.
    - Enterprise and Datacenter Edition have no connection limits.

Thing #5: Your RemoteApps

- Next step:
  Adjusting RemoteApp Settings to route through RDG.

- Any deployed RemoteApps will require adjustment.
  - This is easier if you use RDWA or RADC.
  - This is harder if you've installed RDP files with MSIs.



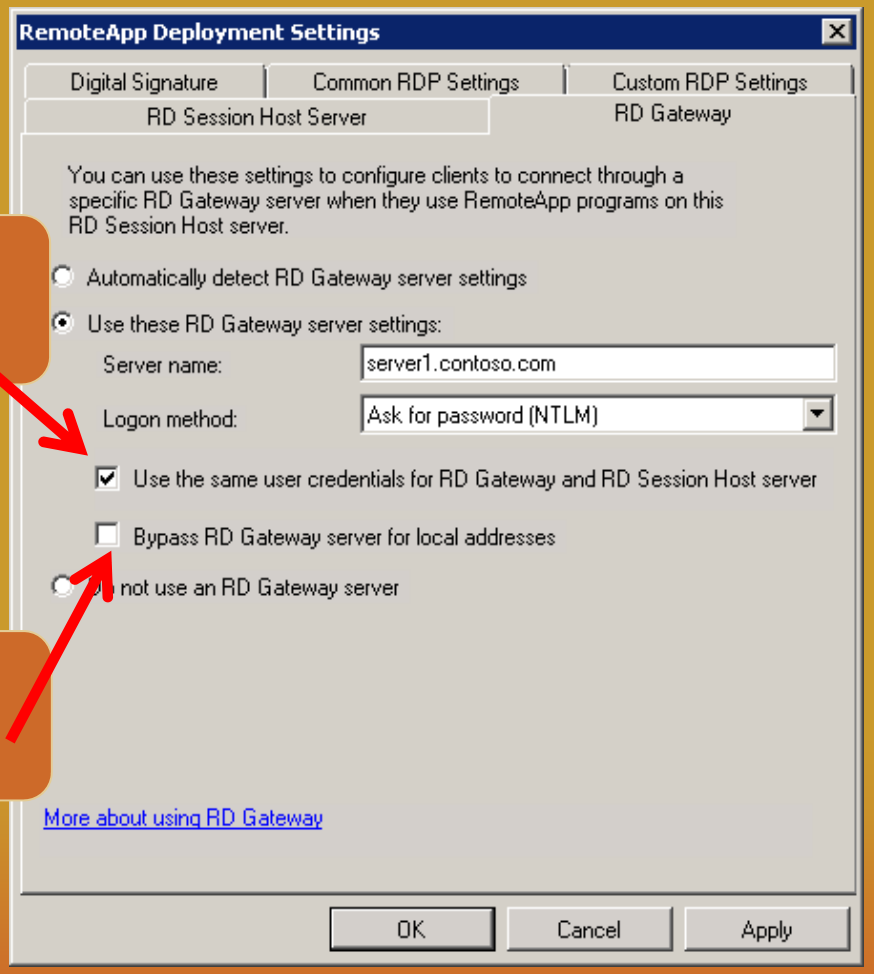
concentrated technology

Thing #5: Your RemoteApps

- Next step:
  Adjusting RemoteApp Settings
  to route through RDG.

Enables SSO between RDG and RDSH

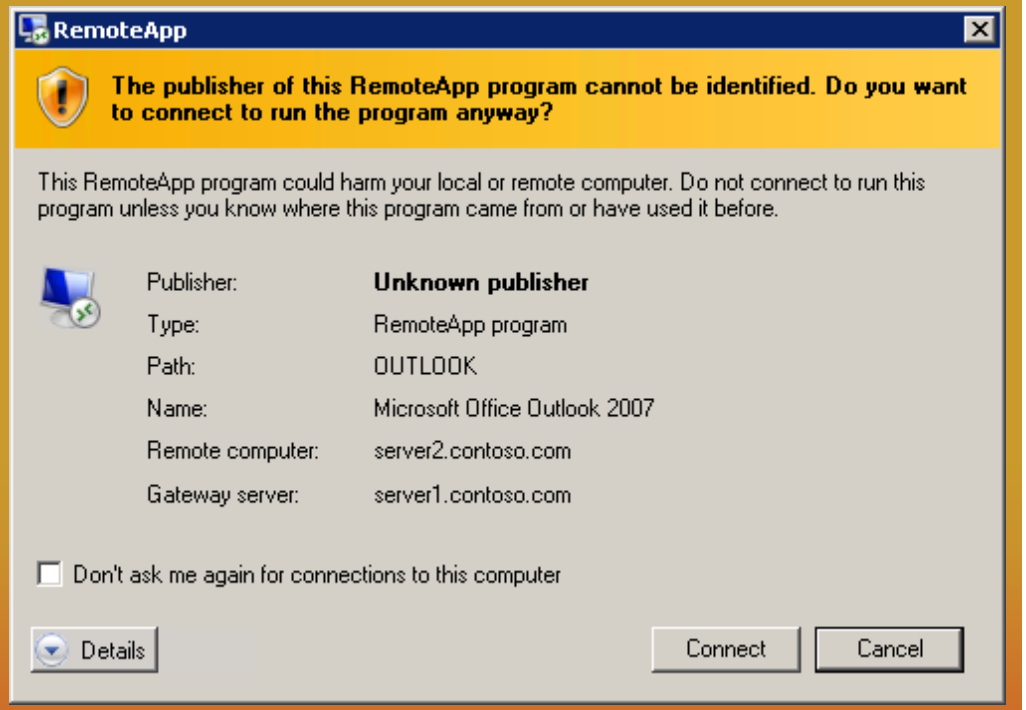
Enables direct RDSH access for LAN clients



concentrated technology

Too Many Error Messages!

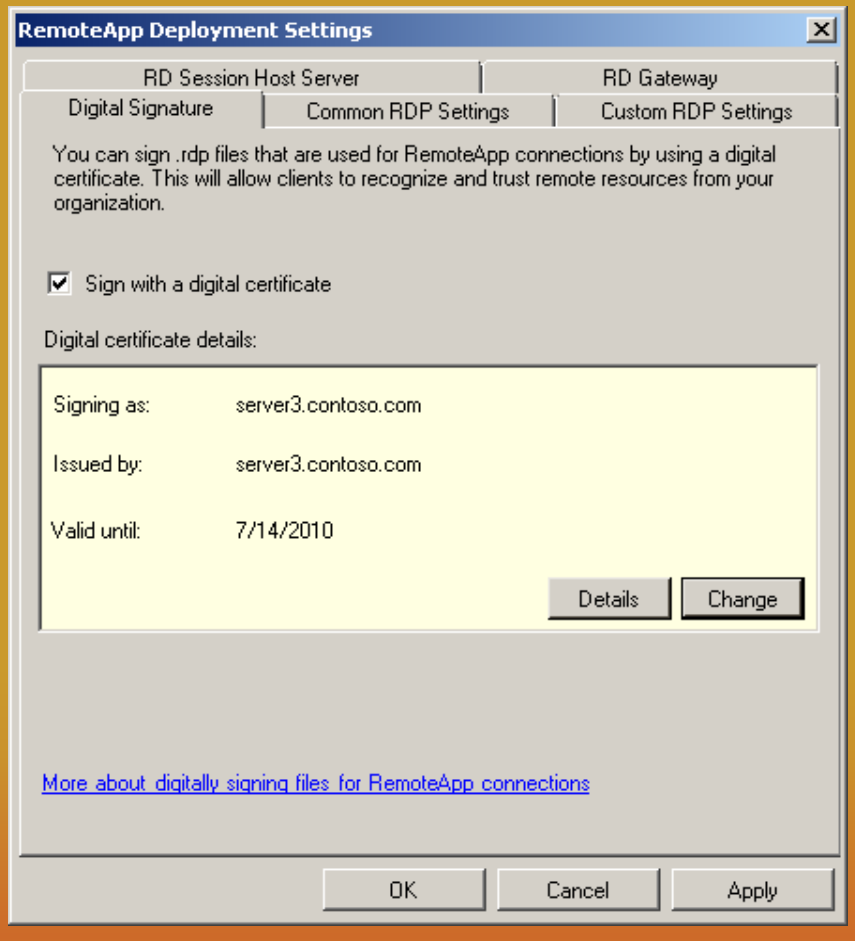
- At this point, your clients can invoke the RDP file to connect either locally or via the Internet.
- For reasons of scripting security, Microsoft requires an authentication at connection.
  - This confuses users.
  - Creates pain for we admins.



concentrated technology

Eliminate Error Messages!

- Eliminate one of the two error messages by digitally signing each RemoteApp.
- Possible to use RDG's Server Certificate.
- Install certificate to RDSH's local computer Personal Store.



concentrated technology

Error Messages become Questions

- Signing the file creates the necessary authentication between client and server.
  - Prevents RDP file from being tampered with.
  - RDP files cannot be modified in any way, or it will break the certificate signage.
- However, it doesn't entirely eliminate the error message.
  - Instead, the user sees: "Do you trust the publisher of this RemoteApp program?"
  - User can click Yes, also can click "Don't ask me again".

Reconfiguring and Running RemoteApps.

tip your waiters and waitresses

Seven Simple Steps to Successful Security!

- Attend this Session. [Check!]
- Get a Server Certificate.
- Build an RDG.
- Create a TS CAP and a RS RAP.
- Deploy a Reverse Proxy Server.
- Reconfigure and Redeploy RemoteApps.

Seven Simple Steps to Successful Security!

- Attend this Session. [Check!]
- Get a Server Certificate.
- Build an RDG.
- Create a TS CAP and a RS RAP.
- Deploy a Reverse Proxy Server.
- Reconfigure and Redeploy RemoteApps.
- Remember Fondly how much you Learned, Particularly when Filling Out Evaluations.

concentrated technology

Extending Applications to…Everywhere!

Your Guide to Internet-enabling Remote Desktop Services

Greg Shields
Senior Partner and Principal Technologist,
Concentrated Technology, LLC
http://ConcentratedTech.com

concentrated technology