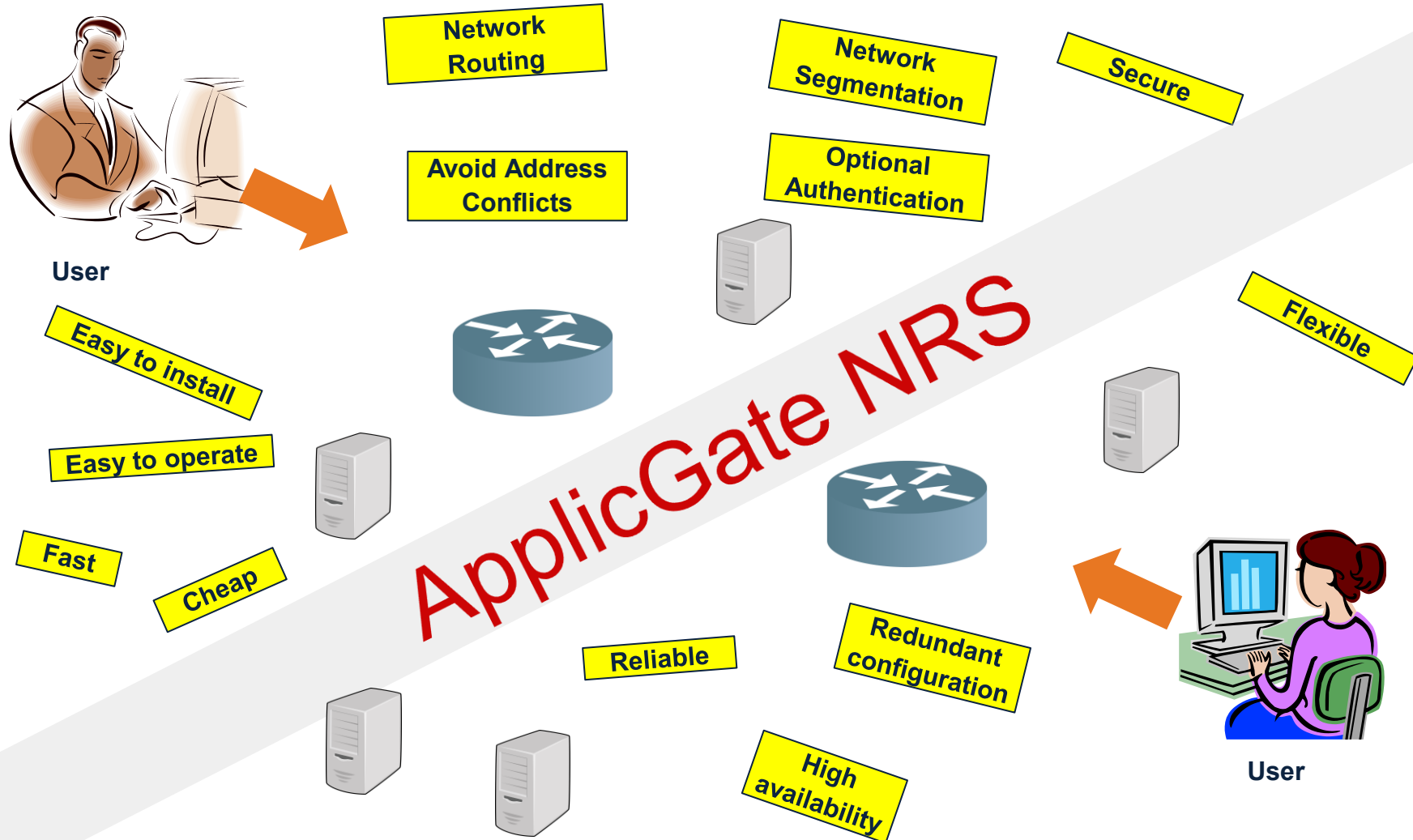




ApplicGate NETRS Network Routing & Segmentation

A new approach to secure networks...

ApplicGate NETRS Network Routing and Segmentation



ApplicGate NETRS - Overview

Goals

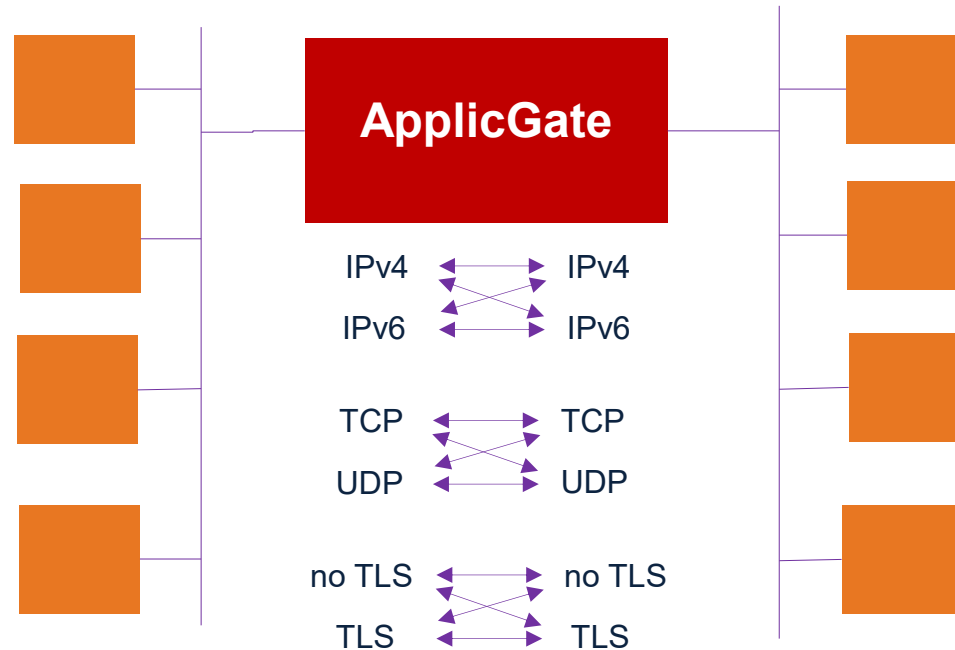
- Network Segmentation
- Routing on Transport Layer
- No routing on Network Layer to avoid IP address conflicts
- Secure authentication

Prerequisites

- Any Windows system (Windows 11, Windows Server) with .NET 4.8 Framework or .NET 8 or higher
- Any Linux system with .NET 8 or higher

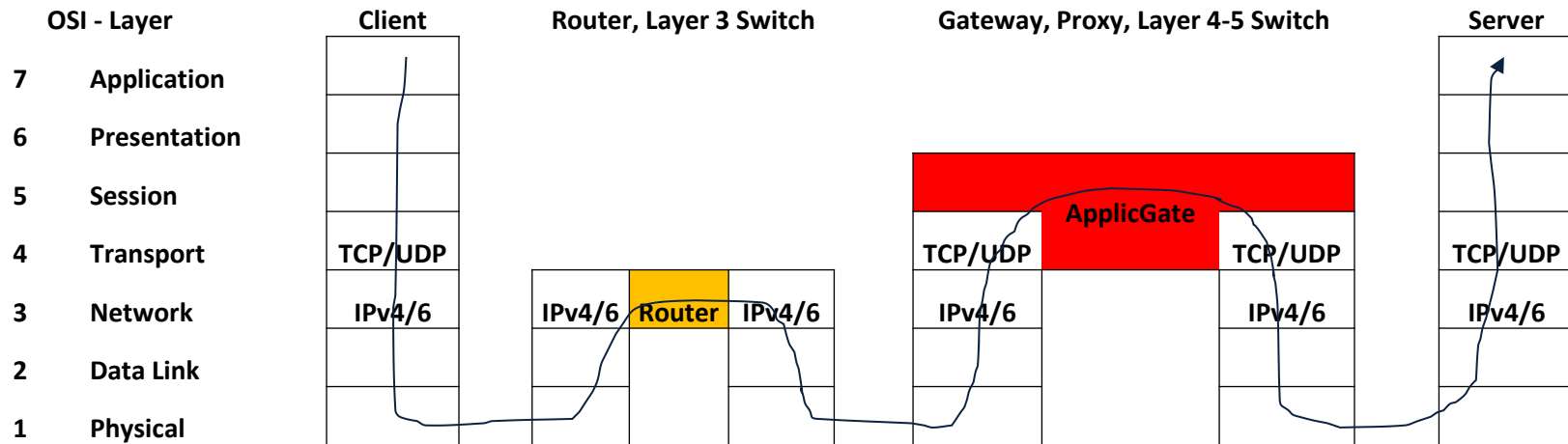
Functions

- Transparent routing of protocols based on TCP such as RDP, SMB, VNC, http(s) ...
- Support of IPv4 and IPv6
- Optional secure authentication via smartcards, soft certificates, One-Time-Password, Authenticator, FIDO2, OAuth 2.0 ...
- Integrated management and logging



- **Network Routing is turned off in Windows/Linux where ApplicGate is installed.**
- **Routing is based on the ApplicGate routing table.**

ApplicGate NETRS - Schema



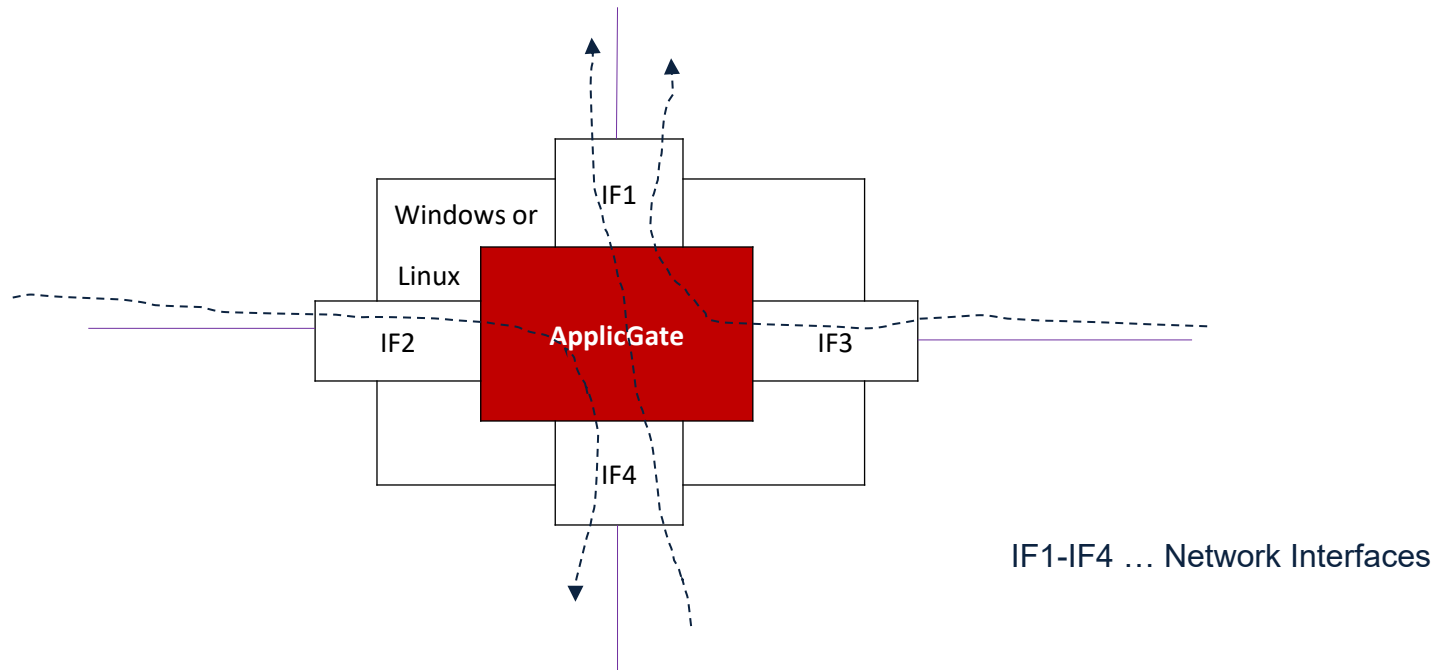
- **ApplicGate routes TCP/UDP connections according to the definitions within a local routing table**
- **As there are no direct connections on the network layer there cannot be any IP addressing conflicts, no IP address coordination necessary**
- **ApplicGate can route between IPv4 and IPv6 connections**

ApplicGate NETRS – Routing Table (simplified)

Field Name	Description	Used for routing decision
SourceIP	allowed source (optional)	yes
GatewayIP	listening address (IPv4 or IPv6)	yes
GatewayPort	listening ports (UDP or TCP)	yes
GatewayIP2	local IP for outgoing connections (optional)	no
DestinationIP	DNS name or IPv4/6 address of destination	no
DestinationPort	Port of destination (UDP or TCP)	no
Expiration	Date/Time when the entry expires (optional)	yes

- **Routing table entries are searched from top to bottom. The first matching entry will be processed.**
- **Incoming connections to GatewayIP:GatewayPort are forwarded to DestinationIP:DestinationPort using the local address GatewayIP2 (if specified).**
- **Protocol specific processing and various other functions are defined by keywords in the additional field “Type”.**

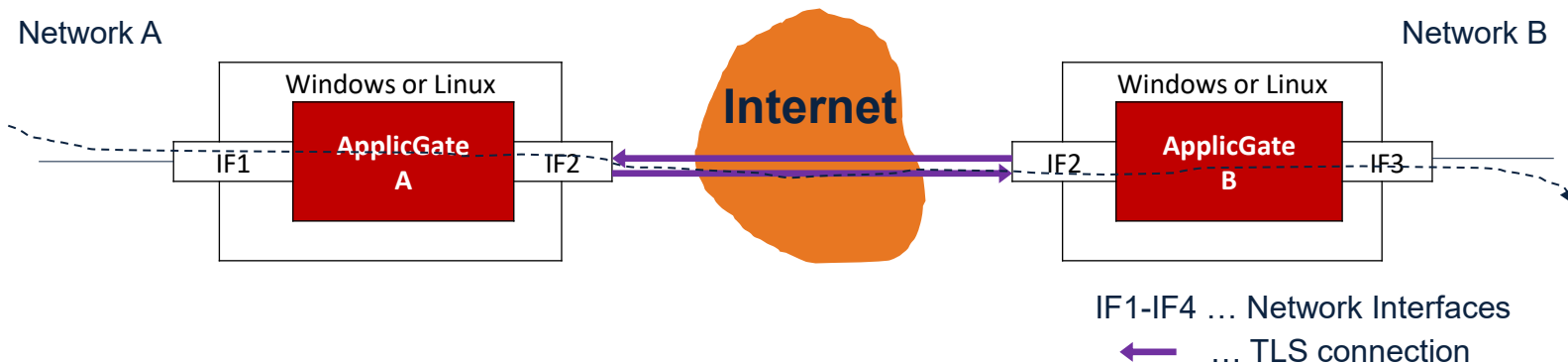
ApplicGate NETRS – Network Segmentation



- **Network Routing is turned off in Windows/Linux where ApplicGate is installed.**
- **Routing is based on the ApplicGate routing table.**

ApplicGate NETRS

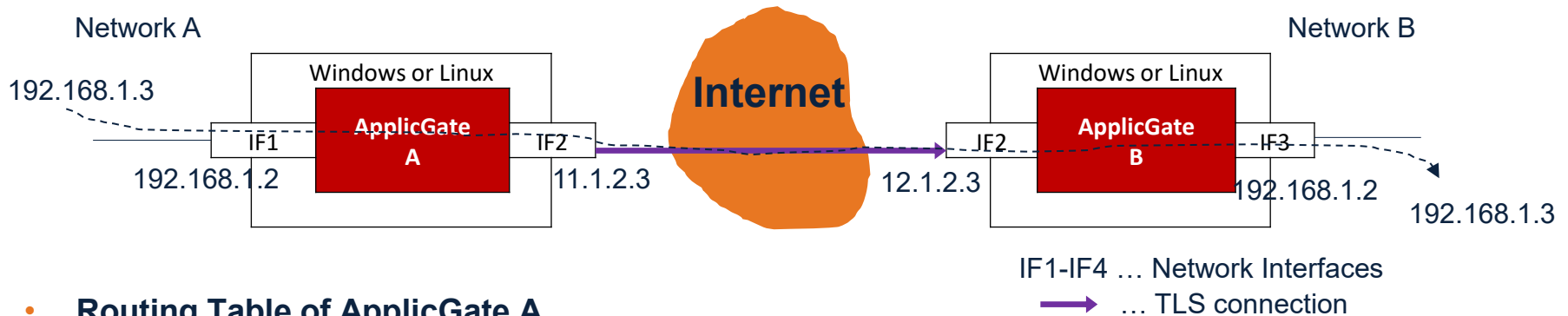
Linking independent networks via Internet



- **Network Routing is turned off in Windows/Linux**
- **Routing is based on the ApplicGate routing table**
- **The networks A and B may have the same IP addresses**
- **A user in network A connects to a local IP addresses of ApplicGate A that sends the data via an Internet TCP link to ApplicGate B.**
Optional: This link can be TLS encrypted with client authentication, (license WEBAUTH required).
- **If ApplicGate B is configured as a proxy (license WEBAUTH required) any local IP Address in network B is reachable via one routing entry at ApplicGate B because ApplicGate A sends a CONNECT string.**

ApplicGate NETRS

Linking independent networks via Internet – Example 1



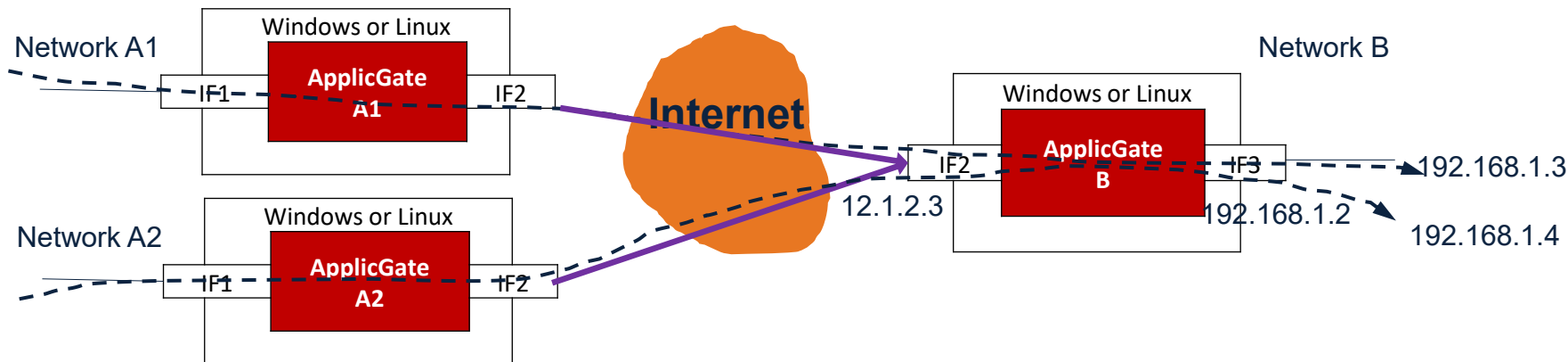
- **Routing Table of ApplicGate A**

```
SourceIP;GatewayIP ;GatewayPort;GatewayIP2 ;DestinationIP;DestinationPort;Type
* ;192.168.1.2;3390 ;* ;12.1.2.3 ;444 ;SSLTARGET:B.comp.com,SSLCC:A.cer,
CONNECT:192.168.1.3:3389
```

- **Routing Table of ApplicGate B**

```
SourceIP;GatewayIP ;GatewayPort;GatewayIP2 ;DestinationIP;DestinationPort;Type
* ;12.1.2.3 ;444 ;192.168.1.2;* ;* ;SSL:B.cer,CCR:A@comp.com,PRX
```

- **A user at 192.168.1.3 in network A wants to establish an RDP session to 192.168.1.3 in network B:**
 The user issues the command “mstsc /v:192.168.1.2:3390”
 ApplicGate A accepts the connection, connects to 12.1.2.3, identifies itself using the client certificate A.cer (that is a reference to the certificate store) via the TLS session and sends the CONNECT string
 AppliGate B builds a TLS session using the certificate B.cer, requests a client certificate, checks the email address, receives the CONNECT string and connects to the target 192.168.1.3
 After connection setup there is a full-duplex TCP session between computer 192.168.1.3 in network A and computer 192.168.1.3 in network B.
- **Note:** For the optional TLS encryption, authentication and proxy function the license WEBAUTH is required!



- If there are different sites accessing site B: In ApplicGate B different routes for ApplicGate A1 and A2 can be configured depending on listening port for IF2 or depending on client certificate from A1 or A2 as shown below:

• Routing Table of ApplicGate A1

```
SourceIP;GatewayIP ;GatewayPort ;GatewayIP2 ;DestinationIP;DestinationPort;Type
* ;* ;3389,443,445 ;* ;12.1.2.3 ;444 ;SSLTARGET:B.comp.com,SSLCC:A1.cer,
CONNECT:192.168.1.3:*
```

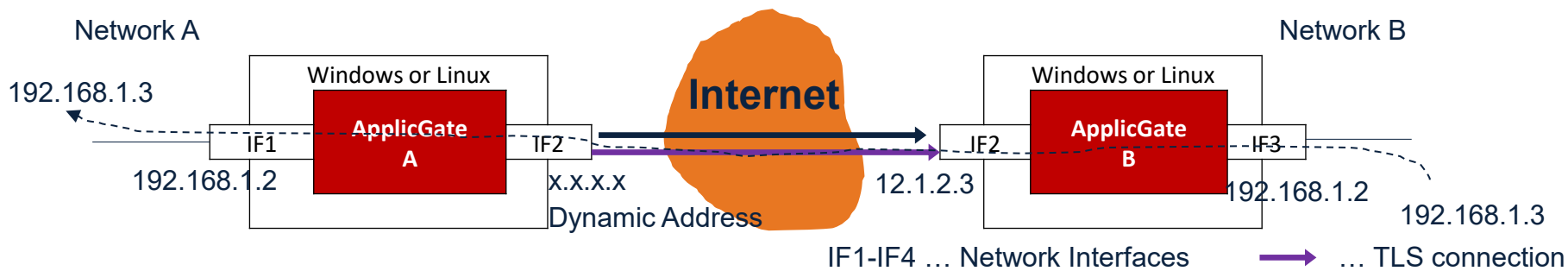
• Routing Table of ApplicGate A2

```
SourceIP;GatewayIP ;GatewayPort ;GatewayIP2 ;DestinationIP;DestinationPort;Type
* ;* ;3389,443,445 ;* ;12.1.2.3 ;444 ;SSLTARGET:B.comp.com,SSLCC:A2.cer,
CONNECT:192.168.1.4:*
```

• Routing Table of ApplicGate B

```
SourceIP;GatewayIP ;GatewayPort;GatewayIP2 ;DestinationIP;DestinationPort;Type
* ;12.1.2.3 ;444 ;forward ;local:F1 ;* ;SSL:B.cer,CCR:*@comp.com
incoming;F1 ; ; ;FilterA1 ; ;PRX,CCRI:a1@comp.com
incoming;F1 ; ; ;FilterA2 ; ;PRX,CCRI:a2@comp.com
```

- Note: For A1 and A2 multiple GatewayPorts are configured. Therefore the CONNECT keyword has * as port. Additionally FilterA1 and FilterA1 defines groups with allowed destinations.



- A user in network B likes to connect to a resource in Network A. Because **IF2 has a dynamic address** the routing can be configured as shown below:

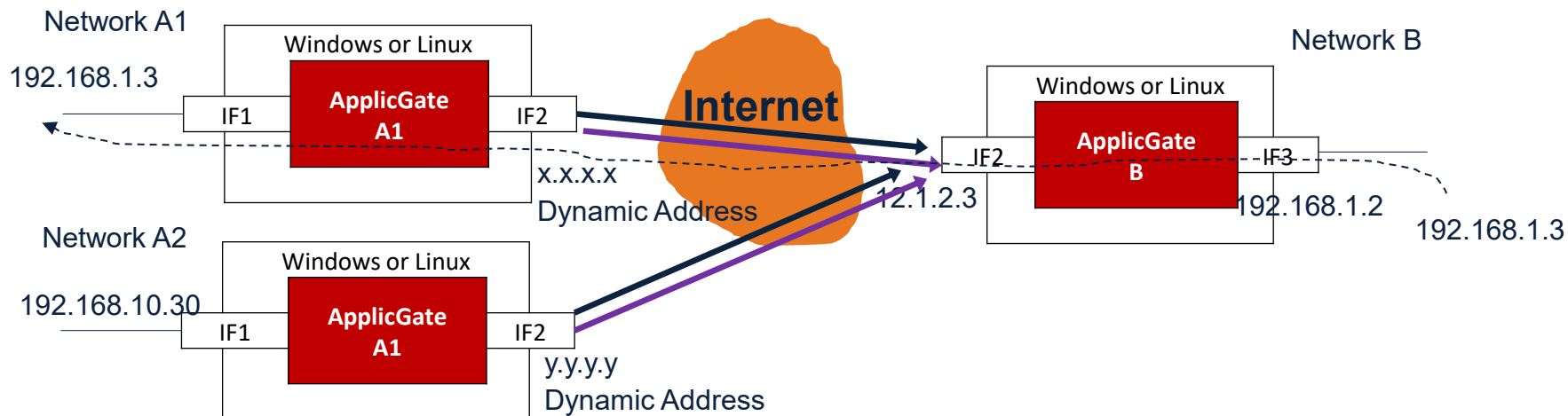
• Routing Table of ApplicGate A

```
SourceIP ;GatewayIP;GatewayPort;GatewayIP2;DestinationIP;DestinationPort;Type
autologon;R3 ;* ;* ;12.1.2.3 ;444 ;SSLTARGET:B.comp.com!*!A.cer,RETRY:20s,TTL:6
incoming ;R3 ;* ;* ;* ;* ;PRX
```

Routing Table of ApplicGate B

```
SourceIP;GatewayIP ;GatewayPort;GatewayIP2 ;DestinationIP ;DestinationPort;Type
* ;12.1.2.3 ;444 ;reverselogon;R3 ;* ;SSL:B.cer,CCR:A@comp.com
* ;192.168.1.2;3390 ;forward ;a@comp.com;R3 ;* ;CONNECT:192.168.1.3:3389
```

- **ApplicGate A logs on to ApplicGate B automatically and offers a proxy rule**
- **A user at 192.168.1.3 in network B wants to establish an RDP session to 192.168.1.3 in network A:** The user issues the command “mstsc /v:192.168.1.2:3390”.
ApplicGate B sends a request via the established autologon session (email addresses must match!) to ApplicGate A.
ApplicGate A establishes a new session to ApplicGate B. ApplicGate B uses this session to send the CONNECT request to ApplicGate A. ApplicGate B connects to the required target.



- Same as example 3 but with 2 destination sites A1 and A2:

- **Routing Table of ApplicGate A1**

```
SourceIP ;GatewayIP;GatewayPort;GatewayIP2;DestinationIP;DestinationPort;Type
autologon;R3 ;* ;* ;12.1.2.3 ;444 ;SSLTARGET:B.comp.com!!A1.cer,RETRY:20s,TTL:6
incoming ;R3 ;* ;* ;* ;* ;PRX
```

- **Routing Table of ApplicGate A2**

```
SourceIP ;GatewayIP;GatewayPort;GatewayIP2;DestinationIP;DestinationPort;Type
autologon;R3 ;* ;* ;12.1.2.3 ;444 ;SSLTARGET:B.comp.com!!A2.cer,RETRY:20s,TTL:6
incoming ;R3 ;* ;* ;* ;* ;PRX
```

- **Routing Table of ApplicGate B**

```
SourceIP;GatewayIP ;GatewayPort;GatewayIP2 ;DestinationIP ;DestinationPort;Type
* ;12.1.2.3 ;444 ;reverselogon;R3 ;* ;SSL:B.cer,CCR:A*@comp.com
* ;192.168.1.2;3390 ;forward ;a1@comp.com:R3 ;* ;CONNECT:192.168.1.3:3389
* ;192.168.1.2;3391 ;forward ;a2@comp.com:R3 ;* ;CONNECT:192.168.10.30:3389
```

Logon to RSP

- Connect to ApplicGate by a web browser.
- Use soft certificate, smartcard, one-time password (OTP), FIDO2 or OAuth 2.0 etc. for authentication.
- Then routing entries with matching email address in SourceIP are accessible.

Client Certificate

- A TLS connection is accepted only if the client has an appropriate certificate.
- An incoming TLS session can be forwarded dependent on the client certificate

Reverse Proxy

- Routing based on the http header Host

Note: For logon, TLS client certificate and proxy support the license WEBAUTH is required!

ApplicGate NETRS - FAQs (1)

- **Can dynamic IP address for the Internet be used for configurations like the example “Linking independent networks via Internet” above?**

We need at least one fixed IP address, the second may be dynamic.

In that case the site with the dynamic IP address has to open a “command” session that is used if the site with the fixed IP address wants to connect to the site with the dynamic address (license RSP is required).

- **Is there a restriction of number of interfaces and/or IP addresses used by ApplicGate?**

No. Hint: Loopback Adapter can be used.

- **What about redundancy and high availability?**

Application Gateways can be configured as hot-standby (license HOT-STANDBY is required).

Two Destination addresses can be configured:

If the connection to the first address fails, an attempt to connect to the secondary address will be made.

Contact

Reinhold Leitner

ApplicGate Network Security e.U.

Birkenweg 5

4048 Puchenau

Austria

Mobil: +43 (663) 03118601

E-mail: reinhold.leitner@applicgate.com

www.applicgate.com

ApplicGate Network Security excludes any liability whatsoever under or in connection with any provided information, estimates and assumptions. The provided information, estimates and assumptions shall be without prejudice to any possible future offer and/or contract.

Any use of information provided by ApplicGate Network Security to the recipient shall be subject to applicable confidentiality obligations and for the own convenience of and of the sole risk of the recipient.