Azure Bastion

Sicherer Zugriff auf Azure VMs

Tim Niklas Vinkemeier

Senior Software Engineer @ prodot

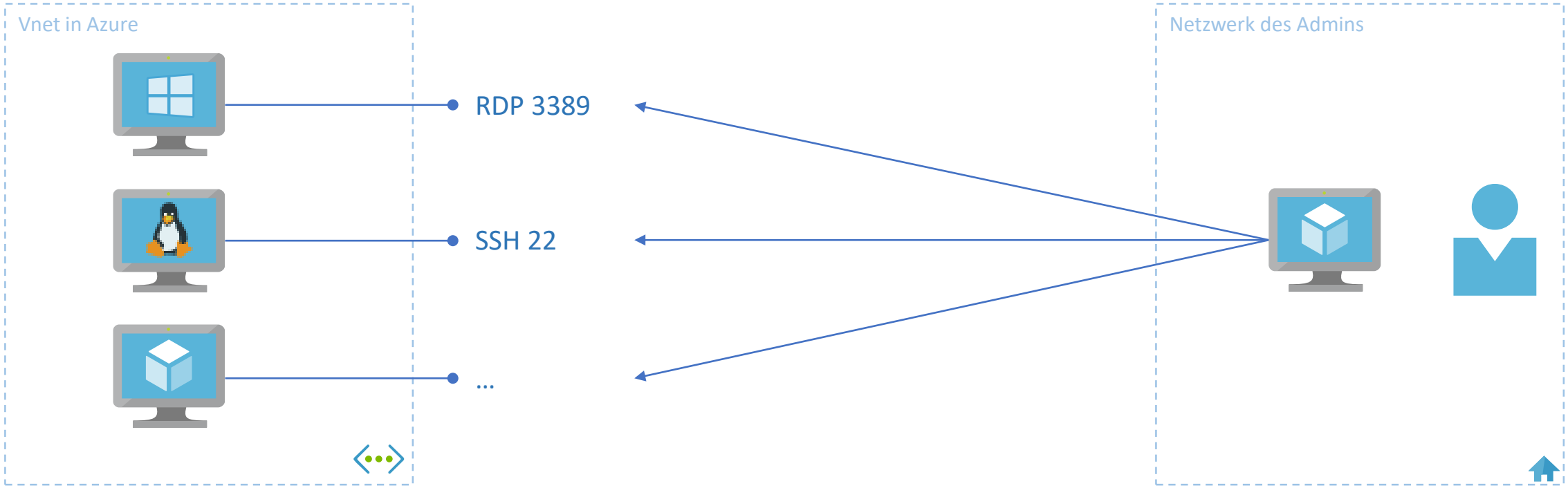
- Cloud, IoT, Web

@TimVinkemeier

github.com/TimVinkemeier

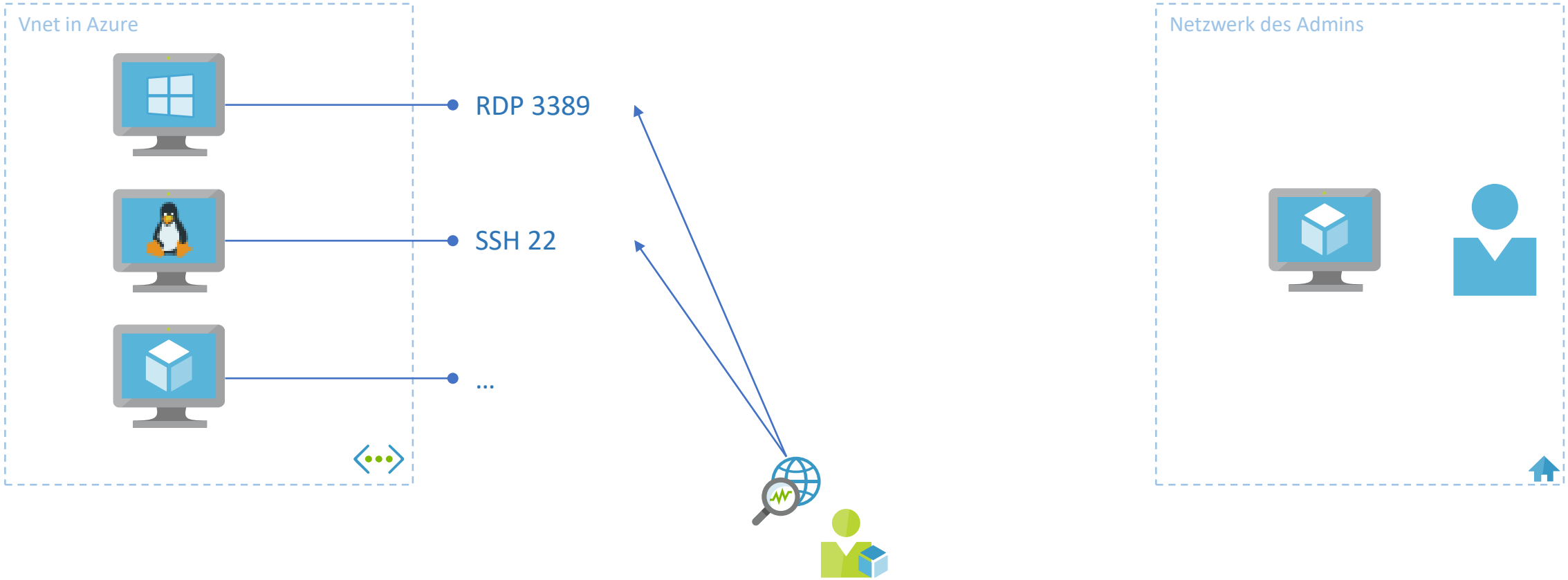
Die Herausforderung

Administratoren brauchen Zugriff auf die Maschinen



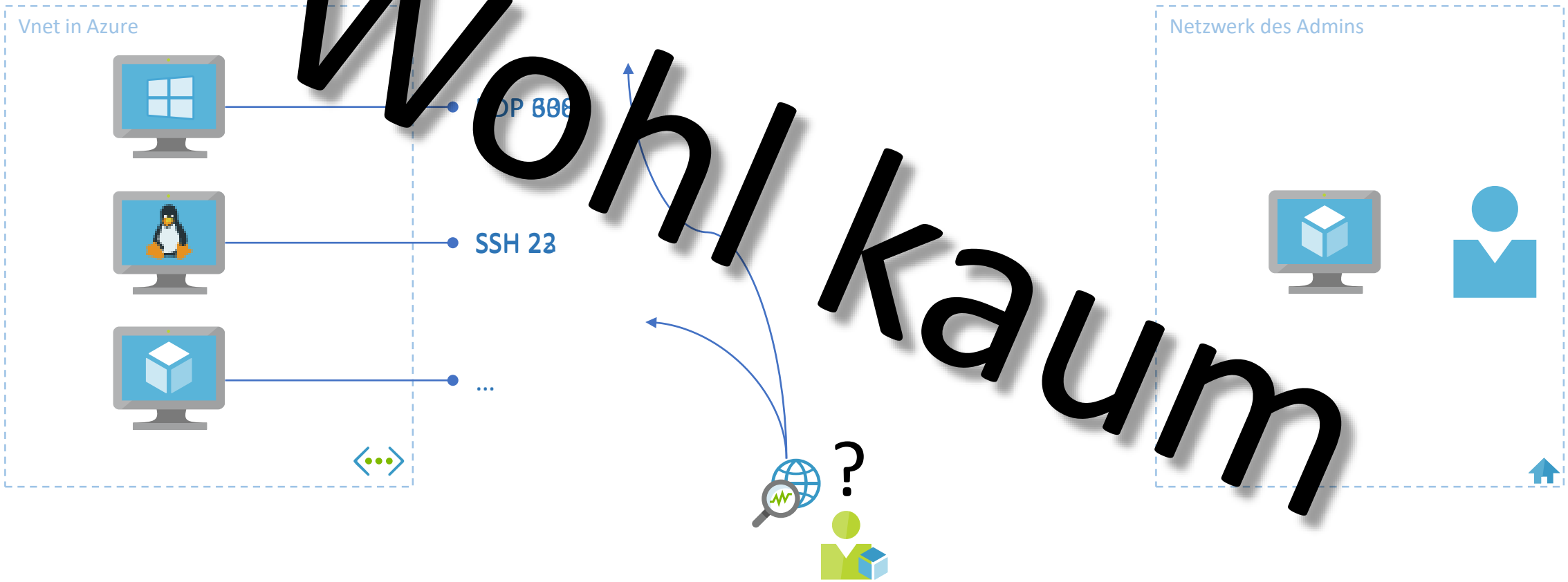
Das Problem

Portscanner finden öffentliche Maschinen ohne Probleme und können Schwachstellen ausnutzen



Lösungsversuche – Teil 1

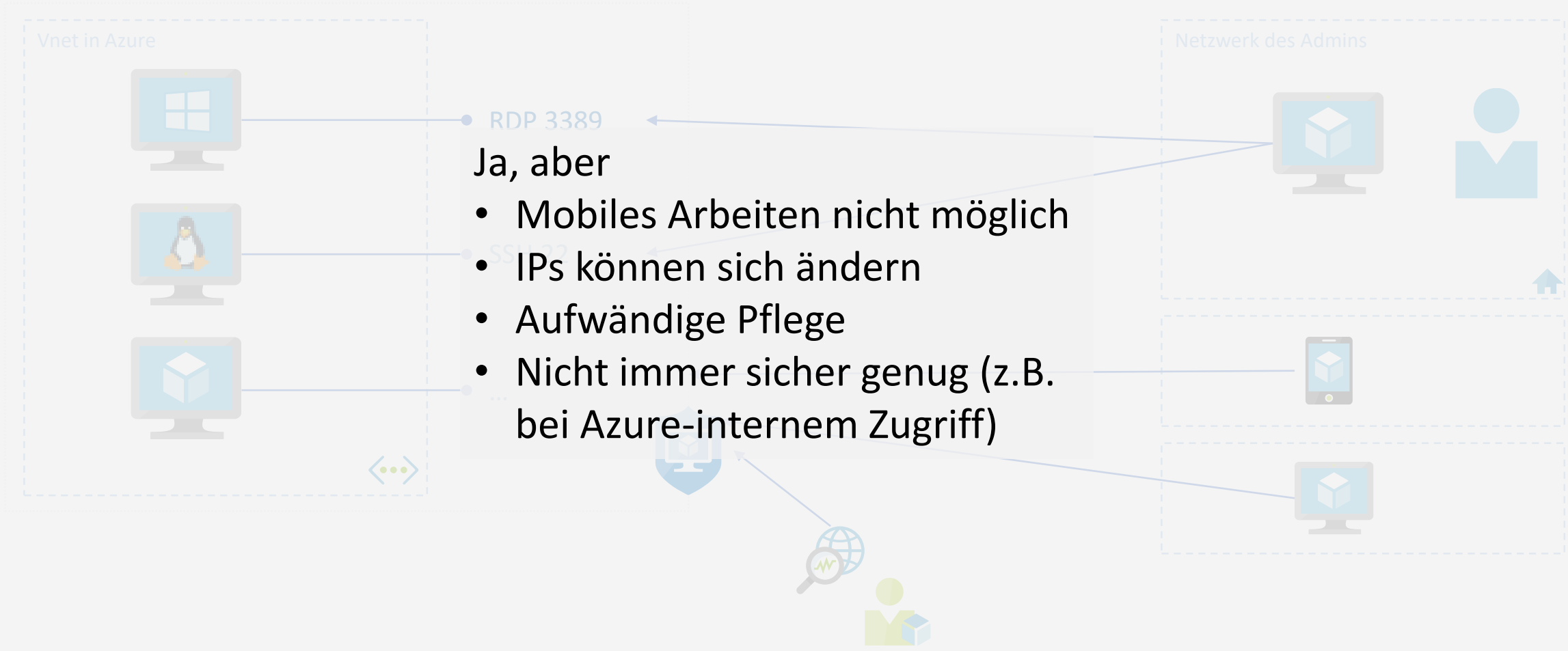
Unbekannter Port = keine Probleme?!



Wohl kaum

Lösungsversuche – Teil 2

Mit Network Security Group auf IPs einschränken

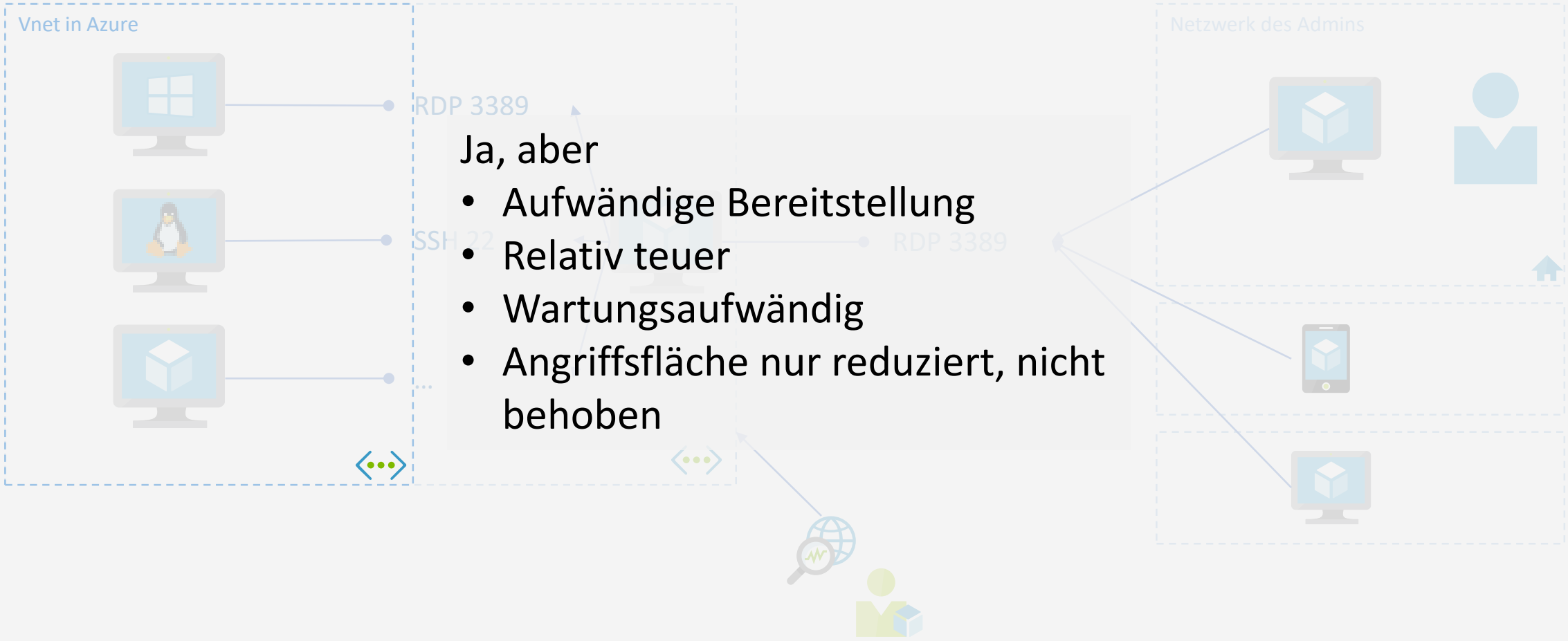


Ja, aber

- Mobiles Arbeiten nicht möglich
- IPs können sich ändern
- Aufwändige Pflege
- Nicht immer sicher genug (z.B. bei Azure-internem Zugriff)

Lösungsversuche – Teil 3

Verbindung via Jump Box

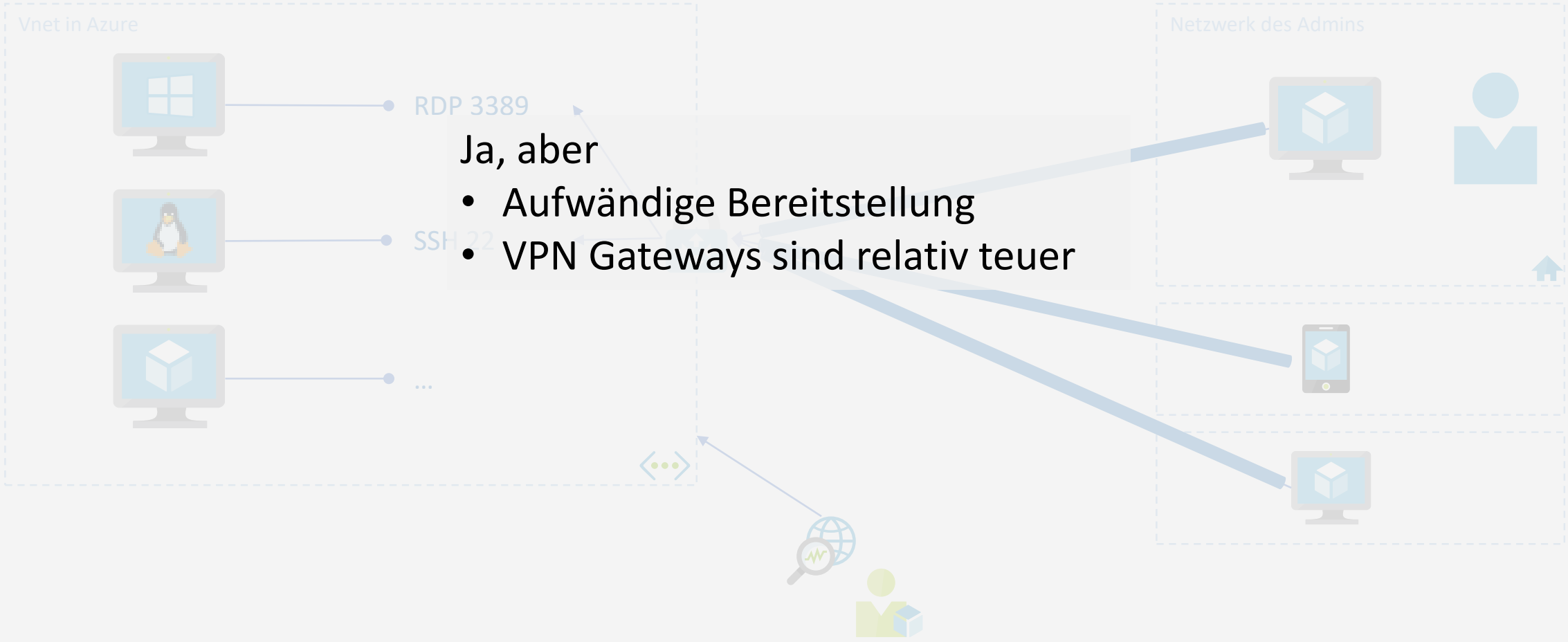


Ja, aber

- Aufwändige Bereitstellung
- Relativ teuer
- Wartungsaufwändig
- Angriffsfläche nur reduziert, nicht behoben

Lösungsversuche – Teil 4

Zugriff nur per VPN



Ja, aber

- Aufwändige Bereitstellung
- VPN Gateways sind relativ teuer

Lösungsversuche – Sonstige

- RDP/SSH deaktivieren, wenn es nicht genutzt wird
  Aufwändig, fehleranfällig, unflexibel

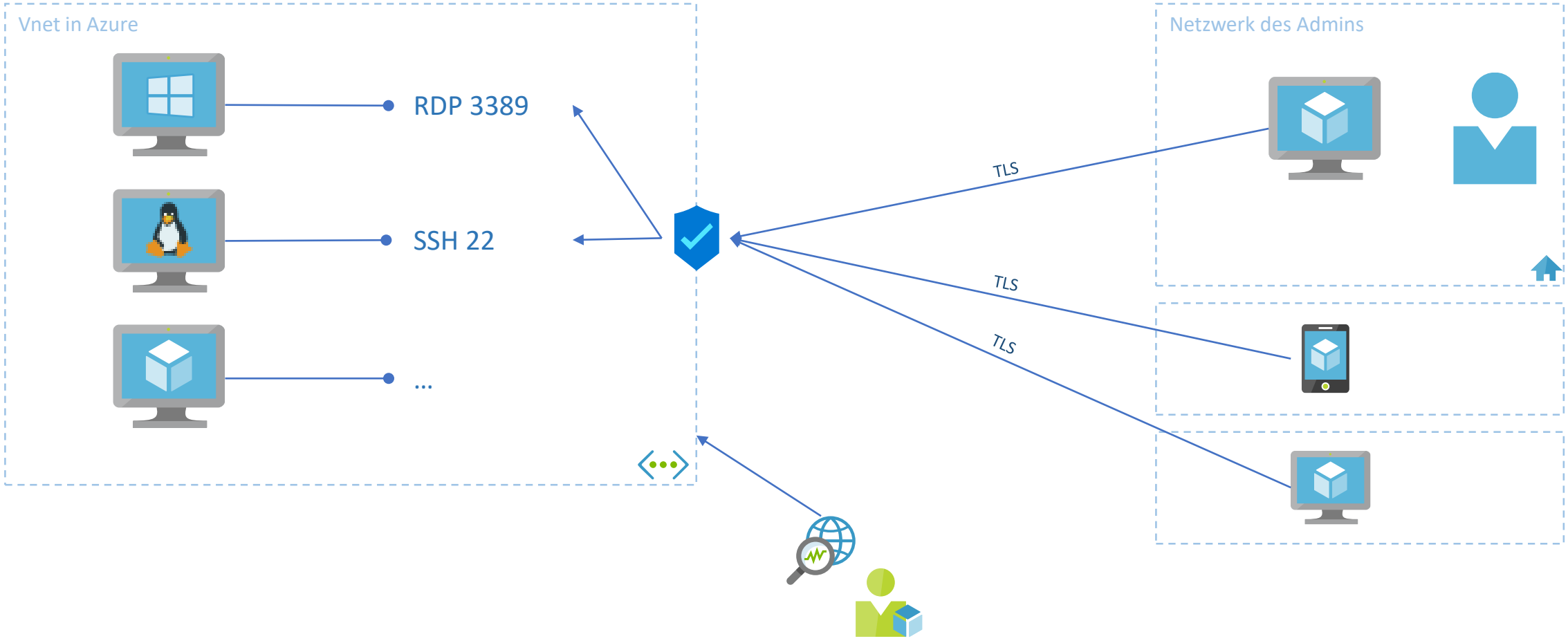
- Azure Security Center Just-in-Time-Access
  Automatisches Blocken der entsprechenden Ports, automatisierte Freigabe, automatisierte Deaktivierung

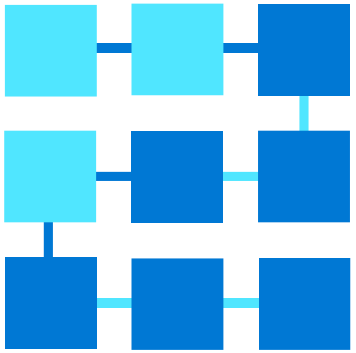
Anforderungen

- Hohe Sicherheit
- Einfache Bereitstellung und Wartung
- Einfache Nutzung
- Für alle Arbeitsszenarien geeignet

Die wirkliche Lösung – Azure Bastion

Gemanagter Bastion-Host mit Webzugriff





Demo

Azure Bastion - Zusammenfassung

- Einfach einsetzbar
- Voll gemanagt
- Permanent überwacht und abgesichert
- Zugriff von jedem Browser aus
- Entwickelt sich permanent weiter

- „Günstig“
  0,161€/h (≈120€/Monat) für ein ganzes VNet

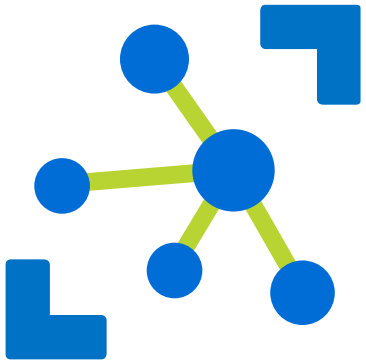
Azure Bastion - Ausblick

- Unterstützung für VNet-Peering und Hub-and-Spoke-Designs
- Unterstützung für Dateitransfers

Azure Bastion - Ausblick

- Zusätzliche Compliance-Möglichkeiten
  z.B. Deaktivierung des Dateitransfers und der Zwischenablage
- Integration mit Azure AD
- Unterstützung für MFA
- Richtige Globalisierung
  Tastaturlayouts, etc.

Azure Bastion - Ausblick



- Zugriff mit nativen RDP-Clients
- Aufzeichnung von Sessions
- Verbindung zu IoT Edge Geräten über AMQP
  Auch ohne direkte Internetverbindung via ExpressRoute

Vielen Dank!

Fragen? Gern ☺