Home Office:
A more secure network with SCION

Peter Thüring
Head Information Technology
Swiss National Bank (SNB)

SCHWEIZERISCHE NATIONALBANK
BANQUE NATIONALE SUISSE
BANCA NAZIONALE SVIZZERA
BANCA NAZIUNALA SVIZRA
SWISS NATIONAL BANK

SCION™
ELEVATING SECURE COMMUNICATION

SNB’s experience with SCION

- Testing SCION since 2016

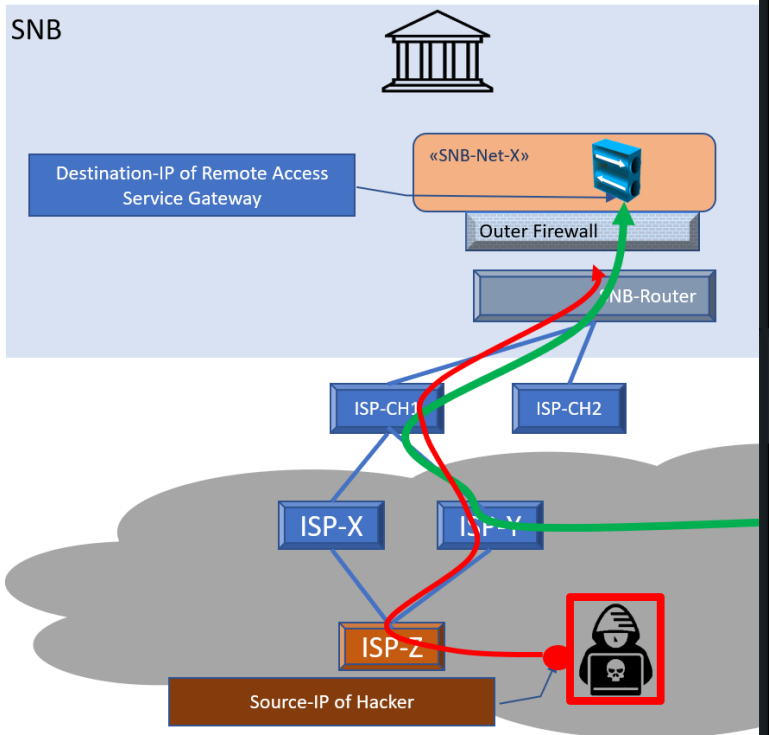
- Productive Use Cases:
  - Multipath Connection between Branch Singapore and SNB Data Center CH (2018)
  - Secure Swiss Finance Network SSFN (2022)
  - Home Office Capability (2024)

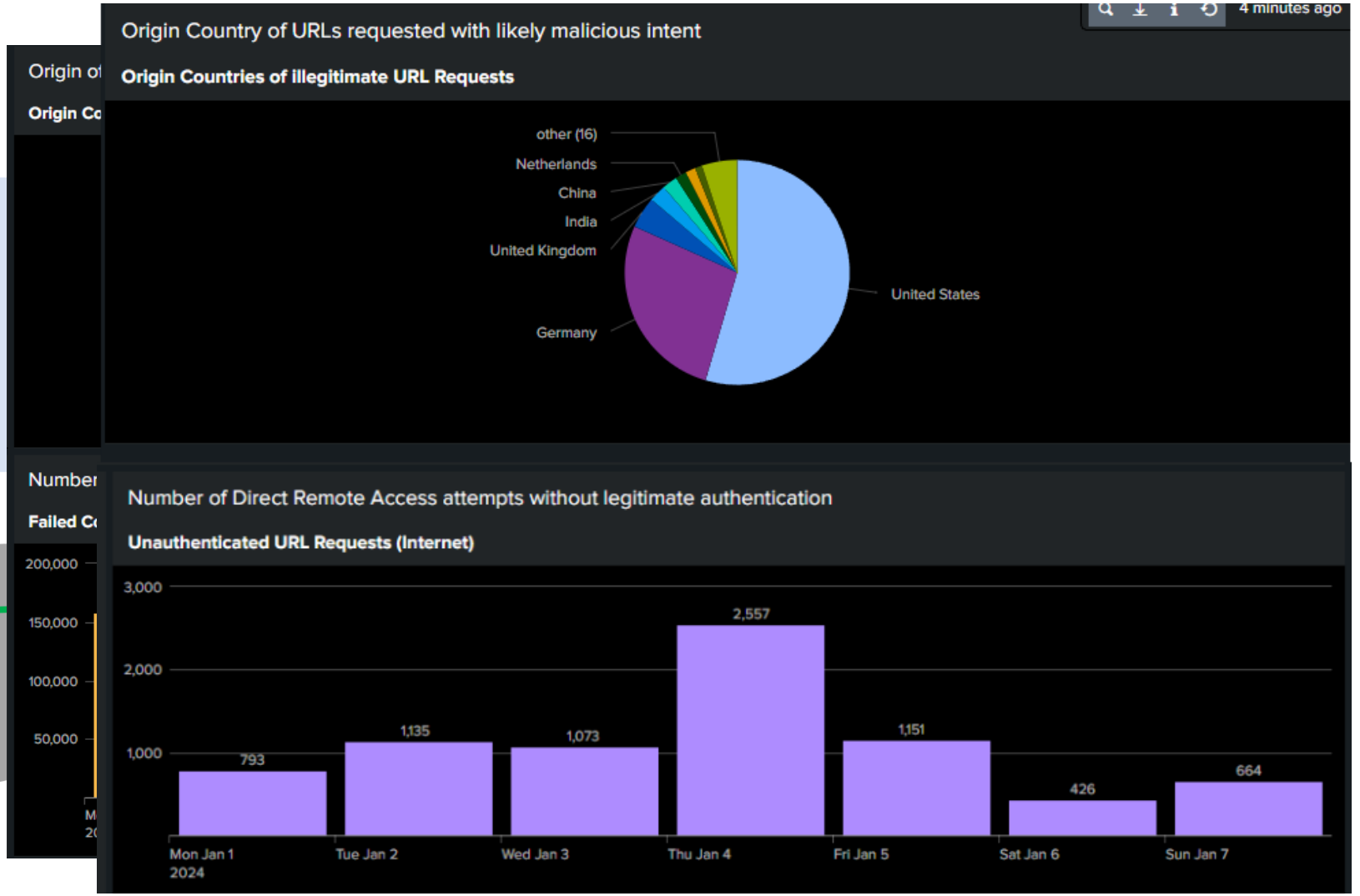
Home Office Requirements

- Solid and secure Remote Access Infrastructure
  - Business continuity… during pandemic a «Life Line»
  - Workforce attractiveness
- Protect from threats by Global Internet
  - Avoid communication loss between Home Office User and Data Center
  - Reduction of exposure to security vulnerabilities on devices and systems
- Enhancing resiliency
  - Reducing surface against global attacks
  - Higher availability by preferring multi-provider solutions

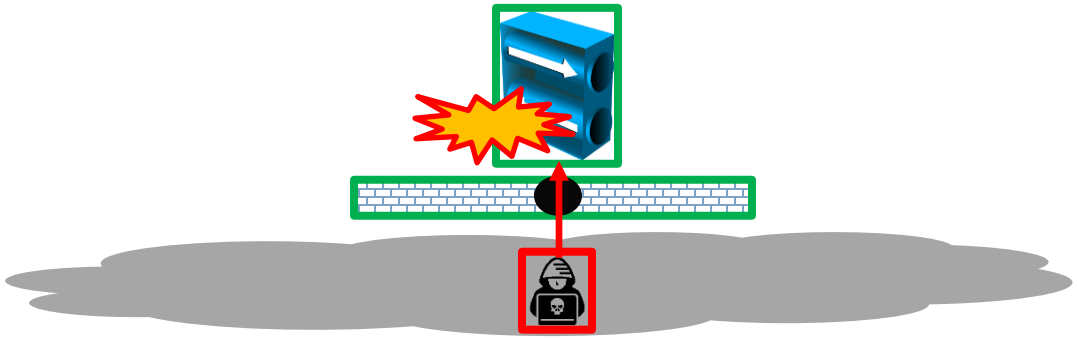
Global reachability comes with a global attack surface

Example week:
January 1 – 7 2024





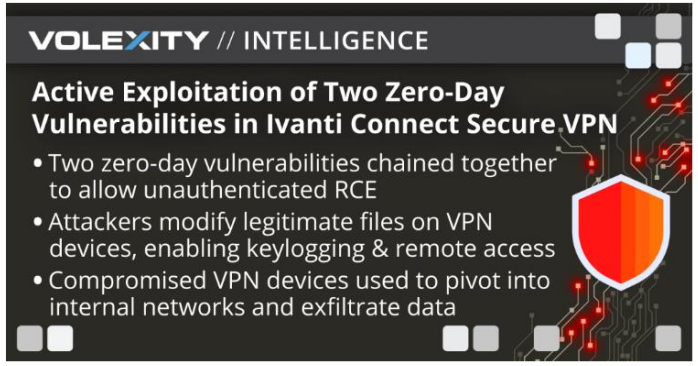
And suddenly this attack surface became very real



Active Exploitation of Two Zero-Day Vulnerabilities in Ivanti Connect Secure VPN

JANUARY 10, 2024

by Matthew Meltzer, Robert Jan Mora, Sean Koessel, Steven Adair, Thomas Lancaster



Ivanti Connect Secure VPN Exploitation Goes Global

JANUARY 15, 2024

by Cem Gurkok, Paul Rascagneres, Sean Koessel, Steven Adair, Thomas Lancaster

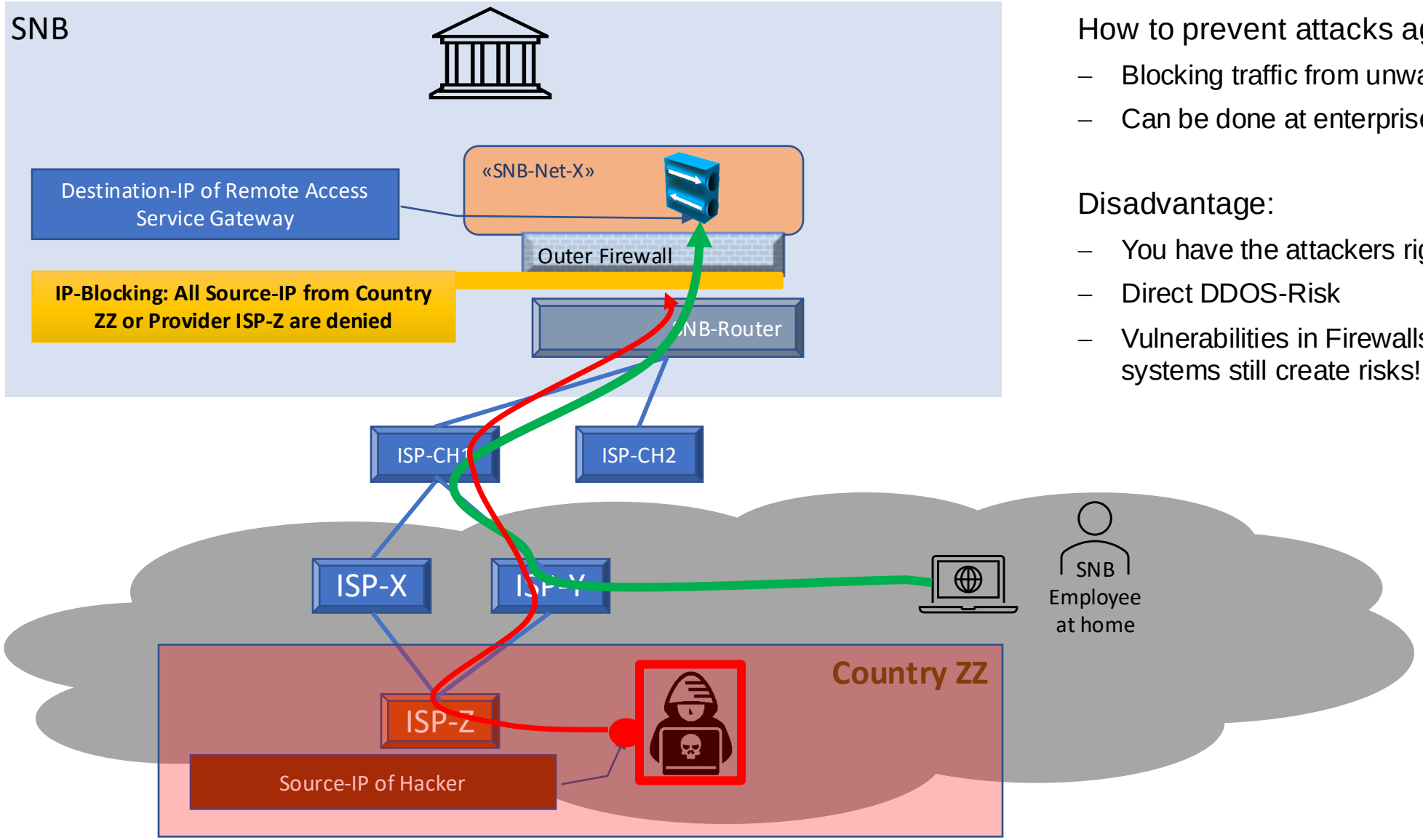
Effectively reducing the attack surface is important

Common Solutions:

- GEO-IP Blocking on outer Firewall in SNB Data Center
- Service by a Single Security Provider
- BGP-Advertisement Limit by CH-Internet Providers

Each of them has its shortcomings compared to our requirements

GEO-IP Blocking on outer Firewall of SNB Data Center



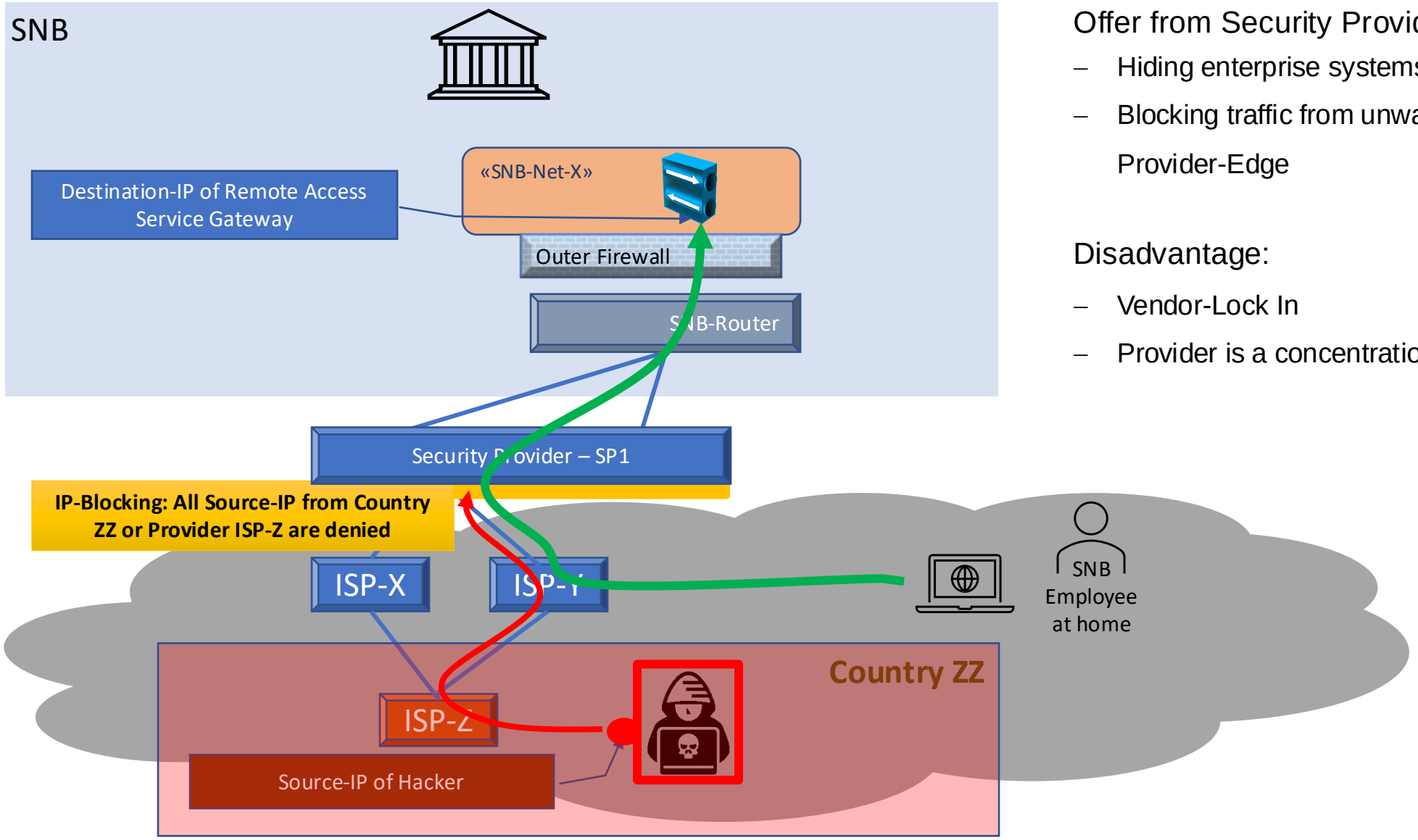
How to prevent attacks against systems?

- Blocking traffic from unwanted IP-sources
- Can be done at enterprise firewall

Disadvantage:

- You have the attackers right at your door
- Direct DDOS-Risk
- Vulnerabilities in Firewalls and other front systems still create risks!

Solution by a single Security Provider



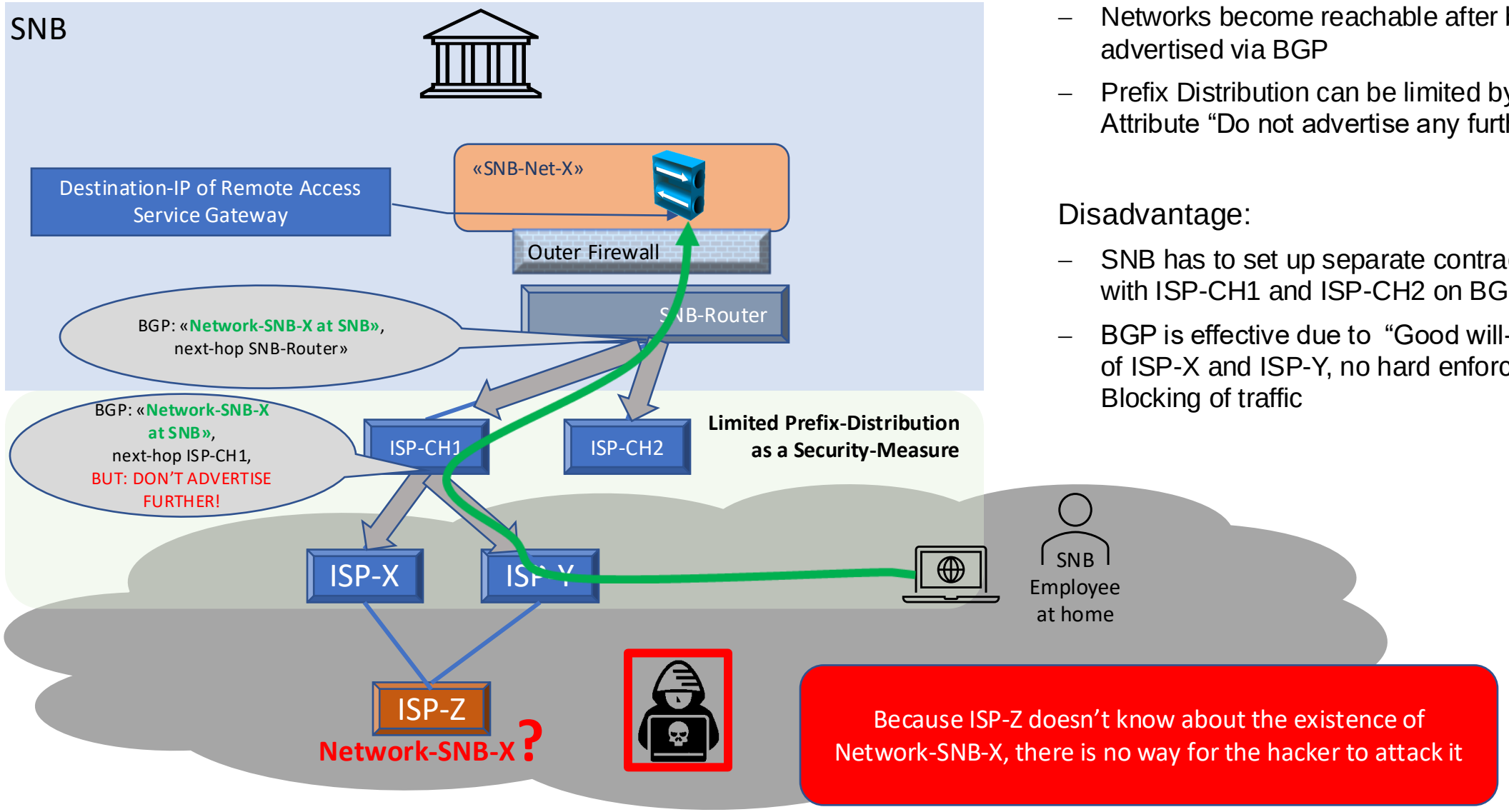
Offer from Security Provider:

- Hiding enterprise systems behind Provider
- Blocking traffic from unwanted IP-sources at Provider-Edge

Disadvantage:

- Vendor-Lock In
- Provider is a concentration risk

Usage of Standard-BGP-Feature in Internet Routing



- Networks become reachable after being advertised via BGP
- Prefix Distribution can be limited by adding BGP-Attribute "Do not advertise any further"

Disadvantage:

- SNB has to set up separate contracts with ISP-CH1 and ISP-CH2 on BGP-Policy
- BGP is effective due to "Good will-behaviour" of ISP-X and ISP-Y, no hard enforcement, no IP-Blocking of traffic

Effectively reducing the attack surface is important

Common Solutions:

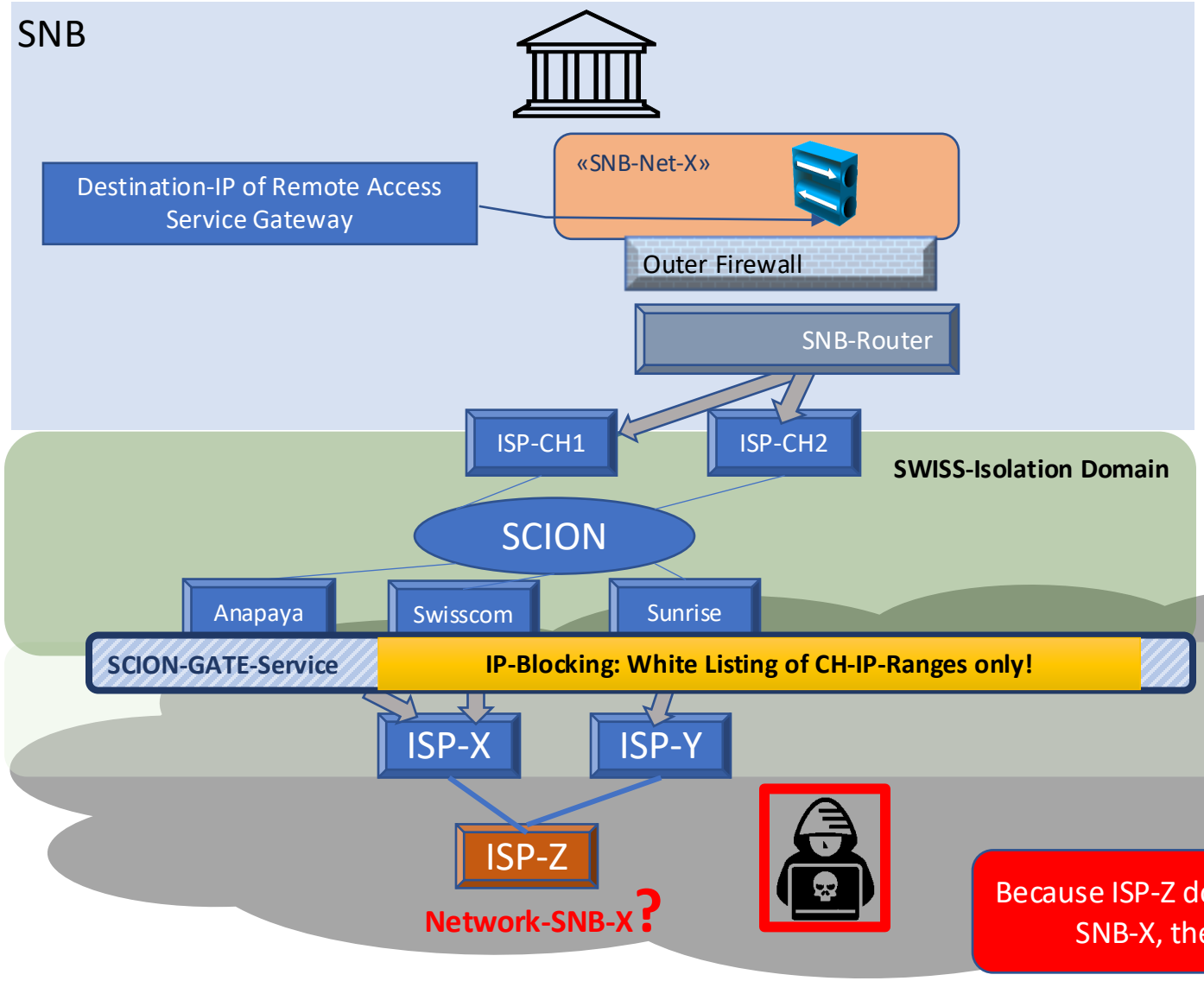
- GEO-IP Blocking on outer Firewall in SNB Data Center
- Service by a Single Security Provider
- BGP-Advertisement Limit by CH-Internet Providers

Our chosen solution:

➢ GATE-Service offered by CH-SCION-Provider Federation

- Federation created initially for the «Secure Swiss Finance Network»
- Providers have built a separate «SWISS» SCION Isolation Domain
- GATE-Service as a bridge between SWISS-ISD and Public Internet

Re-Use of CH-SCION-Provider-Federation -> SCION-GATE



- Re-Use of «SWISS»-Isolation Domain
- «SCION-GATE-Service» as a bridge between SCION-controlled network and public Internet
- Limit Prefix-Distribution by common BGP-Signaling as mentioned before
- IP-Blocking with White-Listing at «Gate Service»-Edge

Advantage:

+ Avoiding unnecessary visibility
+ No single provider risk
+ Single contact for multi-provider solution

SNB Home Office Use Case - Conclusion

- It is not a genuine SCION dependent approach
  - But it is a pragmatic and efficient Service Offer by Swiss Internet Providers who expand their cooperation to more and more realms
- SCION is an INTER-Provider Technology!
  - It’s fruits can only be harvested when Providers cooperate
- Institutions and Enterprises have to consider if a SCION-based Multi-Provider-Service would be of interest to them
  - The expectations of the SNB were met perfectly

… but we still have a «bucket list»

What else we would like to see from “SCION”?

- Integration of smaller locations into CH-SCION-Provider coverage
  (already testing)

- SCION-protected connectivity to national and international Cloud Providers
  (already planning)

- SCION-Software interface directly on Endpoints as Laptops and Smart Phones
  (this would be a complete game changer!)

Thank you for your attention!

SCHWEIZERISCHE NATIONALBANK
BANQUE NATIONALE SUISSE
BANCA NAZIONALE SVIZZERA
BANCA NAZIUNALA SVIZRA
SWISS NATIONAL BANK