SAND2013-4315C

Exceptional service in the national interest

Cyber Zone Defense

External Browsing Zone

Cristina Montoya
Cyber Security
Sandia National Laboratories

Sandia National Laboratories is a multi-program laboratory managed and operated by Sandia Corporation, a wholly owned subsidiary of Lockheed Martin Corporation, for the U.S. Department of Energy's National Nuclear Security Administration under contract DE-AC04-94AL85000. SAND NO. 2011-XXXXP

Problem: Malware and Data Exfiltration

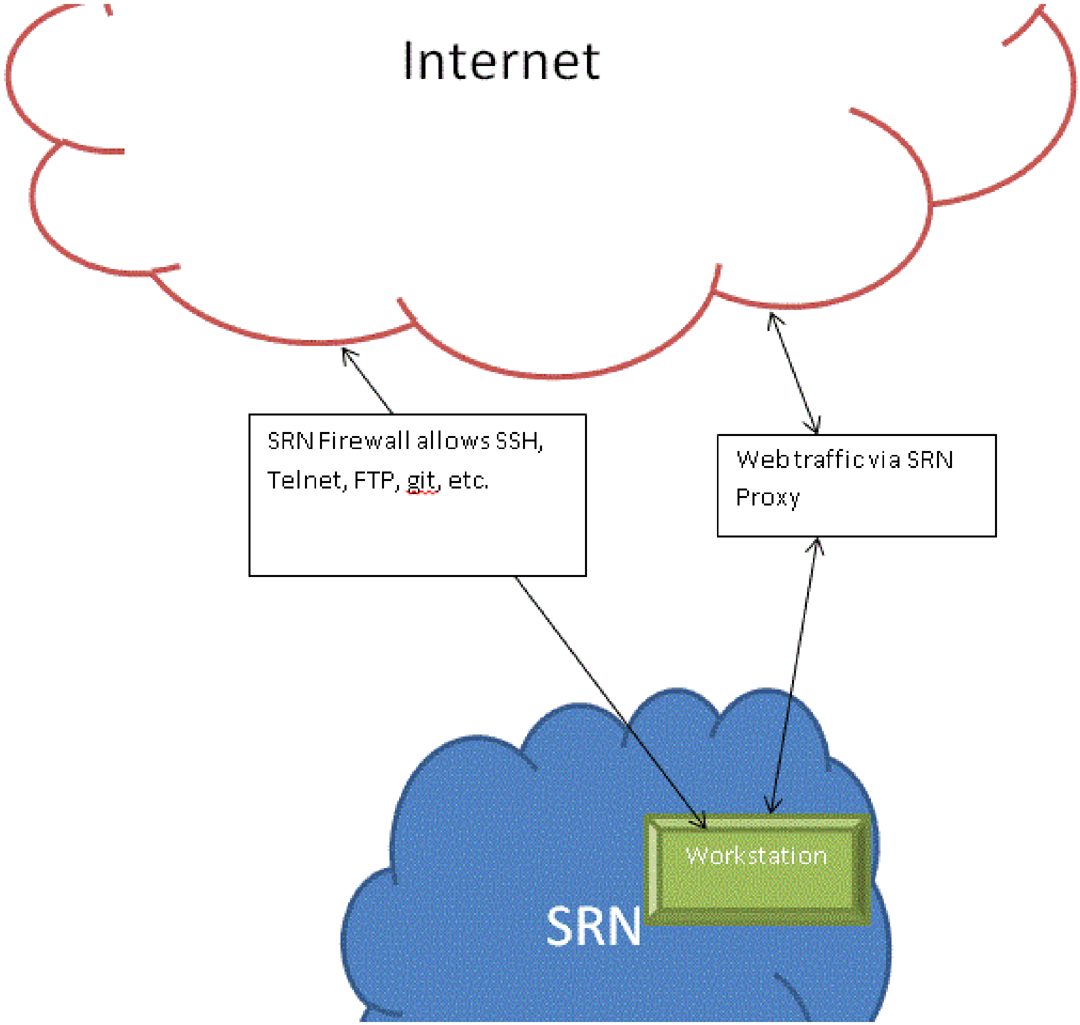
- Malware from the Internet
  - Typical day's browsing > 42K unique sites, >40 Million connections
  - Intermingles the internal network and Internet
  - Malware from internet browsing is a large issue
  - Malware from email phishing is anther large issue

- Data Exfiltration plus Command & Control
  - Adversary hides in outgoing Web traffic
  - Sends data out on port 80 (http) and 443 (https)
  - Phones home on same ports
  - Currently members of the workforce browse the internet and it is difficult to effectively block the adversary from exfiltration of data

Solution: Move the Problem Shift the Risk

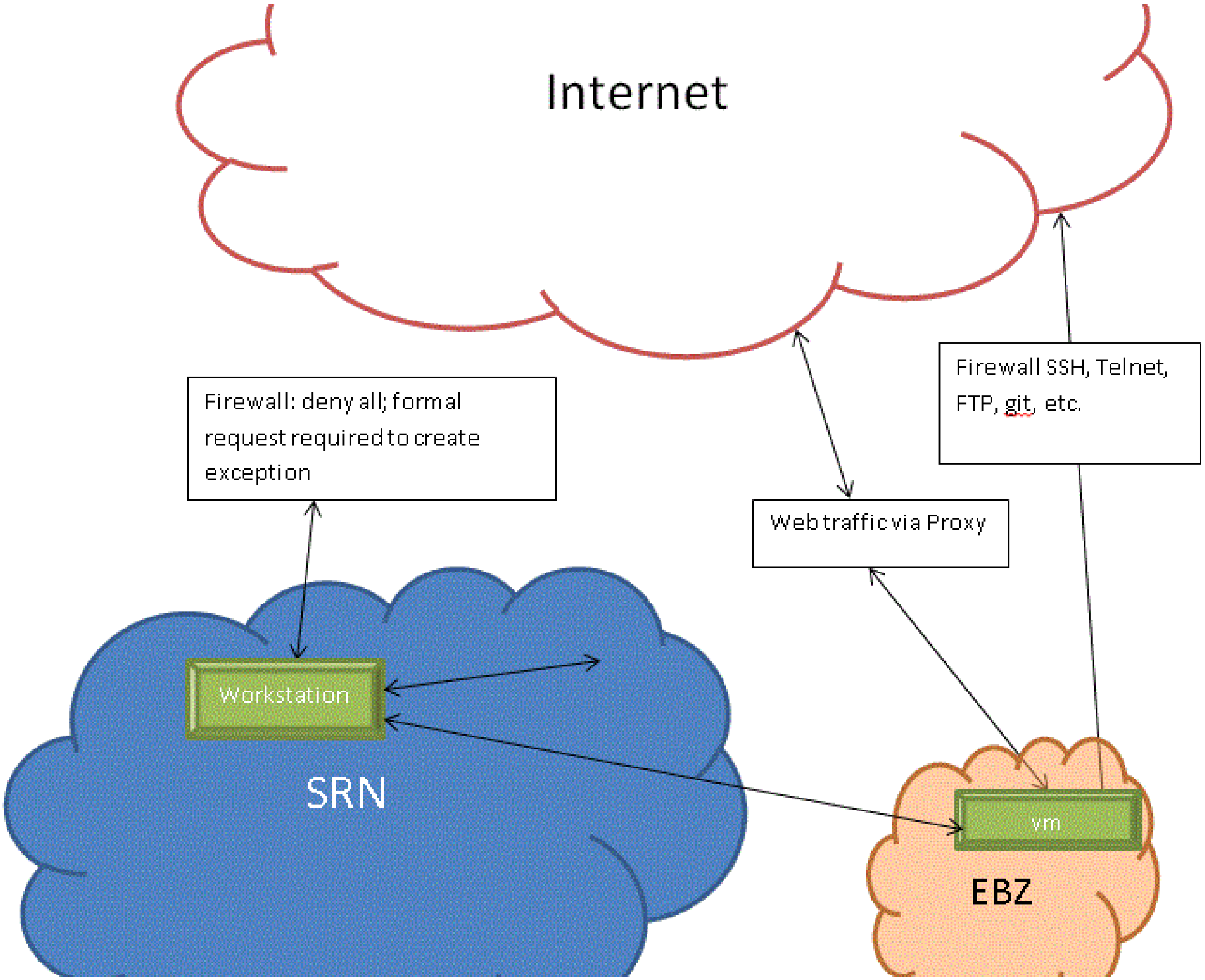
- Browsing is Essentially a Visual Activity
  - We don’t need to communicate directly with web sites
  - We can remotely browse
- Use External Browsing Zone (EBZ) to browse
  - Infect the EBZ, not Sandia’s internal network
  - Close exfiltration paths (don’t need them for browsing anymore)
- EBZ provides virtual desktops outside the internal network
  - Windows 7 with IE, Firefox and Chrome
  - Daily revert to known good image
  - Connect from SRN using Citrix VDI-in-a-Box
  - Good multimedia, local printing, file transfer
  - Automated URL transfer (click on internal network, opens in EBZ)

SRN Architecture

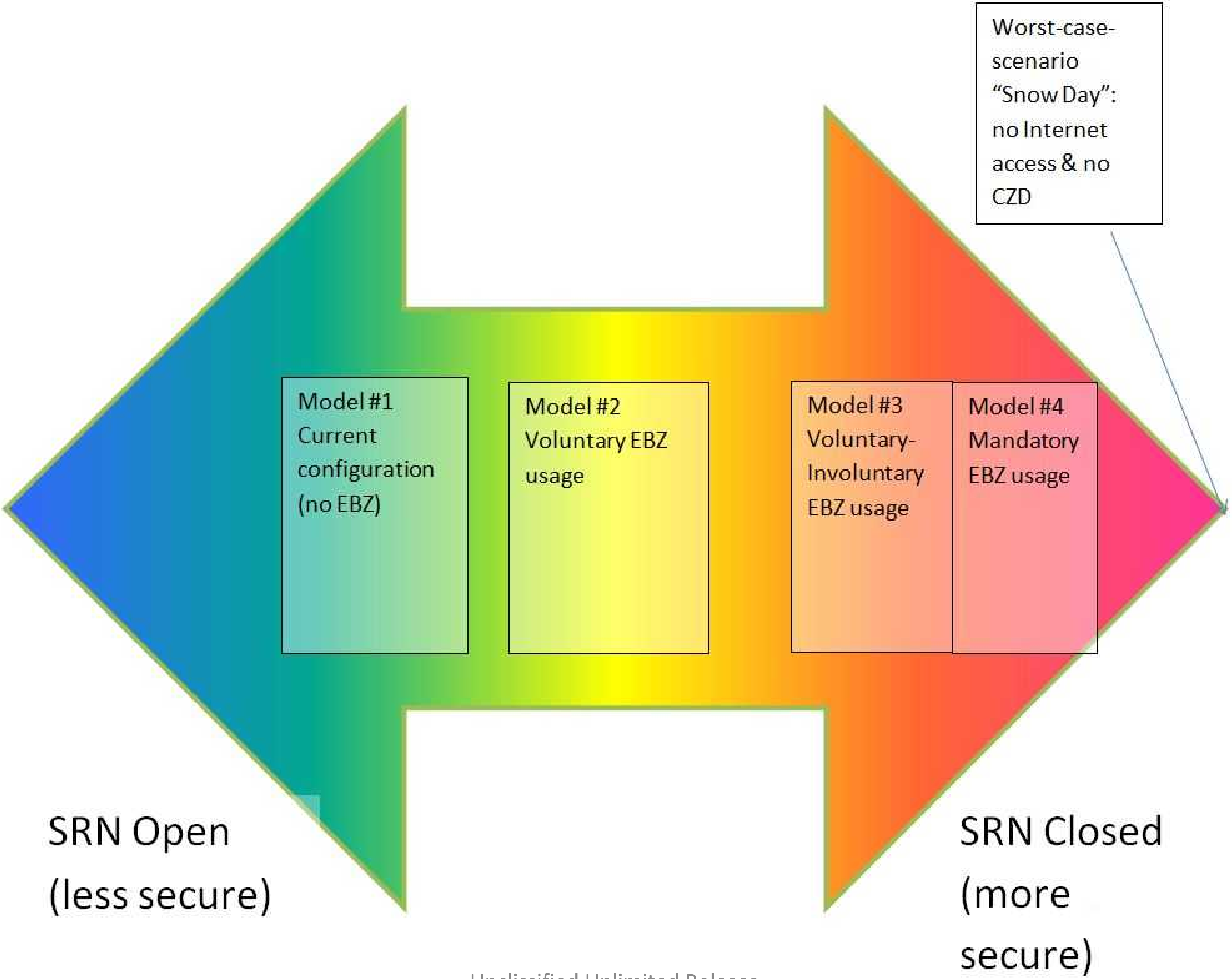


Internet
SRN Firewall allows SSH, Telnet, FTP, git, etc.
Web traffic via SRN Proxy
Workstation
SRN

EBZ/SRN Architecture



Internet
Firewall: deny all; formal request required to create exception
Web traffic via Proxy
Firewall SSH, Telnet, FTP, git, etc.
Workstation
SRN
vm
EBZ



Worst-case-scenario "Snow Day": no Internet access & no CZD

Model #1 Current configuration (no EBZ)

Model #2 Voluntary EBZ usage

Model #3 Voluntary-Involuntary EBZ usage

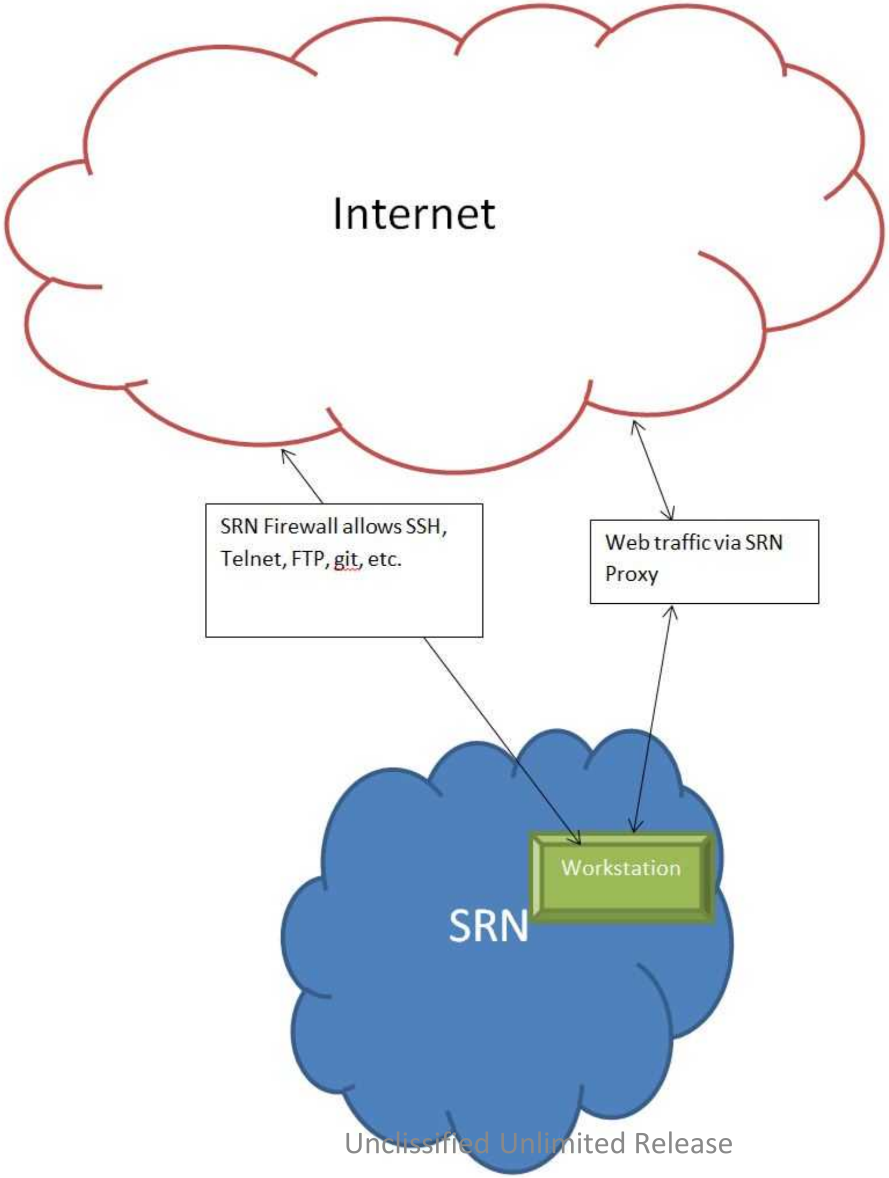
Model #4 Mandatory EBZ usage

SRN Open (less secure)

SRN Closed (more secure)

Model #1: Current Configuration without EBZ

SRN and Internet comingled via web browsing and other connections



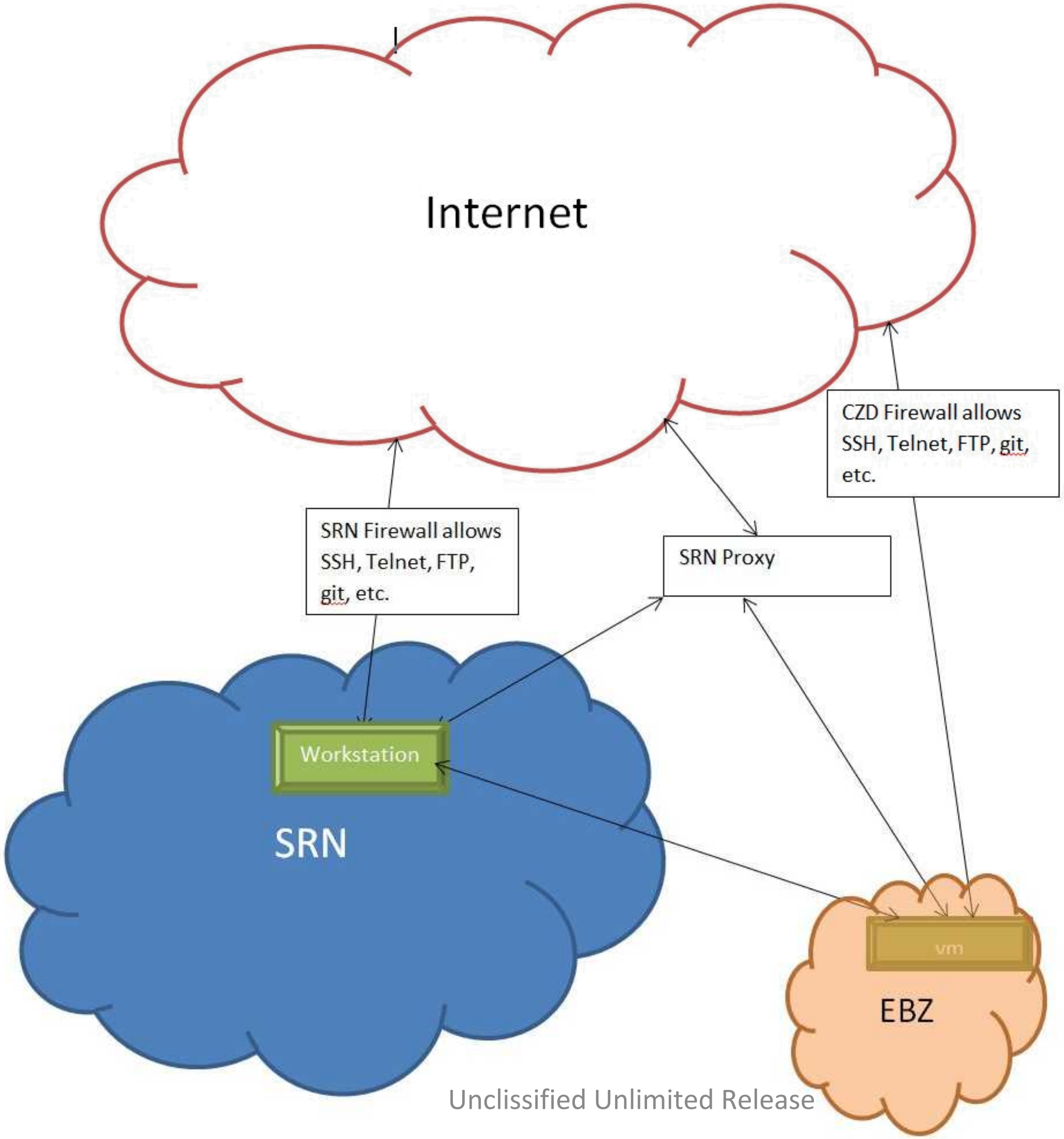
Internet

SRN Firewall allows SSH, Telnet, FTP, git, etc.

Web traffic via SRN Proxy

Model #2: Voluntary EBZ Usage

SRN keeps its current firewall and proxy configuration; EBZ operates in parallel



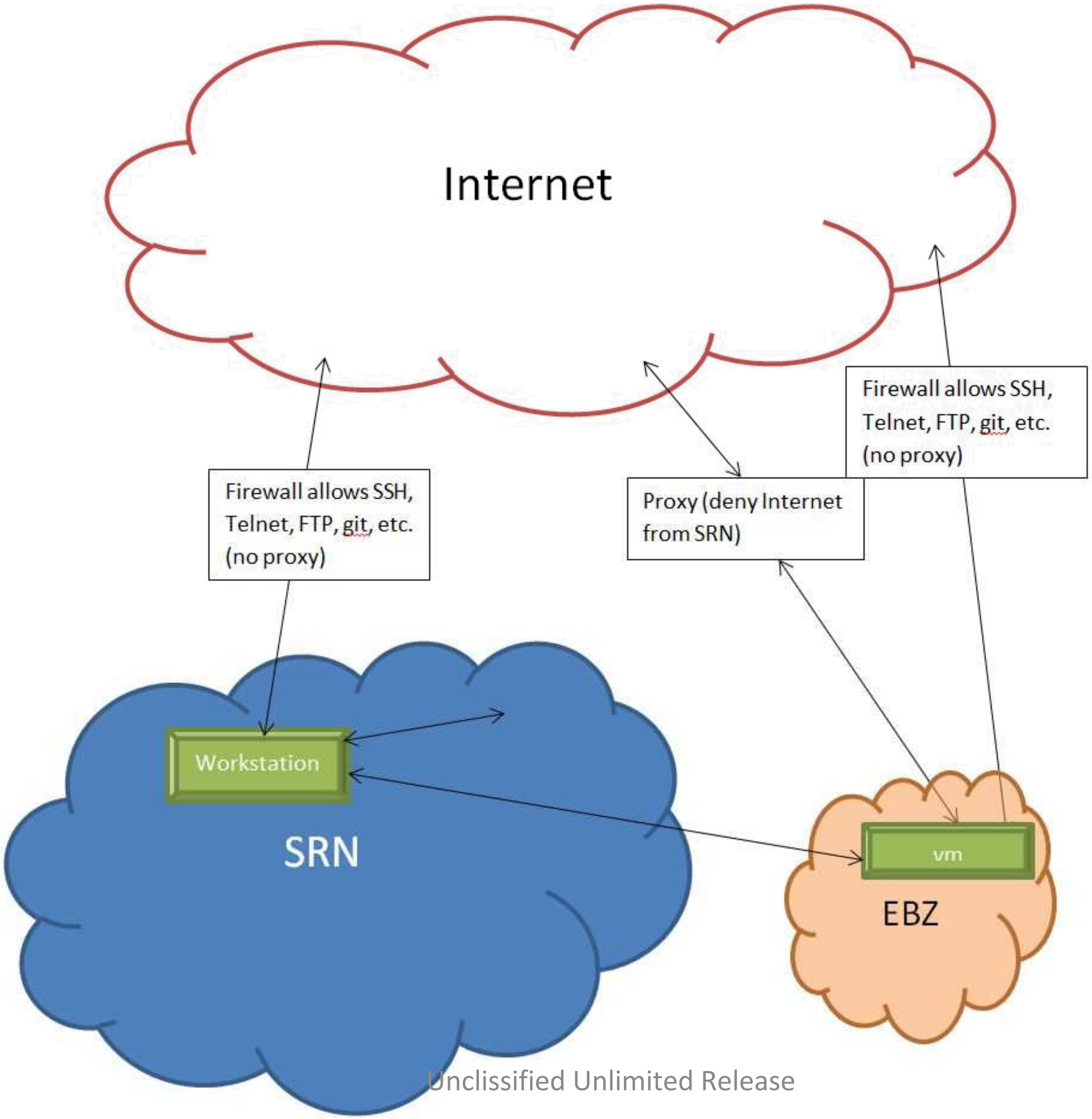
SRN Firewall allows SSH, Telnet, FTP, git, etc.

SRN Proxy

CZD Firewall allows SSH, Telnet, FTP, git, etc.

Model #3: Voluntary/Involuntary EBZ Usage

SRN proxy denies external browsing; SRN firewall unchanged



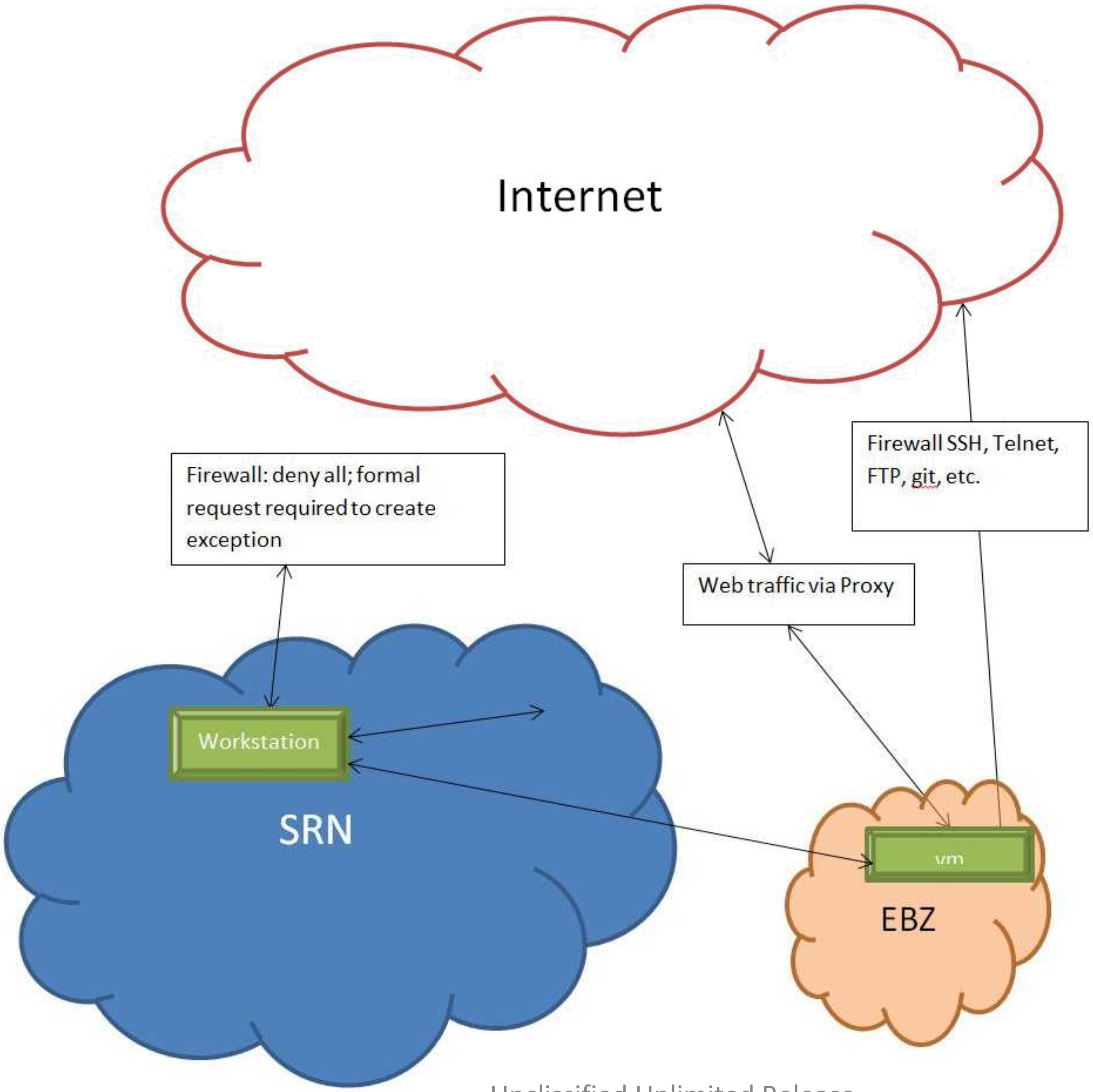
Firewall allows SSH, Telnet, FTP, git, etc. (no proxy)

Proxy (deny Internet from SRN)

Firewall allows SSH, Telnet, FTP, git, etc. (no proxy)

Model #4: Mandatory EBZ Usage

SRN proxy denies external browsing; SRN firewall denies external access


Internet
Firewall: deny all; formal request required to create exception
Web traffic via Proxy
Firewall SSH, Telnet, FTP, git, etc.
Workstation
SRN
vm
EBZ

Pilot Results

- Completed successful pilot
- 400 participants
- Provided positive feedback on ease of use and performance
- Many departments requesting to be on the pilot for various use cases
  - Non-Attribution
  - When SSL encryption blocks access and the risk is to high to allow exemption – EBZ was used instead
  - Training and collaborating with other entities that are not allowed on the SRN
  - People want Cyber to give them a “SAFE” way to browse