NDISAC

Welcome to User Authentication DIB Supplier Webinar:

March 27, 2019

NDISAC Welcomes Suppliers to the Webinar!

- Brief overview of NDISAC
- Introduction of Panelists
- Webinar Logistics

Questions during the presentation?

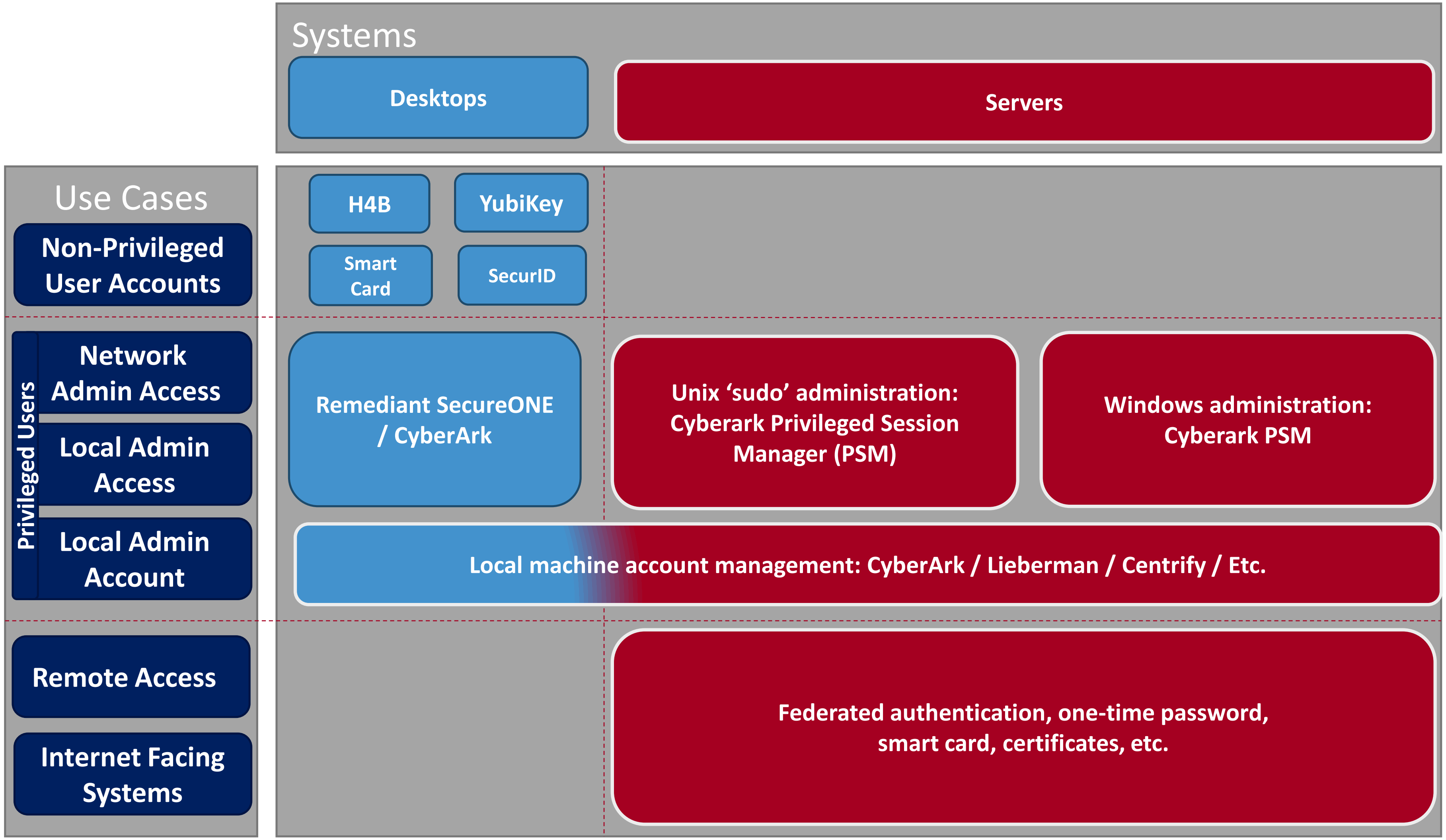
1. Write your question in the chat area
2. E-Mail info@ndisac.org

We will answer your questions at the end of the webinar.

Scope

- Single factor static passwords are vulnerable to guessing and replay
- Risk mitigation and some regulations (e.g. NIST SP 800-171) require multifactor authentication (MFA)
  - 3.5.3 Use multifactor authentication for local and network access to privileged accounts and for network access to non-privileged accounts.
- MFA enforces the use of at least two different factors in a single transaction
  - Something only you know: e.g. password, PIN
  - Something only you have: e.g. hardware token, software token, smart card with a private key, phone that receives SMS or push notifications
  - Something only you are: e.g. fingerprint, face geometry
- No one technology solves every use case, so expect many components
- There are many options for each use

Multi-Factor Authentication



Systems

Desktops

Servers

Use Cases

Non-Privileged User Accounts

H4B

YubiKey

Smart Card

SecurID

Privileged Users

Network Admin Access

Local Admin Access

Local Admin Account

Remediant SecureONE / CyberArk

Unix 'sudo' administration: Cyberark Privileged Session Manager (PSM)

Windows administration: Cyberark PSM

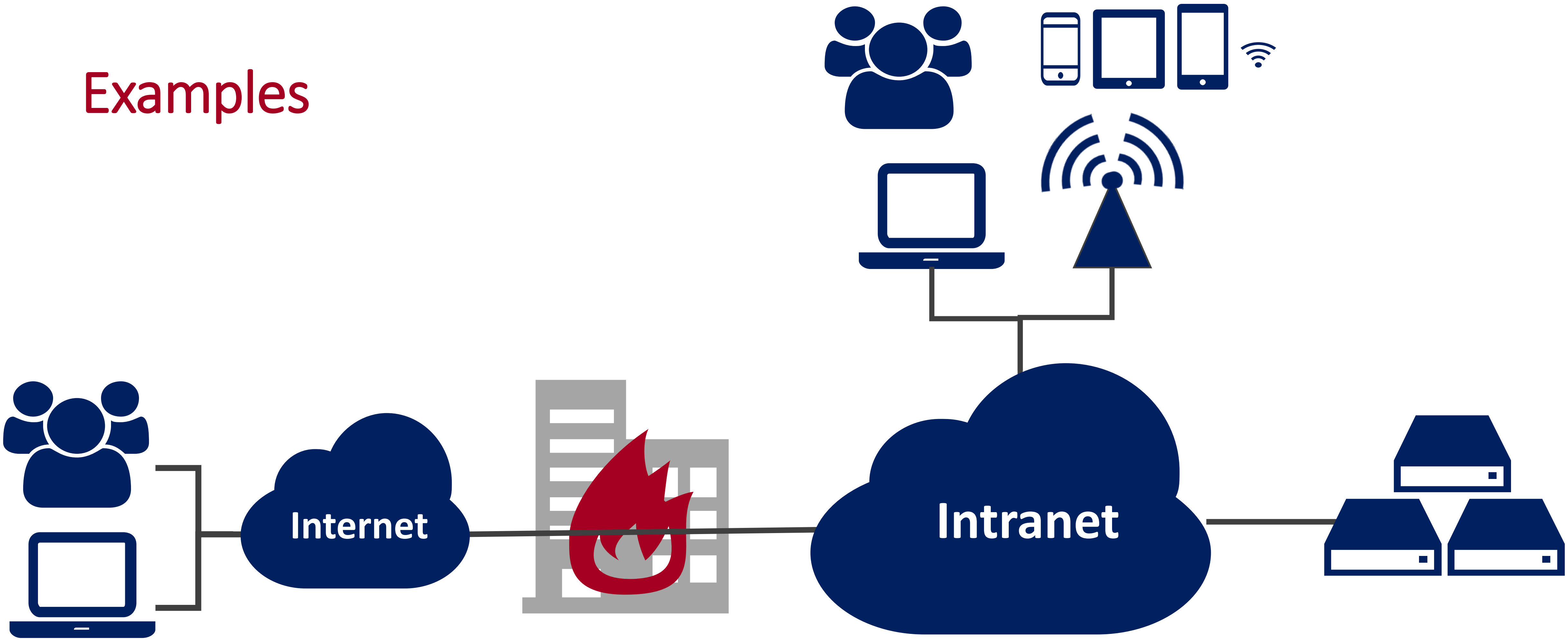
Local machine account management: CyberArk / Lieberman / Centrify / Etc.

Remote Access

Internet Facing Systems

Federated authentication, one-time password, smart card, certificates, etc.

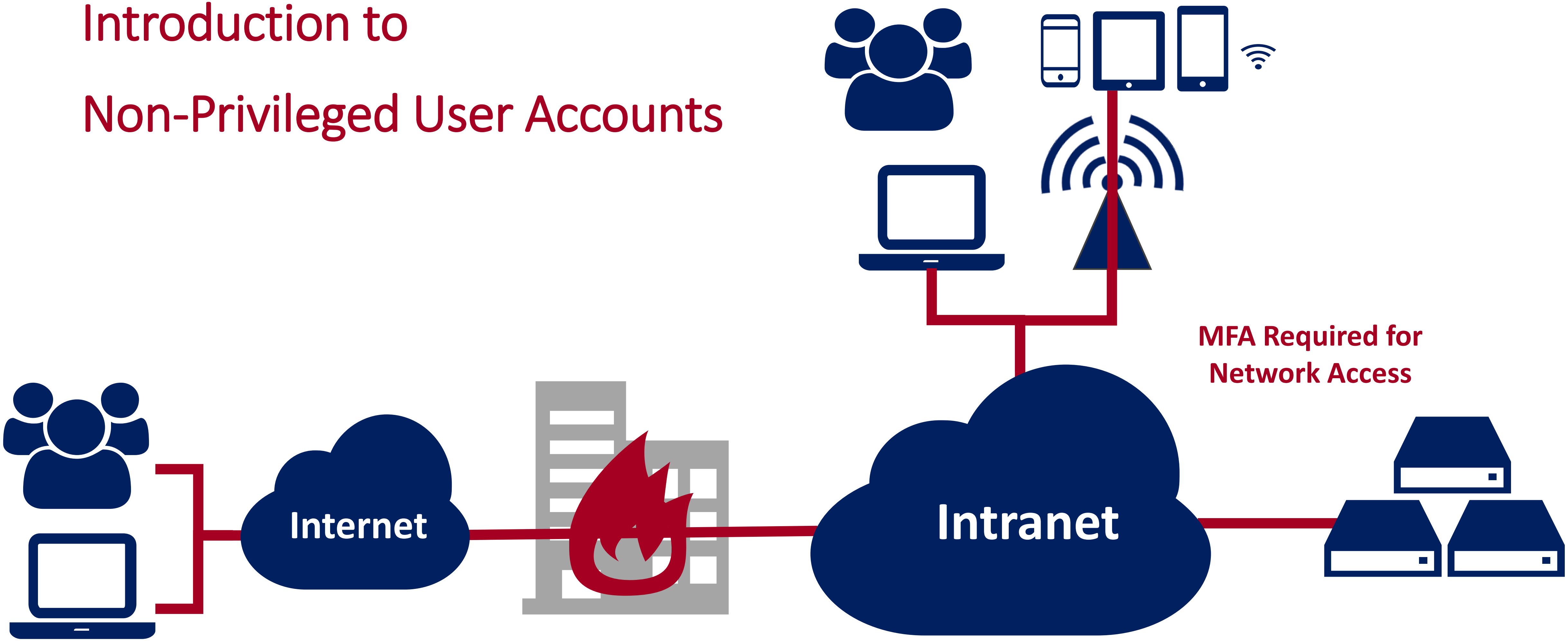
Examples



NDISAC

©NDISAC 2019

Introduction to Non-Privileged User Accounts

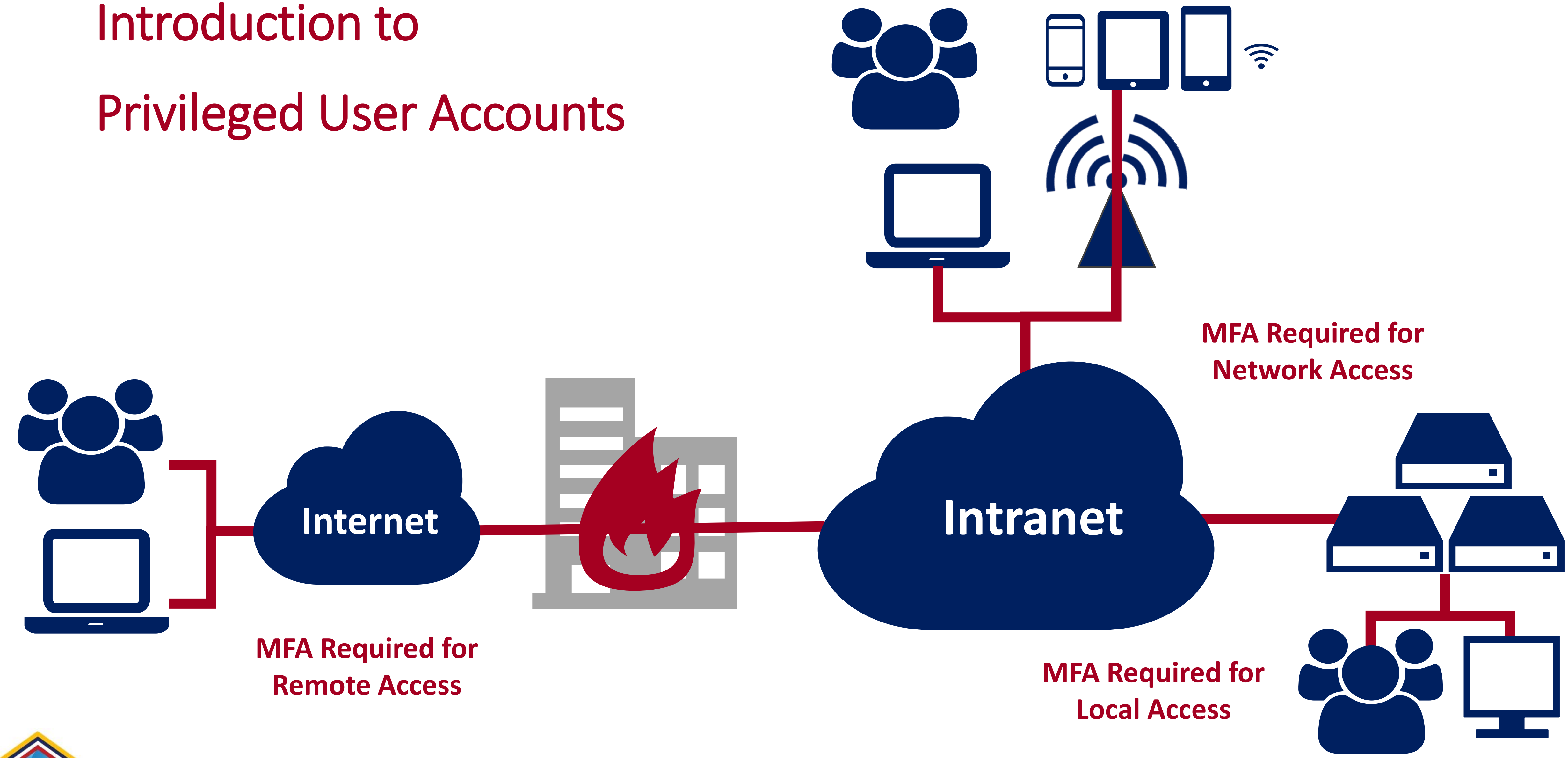


MFA Required for Network Access

MFA Required for Remote Access

NDISAC

Introduction to Privileged User Accounts



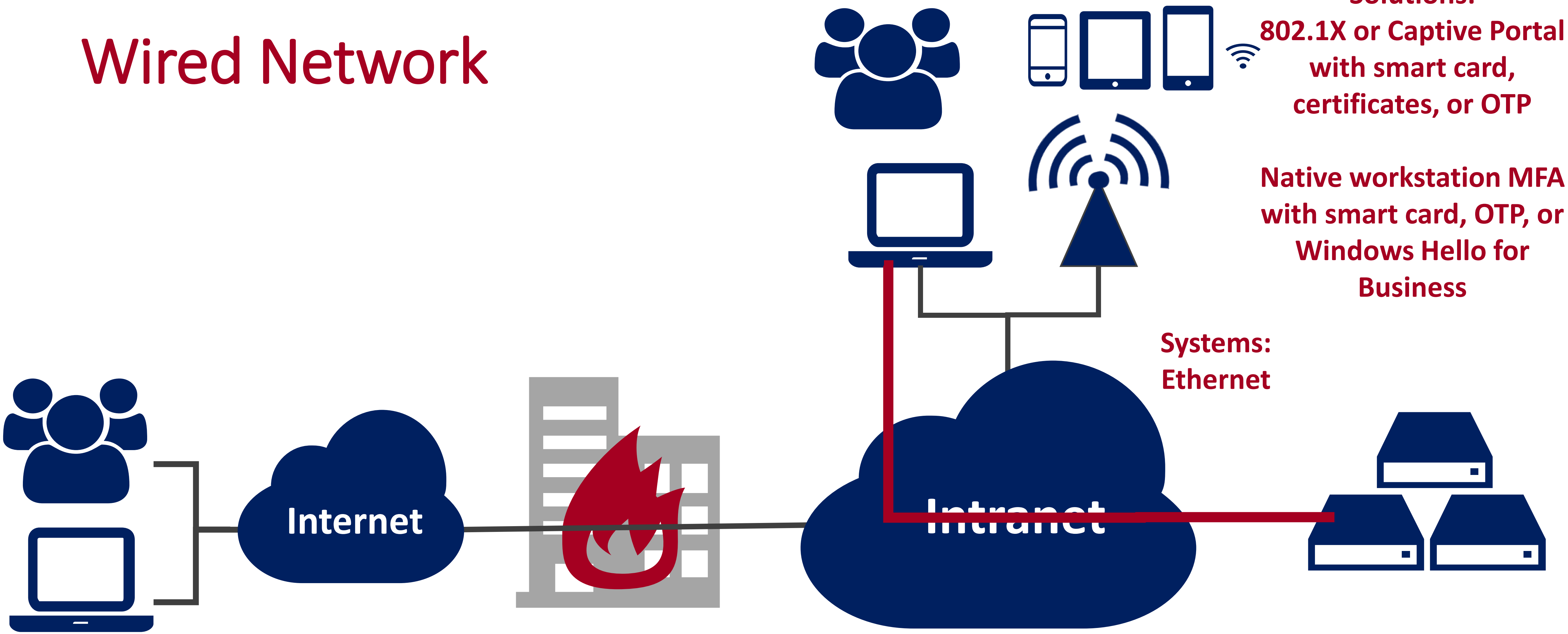
MFA Required for Network Access

MFA Required for Remote Access

MFA Required for Local Access

NDISAC

Wired Network



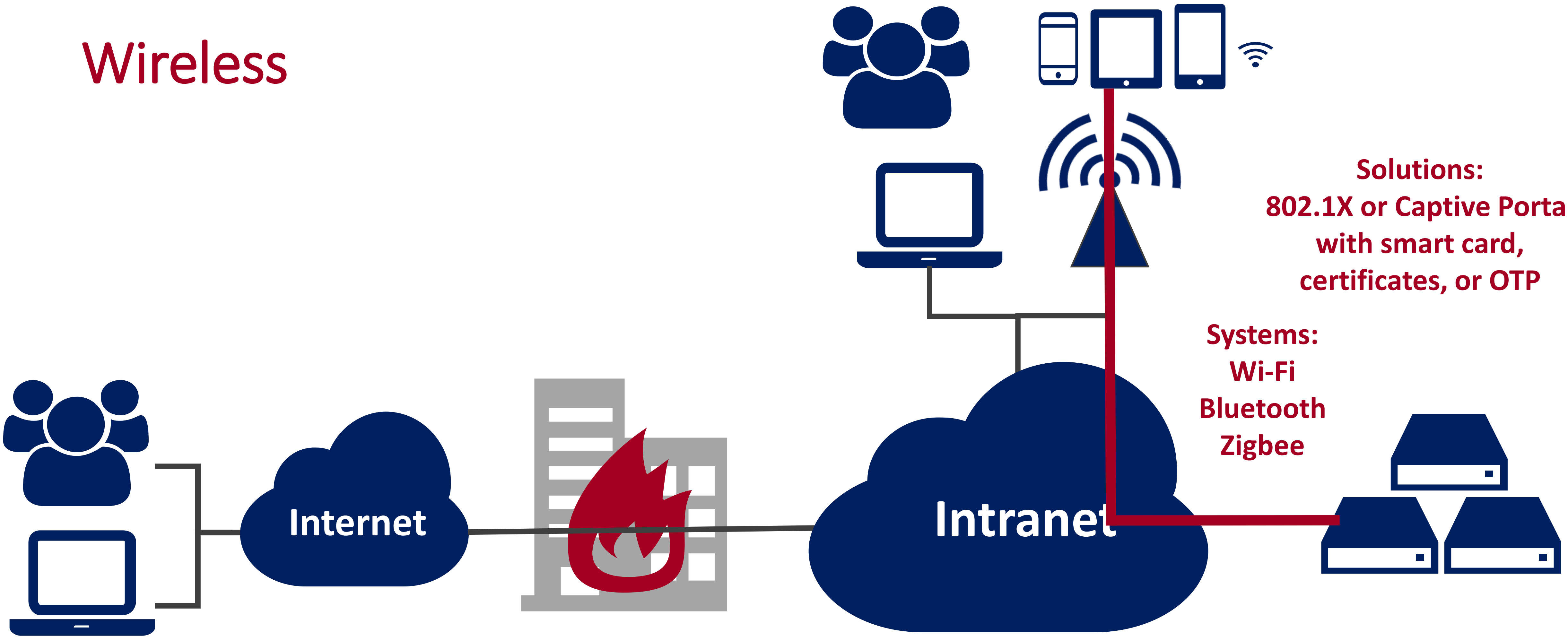
Solutions:
802.1X or Captive Portal with smart card, certificates, or OTP

Native workstation MFA with smart card, OTP, or Windows Hello for Business

Systems:
Ethernet

NDISAC

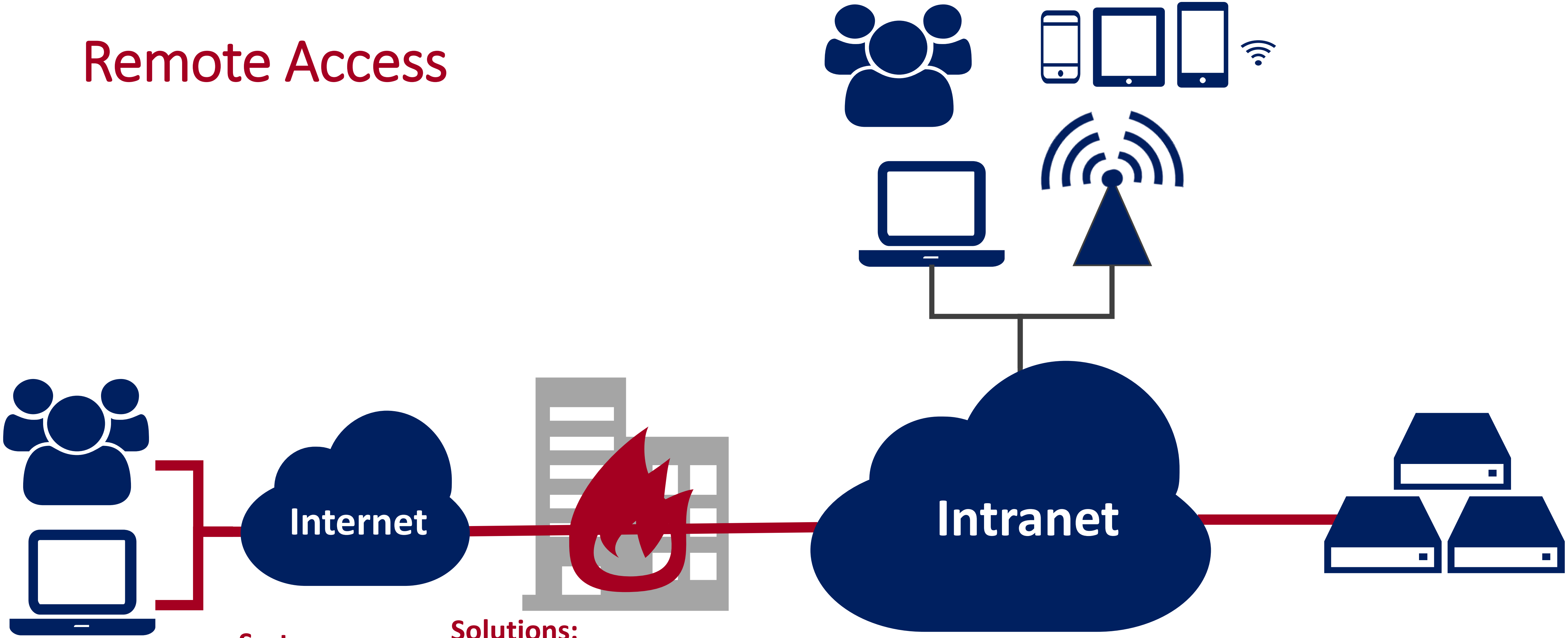
Wireless



Solutions:
802.1X or Captive Portal
with smart card,
certificates, or OTP

Systems:
Wi-Fi
Bluetooth
Zigbee

Remote Access



Systems:
VPN
Reverse Proxy
Customer Portals
SSLVPN

Solutions:
Smart Card
OTP
Certificates
CAC
Federation

Thank You!

Comments or questions?
info@ndisac.org

Q/A from Webinar:

QUESTION: I see that end user machines and servers are discussed in the slides. What is the guidance in relation to MFA for network devices for network device (switch/router/etc.) administration?

- A good practice is to treat a network device analogous to a server with respect to authenticating administrators that seek to gain privileged access to it – MFA is typically provided by a RADIUS, LDAP, or TACAC+ service that validates the one-time password provided by the network administrator at login time. Also, don't forget that network devices have local administrator accounts, too, which need to be managed (e.g. periodically rotated, and kept locked up in a service account management platform that validates MFA before the service account password is "checked out" to an admin).
- Please also refer to DoD FAQ: Q76: "Security Requirement 3.5.3 – Native 2-factor authentication support for network access on all platforms is problematic; how is the multifactor requirement met?"

QUESTION: If a user uses MFA at the workstation (for a workstation login), must the user use MFA again when connecting to a server/AD on the network?

- No. As long as MFA must be satisfied as a condition to access the network (defined as wired, wireless, or remote access) the MFA requirement has been met. This will, however, not apply to the need for separate MFA access using privileged account for administration. MFA to the network itself also doesn't eliminate the need for role-based access control on systems the user may access.

QUESTION: For the use case of something trying to discover a password, password lock-outs seem sufficient. It can be argued that when someone connects to the network from within the Enterprise, MFA is already in place - one factor being physical presence in the building.

- That's not how MFA works. MFA is designed to be something you have & something you know or something you are that's irrefutable. I as an attacker can spoof being inside the building. See Q75 of the DoD FAQ at https://dodprocurementtoolbox.com/faqs/cybersecurity/cybersecurity-faqs, which says in part: “Where you are, even in a controlled access facility is not one of these factors and, generally, would be a condition that applied to many and not unique to the individual being authenticated.”

QUESTION: Is an OTP (one-time PIN) delivered via e-mail considered MFA when used with UID/PWD (user ID/password)?

- No, it is not, because e-mail is not delivered to a single piece of hardware that only you have. It will get queued and stored in multiple mail transfer servers and delivered to a server that has your mailbox. The mail can then be retrieved from multiple mail clients.
- OTPs are subject to interception from most mediums not utilizing PTP tunneling protocols for encryption. SMS and E-mail are not recommended as “secure or strong” MFA options.

QUESTION: If you are using a smart card for MFA with a Windows login, how is the complexity and longevity of the password impacted? Can you make the password easier than those required in standard PW requirements?

- If you use a smart card to enforce MFA to log in to windows, you must prevent the user from bypassing the MFA by logging in with a password. This can be done by either removing the password option on the user account or setting the client machine policy to prohibit login with a password. In the first option, there is no password complexity concern, because the password is eliminated. In the second option, be aware that the user still has a password in active directory, and an adversary or insider that has access to a machine or gets code running on a machine could retrieve or guess that password, so the usual password management practices and guidelines should still be applied.
- SmartCard PINs can be simpler than passwords because smart cards have built-in anti-tampering capabilities including lockout mechanism to deter brute force attacks. See NIST 800-63: https://pages.nist.gov/800-63-3/sp800-63b.html "5.1.9.1 Multi-Factor Cryptographic Device Authenticators: Any memorized secret used by the authenticator for activation SHALL be a randomly-chosen numeric value at least 6 decimal digits in length or other memorized secret meeting the requirements of Section 5.1.1.2 and SHALL be rate limited as specified in Section 5.2.2. A biometric activation factor SHALL meet the requirements of Section 5.2.3, including limits on the number of consecutive authentication failures."

QUESTION: If I understood correctly, standalone PCs connected to an Intranet that is not connected to the internet or any outside network that intranet does not then require MFA, correct?

- See Q74 of the DoD FAQ at https://dodprocurementtoolbox.com/faqs/cybersecurity/cybersecurity-faqs, which says in part: "For a NON-PRIVILEGED user, if it's a standalone computer (e.g., a laptop computer), with no network access, the access can be via single factor authentication (SFA) - MFA is not required. However, if used to connect to a LAN, the network access has to be MFA. Typically, organizational desktops are used for network access and so the user has to use MFA to access their network account. For a PRIVILEGED user, even local access (e.g., to the standalone) requires MFA."

QUESTION: Do service accounts require MFA?

- For service accounts with no humans associated: No, service accounts can't implement MFA because there is no human involved to provide "something you are" or "something you have". Service accounts need to be managed separately using a management platform that can ensure long complex passwords are used and periodically rotated. The service account management system must also enforce MFA on people who need to "check out" the service account for privileged actions.
- For service accounts with humans associated: You should add as many layers to your defense of these accounts as you can. Using IP address controls in addition would be an option in this regard as spoofing a public IP address is difficult. Using a certificate and private key would also be good practice. Microsoft Group Managed Service Accounts with frequently rolling passwords also make it challenging for a service account to be compromised. Consider leaving the account disabled when not in use.

QUESTION: These systems cost money. How do you suggest approaching this from a Risk Management/Cost analysis?

- Utilizing known breaches and the impact/cost to the business, such as the Ponemon cost of breach studies, have been my most effective method for gaining additional funding. With MFA there is a pretty clear train of breaches (and costs) that could have been prevented with the implementation of MFA. Conducting an assessment of systems that do not currently have MFA, providing a cost estimate of implementation and contrasting that with the estimated cost of a breach makes a reasonable business case. Additionally, MFA is highlighted in multiple studies and 800-171 as a critical control and lack of implementation could lead to ineligibility when competing for DoD contracts.

QUESTION: YubiKey - does the user need a cell phone to read the PIN?

- No, however the YubiKey form factors used require NFC capability or a computer USB port.

QUESTION: How is equipment handled that does not use a commercial operating system? In our case we use a simple task scheduler that supports SSL but no MFA capability, and has no useful information but basic unit status.

- Network segmentation could and should be employed. Performing MFA at the perimeter to the network segment could be leveraged as the protection mechanism for these devices. In addition, discussions between the authors of 800-171 and DIB partners on this question have boiled down to the guidance that if a control is not "operationally or technically feasible" to meet, then an enduring exception to that control would be warranted. This should be included in your SSP as explained in Q53 of the DoD FAQ at https://dodprocurementtoolbox.com/faqs/cybersecurity/cybersecurity-faqs; “Questions remained, however, about how certain things should be documented, demonstrated or managed - in particular, any enduring exceptions to the requirements to accommodate special circumstances (e.g., medical devices), or any individual, isolated or temporary deficiencies. This drove the need to add the system security plan as an explicit security requirement.”

NDISAC

QUESTION: We have an employee base that does not have high technology skill level, they do, however, need non-privileged user access. We are thinking the Yubikey device is an option. Do you have any actual user experience with this in a low skill employee base?

- Currently our experiences show that the YubiKey is easy to use, just plug into the USB port and type in the PIN associated with certificate.

QUESTION: Can IP address of a system (static IP of server) be used for "something you are" criteria for properly configured networks? E.g. service can only be used by specific account from a specific IP address for automated services/processes?

- An IP address of a system doesn't count as a factor for MFA. IP addresses are identifiers, not authenticators, and they are for systems, not users. They can however be used as a part of a defense in depth strategy and we would advocate that. Depending on your architecture network, spoofing can be more or less difficult to perform for the attacker. Alerting on access other than ‘normal’ IP address would be prudent.

QUESTION: All staff have access to two servers from their work stations with their own passwords. How would I go about implementing MFA on Macs?

- MFA on Macs can be enforced with Centrify DirectControl to apply a smart card login requirement through AD GPO settings, or by enabling smart card sign-in on devices running MacOS High Sierra or higher. With smart card sign-in enabled, Macs can use a smart card with a USB smart card reader or a YubiKey with smart card certificates.
- If after the initial MFA sign-in into the workstation the user needs to sign into the server for non-privileged work, then no additional MFA sign-in is required. However, if the sign-in to the server is to perform privileged work (tied to privileged access), then additional MFA is required.

QUESTION: How do we obtain a copy of this webinar, so we can share this with a couple of employees who are in the field today?

- E-Mail info@ndisac.org to receive a copy of the slides from the webinar.

NDISAC