

TUNNEL VISION

EXPLORING VPN

POST-EXPLOITATION

TECHNIQUES

ORI DAVID



Agenda

- VPN exploitation
- VPN post-exploitation
- What can we do about it

whoami

Ori David

Security Researcher at Akamai

Background in red teaming & threat hunting



CVE-2023-20269: Zero-Day Vulnerability in

Cisco Adaptive Security
Firepower Threat De

CVE-2023-27997: Fortinet Fortigate SSL VPN
Pre-Auth RCE critical vulnerability

Explo

RedTail Cryptominer Threat Actors Adopt PAN-OS CVE-2024-3400 Exploit


Critical
2176

Feb 12, 2024



Ryan Barnett, Stiv Kupchik, and
Maxim Zavodchik

May 30, 2024

Share    

24-

Vulnerability Exp
Verify with Node

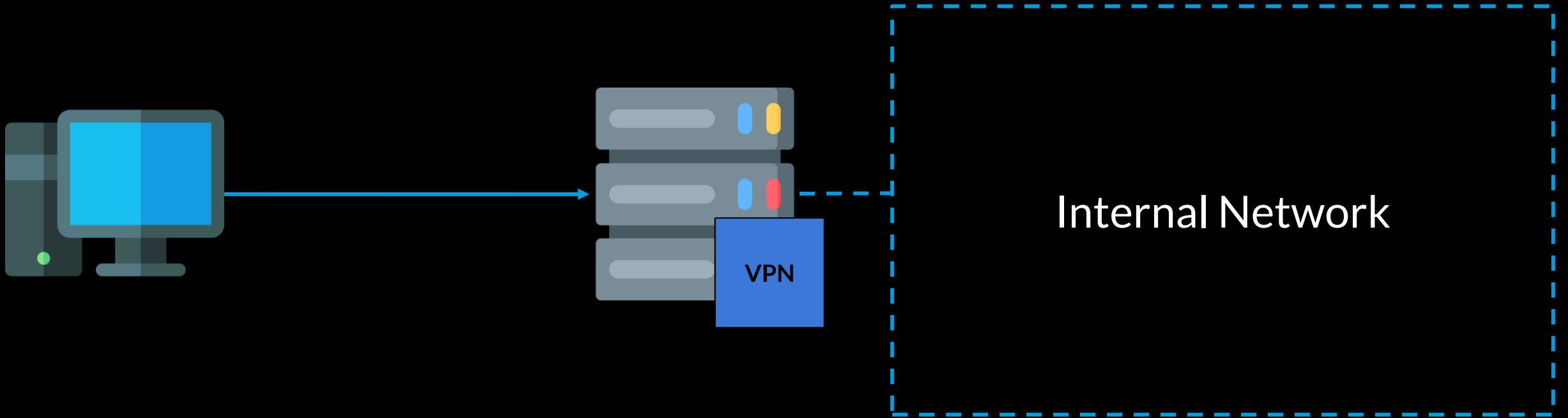


Noam Atias and Sam
Tinklenberg

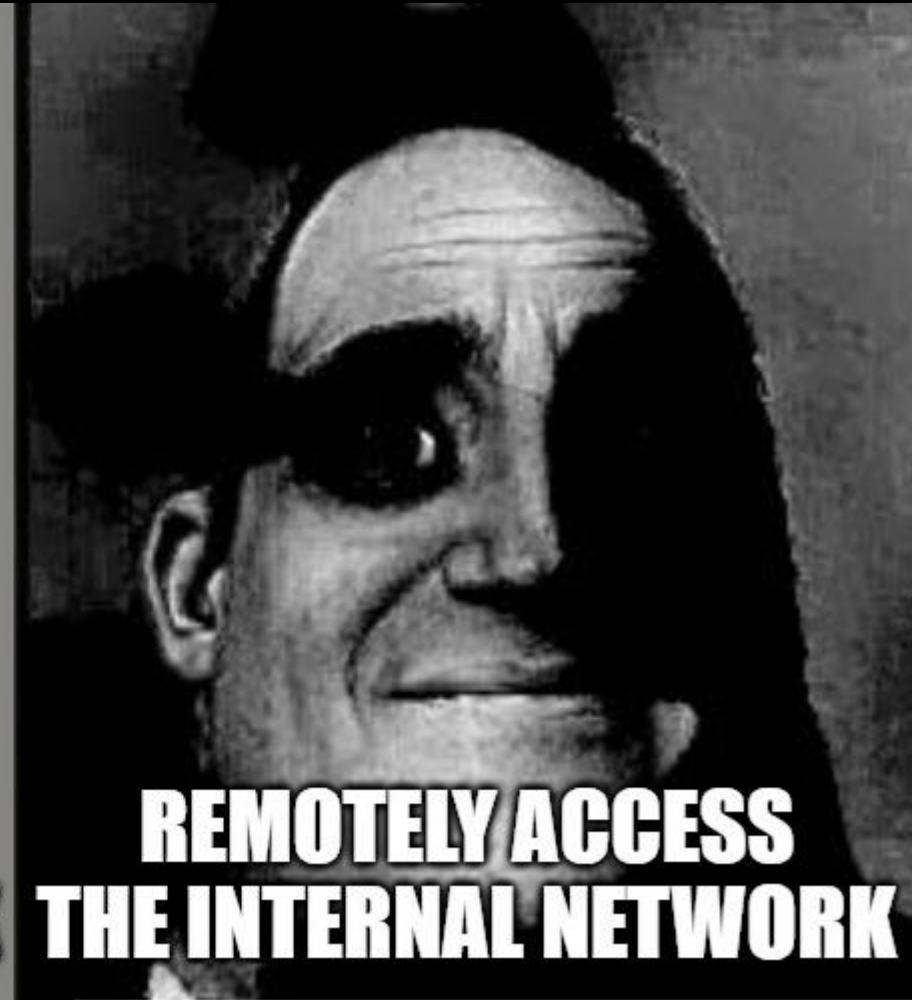
February 21, 2024

Share    

Why VPNs are appealing to attackers?

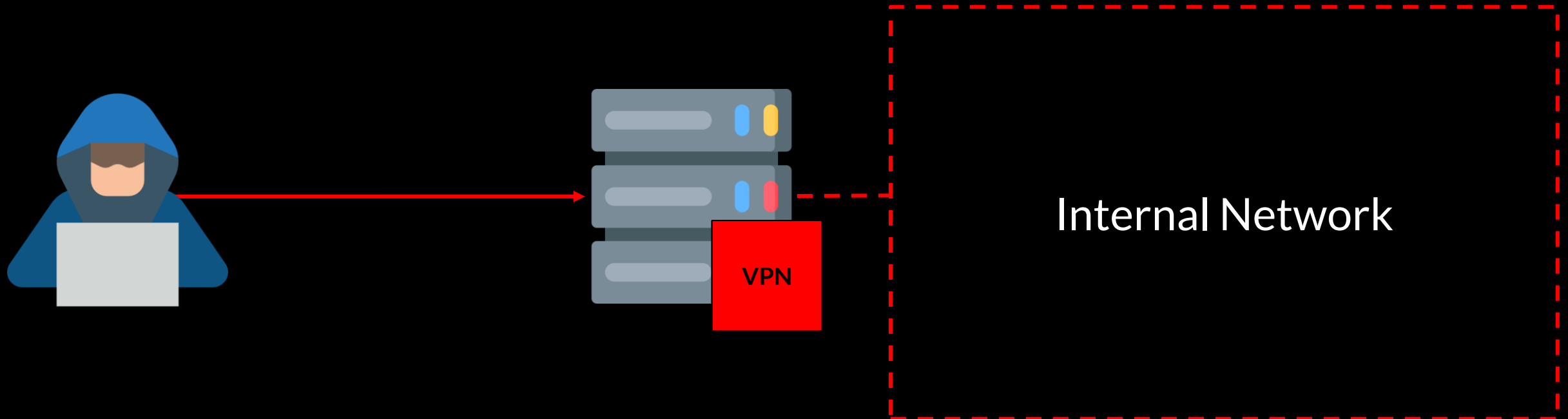


Why VPNs are appealing to attackers?



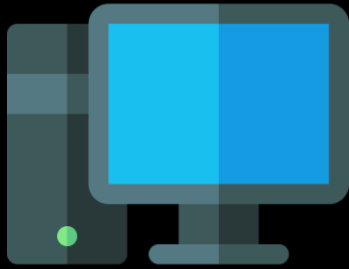
“Classic” VPN exploitation

Abused mainly to gain initial access to the network



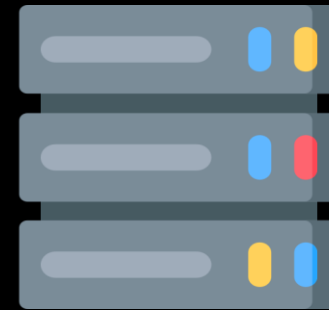
VPN Post-Exploitation?

VPN post-exploitation



Windows

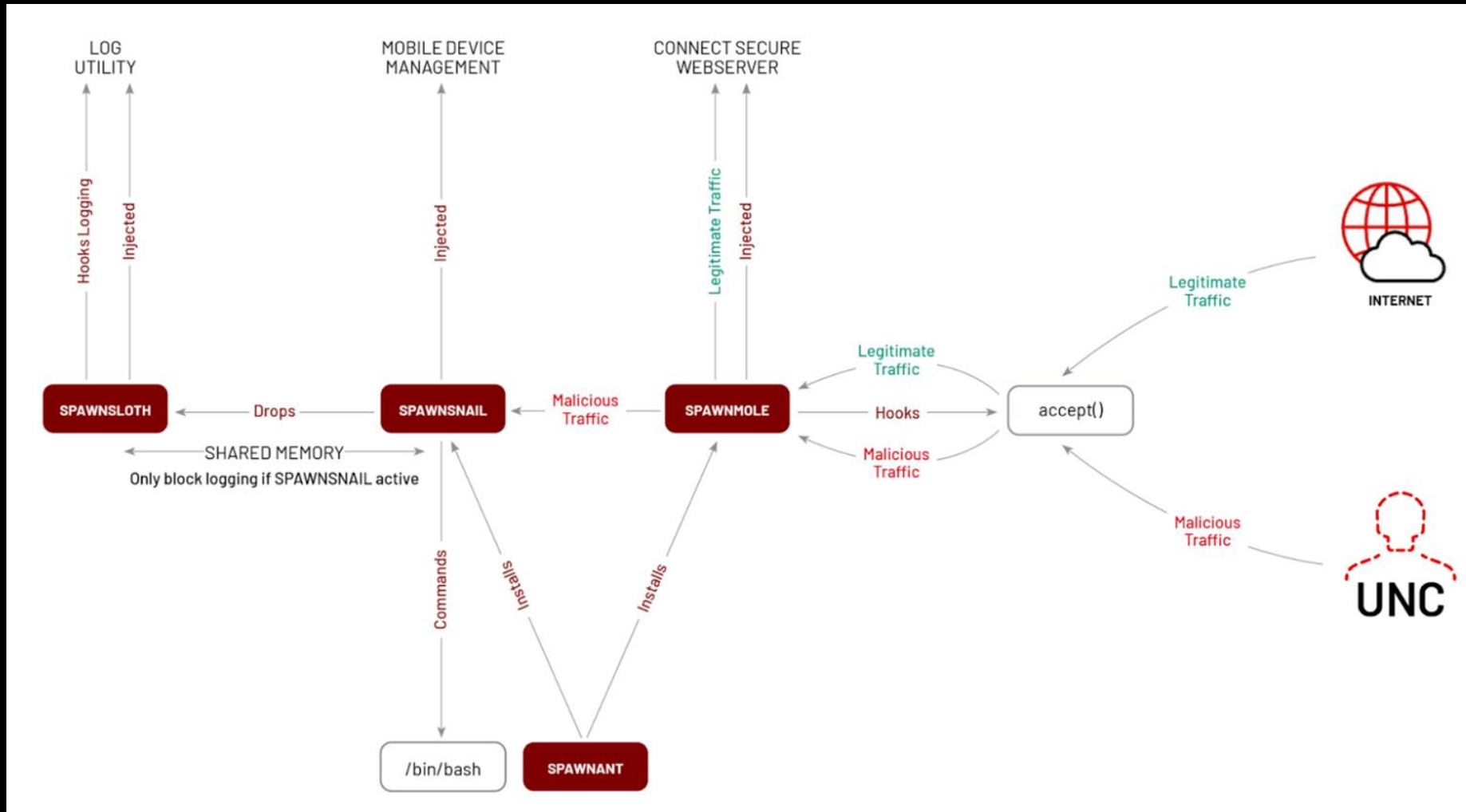
- Persistency
- Credential Access
- ...



VPN

?

Implant based post-exploitation



Implant based post-exploitation

- Run a custom implant on the underlying device OS
- Modify system files or hook functions



Full control over
device functionality

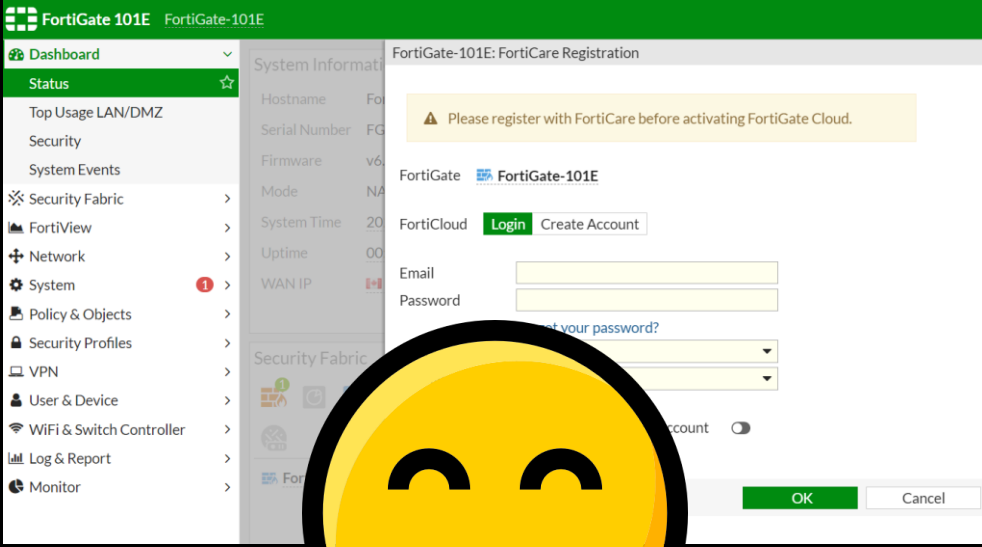


Expensive to develop
and maintain

VPN

Living off the ~~land~~

Living off the VPN

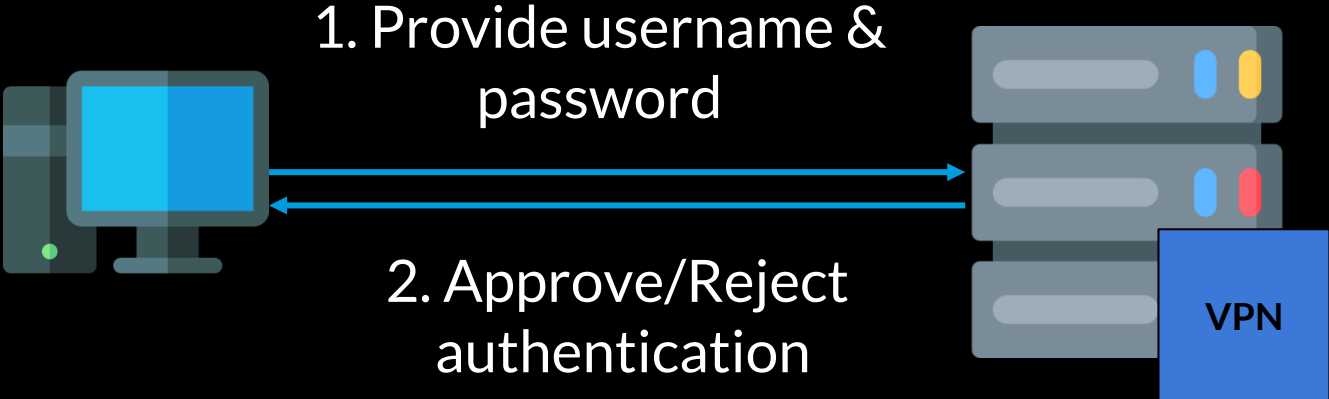


Our test subjects

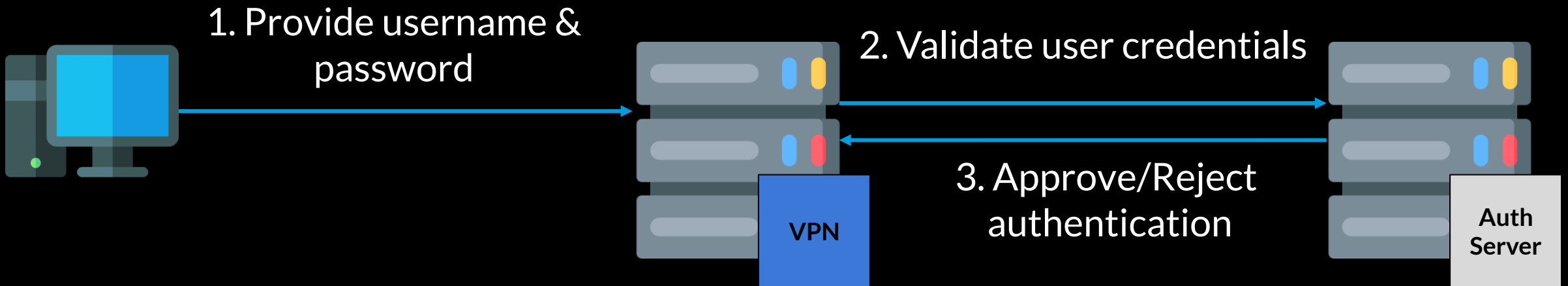


Abusing Remote Authentication Servers

Local user authentication

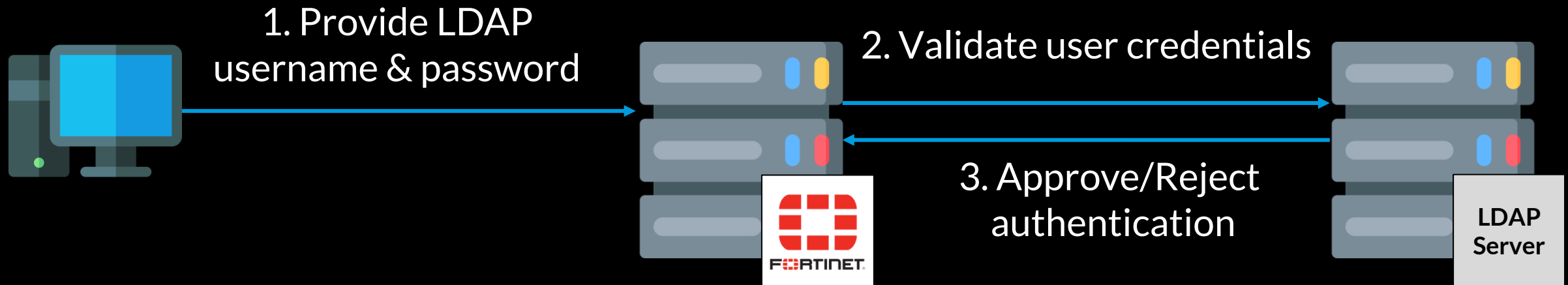


Remote authentication servers



Abusing LDAP Authentication

Fortigate LDAP authentication

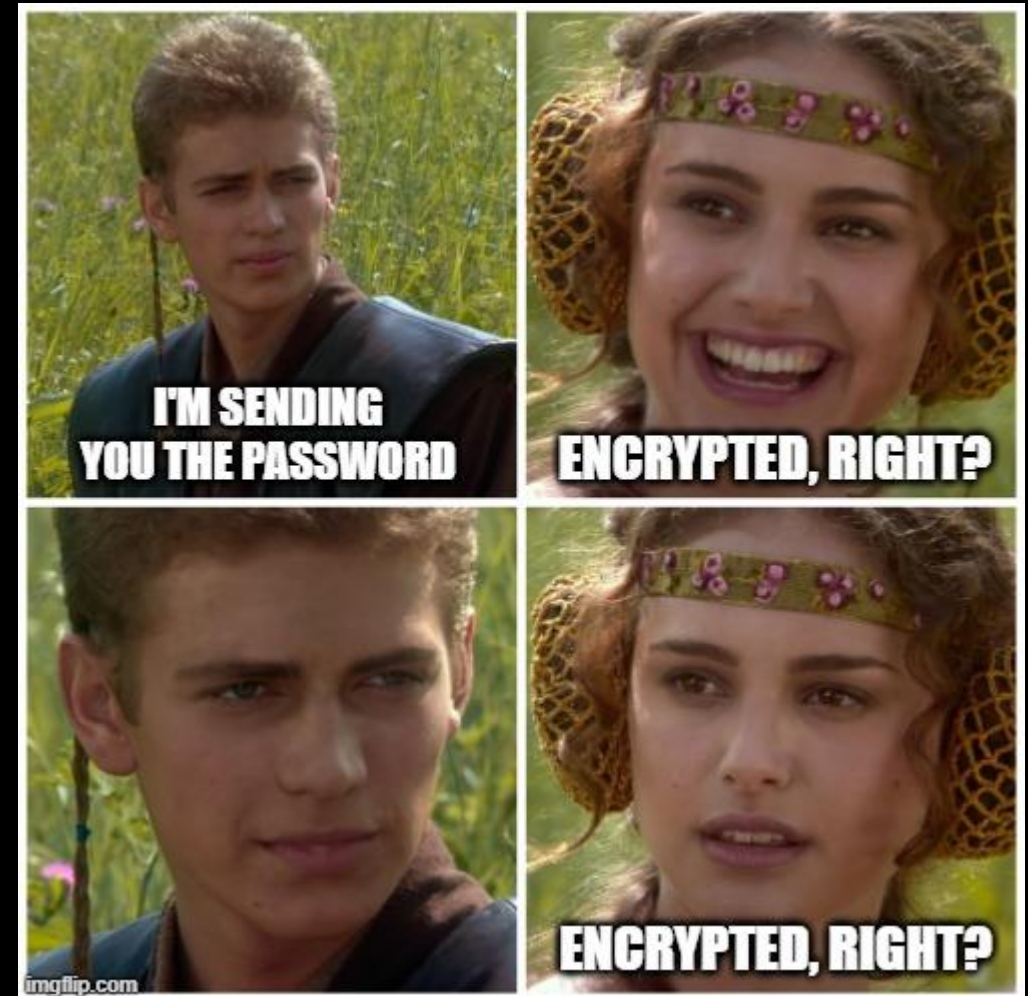


CLEARTEXT LDAP authentication

```
✓ Lightweight Directory Access Protocol
  ✓ LDAPMessage bindRequest(3) "CN=fortigate-ldap,CN=Users,DC=aka,DC=test" simple
    messageID: 3
    ✓ protocolOp: bindRequest (0)
      ✓ bindRequest
        version: 3
        name: CN=fortigate-ldap,CN=Users,DC=aka,DC=test
        ✓ authentication: simple (0)
          simple: abcdefg1234567890!#$
```

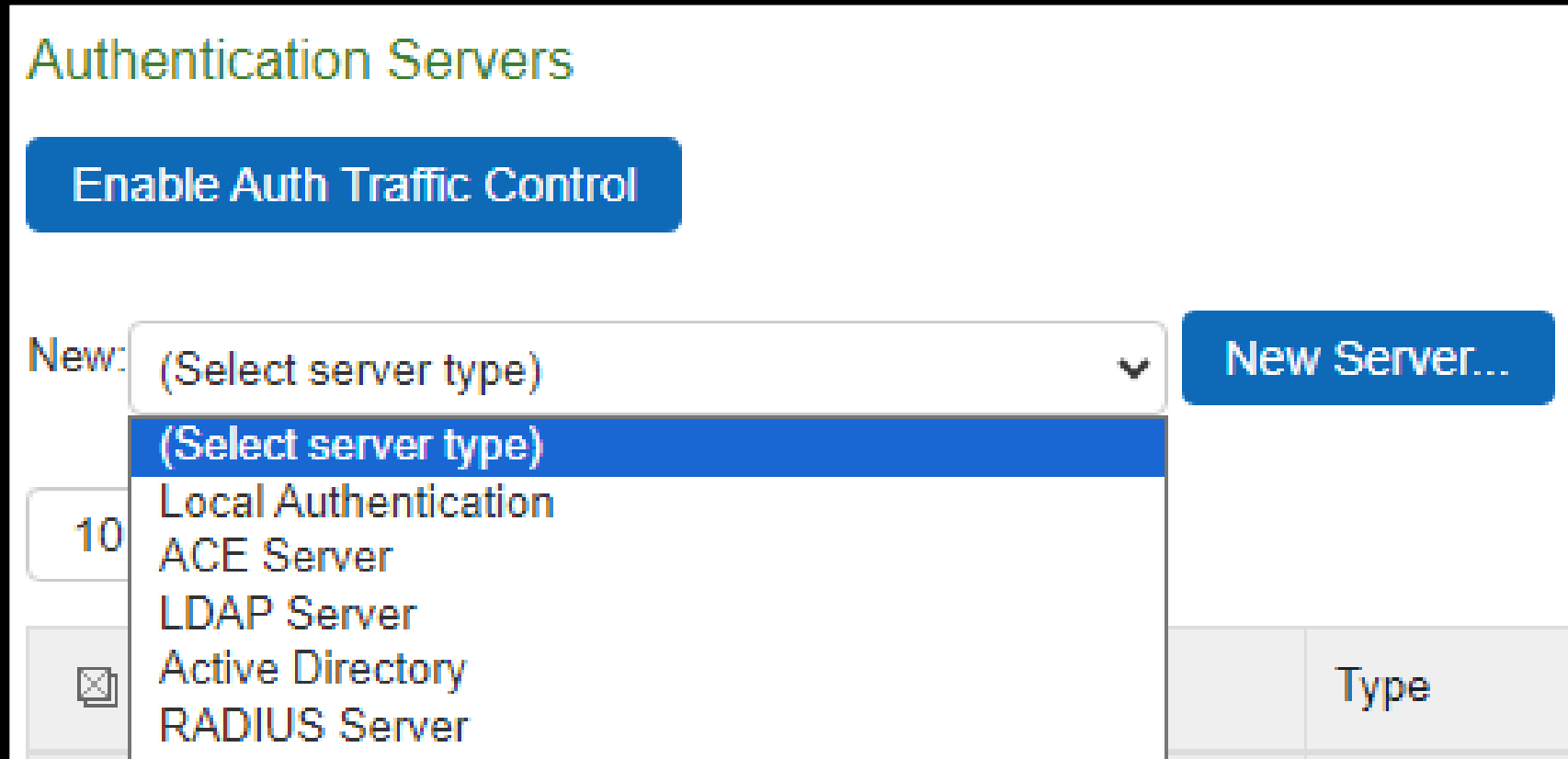
CLEARTEXT LDAP authentication

- Leaks 2 sets of credentials:
 - The configured Fortigate LDAP service account
 - The credentials of the authenticating user
- LDAPS is supported, but not used by default



Ivanti LDAP authentication

- Two types of LDAP authentication servers:
 - LDAP
 - Active Directory



LDAP authentication server

- The default setting uses TLS
- When LDAP is used - a simple bind is performed

```
✓ Lightweight Directory Access Protocol
  ✓ LDAPMessage bindRequest(1) "cn=Administrator,cn=users,dc=aka,dc=test" simple
    messageID: 1
    ✓ protocolOp: bindRequest (0)
      ✓ bindRequest
        version: 3
        name: cn=Administrator,cn=users,dc=aka,dc=test
        ✓ authentication: simple (0)
          simple: P@ssw0rd
```

Active Directory authentication server

Uses Kerberos authentication

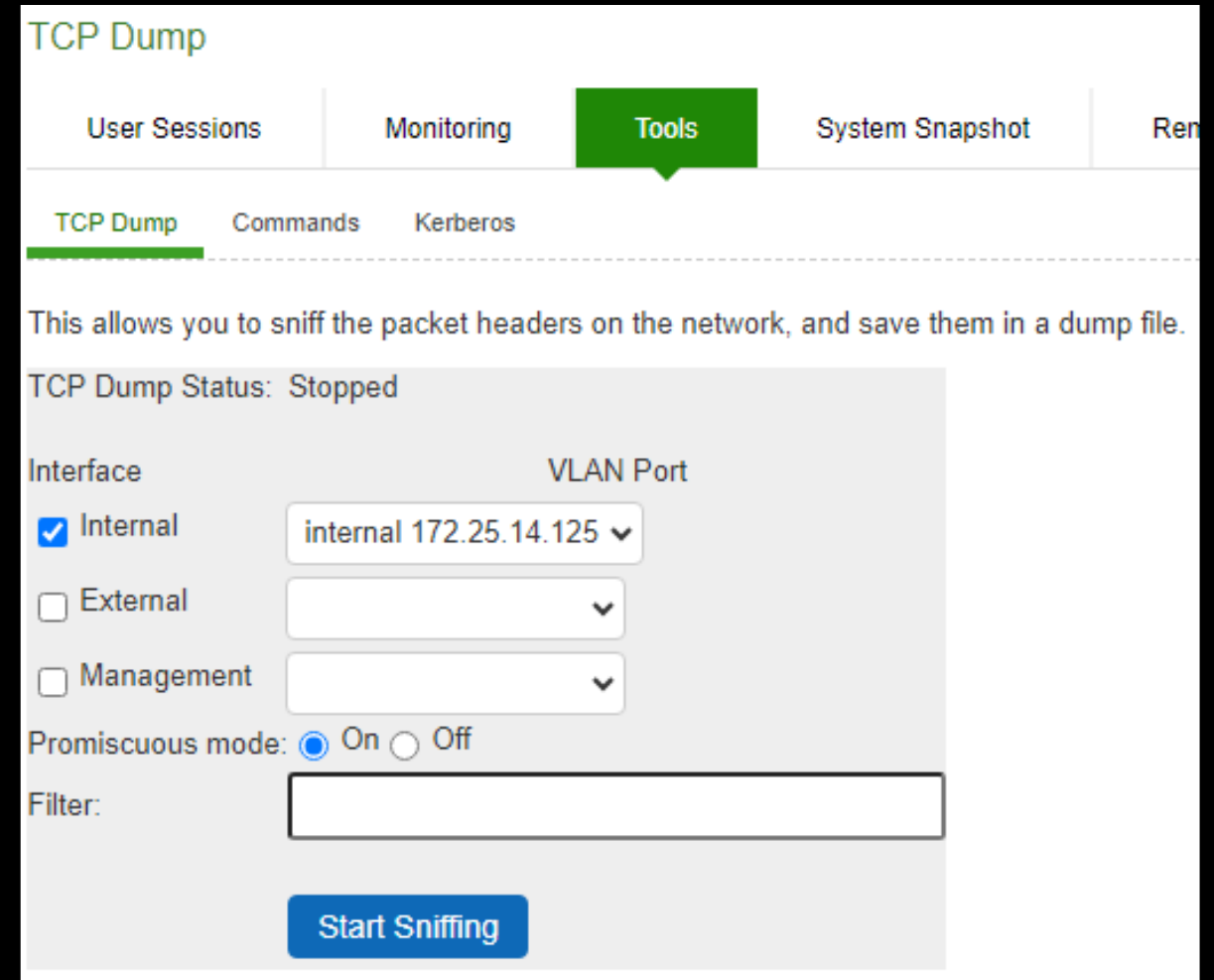
```

v LDAPMessage bindRequest(4) "<ROOT>" sasl
  messageID: 4
  v protocolOp: bindRequest (0)
    v bindRequest
      version: 3
      name:
      v authentication: sasl (3)
        v sasl
          mechanism: GSS-SPNEGO
          credentials: 60820b9806062b0601050502a0820b8c30820b88a018301606092a864882f71201020206...
          v GSS-API Generic Security Service Application Program Interface
            OID: 1.3.6.1.5.5.2 (SPNEGO - Simple Protected Negotiation)
            v Simple Protected Negotiation
              v negTokenInit
                > mechTypes: 2 items
                  mechToken: 60820b6206092a864886f71201020201006e820b5130820b4da003020105a10302010ea2...
                  > krb5_blob: 60820b6206092a864886f71201020201006e820b5130820b4da003020105a10302010ea2...

```


Capturing LDAP credentials

- If LDAPS/Kerberos is used - downgrade to LDAP 🙄
- Use the built in packet capture utility to intercept passwords



The screenshot shows the FortiGate web interface for configuring a TCP Dump. The 'Tools' menu is active, and the 'TCP Dump' sub-menu is selected. The page title is 'TCP Dump'. Below the navigation tabs, there is a description: 'This allows you to sniff the packet headers on the network, and save them in a dump file.' The 'TCP Dump Status' is 'Stopped'. The configuration section includes:

- Interface:** A list of checkboxes for 'Internal', 'External', and 'Management'. 'Internal' is checked.
- VLAN Port:** A dropdown menu for the selected interface, currently showing 'internal 172.25.14.125'.
- Promiscuous mode:** Radio buttons for 'On' (selected) and 'Off'.
- Filter:** An empty text input field.
- Start Sniffing:** A blue button to begin the capture.

LDAP authentication summary

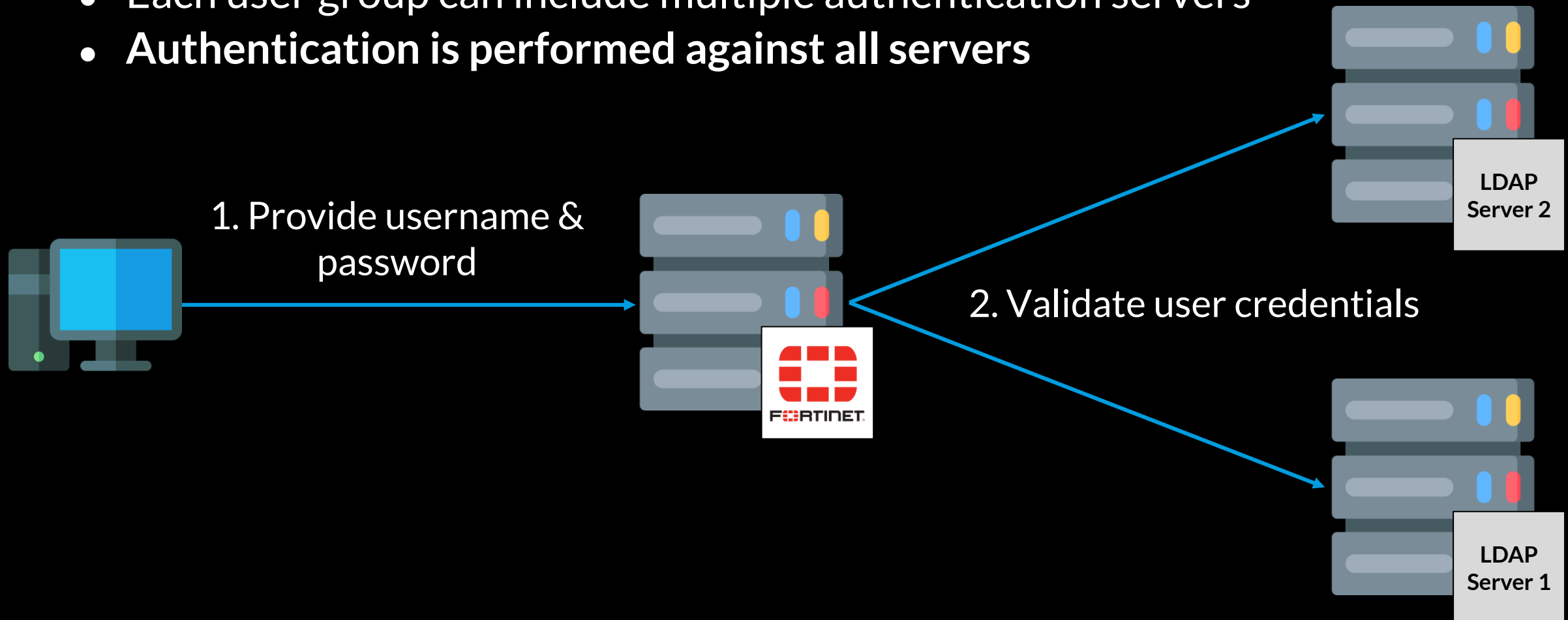
LDAP credentials sent to a compromised VPN can be trivially captured



Abusing Multiple Authentication Servers

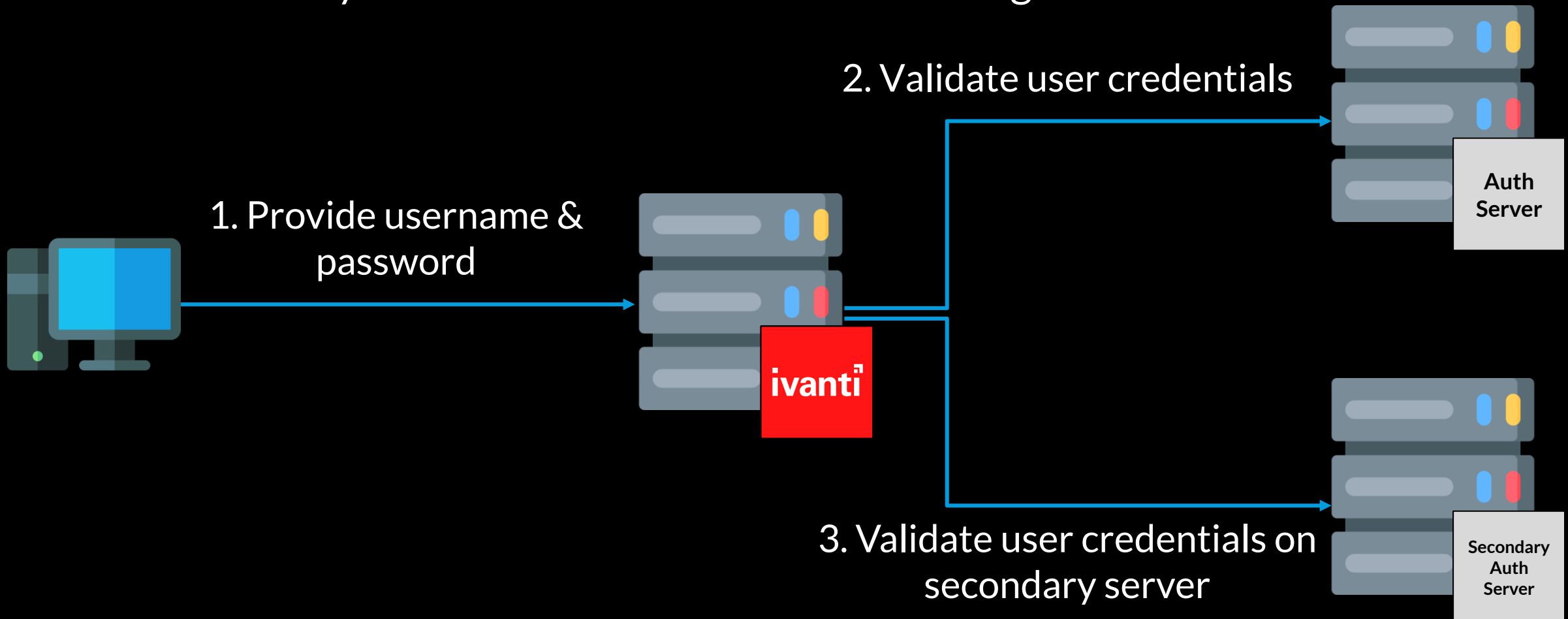
Fortigate multiple authentication servers

- Authentication is managed using user groups
- Each user group can include multiple authentication servers
- **Authentication is performed against all servers**

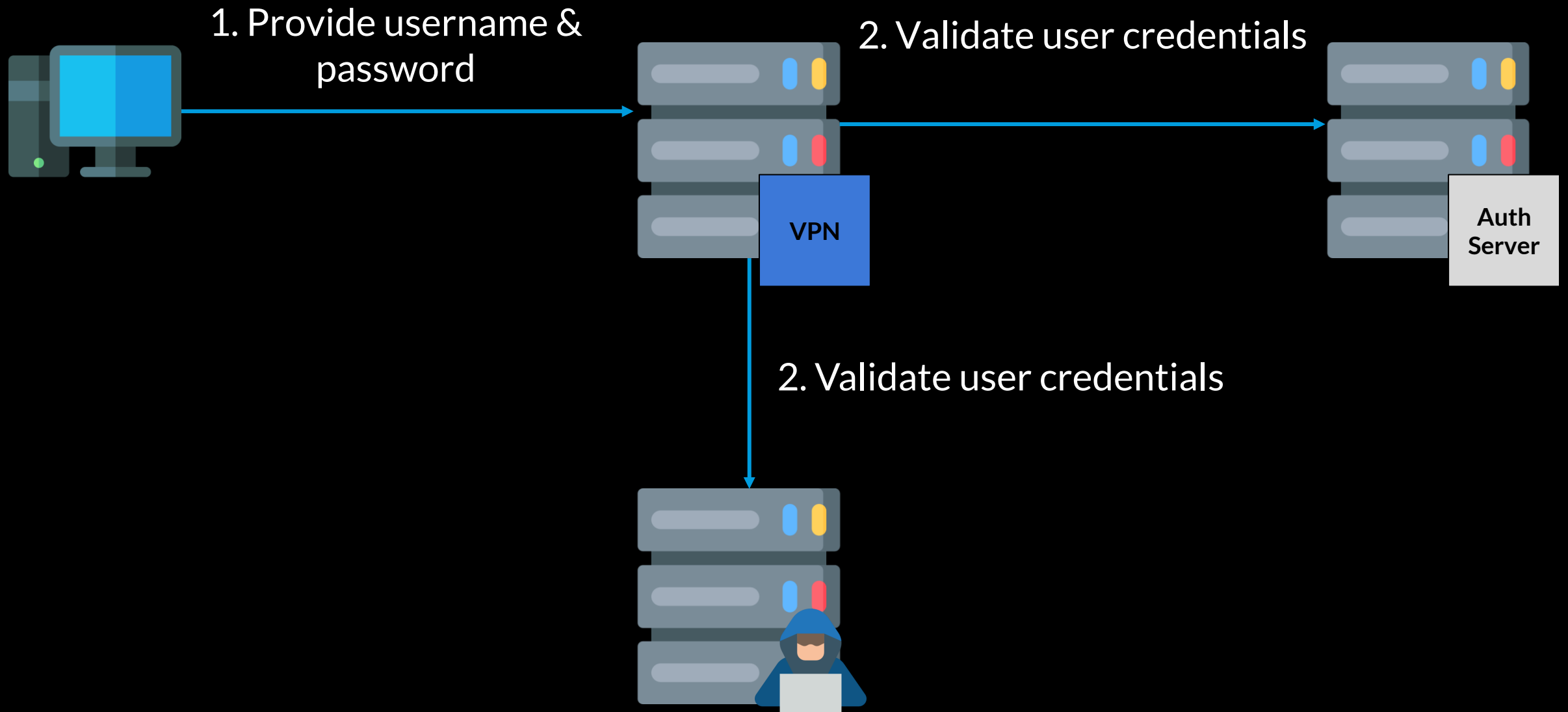


Ivanti multiple authentication servers

- Only one authentication server per group
- A secondary authentication server can be configured



Rogue authentication server



Rogue authentication server summary

- Compromise any credential sent to the VPN
 - Local VPN users
 - Remote LDAP users
 - RADIUS authentication
 - ...

Extracting configuration passwords

Configuration file passwords

- VPNs store a variety of secrets in their configuration
 - Local user passwords
 - SSH Keys
 - **3rd party integration accounts**
- Secrets are stored in an **encrypted** form (not hashed!)

```
user_local:  
  - guest:  
    type: password  
    passwd: ENC BAhcRumOucwyKL1o7WbjHq0LX3qVS1T1UIdn
```

Fortigate password encryption

- Configuration passwords on all Fortigate devices were encrypted using a hard coded key
- And it's not a good one

Decrypting FortiGate passwords (CVE-2019-6693)



Bart Dopheide · [Follow](#)

10 min read · Jan 12, 2020



Fortigate CVE-2019-6693

- Fix - allow users to specify a custom encryption key
- **Disabled by default - same key is still used today**



Bypassing Fortigate custom key

- The custom encryption key feature can be disabled by an admin
- **Reverts password encryption to the default key!**



Ivanti password encryption

How are passwords encrypted?

```
my $adminkey = "[REDACTED]";  
sub getSmbAdminPwdKey {  
    return $adminkey;  
}
```

(Juniper last owned Connect Secure in 2015)

Decrypting Ivanti config passwords

- Same static key is used across all secrets
- Uses AES-based custom encryption routine

AIN'T NOBODY GOT

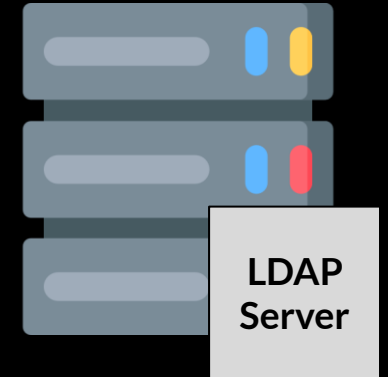
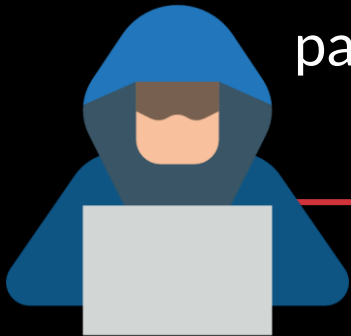
TIME FOR THAT



Decrypting Ivanti config passwords

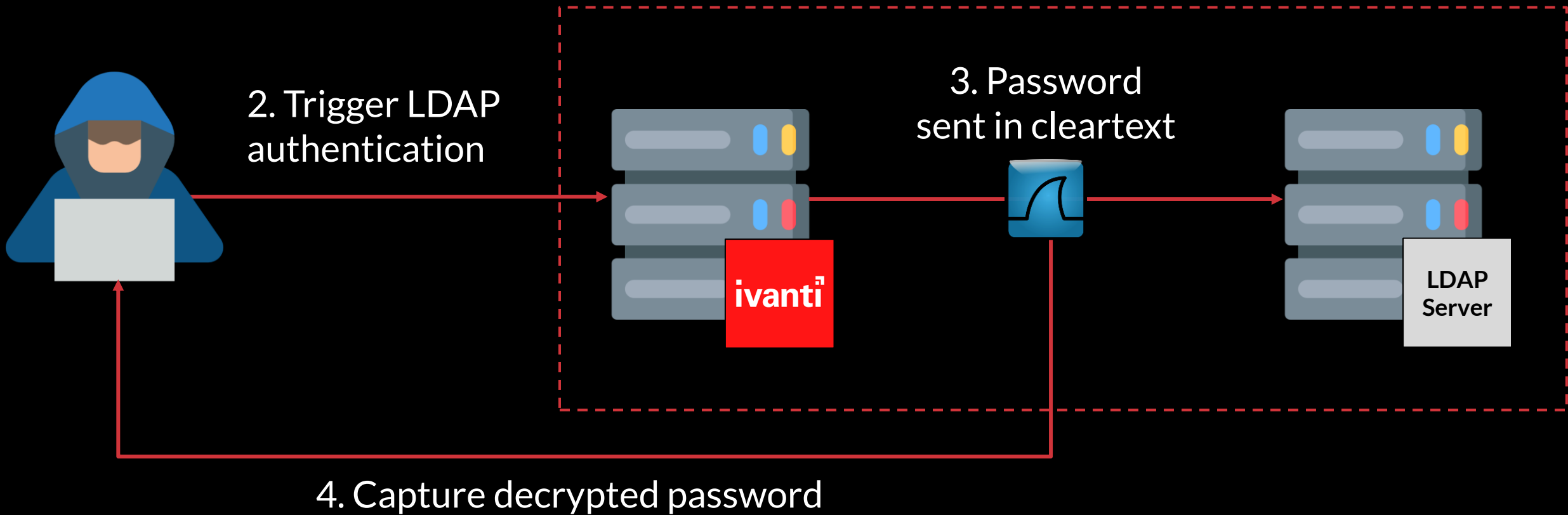
Attacker Lab
Environment

1. Insert encrypted
password into LDAP
config



Decrypting Ivanti config passwords

Attacker Lab Environment



Decrypting Ivanti config passwords

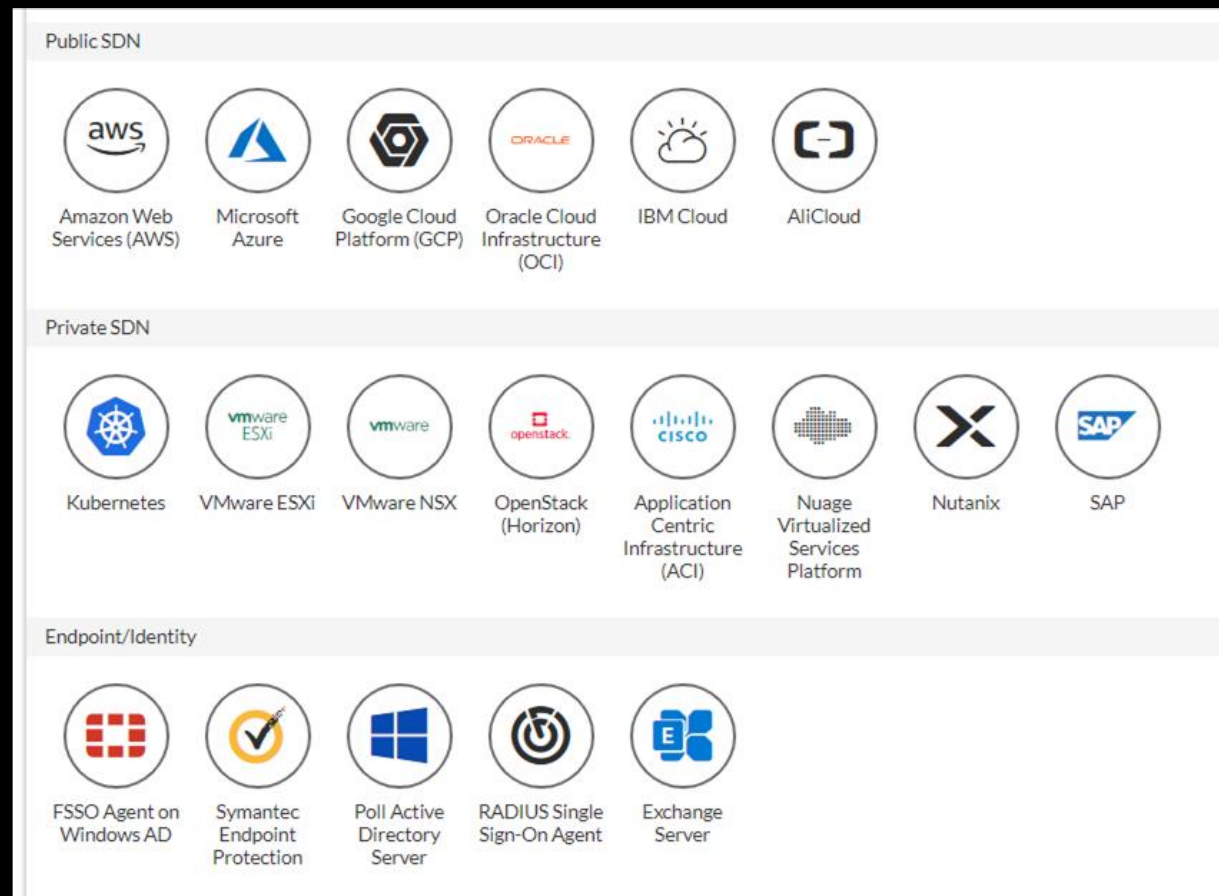
```
Lightweight Directory Access Protocol
  v LDAPMessage bindRequest(2) "admin2" simple
    messageID: 2
    v protocolOp: bindRequest (0)
      v bindRequest
        version: 3
        name: admin2
        v authentication: simple (0)
          simple: 123456
```

Ivanti MDM passwords

```
<name>MDM_SERVER</name>
<mdm>
  <settings>
    <mdm-server-type>airwatch</mdm-server-type>
    <intune-cloudtype>globalService</intune-cloudtype>
    <mi-servertype>miCore</mi-servertype>
    <client-id></client-id>
    <client-secret-encrypted></client-secret-encrypted>
    <server-url>http://www.a.com</server-url>
    <viewer-url></viewer-url>
    <request-timeout>15</request-timeout>
    <username>mdm_admin</username>
    <password-encrypted>[REDACTED]</password-encrypted>
    <password-cleartext>[REDACTED]</password-cleartext>
    <tenant-code>123456</tenant-code>
    <device-identity>require-certificate</device-identity>
    <id-template>&lt;certDN.CN&gt;</id-template>
    <id-type>udid</id-type>
```

Configuration passwords summary

An attacker with control over a VPN can easily obtain any secret from the configuration file



Fortinet's response

- Updated documentation to strongly discourage plain LDAP usage
- Custom encryption key bypass fix (No CVE)

Ivanti's response

- CVE-2024-37374: Static encryption key for configuration secrets
- CVE-2024-37375: MDM passwords saved in cleartext

Lateral Movement Leading to Active Directory Compromise

UNC5330 gained initial access to the victim environment by chaining together CVE-2024-21893 and CVE-2024-21887, a tactic outlined in [Cutting Edge Part 3](#). Shortly after gaining access, UNC5330 leveraged an LDAP bind account configured on the compromised Ivanti Connect Secure appliance to abuse a vulnerable Windows Certificate Template, created a computer object, and requested a certificate for a domain administrator. The threat actor then impersonated the domain administrator to perform subsequent DCSyncs to extract additional credential material to move laterally.

Detection & Mitigation

Detection



Collect and analyze logs



Monitor configuration changes

Mitigation



Limit service account permissions



Use dedicated identities for VPN authentication



Employ Zero Trust Network Access (ZTNA)

Summary

- Threat actors are after your VPN
- A compromised VPN can provide much more than network access
- Do not trust your VPN - assume breach and attempt to minimize the risks



Thank you

Questions?

 @oridavid123