Enterprise VPN Security Guideline

hkpc

HKCERT

Disclaimer

The Hong Kong Computer Emergency Response Team Coordination Centre (HKCERT) and the Hong Kong Productivity Council (HKPC) reserve the right to amend the document from time to time without prior notice.

While we have made every attempt to ensure that the information contained in this document is obtained from reliable sources, HKCERT is not responsible for any errors or omissions, or for the results obtained from the use of this information. All information in this document is provided "as is", with no guarantee of completeness, accuracy, timeliness or of the results obtained from the use of this information, and without warranty of any kind, express or implied, including, but not limited to warranties of performance, merchantability and fitness for a particular purpose.

The information contained in this document is intended to provide general information and for reference only. Reliance or use of this information shall be at the reader's own risk. Nothing herein shall to any extent substitute for the independent investigations and the sound technical and business judgment of the reader. In no event will HKCERT, HKPC or its partners, employees or agents, be liable to you or anyone else for any decision made or action taken in reliance on the information in this document, or for any consequential, special or similar damages, even if advised of the possibility of such damages.

Licence

Table of Contents

Enterprise VPN Security Guideline

The Enterprise VPN is a common technology to support remote working during global pandemic outbreak, however, adopting enterprise VPN without proper risk assessment and corresponding mitigation measures could lead to a security incident. It is common to find that cyber-attacks targeting enterprise VPN appliances, while sensitive information disclosure and reputation damage due to ransomware campaign targeting unpatched VPN devices is one of the examples. To cope with the evolving cyber security risks, secure the enterprise VPN is essential nowadays.

1. Objectives and Scope

This Guideline aims to identify the common security issues in enterprise VPN implementation, provide best practices of related security issues for IT manager and IT staff to address the risks, and suggest corresponding countermeasures.

This guideline organised as a checklist to facilitate readers to adopt and perform self-assessment on the security best practices. It is divided into 3 sections:

(A) Security management and planning
This part describes the security policies, capacity planning, performance tuning and change management for the enterprise VPN, to support business requirements. It is mainly for IT manager.

(B) Security architecture, hardening and access control
This part describes security considerations about the architecture design of the enterprise VPN and preventive measures to reduce attack surfaces through regular maintenance and security control. It is mainly for IT staff.

(C) Security monitoring and incident response
This part describes security logging with proper management to increase network visibility and support incident response. It is mainly for IT staff.

2. Security management and planning

This section is for IT manager.

Common Security Issues	Security Best Practices
1. Lack of knowledge in the rules of using the enterprise VPN. For example: • Purpose of using the VPN • Users of the VPN • How to setup and use • Dos and Don'ts • What should the users take care of • Which devices can be supported	1) Define and enforce the enterprise VPN security policy to support business needs, e.g. a business continuity plan (BCP). ☐ Define a high-level enterprise VPN security policy, which should consist of all information that employees/ users can understand and agree to. The policy should clearly state the purpose of the VPN, the acceptable usage and the

Common Security Issues	Security Best Practices
• Contact point for trouble shooting • What are the users' responsibilities	accountability of VPN users. It should also contain security requirements that can meet the management's expectation on addressing the cyber security risks. e.g. To avoid bringing the virus to the corporate network, the computer must be patched with the latest security update and installed with an anti-virus before connecting to the enterprise VPN. Please refer to the security policy template from SANS if necessary : https://www.sans.org/information-security-policy/ (Select the "Virtual Private Network Policy" or "Remote Access Policy" from the link above to access the policy templates)
2. Insufficient enterprise VPN capacity. For example, • Incapable of supporting all users simultaneously • Some users were unable to connect during peak hours • Slow VPN speed	2) Conduct capacity planning and performance tuning regularly. ☐ Plan in advance by estimating the number of concurrent users that the VPN appliance can support and purchasing additional resources if necessary. Usually, the company should also take future user growth into consideration. ☐ Conduct estimation based on business requirements and historical data, which are viewed as key factors generally speaking. ☐ It is recommended to add 20-30% buffer from the estimated capacity in case of an unexpected surge in demands. Please refer to "Appendix 1" for a scenario example to illustrate this security best practice in details.
3. Urgent deployment/expansion of enterprise VPN without going through a proper change management process, e.g. did not review by stakeholders before taking actions. It introduces risks to the enterprise network.	3) Change management is necessary for enterprise VPN deployment/expansion. ☐ Evaluate of the risk of the change ☐ Craft a phase by phase change plan and process accordingly ☐ Prepare a roll-back plan when an unexpected situation occurs ☐ Test and review after the change

Common Security Issues	Security Best Practices
	Please refer to "Appendix 2" for a scenario example to illustrate this security best practice in details.

3. Security architecture, hardening and access control

This section is for IT staff.

Common Security Issues	Security Best Practices
1. The enterprise VPN architecture design neglects security issues. For example, • Use the existing network zone and IP subnet on the firewall for the enterprise VPN • Leave the enterprise VPN public accessible without proper control, for example, if the management interface of the enterprise VPN is publicly accessible, it may suffer from cyber-attacks • Allow split tunneling, which bypasses enterprise security controls • The enterprise VPN is a single point of failure	1) "Security by design" and "Defense in depth" ☐ Use a dedicated network zone(s) and IP subnet(s) on the firewall for the enterprise VPN to implement a granular access control. ☐ Protect the management interface of the enterprise VPN appliance by the internal firewall and deny any access other than from the internal network. ☐ Use a firewall to protect VPN appliance and setup "Static NAT" (mapping of public IP to private IP) for the VPN service. As the firewall controls the "Static NAT" mapping, the VPN requests must first be checked by the firewall before being routed to the VPN appliance. ☐ Adopt full tunneling to mandate all client traffics to be routed through VPN appliances as much as possible to make sure enterprise security controls are in place. ☐ Adopt fault-tolerant/ high availability design (if applicable). Please refer to "Appendix 3" for a scenario example to illustrate this security best practice in details.
2. Use a default setting for the enterprise VPN without maintenance. For example, • Legacy protocols SSL3.0, DES, RC4 • Running an outdated software/ firmware of the enterprise VPN, the VPN is exposed to vulnerabilities. • Enable unnecessary or unused services/ features	2) Hardening and maintenance ☐ Use secure protocols and crypto algorithms. Note: In general, suggested to use "SSL VPN" and "IPsec VPN" for "client to site" VPN and "site to site" VPN respectively, to strike a balance between the compatibility and security.

• In SSL-VPN, use Portal VPN (Web mode) • Use default service port	Use cases: • "Client to site" VPN: An employee connects to the enterprise network by a notebook computer to access internal documents; • "Site to site" VPN: The branch office connects with the head office to synchronise the sales data. Please refer to "Appendix 4" for the list of secure protocols and crypto algorithms. ☐ Update/ upgrade the software/ firmware of the enterprise VPN to fix the known vulnerabilities and support latest protocols/ features. ☐ Disable unnecessary services in the enterprise VPN appliance. ☐ Use Tunnel VPN (tunnel mode) in SSL-VPN with VPN client software as much as possible to minimise the risk of web related vulnerabilities from Portal VPN (Web mode). ☐ Use non-default port if feasible, e.g. 443 port is a default port for SSL-VPN, use 10443 port instead. Note: Using non-default port may not feasible for some occasions. Some non-default ports are blocked overseas, thus it may cause remote users unable to use the enterprise VPN during travel.
3. Weak or inappropriate access control. For example, • All VPN user can access to all systems and resources of a company through enterprise VPN • There are multiple entrances (IP/URL) to access the enterprise VPN, some entrance has better controls but some are not • All public IP addresses can access the enterprise VPN • Devices with outdated antivirus signatures can connect to the enterprise VPN • Weak password is allowed	3) Access control ☐ Adopt need-to-know access and only grant particular access to the specific users who are required to use such resources to perform their duties. For example, only users from HR team can access the HR system through VPN while access from sales team is forbidden. ☐ Limit the number of the entrance (IP/URL) of the enterprise VPN to make sure access controls are in place. ☐ Only allow certain IP addresses and/or devices to connect the enterprise VPN ☐ Perform compliance check for the endpoint before they can connect to the

• Single factor or password only authentication • No failed login attempts threshold • Local user account is in use. It bypass the centralised identity and access management system • The session of enterprise VPN will not timeout even user has idle for a hour • User can connect to the enterprise VPN anytime	enterprise VPN, e.g. the anti-virus must be installed and updated , and went through vulnerability scanning. Note: Some VPN client softwares or network access control solutions may provide more functions and features on endpoint compliance checking. Please refer to the vendor manual for more information. ☐ Enforce strong password policy (including IT department). ☐ Enforce Two-factor Authentication (2FA). ☐ Set up failed login attempts threshold. ☐ Use LDAP or RADIUS for user authentication to enable account management and control. ☐ Don't allow the user to establish more than one enterprise VPN connection simultaneously. ☐ Configure idle timeout to minimise internal network exposure and preserve the resource, e.g. the VPN session of user will be disconnected automatically after reached 20 minutes idle. ☐ Set up the service period for the enterprise VPN, e.g. general employees can only access the enterprise VPN within office hours.

4. Security monitoring and incident response

This section is for IT staff.

Common Security Issues	**Security Best Practices**
1. Logging for the enterprise VPN is missing or insufficient. For example, • No logging on login attempts to the VPN at a specific point in time • No logging on successful login or failed login • No logging on the network access by the client after connected to the enterprise VPN	1) Enable adequate logging to enforce accountability and facilitate monitoring and incident response. ☐ Log for who (e.g. IP/User account) has tried to connect to the enterprise VPN in a point in time ☐ Log for both successful and failed login attempts ☐ Log for the "next station" where the VPN user tries to visit after connected to the enterprise VPN, e.g. access an internal file server.

2. No periodic log reviewing of the enterprise VPN. For example, • Some users reported that their accounts were locked, which revealed that some overseas IP addresses made unauthorised enterprise VPN login attempts two weeks ago	2) Review the log regularly on abuse, credentials exposure and potential cyber threats. ☐ Set up a VPN log review cycle and review the log regularly, e.g. weekly review.
3. Centralised logging is not available. For example, • Insufficient log retention period due to disk space limitation of the local device • Difficulties in correlating logs with other devices' logs • Lack of trend/ pattern information for analysis	3) Adopt centralised logging ☐ Ensure the capacity of the centralised log server (e.g. disk space, memory, etc.) is sufficient to support the requirements stated in the security policy, e.g. the retention period of logs should be at least 3 months. ☐ Perform log correlation between various devices to enable the visibility of network activities. It is useful when an attacker intrude the network via the VPN successfully, the log correlation could identify what he did on the systems (e.g. accessing the application server, the internal network, and databases, etc). ☐ Create reports for system security statistics and trends, e.g. dashboard.
4. The following symptoms show as an indicator of being targeted by cyber-attacks: <u>Credentials stealing:</u> • Fake account verification website for the enterprise VPN was found from a phishing email <u>Brute-force attacks/ Compromise attempts:</u> • Multiple failed login attempts were made by the same user account/IP • Multiple automated account lock out records for the same user account • Failed login attempts with different user name pattern e.g. peterchan , peter_chan, peter.chan, peterchan@companyname.hk, peter_chan@companyname.hk etc • Login attempts were made in non-office hours (e.g. midnight) • Login attempts were made by oversea IP address but all employees are in Hong Kong	4) Prepared to react on incidents ☐ Prepare the incident response (IR), actions include: • Assign roles for IR, e.g. form a IR team. • Compile an emergency contact list for notification and escalation, e.g. to include vendors and service providers, the senior management, the regulators, the stakeholders and the media etc. • Put necessary tools and resources in a easily accessible location. Tools and resources including documents and network diagram, system change record, notebook computer, tools for analysis and backup recovery. ☐ Response to security incidents efficiently while detailed incident response procedures on common

Malicious scan/ Port scanning: • Received IPsec error logs with unknown destination IP address • Some connection error logs keep generated from the same IP address Post-compromise: • An enterprise VPN account uses local authentication was created. • A VPN user tried to connect some systems that the user should not connect in general	incident types should be ready and drilled regularly. The procedures should include: • Analyse the situation, assess the impact and identify the possible causes. • Notification and escalation • Follow up actions for containment (to stop the bleeding and avoid getting worst, e.g. isolate the affected part), eradication (to remove the threat and strengthen control to avoid recurrence) and recovery (resume the business, test and monitor). • Lesson learn from the incident

5. Conclusion

The enterprise VPN can be a useful tool to enable remote working if the corresponding risks have been addressed. An enterprise should pay attention to the cyber security risk and raise staff awareness on security when they digitalise their work during the global pandemic situation.

6. References

1. NCSC: Advisory: COVID-19 exploited by malicious cyber actors
   https://www.ncsc.gov.uk/news/covid-19-exploited-by-cyber-actors-advisory
2. certnz: Active ransomware campaign leveraging remote access technologies
   https://www.cert.govt.nz/it-specialists/advisories/active-ransomware-campaign-leveraging-remote-access-technologies/
3. SenseCy: GLOBAL RANSOMWARE ATTACKS IN 2020: THE TOP 4 VULNERABILITIES
   https://blog.sensecy.com/2020/08/20/global-ransomware-attacks-in-2020-the-top-4-vulnerabilities/
4. SANS: Security Policy Templates
   https://www.sans.org/information-security-policy/
5. SANS: NewsBites Drilldown for the Week Ending 10 July 2020
   https://www.sans.org/blog/newsbites-drilldown-for-the-week-ending-10-july-2020/
6. SANS: VPN Access and Activity Monitoring
   https://isc.sans.edu/forums/diary/VPN+Access+and+Activity+Monitoring/25906/
7. SANS: What's in Your Change Control Form?
   https://isc.sans.edu/diary/What%27s+in+Your+Change+Control+Form%3F/14563
8. Mozilla : Security/Server Side TLS
   https://wiki.mozilla.org/Security/Server_Side_TLS
9. IPsec VPNs vs. SSL VPNs
   https://www.cloudflare.com/learning/network-layer/ipsec-vs-ssl-vpn/
10. Four Risks to Consider with Expanded VPN Deployments
    https://www.f5.com/labs/articles/cisotociso/four-risks-to-consider-with-expanded-vpn-deployments
11. Cisco: SSL VPN Security

https://tools.cisco.com/security/center/resources/ssl_vpn_security
12. Enterprise VPN Security
https://us-cert.cisa.gov/ncas/alerts/aa20-073a
13. Guide to IPsec VPNs NIST.SP.800-77r1
https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-77r1.pdf
14. Guide to SSL VPNs NIST SP 800-113
https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-113.pdf
15. Incident Response Steps and Frameworks for SANS and NIST
https://cybersecurity.att.com/blogs/security-essentials/incident-response-steps-comparison-guide
16. Computer Security Incident Handling Guide NIST.SP.800-61r2
https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-61r2.pdf

7. Appendix

Appendix 1: Conduct capacity planning and performance tuning regularly

Example: A start-up company has 10 employees, they have added 2 new headcounts every year, and all employees are required to use the enterprise VPN. The Internet service for the enterprise VPN is 100Mbps and the bandwidth utilization is 100% during peak hours. The enterprise VPN appliance is able to support 10 users concurrently (license).

According to historical data above, the estimated capacity for the next 3 years would be an extra 60% plus the buffer 20-30%, i.e. around extra 80-90%.

In this case, we can also understand the performance bottlenecks are the bandwidth and the VPN appliance. Addressing them may directly increase the availability of the enterprise VPN.

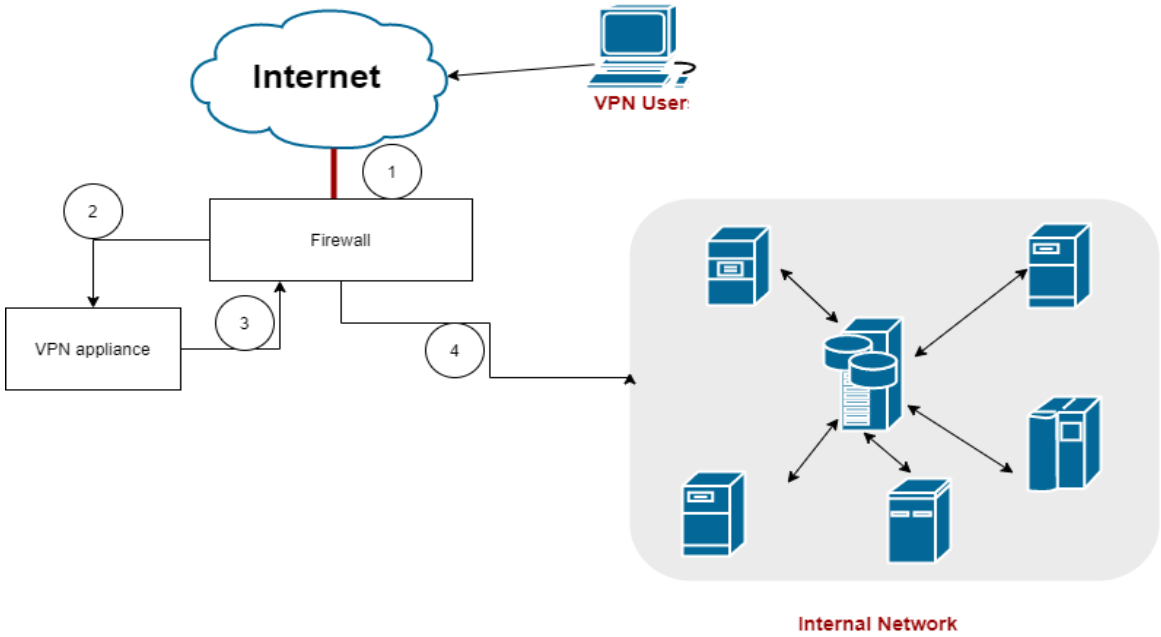
Appendix 2: Change management is necessary for enterprise VPN deployment/expansion

Example:A start-up company is going to expand the capacity of the enterprise VPN. To make sure the change to be performed in an orderly manner, a change plan has been written. It listed out key information, including the procedure of change, the roll-back plan, involved parties, affected services and related information.

The change can be performed after involved parties, including the security team and management, have reviewed and approved the change plan. In case they encountered unexpected behavior during the change, they can still roll-back systematically.

Appendix 3: Security by design and Defense In Depth

This sample design below is illustrating "Defense In Depth": when VPN user want to connect to the VPN, his request must first pass the firewall (first control, **step1**) and then the VPN appliance (second control, **step2**). After successful authentication, in order to access the internal network, the request from user must pass 2 layers of controls as well, the VPN appliance itself (first control, **step3**) and the firewall (second control, **step4**).



{Fig 1 Sample design for the enterprise VPN }

Appendix 4: Hardening and maintenance

SSL VPN	
TLS protocol(s)	**Cipher suites**
TLS 1.3	• TLS_AES_128_GCM_SHA256 • TLS_AES_128_CCM_8_SHA256 • TLS_AES_128_CCM_SHA256 • TLS_AES_256_GCM_SHA384 • TLS_CHACHA20_POLY1305_SHA256
TLS 1.2 and TLS 1.3	• TLS_AES_128_GCM_SHA256 • TLS_AES_256_GCM_SHA384 • TLS_CHACHA20_POLY1305_SHA256 • ECDHE-ECDSA-AES128-GCM-SHA256 • ECDHE-RSA-AES128-GCM-SHA256 • ECDHE-ECDSA-AES256-GCM-SHA384 • ECDHE-RSA-AES256-GCM-SHA384 • ECDHE-ECDSA-CHACHA20-POLY1305 • DHE-RSA-AES128-GCM-SHA256 • DHE-RSA-AES256-GCM-SHA384

IPSec VPN (Minimum recommended settings by NSA)	
ISAKMP/IKE	**IPsec**
• Diffie-Hellman group: 16 • encryption: AES-256 • hash: SHA-384	• encryption: AES-256 • hash: SHA-384 • block cipher mode : CBC

- End -