VPN Job Interview Questions And Answers

Interview Questions Answers

https://interviewquestionsanswers.org/

About Interview Questions Answers

Interview Questions Answers . ORG is an interview preparation guide of thousands of Job Interview Questions And Answers, Job Interviews are always stressful even for job seekers who have gone on countless interviews. The best way to reduce the stress is to be prepared for your job interview. Take the time to review the standard interview questions you will most likely be asked. These interview questions and answers on VPN will help you strengthen your technical skills, prepare for the interviews and quickly revise the concepts.

If you find any **question or answer** is incorrect or incomplete then you can **submit your question or answer** directly with out any registration or login at our website. You just need to visit VPN Interview Questions And Answers to add your answer click on the *Submit Your Answer* links on the website; with each question to post your answer, if you want to ask any question then you will have a link *Submit Your Question*; that's will add your question in VPN category. To ensure quality, each submission is checked by our team, before it becomes live. This VPN Interview preparation PDF was generated at **Wednesday 29th November, 2023**

You can follow us on FaceBook for latest Jobs, Updates and other interviews material.
www.facebook.com/InterviewQuestionsAnswers.Org

Follow us on Twitter for latest Jobs and interview preparation guides.
https://twitter.com/InterviewQA

If you need any further assistance or have queries regarding this document or its material or any of other inquiry, please do not hesitate to contact us.

Best Of Luck.

Interview Questions Answers.ORG Team
https://InterviewQuestionsAnswers.ORG/
Support@InterviewQuestionsAnswers.ORG

VPN Interview Questions And Answers Guide.

Question - 1:

Can you list some items for a VPN checklist from deciding whether to use, then selecting, then deploying, then maintaining VPN?

Ans:

Well, IPSEC - real IPSEC as it exists today - is still morphing, but not so much that one shouldn't require it as a basis for a VPN. So we might have:
* IPSEC compliant (including ISAKMP/Oakley)
* Interoperability with other IPSEC compliant vendors
* Strong encryption, long key length
* If the VPN solution is not part of the firewall, which is fine, will it work with the firewall?
* Does the VPN product work both with and without trust? (Remember, it requires working closely with the firewall.)
* For an "add on" VPN, does it work in conjunction with the firewall, or does it simply circumvent the firewall? (I'm not suggesting one way is good and the other bad, but it may be something the security manager cares about, and the answer should be known.)
* Does the VPN support automatic creation of user-level VPNs (for mobile users)? In a very large organization, the system manager probably would rather not have to manually create VPN accounts for every user.
* Has the VPN been certified by a recognized organization? (The ICSA has a certification and testing process for VPNs. Others probably exist as well.)

View All Answers

Question - 2:

What kind of policies and procedures need to be developed for VPN?

Ans:

If we are imaging an IPSEC world, where eventually the majority of gateways we might connect to supports IPSEC, things become both easy and interesting. If we have a mechanism that can invite encryption use, respond to such invitations, but also talk without encryption if required, we need to think about things such as:
* What risk are we under from eavesdroppers?
* Do we always want to talk encrypted if we can?
* What are the list of sites or networks with whom we must talk encrypted?
* If we cannot talk encrypted to those "must encrypt" sites, what do you want the fall back to be?
* What if we're invited to talk encrypted, but using weak crypto (answer this question both for the general case as well as for the "must encrypt" set of networks)?
* How often do we change session keys?
* Do we need the ability to recover data or keys for encrypted sessions? (I'm arguing that this is almost a 100% "yes" if we were talking about file encryption, but almost 100% "no" for network communications.)
* Are we going to have the encryption be certificate-based? Who do we trust to be a Certification Authority?
* Will we allow encryption through the firewall or only up to the firewall?
* How do we protect the keys? Who has access to the keys?

View All Answers

Question - 3:

What are unreasonable expectations for VPN?

Ans:

With firewalls, we went from a very small number of security-wise companies using real firewalls to firewalls becoming a "must have" on a checklist. But somehow, having a firewall became synonymous with "all my Internet security problems are solved!" VPNs and IPSEC have started off that way too. There has been a lot of "When we have IPSEC on the desk top we won't need firewalls." This is nonsense. VPNs cannot enforce security policies, they cannot detect misuse or mistakes, and they cannot regulate access. VPNs can do what they were meant to do: keep communications private.

View All Answers

Question - 4:

What are reasonable expectations for a VPN?

Ans:

Privacy from end to end. The cryptography used, generally speaking, is very good. Whatever you do, that is encrypted, is very well hidden from sniffers on the net. Whatever is not encrypted, you may as well shout from the rooftops or post on your web page.

View All Answers

Question - 5:

What kind of resources (staff, computational muscle, bandwidth, etc.) are required for VPN deployment, usage, maintenance?

Ans:

VPNs are typically handled as just another job by the network or system administrator staff. Whoever is managing the firewall today can easily add VPN management to the plate because once a VPN is set up there is little else to do on most implementations.

View All Answers

Question - 6:

What firewall issues are relevant to VPN selection and deployment?

Ans:

Well, the perimeter security issues mentioned above, plus a firewall should give the option of VPN with or without trust. For example, I would prefer all sessions between my firewall and my clients and business partners to be encrypted - to be VPNs. But, I want all of them to run up against my firewall if they try to do anything besides what I permit. On the other hand, if I dial in from the speaker's lounge at a conference, I would like a private connection (that is to say, encrypted) that also looks and feels like a virtual "inside" connection, just as if I was sitting in the office.

View All Answers

Question - 7:

What is the relationship between VPN and firewalls?

Ans:

While VPNs were available before firewalls via encrypting modems and routers, they came into common use running on or with firewalls. Today, most people would expect a firewall vendor to offer a VPN option. (Even though most people today don't use VPNs.) Also, they want it managed via the same firewall management interface. But then, users today seem to want nearly everything on the firewall: mail server, name server, proxy servers for HTTP, FTP server, directory server, and so on. That's terrible and a subject in itself.

View All Answers

Question - 8:

Are there applications or environments in which VPNs would really be detrimental?

Ans:

Only the things you want everyone to be able to eavesdrop on. In general, the answer is "no," but if a VPN is in use from a system behind a firewall to a system outside the firewall, the firewall cannot enforce an organization's security policy beyond connection rules.

View All Answers

Question - 9:

Are VPNs used for specific kinds of applications or environments? If so, what are some examples of where and why VPNs would be deployed?

Ans:

VPNs should be used for all information exchange. I don't want to have to "go encrypted" when something secret is about to be sent. I want everything to be encrypted. It should be as commonplace as people sending postal mail in sealed envelopes. It will also ensure that the VPN mechanism is working.

View All Answers

Question - 10:

What crypto issues are relevant in the VPN context?

Ans:

Businesses who understand the use of crypto for privacy in electronic documents also understand the need for the emergency recovery of that data. Whether this is done by saving an individual's private key information, encrypting it with a trusted third party's key, or saving all keys used to encrypt all documents, it is well understood that some mechanism is needed for the recovery of encrypted files owned by an individual, by the individual, or a company, by the company for business or law enforcement reasons. Key recovery of session keys used to encrypt a network connection is a requirement of law enforcement. VPNs must use the strongest crypto available and feasible given the hardware on which it is being run. Weak cryptography (for example, 40 bit key length) should be completely avoided.

View All Answers

Question - 11:

What kind of performance issues does VPN raise?

Ans:

Encryption takes more horsepower than sending data in the clear. It really shows up on mobile PCs transmitting large hunks of data - for example, a PowerPoint presentation - over a dial-up phone line. Firewalls and other server systems should employ hardware crypto engines. With these there are no performance issues. I expect that this functionality for mobile PCs will migrate to PC cards with crypto engines. When will this happen? Within the next 18 months.

View All Answers

Question - 12:

Who are the major players in the market?

Ans:

Aventail is a leader in this market. All the major firewall vendors and router vendors are in it as well. On the client side, Timestep and V-ONE are big.

View All Answers

Question - 13:

What are some of the tough questions to pose to VPN product vendors?

Ans:

Many vendors claim to be IPSEC-compliant. The real requirement should be "list the other products with which you can communicate" Also, a customer should want to know how automatic the key exchange mechanism is? In a perfect world - in an IPSEC world - it would be automatic. If a Virtual Network Perimeter (VNP, not VPN) is used, how easy is it to deploy the software to mobile PC users? How much does it interfere with normal network operation from a mobile PC, if at all? What crypto algorithms are used? What key length?

View All Answers

Question - 14:

What security vulnerabilities are unique to or heightened by VPN?

Ans:

Even though VPNs provide ubiquitous, perimeter security, firewalls are still needed. Walls around cities went away because it became inexpensive to bring them in closer to individual homes. Only a perimeter enforcement mechanism can guarantee adherence to an organization's security policies. However, as part of policy enforcement, a firewall might need to be able to look at the information in a packet. Encryption makes that rather difficult. VPNs - improperly deployed - take away a firewall's ability to audit useful information, or to make decisions beyond the level of "who is allowed to talk to whom." There are ways around this. The easiest way is to make the firewall a trusted third member of the conversation. People who value privacy above everything else chafe at this. But people who value the security of their organization realize that this is a necessity.

View All Answers

Question - 15:

What security vulnerabilities are addressed by VPN?

Ans:

VPNs directly protect the privacy of a communication, and indirectly provide an authentication mechanism for a gateway, site, computer, or individual. Whether you need privacy or not is a function of your business, the nature of what you discuss electronically, and how much it is worth to someone else. Authentication is a side effect, even without IPSEC, because if site A knows it talks to site B over an encrypted channel, and someone else pretends to be site B, they will also have to be able to talk encrypted to site A, since site A expects it and will reciprocate. Typically, the secrets are sufficiently protected that no one could pretend to be site B and pull it off. Again, it comes down to the risk, which is a function of the information you are transmitting. The threats and vulnerabilities are there, in any case. It is very easy to capture traffic on the Internet or on your phone line. Is it important enough information to care? That is the question that most people answer wrong. It is my experience that while people may understand the value of what they have and they may understand the risk of losing or compromising what they have, few understand both at the same time.

View All Answers

Question - 16:

Is VPN a long-term solution or a short-term stop gap kind of thing?

Ans:

VPNs are long-term solutions. VPNs may become ubiquitous and transparent to the user, but they will not go away. Because the problem VPNs address - privacy over a public network - will not go away. VPNs will exist from the desktop to the server, and at the IP packet level as well as the application data level.

View All Answers

Question - 17:

Is there market penetration for these products?

Ans:

Those companies who were early adopters of firewalls are the ones using VPNs today. VPNs are still early in the use cycle. Three years ago, they hardly existed. Then firewall products started to include them - first ANS Interlock, then TIS Gauntlet. Soon, customers started demanding VPN functionality in their firewalls, even though few of them actually used it. But the Security Architecture for Internet Protocol (IPSEC) standard is changing that - with IPSEC-compliant off-the-shelf products, using encryption to protect the privacy of communications will be an automatic decision. It may take awhile. I predicted that 1998 would be the "Year of the VPN," but maybe 1999 is more realistic. Look, over four years after the famous Internet password sniffing incident, most people still seem to be working with reusable passwords.

View All Answers

Question - 18:

What is a Virtual Private Network (VPN)?

Ans:

The term Virtual Private Network (VPN) means "an encrypted connection from one point to another over any network giving the illusion of being a private network." Originally, Marcus Ranum and I coined the term "virtual network perimeter," which in today's language means a VPN with trust - i.e., a network security perimeter extended to include other offices and remote users through a VPN link plus common name space, security policies, and management. Of course, networks are not private unless encryption is being employed. To put it plainly, unless you own the space around every wire, fiber, or radio signal used in the communication path, your connection is not private unless it is encrypted.

View All Answers

Networking Most Popular & Related Interview Guides

1 : **CCNA Interview Questions and Answers.**

2 : MCSE Interview Questions and Answers.

3 : MCSA Interview Questions and Answers.

4 : CCNP Interview Questions and Answers.

5 : Network Administrator Interview Questions and Answers.

6 : Active Directory Interview Questions and Answers.

7 : CCNA Security Interview Questions and Answers.

8 : Basic Networking Interview Questions and Answers.

9 : System Administration Interview Questions and Answers.

10 : VoIP Interview Questions and Answers.

Follow us on FaceBook
www.facebook.com/InterviewQuestionsAnswers.Org

Follow us on Twitter
https://twitter.com/InterviewQA

For any inquiry please do not hesitate to contact us.

Interview Questions Answers.ORG Team
https://InterviewQuestionsAnswers.ORG/
support@InterviewQuestionsAnswers.ORG