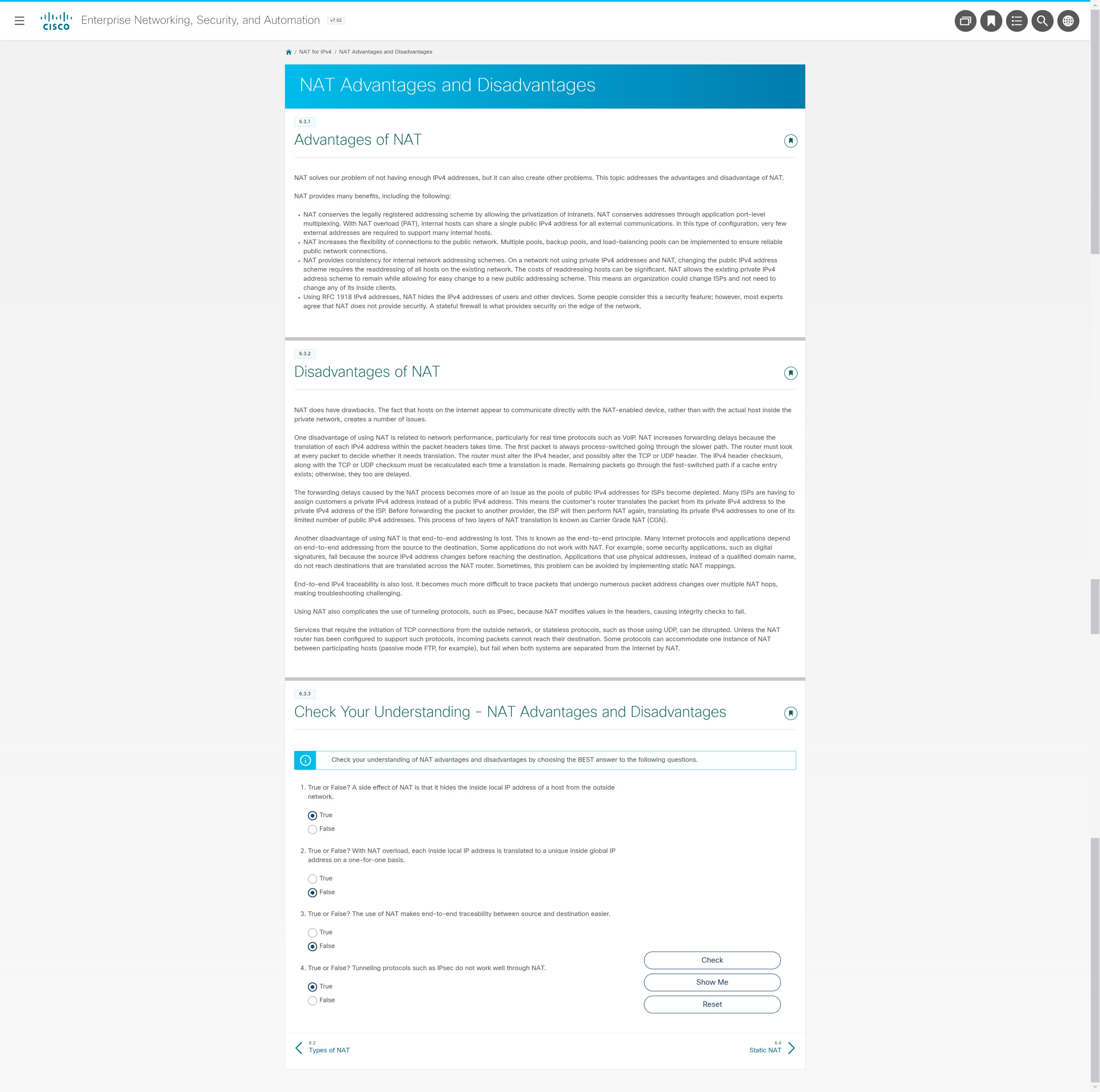

NAT Advantages and Disadvantages

6.3.1

Advantages of NAT

NAT solves our problem of not having enough IPv4 addresses, but it can also create other problems. This topic addresses the advantages and disadvantage of NAT.

NAT provides many benefits, including the following:

- NAT conserves the legally registered addressing scheme by allowing the privatization of intranets. NAT conserves addresses through application port-level multiplexing. With NAT overload (PAT), internal hosts can share a single public IPv4 address for all external communications. In this type of configuration, very few external addresses are required to support many internal hosts.
- NAT increases the flexibility of connections to the public network. Multiple pools, backup pools, and load-balancing pools can be implemented to ensure reliable public network connections.
- NAT provides consistency for internal network addressing schemes. On a network not using private IPv4 addresses and NAT, changing the public IPv4 address scheme requires the readdressing of all hosts on the existing network. The costs of readdressing hosts can be significant. NAT allows the existing private IPv4 address scheme to remain while allowing for easy change to a new public addressing scheme. This means an organization could change ISPs and not need to change any of its inside clients.
- Using RFC 1918 IPv4 addresses, NAT hides the IPv4 addresses of users and other devices. Some people consider this a security feature; however, most experts agree that NAT does not provide security. A stateful firewall is what provides security on the edge of the network.

6.3.2

Disadvantages of NAT

NAT does have drawbacks. The fact that hosts on the internet appear to communicate directly with the NAT-enabled device, rather than with the actual host inside the private network, creates a number of issues.

One disadvantage of using NAT is related to network performance, particularly for real time protocols such as VoIP. NAT increases forwarding delays because the translation of each IPv4 address within the packet headers takes time. The first packet is always process-switched going through the slower path. The router must look at every packet to decide whether it needs translation. The router must alter the IPv4 header, and possibly alter the TCP or UDP header. The IPv4 header checksum, along with the TCP or UDP checksum must be recalculated each time a translation is made. Remaining packets go through the fast-switched path if a cache entry exists; otherwise, they too are delayed.

The forwarding delays caused by the NAT process becomes more of an issue as the pools of public IPv4 addresses for ISPs become depleted. Many ISPs are having to assign customers a private IPv4 address instead of a public IPv4 address. This means the customer's router translates the packet from its private IPv4 address to the private IPv4 address of the ISP. Before forwarding the packet to another provider, the ISP will then perform NAT again, translating its private IPv4 addresses to one of its limited number of public IPv4 addresses. This process of two layers of NAT translation is known as Carrier Grade NAT (CGN).

Another disadvantage of using NAT is that end-to-end addressing is lost. This is known as the end-to-end principle. Many internet protocols and applications depend on end-to-end addressing from the source to the destination. Some applications do not work with NAT. For example, some security applications, such as digital signatures, fail because the source IPv4 address changes before reaching the destination. Applications that use physical addresses, instead of a qualified domain name, do not reach destinations that are translated across the NAT router. Sometimes, this problem can be avoided by implementing static NAT mappings.

End-to-end IPv4 traceability is also lost. It becomes much more difficult to trace packets that undergo numerous packet address changes over multiple NAT hops, making troubleshooting challenging.

Using NAT also complicates the use of tunneling protocols, such as IPsec, because NAT modifies values in the headers, causing integrity checks to fail.

Services that require the initiation of TCP connections from the outside network, or stateless protocols, such as those using UDP, can be disrupted. Unless the NAT router has been configured to support such protocols, incoming packets cannot reach their destination. Some protocols can accommodate one instance of NAT between participating hosts (passive mode FTP, for example), but fail when both systems are separated from the internet by NAT.

6.3.3

Check Your Understanding - NAT Advantages and Disadvantages

Check your understanding of NAT advantages and disadvantages by choosing the BEST answer to the following questions.

1. True or False? A side effect of NAT is that it hides the inside local IP address of a host from the outside network.

   ● True
   ○ False

2. True or False? With NAT overload, each inside local IP address is translated to a unique inside global IP address on a one-for-one basis.

   ○ True
   ● False

3. True or False? The use of NAT makes end-to-end traceability between source and destination easier.

   ○ True
   ● False

4. True or False? Tunneling protocols such as IPsec do not work well through NAT.

   ● True
   ○ False

Check

Show Me

Reset