Häufig gestellte Fragen zum Router

Ziel

In diesem Dokument werden allgemeine Fragen zu den Funktionen eines Cisco Routers sowie zu deren Verwendung und Verwendung beantwortet. Wenn Sie an Videoinhalten interessiert sind, sehen Sie sich unsere Video-Playlist an, indem Sie hier klicken.

Anwendbare Geräte

- Serie RV100
- Serie RV200
- Serie RV300

Inhaltsverzeichnis

1. Was sind Zugriffsregeln?

Zugriffskontrollregeln sind Regeln, die festlegen, dass bestimmter Datenverkehr von bestimmten Benutzern in einem Netzwerk an diese gesendet wird. Zugriffsregeln können so konfiguriert werden, dass sie jederzeit gültig sind oder auf einem definierten Zeitplan basieren. Während eine Zugriffsregel auf einem Router oder Switch konfiguriert werden kann, wird sie anhand verschiedener Kriterien konfiguriert, um den Zugriff auf einige oder alle Ressourcen im Netzwerk zuzulassen oder zu verweigern.

2. Welche Optionen sind für TFTP-Server 66, 67 und 150 verfügbar?

Ein TFTP-Server ermöglicht dem Administrator, Konfigurationsdateien für Geräte in einem Netzwerk zu speichern, abzurufen und herunterzuladen. Ein Dynamic Host Configuration Protocol (DHCP)-Server leitet IP-Adressen an Geräte im Netzwerk weiter. Wenn ein Gerät hochgefahren wird und keine IPv4- oder IPv6-Adresse und IP-Adresse des TFTP-Servers vorkonfiguriert sind, sendet das Gerät eine Anfrage an den DHCP-Server mit den Optionen 66, 67 und 150. Diese Optionen sind Anfragen an den DHCP-Server, um Informationen über den TFTP-Server abzurufen.

- Die DHCP-Option 150 ist eine proprietäre Option von Cisco. Es stellt die IP-Adressen in einer Liste von TFTP-Servern bereit. Das IEEE-Standard-Äquivalent (Institute of Electrical and Electronics Engineers) ist Option 66.
- Die DHCP-Option 66 gibt die IP-Adresse oder den Hostnamen eines einzelnen TFTP-Servers an.
- Die DHCP-Option 67 stellt den Namen der Boot-Datei für den TFTP-Server bereit.

3. Welche Unterschiede bestehen zwischen der Ausführung im Router- und Gateway-Modus?

Der Router kann in zwei Modi betrieben werden: im Router-Modus und im Gateway-Modus. Der Router-Modus ist der Betriebsmodus, der die Network Address Translation (NAT) auf dem Gerät deaktiviert und zum Verbinden von mehr als einem Router und mehreren Netzwerken verwendet wird. Diese Funktion eignet sich am besten für Weitverkehrsnetzwerkumgebungen.

Der Gateway-Modus ist der empfohlene Modus, wenn der Router eine Netzwerkverbindung direkt zum Internet hostet. NAT wird ausgeführt, wenn der Gateway-Modus aktiviert ist. Das bedeutet, dass eine einzelne WAN-IP-Adresse verwendet wird und ein ganzer Block von LAN-IP-Adressen vorhanden ist.

4. Was sind Systemprotokolle?

Systemprotokolle (Syslog) sind Datensätze von Netzwerkereignissen. Im Falle einer Systemstörung können Sie die Protokolle abrufen, um das Systemproblem zu diagnostizieren.

Protokolle sind wichtige Tools, mit denen ein Netzwerk so funktioniert, dass es reibungslos funktioniert und Ausfälle verhindert. Sie eignen sich für Netzwerkmanagement, Fehlerbehebung und Überwachung.

5. Was sind DHCP-Modi?

Das Dynamic Host Configuration Protocol (DHCP) verfügt über zwei Modi: DHCP-Server und DHCP-Relay. Ein DHCP-Server weist einem DHCP-Client oder -Host im Netzwerk automatisch die verfügbaren IP-Adressen zu. Der DHCP-Server und der DHCP-Client müssen mit derselben Netzwerkverbindung verbunden sein. In größeren Netzwerken, in denen sich die Clients und Server nicht im gleichen physischen Subnetz befinden, enthält jede Netzwerkverbindung einen oder mehrere DHCP Relay Agents. Ein DHCP Relay Agent kann ein Router sein. Wenn ein Client dem Router eine DHCP-Anfrage sendet, leitet der Router diese dann an den DHCP-Server weiter und fordert ihn auf, eine IP-Adresse für den Client anzugeben. Der DHCP-Server sendet seine Antwort an den Router, und der Router leitet sie dann an den Client weiter. Der Router und der DHCP-Server müssen sich nicht im gleichen Subnetz befinden, um zu funktionieren. Der Router fungiert als Verbindung zwischen dem Client und dem DHCP-Server.

6. Was ist 3G/4G?

Es ist die Technologie für mobiles Breitband oder drahtloses Internet, auf die über Mobiltelefone oder tragbare Modems zugegriffen werden kann. Der Buchstabe G steht für die Generation. Die 4G-Technologie ist nach Long Term Evolution (LTE) eine der neuesten und schnellsten heute. Bei einigen Cisco VPN-Routern können Sie die Internetverbindung von unterstützten 3G/4G-USB-Dongles freigeben, die an diese angeschlossen werden können, um als Failover zu dienen, falls der Internet Service Provider (ISP) ausfällt oder ausfällt.

7. Was ist ein Zertifikatsgenerator und wann sollte ich ihn verwenden?

Ein digitales Zertifikat bescheinigt das Eigentum an einem öffentlichen Schlüssel durch den benannten Subjekt des Zertifikats. Dadurch können sich die Parteien auf Signaturen oder Behauptungen des privaten Schlüssels verlassen, der dem öffentlichen Schlüssel entspricht, der zertifiziert ist. Ein Router kann ein selbstsigniertes Zertifikat generieren, ein Zertifikat, das vom Netzwerkadministrator erstellt wurde. Sie kann auch Anfragen an Zertifizierungsstellen (Certificate Authority, CA) senden, um ein digitales Identitätszertifikat zu beantragen. Es ist wichtig, legitime Zertifikate von Drittanbieteranwendungen zu erhalten.

8. Was ist eine Firewall, und wann sollte ich diese verwenden?

Das Hauptziel einer Firewall ist die Kontrolle des ein- und ausgehenden Netzwerkverkehrs, indem die Datenpakete analysiert und anhand eines vordefinierten Regelsatzes ermittelt wird, ob sie durchgelassen werden sollen oder nicht. Ein Router gilt aufgrund von Funktionen, die das Filtern eingehender Daten ermöglichen, als starke Hardware-Firewall. Eine Netzwerk-Firewall baut eine Brücke zwischen einem internen Netzwerk, das als sicher und vertrauenswürdig gilt, und einem anderen Netzwerk, in der Regel einem externen Internetwork wie dem Internet, das als nicht sicher und nicht vertrauenswürdig angesehen wird.

9. Was ist ein vertrauenswürdiges IPSec-Zertifikat?

Internet Protocol Security (IPSec) ermöglicht die sichere, authentifizierte und zuverlässige Kommunikation über IP-Netzwerke. Sie wird für den Austausch von Schlüsselgenerierungs- und Authentifizierungsdaten, des Key-Establishment-Protokolls, des Verschlüsselungsalgorithmus

oder des Authentifizierungsmechanismus für die sichere Authentifizierung und Validierung von Online-Transaktionen mit SSL-Zertifikaten (Secure Socket Layer) verwendet. Auf der RV320 können Sie maximal 50 Zertifikate hinzufügen, die entweder selbst signiert oder von einer Zertifizierungsstelle eines Drittanbieters autorisiert sind. Diese Zertifikate können auf einen Computer oder ein USB-Gerät exportiert und zur Verwendung durch einen Client oder Administrator importiert werden.

10. Was ist ein vertrauenswürdiges SSL-Zertifikat?

Zertifikate werden verwendet, um die Benutzeridentität auf einem Computer oder im Internet zu überprüfen und um ein privates oder sicheres Gespräch zu verbessern. Secure Sockets Layer (SSL) ist die standardmäßige Sicherheitstechnologie zum Erstellen einer verschlüsselten Verbindung zwischen einem Webserver und einem Browser. Diese Zertifikate können auf einen Computer oder ein USB-Gerät exportiert und zur Verwendung durch einen Client oder Administrator importiert werden.

11. Was ist Client-to-Gateway-VPN?

Virtual Private Network (VPN) Client-to-Gateway: Ein Benutzer kann verschiedene Zweigstellen Ihres Unternehmens, die sich in verschiedenen geografischen Gebieten befinden, remote miteinander verbinden, um die Daten sicher zwischen den Gebieten zu übertragen und zu empfangen. In der Regel ist auf einem Computer eine VPN-Clientsoftware wie der Cisco AnyConnect Secure Mobility Client installiert, die Anmeldung mit den erforderlichen Anmeldeinformationen erfolgt und eine Verbindung zu einem Remote-Router oder -Gateway herstellt.

Hinweis: Ab Version 1.0.3.15 wurden die Lizenzierungsanforderungen für die Serie RV340 aktualisiert. Weitere Informationen hierzu finden Sie hier.

12. Was ist Content-Filterung?

Content-Filterung ist eine Funktion, mit der ein Administrator bestimmte, unerwünschte Websites blockieren kann. Content-Filterung kann Listen blockieren und den Zugriff auf Websites anhand von Schlüsselwörtern und URLs (Uniform Resource Locators) ermöglichen. Ein Administrator kann einen Zeitplan auf die Inhaltsfilterung anwenden, je nachdem, wann diese aktiviert sein soll.

Weitere Informationen finden Sie im Glossar.

13. Was ist CoS?

Class of Service (CoS) ist eine Methode zur Verwaltung des Datenverkehrs über ein Netzwerk, indem eine Priorität gegenüber anderen Arten von Datenverkehr zugewiesen wird. Er wird verwendet, um Ethernet-Frame-Headern des Netzwerkverkehrs Prioritätsebenen zuzuweisen, und gilt nur für Trunked Links. Durch die Differenzierung des Datenverkehrs ermöglicht CoS die Festlegung von Richtlinien für bevorzugte Datenpakete und deren Priorisierung für die Übertragung, falls im Netzwerk Probleme wie Überlastung oder Verzögerung auftreten. Sie können die CoS-Prioritätseinstellungen der Weiterleitungswarteschlange eines Routers zuordnen.

14. Was ist die DHCP-Option 82?

Der DHCP-Relay ist eine im Router enthaltene Funktion, die die DHCP-Kommunikation zwischen Hosts und Remote-DHCP-Servern ermöglicht, die sich nicht im gleichen Netzwerk befinden. Option 82 ist eine DHCP Relay Agent-Informationsoption, mit der ein DHCP Relay Agent

Informationen über sich selbst weiterleitet, wenn DHCP-Pakete vom Client an einen DHCP-Server weitergeleitet werden. Der DHCP-Server kann diese Informationen verwenden, um IP-Adressen oder andere Parameterzuweisungsrichtlinien zu implementieren. Die gründliche Identifizierung der Verbindung erhöht die Sicherheit des DHCP-Prozesses.

15. Was ist DHCP?

Dynamic Host Configuration Protocol (DHCP) ist ein Netzwerkkonfigurationsprotokoll, das die IP-Adressen von Geräten in einem Netzwerk automatisch so konfiguriert, dass sie sich miteinander verbinden können, anstatt einem Gerät manuell eine IP-Adresse zuzuweisen.

16. Was ist DMZ, und wann sollte ich sie verwenden?

Eine Demilitarized Zone (DMZ) ist ein Subnetz, das der Öffentlichkeit zugänglich ist, aber hinter der Firewall liegt. Mit einer DMZ können Sie Pakete, die an Ihren WAN-Port gesendet werden, an eine bestimmte IP-Adresse in Ihrem LAN umleiten. Sie können Firewall-Regeln konfigurieren, um den Zugriff auf bestimmte Services und Ports in der DMZ sowohl vom LAN als auch vom WAN zu ermöglichen. Bei einem Angriff auf einen der DMZ-Knoten ist das LAN nicht unbedingt anfällig. Es wird empfohlen, Hosts, die dem WAN (z. B. Web- oder E-Mail-Server) ausgesetzt sein müssen, im DMZ-Netzwerk zu platzieren.

17. Was ist DSCP?

Differentiated Services Code Point (DSCP) dient zur Klassifizierung des Netzwerkverkehrs und zur Zuweisung verschiedener Servicelevel an Pakete, indem diese mit DSCP-Codes im Feld "IP-Header" gekennzeichnet werden. Die DSCP-Einstellungen bestimmen, wie DSCP-Werte Quality of Service (QoS) zugeordnet werden. Hierbei handelt es sich um eine Methode zur Verwaltung der Prioritätsstufen des Datenverkehrs in einem Netzwerk. Der Router kann über DSCP die Prioritätsbits im Type of Service (ToS)-Oktett verwenden, um Datenverkehr gegenüber QoS in Layer 3 zu priorisieren.

18. Was ist Dynamic DNS?

Dynamic Domain Name System (DNS) ist eine Methode zur automatischen Aktualisierung eines Namenservers im DNS, häufig in Echtzeit, mit der aktiven DDNS-Konfiguration der konfigurierten Hostnamen, Adressen oder anderen Informationen. Dieser Dienst weist einer dynamischen WAN-IP-Adresse einen festen Domänennamen zu, sodass Sie Ihr eigenes Web, FTP oder einen anderen Typ von TCP/IP-Server in Ihrem LAN hosten können. Der Router verwendet DDNS über ein webbasiertes DDNS-Konto. Wenn sich die WAN-IP-Adresse des Routers ändert, benachrichtigt die DDNS-Funktion den DDNS-Server über die Änderung. Der DDNS-Server aktualisiert dann die Konfiguration, um die neue WAN-IP-Adresse einzuschließen. Dies ist nützlich, wenn sich die WAN-IP-Adresse des Routers häufig ändert. Auf einer der bereitgestellten Websites muss ein DDNS-Konto erstellt werden, um die DDNS-Funktion auf dem Router zu nutzen.

19. Was ist Gateway-to-Gateway-VPN? Wann würden Sie es verwenden?

Eine Gateway-to-Gateway-VPN-Verbindung ermöglicht es zwei Routern, sich sicher miteinander zu verbinden, und einem Client an einem Ende logisch so, als wären sie Teil des Netzwerks am anderen Ende. So können Daten und Ressourcen einfacher und sicherer über das Internet gemeinsam genutzt werden. Die Konfiguration muss auf beiden Routern vorgenommen werden, um ein Gateway-to-Gateway-VPN zu aktivieren.

20. Was sind IP- und MAC-Bindungen? Wann sollte ich es verwenden?

IP- und MAC-Adressbindung ist ein Prozess, der eine IP-Adresse mit einer MAC-Adresse verbindet und umgekehrt. Wenn der Router Pakete mit derselben IP-Adresse, aber einer anderen MAC-Adresse empfängt, verwirft er die Pakete. IP-Spoofing wird verhindert, und die Netzwerksicherheit wird erhöht, da Benutzer die IP-Adressen von Geräten nicht ändern können. Die IP-Adresse des Quell-Hosts und die MAC-Adresse des Datenverkehrs müssen immer übereinstimmen, um Zugriff auf das Netzwerk zu erhalten. Wenn der Router Pakete mit derselben IP-Adresse, aber einer anderen MAC-Adresse empfängt, verwirft er die Pakete.

21. Was ist Lastenausgleich, und wann sollte ich ihn verwenden?

Durch Lastenausgleich kann ein Router mehrere der besten Pfade zu einem bestimmten Ziel nutzen. Sie ist Bestandteil des Weiterleitungsprozesses im Router und wird automatisch aktiviert, wenn die Routing-Tabelle mehrere Pfade zu einem Ziel hat. Die Konfiguration des Lastenausgleichs im Router trägt dazu bei, eine angemessene Ressourcennutzung zu erreichen, den Durchsatz zu maximieren, die Reaktionszeit zu maximieren und hauptsächlich die Überlastung zu vermeiden, da die Workload auf mehrere Computer, Netzwerkverbindungen und andere Ressourcen verteilt wird.

22. Was ist ein MAC-Adressen-Klon, und wann muss ich ihn verwenden?

Der MAC-Adressenklon ist die einfachste Möglichkeit, die genaue Kopie der MAC-Adresse eines Geräts auf ein anderes Gerät (z. B. einen Router) zu kopieren. Manchmal bitten ISPs Sie, eine MAC-Adresse Ihres Routers zu registrieren, um das Gerät zu authentifizieren. Eine MAC-Adresse ist ein 12-stelliger Hexadezimalcode, der jeder Hardware zugewiesen wird, damit sie eindeutig identifiziert werden kann. Wenn Sie bereits eine andere MAC-Adresse bei Ihrem ISP registriert haben, kann ein MAC-Adressen-Klon verwendet werden, um diese Adresse an Ihren neuen Router zu kopieren. Auf diese Weise müssen Sie sich nicht an den ISP wenden, um die zuvor registrierte MAC-Adresse zu ändern, wodurch die Kosten und der Zeitaufwand für die Wartung reduziert werden.

23. Was ist One-to-One NAT, und wann muss ich diese verwenden?

One-to-One Network Address Translation (NAT) erstellt eine Beziehung, die eine gültige WAN-IP-Adresse LAN-IP-Adressen zuordnet, die von NAT aus dem WAN (Internet) verborgen sind. Dies schützt die LAN-Geräte vor Erkennung und Angriffen. Auf dem Router können Sie eine einzelne private IP-Adresse (LAN-IP-Adresse) einer einzigen öffentlichen IP-Adresse (WAN-IP-Adresse) oder einem Bereich von privaten IP-Adressen einer Reihe von öffentlichen IP-Adressen zuordnen.

24. Was ist die Komplexität von Passwörtern, und warum ist sie für mich nützlich?

Die Komplexität von Kennwörtern ist eine Funktion eines Netzwerkgeräts, das eine minimale Passwortkomplexität für Kennwortänderungen erzwingt. Dies ist für alle Netzwerktypen von Vorteil. Kennwörter mit hoher Komplexität können nach einer bestimmten Zeit auf ein Ablaufdatum festgelegt werden.

25. Was ist Port Address Translation (PAT), und wann sollte ich sie verwenden müssen?

Mit dieser Funktion können mehrere Geräte innerhalb eines privaten oder lokalen Netzwerks einer einzigen öffentlichen IP-Adresse zugeordnet werden. PAT wird verwendet, um IP-Adressen zu

speichern. Es handelt sich um eine Erweiterung von Network Address Translation (NAT). PAT wird auch als Portierung, Port-Überladung, Port-Level-Multiplexed NAT und Single-Address NAT bezeichnet.

26. Was ist Port Forwarding, und wann muss ich es verwenden?

Port Forwarding ist eine Funktion, mit der Daten an ein bestimmtes Gerät in einem privaten LAN weitergeleitet werden. Dies geschieht, indem der Datenverkehr von ausgewählten Ports auf Ihrem Gerät den entsprechenden Ports im Netzwerk zugeordnet wird. Der Router unterstützt diese Funktion, mit der Ihr Computer den Datenverkehr dort effizient leiten kann, wo er benötigt wird, um die Leistung und die Eigenschaften des Netzwerkausgleichs zu verbessern. Port Forwarding sollte nur bei Bedarf verwendet werden, da dies ein Sicherheitsrisiko darstellt, da ein konfigurierter Port immer offen ist.

27. Was ist Port-Spiegelung?

Die Portspiegelung ist eine Methode zur Überwachung des Netzwerkverkehrs. Mit der Portspiegelung werden Kopien von eingehenden und ausgehenden Paketen an den Ports (Quell-Ports) eines Netzwerkgeräts an einen anderen Port (Ziel-Port) weitergeleitet, an dem die Pakete untersucht werden.

28. Was ist Port Triggering, und wann sollte ich es verwenden?

Port-Triggering ähnelt der Port-Weiterleitung, ist jedoch sicherer, da die eingehenden Ports nicht ständig geöffnet sind. Die Ports bleiben so lange geschlossen, bis sie ausgelöst werden, wodurch die Möglichkeit eines unerwünschten Port-Zugriffs eingeschränkt wird. Port-Triggering ist eine Methode zur dynamischen Port-Weiterleitung. Wenn ein Host, der mit dem Router verbunden ist, einen Trigger-Port öffnet, der in einer Port-Bereich-Auslöserregel konfiguriert ist, leitet der Router die konfigurierten Ports an den Host weiter. Sobald der Host den getriggerten Port schließt, schließt der Router die weitergeleiteten Ports. Jeder Computer in einem Netzwerk kann die Port-Triggering-Konfiguration verwenden, da keine interne IP-Adresse für die Weiterleitung der eingehenden Ports erforderlich ist, im Gegensatz zu Port Forwarding.

29. Was ist der PPTP-Server? Wann würden Sie es verwenden? Wie würden Sie das einrichten?

Das Point-to-Point Tunneling Protocol (PPTP) ist ein Netzwerkprotokoll zur Implementierung von VPN-Tunneln zwischen öffentlichen Netzwerken. PPTP-Server werden auch als VPDN-Server (Virtual Private Dialup Network) bezeichnet. PPTP verwendet einen Kontrollkanal über das Transmission Control Protocol (TCP) und einen GRE-Tunnel (Generic Routing Encapsulation), um PPP-Pakete zu kapseln. Für Benutzer, die eine PPTP-Client-Software ausführen, können bis zu 25 PPTP-VPN-Tunnel aktiviert werden. Die gängigste PPTP-Implementierung ist bei den Microsoft Windows-Produktfamilien und implementiert verschiedene Stufen der Authentifizierung und Verschlüsselung nativ als Standardfunktionen des Windows PPTP-Stacks. PPTP wird anderen Protokollen vorgezogen, da es schneller ist und auf mobilen Geräten verwendet werden kann. Klicken Sie hier, um eine Vorstellung davon zu erhalten, wie Sie das System einrichten.

30. Was ist QoS?

Quality of Service (QoS) wird hauptsächlich zur Verbesserung der Netzwerkleistung verwendet und wird zur Bereitstellung der gewünschten Dienste für die Benutzer verwendet. Der Datenverkehrsfluss wird anhand der Art des Datenverkehrs priorisiert. QoS kann auf priorisierten

Datenverkehr für latenzempfindliche Anwendungen (z. B. Sprache oder Video) angewendet werden und die Auswirkungen von latenzunempfindlichem Datenverkehr (z. B. Massendatenübertragungen) kontrollieren.

31. Was ist RIPv1? RIPv2?

Routing Information Protocol (RIP) ist ein Distanzvektor-Protokoll, das von Routern zum Austausch von Routing-Informationen verwendet wird. RIP verwendet die Hop-Anzahl als Routing-Metrik. RIP verhindert, dass Routing-Schleifen unbegrenzt fortgeführt werden, indem eine Beschränkung der Anzahl an Hops implementiert wird, die in einem Pfad von der Quelle bis zum Ziel zulässig sind. Die maximale Hop-Anzahl für RIP beträgt 15, wodurch die zu unterstützende Netzwerkgröße eingeschränkt wird. Aus diesem Grund wurde RIPv2 entwickelt. Im Gegensatz zum klassischen RIPv1 ist RIPv2 ein klassenloses Routing-Protokoll, das die Subnetzmasken beim Versenden von Routing-Updates enthält.

Die Zusammenfassung von Routen in RIPv2 verbessert die Skalierbarkeit und Effizienz großer Netzwerke. Die Zusammenfassung von IP-Adressen bedeutet, dass in der RIP-Routing-Tabelle kein Eintrag für untergeordnete Routen (Routen, die für eine beliebige Kombination der einzelnen IP-Adressen in einer zusammengefassten Adresse erstellt werden) vorhanden ist. Dadurch wird die Größe der Tabelle verringert, und der Router kann mehr Routen verarbeiten.

32. Was ist Smart Link Backup?

Smart Link Backup ist eine Funktion, mit der der Benutzer ein zweites WAN einrichten kann, falls die erste oder die primäre Verbindung ausfällt. Diese Funktion stellt sicher, dass die Kommunikation zwischen dem WAN und dem Gerät stets kontinuierlich erfolgt. Diese Funktion wird bei Routern mit dualen WAN-Verbindungen verwendet.

33. Was ist SSL VPN? Wann würden Sie es verwenden?

Ein Secure Sockets Layer Virtual Private Network (SSL VPN), auch als WebVPN bekannt, ist eine Technologie, die Remotezugriff-VPN-Funktionen über die SSL-Funktion bietet, die in einen modernen Webbrowser integriert ist. Dies erfordert nicht, dass Sie einen VPN-Client auf dem Gerät des Clients installieren. Mit SSL VPN können Benutzer von einem beliebigen internetfähigen Standort aus einen Webbrowser starten, um VPN-Verbindungen für den Remote-Zugriff einzurichten. Dadurch werden Produktivitätssteigerungen und eine verbesserte Verfügbarkeit versprochen sowie weitere IT-Kostensenkungen für VPN-Client-Software und -Support erzielt.

34. Was ist VPN-Passthrough?

VPN Passthrough ist eine Möglichkeit, zwei gesicherte Netzwerke über das Internet zu verbinden. Damit wird der VPN-Datenverkehr, der von mit dem Router verbundenen VPN-Clients generiert wird, an das Internet weitergeleitet und die erfolgreiche VPN-Verbindung ermöglicht.

35. Was ist VPN?

Ein Virtual Private Network (VPN) ist eine sichere Verbindung, die innerhalb eines Netzwerks oder zwischen Netzwerken durch die Erstellung eines Tunnels hergestellt wird. VPNs dienen dazu, den Datenverkehr zwischen bestimmten Hosts und Netzwerken vom Datenverkehr nicht autorisierter Hosts und Netzwerke zu isolieren. VPNs bieten Unternehmen Vorteile in einer Weise, dass sie hochgradig skalierbar sind, die Netzwerktopologie vereinfacht und die Produktivität durch die Reduzierung von Reisezeiten und Kosten für Remote-Benutzer verbessert wird.

36. Warum sollte ich die Werte für die Subnetzmaske ändern?

Ein Subnetz ist ein Teil eines Netzwerks, das sich eine Subnetzadresse für Partikel teilt. Eine Subnetzmaske ist eine 32-Bit-Kombination, die verwendet wird, um zu beschreiben, welcher Teil einer Netzwerkadresse auf das Subnetz verweist und welcher Teil auf den Host verweist. Ein Administrator kann die Werte für die Subnetzmaske ändern, falls ein Host nicht mit dem Netzwerk kommunizieren kann. Die Subnetzmasken können auch geändert werden, wenn ein Administrator die Anzahl der Hosts in einem Subnetz erhöhen möchte, ohne physische Änderungen vornehmen zu müssen.