Vaak gestelde vragen van de router

Doel

Dit document is bedoeld om gemeenschappelijke vragen te beantwoorden over de functies en functies die in een Cisco-router aanwezig zijn, evenals hoe en wanneer u deze kunt gebruiken. Als u geïnteresseerd bent in video-inhoud, raadpleegt u onze videoplaylist door hier op te klikken.

Toepasselijke apparaten

- RV100 Series-switches
- RV200 Series-switches
- RV300 Series routers

Inhoud

1. Wat zijn de toegangsregels?

Toegangscontroleregels zijn regels die het specifieke verkeer van en naar bepaalde gebruikers op een netwerk verbieden. Toegangsregels kunnen zo worden ingesteld dat ze de hele tijd of op basis van een vastgesteld schema van kracht zijn. Terwijl een toegangsregel op een router of een schakelaar kan worden geconfigureerd, wordt deze op basis van verschillende criteria ingesteld om toegang tot een of meer of alle bronnen in het netwerk toe te staan of te ontkennen.

2. Wat zijn opties 66, 67 en 150 voor TFTP-server?

Een TFTP-server staat een beheerder toe om configuratiebestanden op te slaan, terug te halen en te downloaden voor apparaten op een netwerk. Een Dynamic Host Configuration Protocol (DHCP) Server leases en verspreidt IP-adressen naar apparaten op het netwerk. Wanneer een apparaat start, en een IPv4- of IPv6-adres en TFTP-server IP-adres niet vooraf zijn ingesteld, stuurt het apparaat een verzoek naar de DHCP-server met Opties 66, 67 en 150. Deze opties zijn verzoeken naar de DHCP-server om informatie over de TFTP-server te verkrijgen.

- DHCP-optie 150 is Cisco-eigendom. Het voorziet de IP-adressen in een lijst van TFTP-servers. Het IEEE-standaard-equivalent (Institute of Electrical and Electronics Engineers) is optie 66.
- DHCP-optie 66 geeft het IP-adres of de hostnaam van één TFTP-server.
- DHCP-optie 67 biedt de naam van het beginbestand voor de TFTP-server.

3. Wat zijn de verschillen tussen het draaien in routermodus in vergelijking met de gatewaymodus?

Er zijn twee modi waarin uw router kan werken, de routermodus en de gatewaymodus. De routermodus is de werkingsmodus die NAT (Network Address Translation) op het apparaat blokkeert en gebruikt wordt om meer dan één router en meerdere netwerken aan te sluiten. Dit wordt het best gebruikt in brede netwerkomgevingen.

De modus van de gateway is de aanbevolen modus als de router een netwerkverbinding rechtstreeks naar het internet host. NAT wordt uitgevoerd wanneer de Gateway-modus is ingeschakeld, wat inhoudt dat het één WAN IP-adres inneemt en een heel blok LAN IP-adressen heeft.

4. Wat zijn systeemregisters?

De logbestanden van het systeem (Syslog) zijn records van netwerkgebeurtenissen. Als het systeem niet goed werkt, kunt u de logbestanden ophalen om te bepalen wat het systeemprobleem is. Logs zijn belangrijke gereedschappen die worden gebruikt om te begrijpen hoe een netwerk werkt om het systeem vlot te laten lopen en fouten te voorkomen. Ze zijn handig voor netwerkbeheer, probleemoplossing en bewaking.

5. Wat zijn DHCP-modi?

Dynamic Host Configuration Protocol (DHCP) heeft twee modi: DHCP-server en DHCP-relay. Een DHCP-server wijst automatisch beschikbare IP-adressen toe aan een DHCP-client of host op het netwerk. De DHCP-server en DHCP-client moeten met dezelfde netwerklink worden verbonden. In grotere netwerken waar de cliënten en de servers niet op hetzelfde fysieke net zijn, bevat elke netwerkverbinding een of meer DHCP Relay-agents. Een DHCP-relais kan een router zijn. Wanneer een client de router een DHCP-verzoek verstuurt, zal de router deze dan naar de DHCP-server doorsturen met het verzoek een IP-adres voor de client te geven. De DHCP-server stuurt zijn antwoord naar de router en de router stuurt het door naar de client. De router en de DHCP-server hoeven niet op dezelfde mate te zijn als u wilt functioneren. De router fungeert als een verbinding tussen de client en de DHCP-server.

6. Wat is 3G/4G?

Het is het type technologie voor mobiel breedband of draadloos internet dat toegankelijk is via mobiele telefoons of draagbare modems. De letter G staat voor de generatie. De 4G-technologie is een van de nieuwste en snelste op dit moment na lange termijn evolutie (LTE). Sommige Cisco VPN-routers staan u toe om de internetverbinding te delen via ondersteunde 3G/4G USB-dongels die aan deze kabel kunnen worden bevestigd om als failover te dienen voor het geval dat de belangrijkste Internet Service Provider (ISP) omlaag gaat of vertraagt.

7. Wat is een certificatengenerator en wanneer zou ik deze gebruiken?

Een digitaal certificaat certificeert de eigendom van een openbare sleutel door het genoemde onderwerp van het certificaat. Dit stelt betrouwbare partijen in staat om afhankelijk te zijn van handtekeningen of beweringen van de privé-sleutel die overeenkomt met de openbare sleutel die gecertificeerd is. Een router kan een zelf-ondertekend certificaat genereren, een certificaat dat is gemaakt door de netwerkbeheerder. Het kan ook verzoeken aan de certificaatautoriteiten (CA) zenden om een digitaal identiteitsbewijs aan te vragen. Het is belangrijk dat er een rechtmatig certificaat is van een verzoek van derden.

8. Wat is een firewall en wanneer zou ik die gebruiken?

Het primaire doel van een firewall is het inkomende en uitgaande netwerkverkeer te controleren door de gegevenspakketten te analyseren en te bepalen of dit al dan niet moet worden toegestaan op basis van een vooraf bepaalde set regels. Een router wordt beschouwd als een sterke hardware firewall vanwege functies die het filteren van inkomende gegevens mogelijk maken. Een netwerkfirewall bouwt een brug tussen een intern netwerk dat verondersteld wordt veilig en vertrouwd te zijn en een ander netwerk, gewoonlijk een extern internetwerk zoals Internet dat niet veilig en onbetrouwbaar wordt verondersteld.

9. Wat is een vertrouwd IPSec-certificaat?

Internet Protocol Security (IPSec) genereert veilige, geauthentiseerde en betrouwbare communicatie via IP-netwerken. Het wordt gebruikt in de uitwisseling van gegevens over sleutelproductie en authenticatie, sleutelvestigingsprotocol, encryptiealgoritme of authenticatiemechanisme voor veilige authenticatie en validatie van online transacties met Secure Socket Layer (SSL) - certificaten. Op de RV320 kunt u maximaal 50 certificaten toevoegen die ofwel zelf zijn ondertekend of door derden zijn geautoriseerd. Deze certificaten kunnen worden geëxporteerd naar een computer of USB-apparaat en worden geïmporteerd om te worden gebruikt door een client of beheerder.

10. Wat is een betrouwbaar SSL-certificaat?

Certificaten worden gebruikt om de gebruikersidentiteit op een computer of internet te controleren en om een privé of beveiligd gesprek te verbeteren. Secure Socket Layer (SSL) is de standaard security technologie voor het maken van een versleutelde link tussen een webserver en een browser. Deze certificaten kunnen worden geëxporteerd naar een computer of USB-apparaat en worden geïmporteerd om te worden gebruikt door een client of beheerder.

11. Wat is client-to-Gateway VPN?

Client-to-Gateway Virtual Private Network (VPN) betekent dat een gebruiker op afstand verschillende takken van uw bedrijf in verschillende geografische gebieden kan verbinden om de gegevens tussen de gebieden beter te verzenden en ontvangen. Een gebruiker zou doorgaans een VPN-clientsoftware hebben zoals de Cisco AnyConnect Secure Mobility Client op een computer geïnstalleerd, inloggen met de benodigde aanmeldingsgegevens en verbinding maken met een externe router of poort.

Opmerking: Er zijn updates over de vergunningsvereisten voor RV340-reeksen, beginnend met de ontwikkeling van versie 1.0.3.15. Klik hier voor meer informatie hierover.

12. Wat is contentfiltering?

Contentfiltering is een functie waarmee een beheerder aangewezen, ongewenste websites kan blokkeren. Contentfiltering kan een lijst blokkeren en lijsttoegang tot websites toestaan volgens zoekwoorden en Unified Resource Locators (URL's). Een beheerder kan een schema toepassen op het filteren van inhoud afhankelijk van het moment dat het actief zou moeten zijn.

Zie de woordenlijst voor aanvullende informatie.

13. Wat is CoS?

Serviceklasse (CoS) is een manier om verkeer via een netwerk te beheren door een prioriteit toe te kennen boven andere soorten verkeer. Het wordt gebruikt om prioriteitsniveaus aan Ethernet frame-headers van netwerkverkeer toe te wijzen en is alleen van toepassing op trunked links. Door een onderscheid te maken tussen verkeer, staat CoS geprefereerde gegevenspakketten toe om te worden gecontroleerd en voorrang te krijgen voor transmissie als het netwerk problemen zoals congestie of vertraging ervaart. U kunt de prioriteitsinstellingen van CoS aan de verkeerspost op een router in kaart brengen.

14. Wat is DHCP-optie 82?

Het DHCP-relais is is een optie die in de router is opgenomen en die DHCP-communicatie tussen hosts en externe DHCP-servers toestaat die niet op hetzelfde netwerk aanwezig zijn. Optie 82 is een optie van de het relais van DHCP optie om een middel van het DHCP-relais informatie over zichzelf te omvatten wanneer het verzenden van client-geïnitieerde DHCP-pakketten naar een DHCP-server. De DHCP-server kan deze informatie gebruiken om IP-adressering of ander parameter-toekenningsbeleid uit te voeren. Haar grondige identificatie van de verbinding voegt beveiliging toe aan het DHCP-proces.

15. Wat is DHCP?

Dynamic Host Configuration Protocol (DHCP) is een protocol voor de netwerkconfiguratie dat automatisch de IP-adressen van apparaten op een netwerk configureren, zodat ze met elkaar

kunnen verbinden in plaats van handmatig een IP-adres aan een apparaat toe te wijzen.

16. Wat is DMZ en wanneer moet ik het gebruiken?

Een gedemilitariseerde zone (DMZ) is een subnetwerk dat open staat voor het publiek maar achter de firewall. Met een DMZ kunt u pakketten die in uw WAN-poort komen, doorsturen naar een specifiek IP-adres in uw LAN. U kunt firewallregels configureren om toegang tot specifieke services en poorten in de DMZ te bieden via zowel LAN als WAN. In het geval van een aanval op een van de DMZ-knooppunten is LAN niet noodzakelijk kwetsbaar. Het wordt aanbevolen om hosts te plaatsen die aan WAN (zoals web- of e-mailservers) moeten worden blootgesteld in het DMZ-netwerk.

17. Wat is DSCP?

Distributed Services Code Point (DSCP) wordt gebruikt om netwerkverkeer te classificeren en verschillende serviceniveaus aan pakketten toe te wijzen door ze met DSCP-codes in het veld IP-header te markeren. De DSCP-instellingen zullen bepalen hoe DSCP-waarden in kaart worden gebracht met Quality of Service (QoS), een methode om prioriteitsniveaus van verkeer op een netwerk te beheren. Het is door DSCP dat de router de prioriteitsbits in het type service-octet (ToS) kan gebruiken om voorrang te geven aan verkeer boven QoS in Layer 3.

18. Wat is Dynamische DNS?

Dynamic Domain Name System (DNS) is een methode om een naamserver in de DNS automatisch en vaak in realtime te uploaden, met de actieve DDNS-configuratie van de geconfigureerde hostnamen, adressen of andere informatie. Deze service kent een vaste domeinnaam toe aan een dynamisch WAN IP-adres, zodat u uw eigen web-, FTP- of een ander type TCP/IP-server op uw LAN kunt opslaan. De router gebruikt DDNS via een op web gebaseerde DDNS-account. Als het WAN IP-adres van de router verandert, zal de DDNS-functie de DDNS-server van de wijziging op de hoogte stellen. De DDNS-server werkt de configuratie dan bij om het nieuwe WAN IP-adres op te nemen. Dit is nuttig als het WAN IP adres van de router vaak verandert. Er moet een DDNS-account op een van de beschikbare websites worden gemaakt om de DDNS-functie op de router te gebruiken.

19. Wat is Gateway-to-Gateway VPN? Wanneer zou je het gebruiken?

Met een poort-naar-gateway VPN-verbinding kunnen twee routers zich veilig met elkaar verbinden en kan een client aan één kant logisch verschijnen alsof ze deel uitmaken van het netwerk aan de andere kant. Hierdoor kunnen gegevens en hulpmiddelen gemakkelijker en veiliger over het internet worden gedeeld. De configuratie moet op beide routers worden uitgevoerd om een gateway-naar-gateway VPN mogelijk te maken.

20. Wat zijn IP- en MAC-binding? Wanneer zou ik het gebruiken?

IP en MAC adresbinding zijn een proces dat een IP-adres aan een MAC-adres koppelt en vice versa. Als de router pakketten met het zelfde IP adres maar een verschillend adres van MAC ontvangt, daalt het de pakketten. Het helpt IP spoofing te voorkomen en verbetert netwerkveiligheid, aangezien het een gebruiker niet toestaat om IP adressen van apparaten te veranderen. Het IP adres van de brongastheer en het adres van MAC van het verkeer moeten altijd aan elkaar passen om toegang tot het netwerk te krijgen. Als de router pakketten met het zelfde IP adres maar een verschillend adres van MAC ontvangt, daalt het de pakketten.

21. Wat is taakverdeling en wanneer zou ik die gebruiken?

Taakverdeling maakt een router in staat om voordeel te halen uit meerdere beste paden naar een bepaalde bestemming. Het is inherent aan het door:sturen proces in de router en wordt automatisch geactiveerd als de routingtabel meerdere paden naar een bestemming heeft. Het configureren van taakverdeling in de router helpt bij het bereiken van een goed gebruik van middelen, maximaliseren doorvoersnelheid, responstijd en vermijdt voornamelijk de overbelasting omdat deze de werkbelasting over meerdere computers, netwerkverbindingen en andere verschillende bronnen distribueert.

22. Wat is MAC-adreskloon en wanneer moet ik die gebruiken?

MAC-adreskloon is de eenvoudigste manier om de exacte kopie van het MAC-adres van het ene apparaat te dupliceren naar een ander apparaat, zoals een router. Soms vragen ISPs u om een MAC-adres van uw router te registreren om het apparaat te authentiseren. Een MAC-adres is een 12-cijferig hexadecimale code die aan elk stuk hardware wordt gegeven zodat het uniek kan worden geïdentificeerd. Als u al een ander MAC-adres bij uw ISP hebt geregistreerd, kan een MAC-adreskloon worden gebruikt om dat adres aan uw nieuwe router aan te sluiten. Op deze manier hoeft u geen contact op te nemen met de ISP om het eerder geregistreerde MAC-adres te wijzigen, dat de kosten en de tijd van het onderhoud beperkt.

23. Wat is één-op-één NAT en wanneer moet ik het gebruiken?

One-to-one Network Address Translation (NAT) maakt een relatie die een geldig WAN IP-adres naar LAN IP-adressen maakt die door NAT verborgen zijn in WAN (Internet). Dit beschermt de LAN-apparaten tegen detectie en aanval. Op de router, kunt u één enkel privé IP adres (LAN IP adres) aan één enkel openbaar IP adres (WAN IP adres), of een reeks privé IP adressen aan een bereik van openbare IP adressen in kaart brengen.

24. Wat is de complexiteit van de wachtwoorden en waarom is het goed voor mij?

De complexiteit van het wachtwoord is een eigenschap van een netwerk apparaat dat een minimum wachtwoordcomplexiteitseis voor wachtwoordveranderingen afdwingt. Dit is voordelig voor alle typen netwerken. Wachtwoorden met complexiteit kunnen worden ingesteld om na een bepaalde tijd te verlopen.

25. Wat is Port Address Translation (PAT) en wanneer moet ik die gebruiken?

Het is een functie die het mogelijk maakt dat meerdere apparaten binnen een privaat of lokaal netwerk in kaart worden gebracht aan één openbaar IP-adres. PAT wordt gebruikt om IP-adressen te besparen. Het is een uitbreiding van Network Address Translation (NAT). PAT staat ook bekend als port, port overloading, port-level multiplexed NAT en Single Address NAT.

26. Wat is het doorsturen van havens en wanneer moet ik het gebruiken?

Port Forwarding is een functie die wordt gebruikt om gegevens naar een specifiek apparaat binnen een privaat LAN door te geven. Dit doet u door verkeer van gekozen poorten op uw apparaat in kaart te brengen naar corresponderende poorten op het netwerk. De router ondersteunt deze functie die uw computer in staat stelt op efficiënte wijze verkeer te sturen waar dit nodig is om de prestaties en de kenmerken van netwerkbalancering te verbeteren. Poortverzending mag alleen indien nodig worden gebruikt, aangezien dit een veiligheidsrisico met zich meebrengt omdat een geconfigureerde haven altijd open is.

27. Wat is Port Mirroring?

Port Mirroring is een methode die wordt gebruikt om het netwerkverkeer te bewaken. Met Port Mirroring worden kopieën van inkomende en uitgaande pakketten in de poorten (bronpoorten) van een netwerkapparaat naar een andere poort (doelpoort) verzonden waar de pakketten worden bestudeerd.

28. Wat is poortrammen en wanneer moet ik die gebruiken?

PoortTrigging is gelijk aan poortverzending behalve dat het veiliger is omdat de inkomende havens niet constant open zijn. De havens blijven gesloten totdat ze worden geactiveerd, waardoor de mogelijkheid van ongewenste toegang tot havens wordt beperkt. Poortontsteking is een methode van dynamisch poorttransport. Wanneer een host die op de router is aangesloten een trigger-poort opent die in een port range is ingesteld om de regel te activeren, stuurt de router de geconfigureerde poorten naar de host door. Zodra de host de geactiveerd poort sluit, sluit de router de doorgestuurd poorten. Elke computer op een netwerk kan de poort gebruiken die een setup-instelling start, omdat er geen intern IP-adres nodig is om de inkomende poorten door te sturen, in tegenstelling tot in Port Forwarding.

29. Wat is PPTP-server? Wanneer zou je het gebruiken? Hoe zou je het opzetten?

Het Point-to-Point Tunneling Protocol (PPTP) is een netwerkprotocol dat wordt gebruikt om VPN-tunnels tussen openbare netwerken uit te voeren. PPTP-servers staan ook bekend als Virtual Private Dialup Network (VPDN)-servers. PPTP gebruikt een controlekanaal over Transmission Control Protocol (TCP) en een generieke Routing Encapsulation (GRE)-tunnel die werkt om PPP-pakketten in te sluiten. Tot 25 PPTP VPN-tunnels kunnen worden ingeschakeld voor gebruikers die een PPTP-clientsoftware gebruiken. De meest gebruikelijke PPTP-implementatie is bij de Microsoft Windows-productfamilies en implementeert verschillende niveaus van verificatie en encryptie als standaard functies van de Windows PPTP-stapel. PPTP heeft de voorkeur boven andere protocollen omdat het sneller is en de mogelijkheid heeft om op mobiele apparaten te werken. Als referentie klik hier om een idee te krijgen hoe het in te stellen.

30. Wat is QoS?

Quality of Service (QoS) wordt voornamelijk gebruikt om de netwerkprestaties te verbeteren en wordt gebruikt om de gewenste services voor de gebruikers te leveren. Het prioriteert de verkeersstroom op basis van het type verkeer. QoS kan worden toegepast op geprioriteerd verkeer voor latency-gevoelige toepassingen (zoals spraak of video) en om het effect van latency-ingevoelig verkeer (zoals bulkgegevensoverdrachten) te beheersen.

31. Wat is RIPv1? RIPv2?

Routing Information Protocol (RIP) is een afstand-vectorprotocol dat door routers wordt gebruikt voor de uitwisseling van routinginformatie. RIP gebruikt hoptelling als zijn routing metriek. RIP voorkomt het verzenden van lijnen om voor onbepaalde tijd door een grens op het aantal hop toe te passen die in een weg van de bron naar een bestemming is toegestaan. Het maximum aantal hop voor RIP is 15 dat de netwerkgrootte beperkt die het kan steunen. Dit is de reden dat het RIPv2 werd ontwikkeld. In tegenstelling tot het klastige RIPv1, is RIPv2 een klasloos routeringsprotocol dat de subnetmaskers omvat wanneer het zijn routingupdates uitstuurt.

Het samenvatten van routes in RIPv2 verbetert schaalbaarheid en efficiëntie in grote netwerken. Het samenvatten van IP adressen betekent dat er geen ingang voor kindroutes (routes die voor elke combinatie van de individuele IP adressen in een samenvattend adres worden gecreëerd) in

de routingtabel van RIP is, die de grootte van de tabel beperkt en de router toestaat om meer routes te behandelen.

32. Wat is Smart Link Backup?

Smart Link Backup is een functie waarmee de gebruiker een tweede WAN kan instellen als de eerste of de primaire link faalt. Deze optie wordt gebruikt om te verzekeren dat de communicatie tussen WAN en het apparaat altijd ononderbroken is. Deze optie wordt gevonden in routers met dubbele WAN-verbindingen.

33. Wat is SSL VPN? Wanneer zou je het gebruiken?

Een Secure Socket Layer Virtual Private Network (SSL VPN), ook bekend als WebVPN, is een technologie die VPN-mogelijkheid op afstand biedt met behulp van de SSL-functie die in een moderne webbrowser is ingebouwd. Dit vereist niet dat u een VPN client op het apparaat van de client installeert. SSL VPN geeft gebruikers van elke door internet ingestelde locatie de mogelijkheid om een webbrowser te starten om VPN-verbindingen op afstand te maken, waardoor productiviteitsverbeteringen en een betere beschikbaarheid worden beloofd, evenals verdere kostenvermindering voor IT voor VPN-clientsoftware en -ondersteuning.

34. Wat is VPN-passthrough?

VPN PassThrough is een manier om twee beveiligde netwerken via het internet aan te sluiten. Dit wordt gebruikt om VPN-verkeer toe te staan dat gegenereerd is door VPN-clients die aangesloten zijn op de router om door te gaan naar het internet en om de VPN-verbinding te laten slagen.

35. Wat is VPN?

Een Virtual Private Network (VPN) is een beveiligde verbinding die binnen een netwerk of tussen netwerken is opgezet door een tunnel te maken. VPNs dient om verkeer tussen gespecificeerde hosts en netwerken te isoleren van het verkeer van onbevoegde hosts en netwerken. VPN's zijn voordelig voor bedrijven op dusdanige wijze dat het zeer schaalbaar is, de netwerktopologie vereenvoudigt en de productiviteit verbetert door reistijd en kosten voor externe gebruikers te reduceren.

36. Waarom zou ik de subnetmasker-waarden wijzigen?

Een net is een gedeelte van een netwerk dat een deeltjesvermetaal adres deelt. Een subnetmasker is een 32-bits combinatie die wordt gebruikt om te beschrijven welk gedeelte van een netwerkadres naar het net verwijst en welk deel naar de host verwijst. Een beheerder kan de netto maskerwaarden willen veranderen in het geval dat een gastheer niet met het netwerk kan communiceren. Subnetmaskers kunnen ook worden gewijzigd voor het geval dat een beheerder het aantal hosts op een subnetwerk wil verhogen zonder dat hij fysieke wijzigingen hoeft aan te brengen.