Knowledgebase > Voice > Best Practices for VoIP- Dual WAN Failover and Load Balancing

Best Practices for VoIP- Dual WAN Failover and Load Balancing

Jeff Pipitone - 2026-01-27 - Comments (0) - Voice

Dual WAN failover and VoIP

Implementing dual WAN failover for VoIP can be a beneficial strategy to enhance reliability and reduce downtime. However, there are potential negative impacts that should be considered. Here are some common issues and suggestions on how to address them:

1. **Latency and Jitter:**
    - **Issue**: Switching between WAN connections can introduce latency and jitter, negatively impacting call quality.
    - **Resolution**: Prioritize low-latency WAN connections, and configure Quality of Service (QoS) settings to give priority to VoIP traffic. Choose WAN connections with consistent performance and low latency.
2. **Out-of-Sequence Packets**:
    - **Issue**: Packets arriving out of order can lead to disruptions in voice quality.
    - **Resolution**: Implement mechanisms like Forward Error Correction (FEC) and use routers that support reordering of packets. This can help ensure that even if packets arrive out of sequence, they are reorganized correctly.
3. **Session Interruptions during Failover:**
    - **Issue**: VoIP calls may experience interruptions during the failover process.
    - **Resolution**: Opt for WAN failover solutions with sub-second failover times to minimize disruptions. Additionally, use Session Initiation Protocol (SIP) trunk redundancy or survivable remote site telephony (SRST) for call continuity during failover.
4. **Impact on VoIP Bandwidth:**
    - **Issue**: Failover processes may lead to increased bandwidth usage, affecting other applications and potentially causing congestion.
    - **Resolution**: Monitor bandwidth usage closely and consider implementing traffic shaping or bandwidth management policies to ensure that VoIP traffic is prioritized without monopolizing available bandwidth.
5. **Configuration Complexity:**
    - **Issue:** Configuring and managing dual WAN failover systems can be complex, leading to potential misconfigurations.
    - **Resolution**: Use simplified and intuitive failover solutions. Regularly audit and update configurations to ensure they align with current network requirements. Consider utilizing SD-WAN (Software-Defined Wide Area Network) solutions for more automated and dynamic failover management.
6. **Compatibility Issues with VoIP Providers:**
    - **Issue**: Some VoIP providers may not support dual WAN failover configurations, leading to compatibility issues.
    - **Resolution**: Consult with your VoIP service provider to ensure compatibility with dual WAN configurations. Consider providers that offer support for diverse network setups and can provide guidance on optimizing performance.
7. **Security Concerns**:
    - **Issue**: Failover mechanisms may expose the network to potential security vulnerabilities during the transition.
    - **Resolution**: Implement secure failover protocols and regularly update and patch network equipment. Use encryption for VoIP traffic to enhance security during failover transitions.
8. **Equipment Reliability**:
    - **Issue**: The reliability of the failover equipment itself can impact VoIP service.

- **Resolution**: Invest in high-quality networking equipment and ensure that failover devices are regularly maintained and tested. Consider redundant hardware for critical failover components.

By addressing these potential issues proactively, businesses can optimize their dual WAN failover setup to enhance VoIP performance and minimize disruptions to communication services. Regular testing and monitoring are essential components of maintaining a robust and reliable dual WAN failover system for VoIP.

Load Balancing and VoIP

While load balancing is a valuable technique for optimizing network performance, it can introduce challenges for VoIP (Voice over Internet Protocol) due to the real-time nature of voice communication. Here are some negative impacts of load balancing on VoIP and suggested resolutions:

1. **Latency and Jitter**:
   - **Issue**: Load balancing can route VoIP traffic unevenly, leading to varying latency and jitter, which negatively affect call quality.
   - **Resolution**: Prioritize low-latency paths for VoIP traffic. Implement Quality of Service (QoS) settings to give priority to voice packets, ensuring they traverse the network with minimal delays.
2. **Out-of-Order Packets**:
   - **Issue**: Load balancing may cause packets to take different paths, resulting in out-of-order packet delivery and potential voice quality degradation.
   - **Resolution**: Use load balancing algorithms that maintain packet order or implement measures like Forward Error Correction (FEC) to correct errors and ensure proper packet sequencing.
3. **Session Persistence**:
   - **Issue**: VoIP sessions require consistent routing to prevent call disruption. Load balancing might lead to sessions being split between different paths.
   - **Resolution**: Utilize load balancing algorithms that support session persistence or sticky sessions, ensuring that VoIP packets follow a consistent path for the duration of a call.
4. **Impact on Bandwidth Allocation:**
   - **Issue:** Load balancing decisions might allocate bandwidth unevenly, potentially causing congestion and impacting VoIP quality.
   - **Resolution**: Regularly monitor bandwidth usage and adjust load balancing algorithms to ensure fair distribution of traffic. Implement traffic shaping to prioritize VoIP traffic and prevent it from being overwhelmed by other data.
5. **Security Concerns**:
   - Issue: Load balancing may expose VoIP traffic to security vulnerabilities, especially if it involves routing through less secure paths.
   - Resolution: Implement secure load balancing protocols and ensure that all paths used for VoIP traffic are appropriately secured. Use encryption for VoIP traffic to enhance security during load balancing.
6. **Complex Configuration**:
   - **Issue**: Load balancing configurations can be complex, leading to misconfigurations that affect VoIP performance.
   - **Resolution**: Simplify load balancing configurations where possible. Regularly audit and update configurations to align with current network requirements. Consider leveraging SD-WAN (Software-Defined Wide Area Network) solutions for more automated and dynamic load balancing.
7. **Compatibility Issues**:
   - **Issue**: Some VoIP systems may not be fully compatible with certain load balancing algorithms or configurations.
   - **Resolution**: Consult with VoIP system vendors to ensure compatibility with your chosen load balancing setup. Choose load balancing solutions that provide flexibility and compatibility with real-time communication protocols.
8. **Continuous Monitoring and Testing**:
   - **Resolution**: Regularly monitor the performance of VoIP traffic under load balancing conditions. Conduct testing and simulations to identify potential issues before they impact real-time communication.

Balancing the benefits of load balancing with the requirements of VoIP demands careful configuration and monitoring. By addressing these potential issues, organizations can optimize load balancing for their specific VoIP needs and ensure consistent, high-quality voice communication across their network.

Example- How to Configure Session Affinity, QOS, and Dedicated Internet Connection on SonicWall

Configuring session affinity, Quality of Service (QoS), and dedicating a specific Internet connection for VOIP on a SonicWall firewall involves accessing the device's management interface and making the necessary adjustments. Keep in mind that the exact steps may vary based on the model and firmware version of your SonicWall device. Always refer to the official SonicWall documentation for your specific device and firmware version.

Session Affinity (Sticky Sessions):

- Log in to the SonicWall management interface.
- Navigate to the "Load Balancer" or "Network" settings, depending on your SonicWall model.
- Look for the option related to session affinity or sticky sessions. Enable this feature.
- Configure the session timeout value. This determines how long a session should stay bound to a specific Internet connection.
- Save your changes and apply the configuration.

Quality of Service (QoS):

- Access the SonicWall management interface.
- Navigate to the "Security Services" or "QoS" section.
- Look for the QoS settings or policies. You may need to create a new policy for VOIP traffic.
- Specify the criteria for identifying VOIP traffic. This may include source and destination IP addresses, ports, or specific protocols.
- Set the priority for VOIP traffic. Ensure that VOIP traffic is assigned a higher priority than other types of traffic.
- Save the QoS configuration.

Dedicating a Specific Internet Connection for VOIP:

- Log in to the SonicWall management interface.
- Go to the "Network" or "Load Balancer" settings.
- Look for the option to specify routing or path selection.

- Tags
- best practices
- dual wan
- failover
- hosted voice
- load balancing
- microsoft teams
- voip