A Preliminary Analysis of Dual-Active Unified Gateway and Security Implementation for Press Networks and Internet (Postprint)

Authors: Jin Jianming

Date: 2023-10-08T00:00:00+00:00

Abstract

Objective: To enhance the efficiency, dual-active capability, and security of network and Internet egress links for press groups.

Methods: Wenzhou Daily Press Group innovatively employed a basket-based approach to achieve flexible combination of various egress services on load balancing devices; and adopted DRNI (Distributed Resilient Network Interconnect) cross-device link aggregation technology in the switching network, which not only realizes link dual-active capability and aggregation, but also provides high-level load balancing and security.

Results: The system enables rapid detection and disposal of various network security threats, and easily mitigates the impact on the group' s entire network egress when localized services are under attack.

Conclusion: Following implementation, the project has achieved excellent results in the network and egress security operation and maintenance of Wenzhou Daily Press Group, and provides valuable reference and guidance for peer press groups in constructing efficient, secure, and dual-active networks and Internet egress.

Full Text

Analysis on the Dual-Active and Security Construction of Unified Newspaper Network and Internet Exit

Wenzhou Daily Press Group, Wenzhou, Zhejiang 325000

Abstract

[**Objective**] To enhance the efficiency, dual-active capability, and security of the newspaper group' s network and internet exit links. [**Method**] Wenzhou

Daily Press Group innovatively employed a "basket-based" approach to flexibly combine various exit services on load balancing devices, while implementing DRNI (Distributed Resilient Network Interconnect) cross-device link aggregation on the switching network. This not only achieved dual-active link aggregation but also delivered high-performance load balancing and enhanced security. [**Result**] The solution enables rapid detection and timely handling of various network security threats, easily mitigating the impact of localized attacks on the group's entire network exit. [**Conclusion**] Since project completion, the system has demonstrated excellent results in network and exit security operations at Wenzhou Daily Press Group, offering valuable reference and guidance for peer newspaper organizations undertaking similar construction of efficient, secure, and dual-active network and internet exit infrastructure.

Keywords: bandwidth; redundancy; dual-active; load balancing; basket-based grouping

1. Necessity of Network and Exit Security Transformation at Wenzhou Daily Press Group

In 2007, Wenzhou Daily Press Group (hereinafter referred to as "the Group") introduced three internet fiber lines from different carriers (Telecom 1G, Netcom 1G, Mobile 500M) and deployed load balancing equipment as the unified internet exit for the Group. All internal internet access and external access to the Group's websites, video platforms, and new media services pass through these three fibers. Because there is only a single unified exit, any network anomaly can potentially impact the Group's global network access, imposing stringent requirements on the security, efficiency, and stability of exit equipment. At that time, few newspaper groups adopted a unified exit approach; most deployed two completely independent internet exits for internal office external access and DMZ external-to-internal access to avoid mutual interference.

1.1 Performance of Original Network and Exit Security Equipment

The original infrastructure comprised two F5 load balancers and two Juniper firewalls configured only for dual-machine hot standby rather than dual-active operation. Netentsec behavior management devices were serially connected between them (creating a single point of failure). The firewalls connected downstream to two hot-standby Extreme 8810 core switches and a gigabit WAF firewall, which then connected to the DMZ aggregation switch. With increasing network threats and attacks, the network and security equipment purchased over a decade ago could no longer meet high-intensity protection requirements, necessitating a comprehensive transformation of the Group's network and exit security.

1.2 Pain Points of Original Architecture: Lack of Dual-Active Capability and Insufficient Bandwidth

The original exit network and security equipment employed a master-backup architecture where all business traffic was handled by a single active device; backup devices could not share the online load. When a Group website suffered a high-traffic attack, it would degrade internet speed for all internal-to-external access and affect access speeds for other Group websites, potentially causing complete interruption and severely impacting normal operations. Furthermore, all core network and security device interfaces were limited to 1G rates, risking network congestion when total peak traffic exceeded 1G. Additionally, individual equipment carried single-point failure risks.

2. Design Philosophy for New Network and Internet Exit Construction

The new network and exit must address these pain points by ensuring security, dual-active capability, and load distribution. Dual-active operation requires at least dual redundancy for each device. However, stringing numerous dual security devices in series at the internet exit would incur prohibitively high costs and complicate dual-active implementation. Therefore, equipment selection must minimize device quantity while integrating maximum functionality within each device. The design philosophy is: achieve online dual-active operation with minimal equipment while ensuring functional requirements; incorporate powerful and detailed statistical analysis capabilities to facilitate future network optimization and troubleshooting. Core network and security device interfaces must be upgraded from 1G to 10G, with all vertical backbone links upgraded to 10G and horizontal cabling reaching 1G. All network devices must support cross-device link aggregation to enhance link stability, achieve load distribution, and provide flexible port mirroring capabilities.

3. Features of New Equipment

The Group introduced two NetGod NSG7000-TX10M-Q next-generation firewalls, two A10 TH3030S load balancers, one Anheng WAF-3000AG, and H3C network equipment for full network replacement. The new equipment deployment maintained the Group' s overall network architecture with minor adjustments: since all new devices feature 10G interfaces, the Netentsec gigabit devices were moved to the core switches for bypass deployment, also eliminating single-point failures. The transformed network topology is shown in Figure 1 [Figure 1: see original paper].

3.1 H3C Switches Supporting DRNI Technology

DRNI (Distributed Resilient Network Interconnect) is a cross-device link aggregation technology that enhances reliability from single-board level to device

level. This transformation employs H3C S10510X core switches, LS-7503E aggregation switches, and S5130 floor switches, all supporting DRNI for link aggregation. This significantly simplifies network configuration while increasing bandwidth, improving link stability, and enabling load distribution. The core adopts an advanced CLOS multi-stage multi-plane switching architecture, enhancing sustainable bandwidth upgrade capabilities to accommodate varying network scales and performance requirements. The new core switches deliver switching capacity $\geq$ 700 Tbps, packet forwarding rate $\geq$ 96,000 Mpps, with all fiber interfaces at 10G (supporting up to 100GE), representing a tenfold performance improvement over the original Extreme cores. They support bidirectional ACL, port ACL, and VLAN ACL, meeting the Group' s original ACL-based isolation and access control requirements for subsidiary publications.

3.2 Multi-Functional Integrated Firewall

As a boundary security device, firewalls isolate internal and external networks —shielding internal networks while blocking external threats and illegal access. In today' s environment of frequent security vulnerabilities and rampant network attacks, deploying a high-bandwidth, high-performance, multi-functional next-generation firewall is particularly crucial. The newly deployed NetGod NSG7000-TX10M-Q next-generation firewall achieves 42 Gbps throughput and integrates conventional NAT, protocol identification, IPS module, virus detection gateway, situational awareness, zombie host detection, and threat cloud detection applications, significantly enhancing boundary security protection capabilities. The firewall provides comprehensive monitoring metrics including session count, traffic volume, various threat quantities, and protocol application ratios, with powerful log analysis and clear result presentation. For network anomalies during specific periods, investigation through various abnormal indicators can ultimately identify corresponding hosts and IPs for mitigation.

3.3 A10 TH3030S Load Balancer with Integrated DDoS Protection and Application Acceleration

The A10 TH3030S load balancer achieves Layer 4-7 throughput $\geq$ 30 Gbps, maximum concurrent connections $\geq$ 20 million, and $\geq$ 6 10G interfaces, with integrated DDoS protection and application acceleration capabilities. The device supports graphical traffic visualization, which proves extremely useful for network troubleshooting.

3.4 High-Performance Web Application-Level Intrusion Prevention WAF System

The newly deployed Anheng WAF-3000AG delivers application-layer throughput $\geq$ 8 Gbps, concurrent connections $\geq$ 400,000, new connections per second $\geq$ 40,000, business latency $<$ 50ms, and unlimited protected sites. The new WAF features CC attack protection, identification of malicious requests such

as cross-site scripting (XSS) and injection attacks, protection against HTTP request segmentation attacks and HTTP response truncation attacks, capability to identify website trojans, and prevention of trojan page access through policies. It can also analyze access behavior characteristics to identify hotlinking and crawler attacks.

4. Project Innovation: Pioneering Basket-Based Dual-Active Architecture

This project innovatively designed the Group' s exit security equipment with a dual-active architecture that addresses original system pain points. It pioneered the successful application of service grouping by category (i.e., "baskets") for network attack emergency response at the exit, preventing attacks on specific websites from affecting other normal operations. Based on business nature, internal and external access channels were divided into four baskets: Basket A contains internal-to-external internet access business, Basket B contains external website services for various publications, Basket C contains Wenzhou Net Phase II (client website services), and Basket D contains the Wenzhou Net main site which is frequently attacked. These four baskets can operate in any combination across the two A10 load balancers, typically running two baskets on each A10 under normal conditions (as shown in Figure 2 [Figure 2: see original paper]). When Basket D is under attack, it can operate independently on one A10 while the other three unaffected baskets run on the other A10, maximizing business continuity (as shown in Figure 3 [Figure 3: see original paper]). Furthermore, the two firewalls can be separated to split the unified exit into two independent exit links, allowing attacked Basket D to exit through a completely independent link and eliminating mutual interference (as shown in Figure 4 [Figure 4: see original paper]). In 2021, when a Group website suffered a large-scale DDoS attack, this method was employed for handling, essentially without impacting other normal operations.

5. Practical Applications and Benefits

5.1 Rapid Identification of "Unknown" Traffic Attacks

Before new equipment deployment, the Group's network exit occasionally experienced intermittent one-to-two-minute interruptions. Due to limited monitoring and analysis capabilities of the decade-old load balancers and firewalls, coupled with irregular occurrence times making packet capture analysis difficult, the root cause remained unidentified. After new equipment deployment, the A10' s graphical network metrics visualization quickly resolved this puzzle. During a large-traffic attack, the team examined network waveforms and discovered the Telecom 1G bandwidth was saturated (as shown in Figure 5 [Figure 5: see original paper]), while the A10' s upstream Unicom/Mobile ports and downstream firewall e9 port showed no large traffic, quickly determining the attack originated from the Telecom line. To identify which internal server was targeted,

the team examined virtual servers on the A10 (each corresponding to a physical server) for the same period and found traffic patterns matching the attack characteristics (as shown in Figure 6 [Figure 6: see original paper]). Figure 6 shows server 99.27' s traffic and concurrency suddenly spiking then dropping to zero—consistent with attack-then-disconnection patterns. The team rapidly identified it as an NTP-flood attack via UDP port 123 and resolved it through appropriate protection measures.

5.2 Rapid Identification of High-Risk Internal Hosts

With over 1,500 internal computers, some with inadequate protection could be compromised by trojans or remote control. Previously, identifying high-risk internal computers relied on Netentsec' s top-10 traffic rankings, yielding high false-positive rates. The new NetGod firewall' s situational awareness, zombie host detection, and threat cloud detection functions can directly identify potentially compromised high-risk hosts from multiple dimensions including traffic, concurrency, protocols, and ports, presenting them in a clear list (as shown in Figure 7 [Figure 7: see original paper]). Following up on IPs from Figure 7, most computers indeed had issues, though 172.27.4.75 was a false positive—a domain controller + DHCP server whose concurrency and traffic exceeded thresholds, causing it to be flagged. Adding it to a whitelist resolved the issue.

5.3 Using Firewall to Investigate Streaming Media Call Failures Caused by DDoS Protection

Between January and March 2022, an App server in the DMZ zone experienced intermittent or interrupted video streaming calls to an internal video server three times. The call path traversed DMZ aggregation switch → WAF → exit firewall → core switch → internal firewall. Since it used port 80, bypassing or restarting the WAF temporarily resolved issues (effectively resetting the link), leading to assumptions that WAF interception was the cause. However, no relevant logs were found on the WAF. Investigation in the NetGod firewall' s analysis center revealed numerous HTTP streaming threat alerts during failure periods (as shown in Figure 8 [Figure 8: see original paper]). During the next occurrence, packet capture at the firewall showed numerous request packets arriving but few reaching the internal video server, indicating packets were being intercepted and dropped. The App server' s requests were hitting the rb-front-web-2 policy, which triggered DDoS protection when HTTP GET requests with video file extensions (flv, mp4) exceeded traffic thresholds, causing request packet drops and intermittent service interruption. Adjusting the DDoS threshold in the rb-front-web-2 policy temporarily resolved the issue.

5.4 Resolving Potential Network Disruption from VLAN Flapping and Achieving More Efficient, Stable Switching

The Group' s original Extreme switches used the ESRP protocol (similar to VRRP) with a master-backup core architecture. Since publications were divided

into multiple VLANs by business function with one master VLAN, all slave VLANs would drift with the master VLAN during core switchover. If a floor' s link to the master switch failed, that publication' s master VLAN would migrate to the backup core, moving all slave VLANs simultaneously. If another floor had link issues to the backup core while its switch also contained that publication' s VLAN, that floor' s switches would lose connectivity and cause network disruption. The DRNI cross-device link aggregation implementation bundles floor uplinks to the S10510X core switches, resolving such disruption while increasing bandwidth. Disconnecting any single uplink line from a floor switch does not affect network operation for that floor or others.

5.5 Simplified Port Mirroring for Security Device Data Sources

The original core switches only supported many-to-one port mirroring, making it inconvenient to connect behavior management and situational awareness bypass devices. The new H3C switches support many-to-one, one-to-many, and many-to-many port traffic mirroring, providing rich port mirroring support for the Group' s situational awareness devices, behavior management equipment, and data packet capture.

The project originally intended to implement dual-active firewalls for better load distribution, but the complexity of monitoring numerous downstream links and switchover processes risked network instability, so firewall dual-active was abandoned. Wenzhou Daily Press Group was among the earliest newspaper groups to integrate internal-to-external and external-to-internal access into a unified exit architecture. In this structure, attacks or abnormal traffic on any Group website could impact all users' external access or even cause complete interruption. The dual-active architecture with load balancing for network and security equipment has resolved long-standing pain points in network switching and exit security. The new equipment significantly improves performance, functionality, and security, with the firewall and WAF each intercepting over 400 million threats annually—well-suited for today' s complex network environment with numerous threats and frequent attacks on news websites. Since deployment, it has effectively safeguarded Group website and network security, particularly during critical periods such as the 100th anniversary of the Communist Party of China and the 20th Party Congress.

References: [1] Cross-device Link Aggregation—Understanding DRNI Technology in One Article [EB/OL]. Chinese Professional IT Community CSDN, https://blog.csdn.net/weixin_{39664998}/article/details/111364209, 2020-11-19/2023-03-25. [2] NTP Amplification Attack [EB/OL]. Blog Garden (Developer' s Online Home), https://www.cnblogs.com/autopwn/p/14694221.html, 2021-04-23/2023-03-13.

Author Bio: Jin Jianming (1974-), male, from Cangnan, Zhejiang, Senior Engineer. Research interests include project management, planning, design,

and construction of computer, network, and audio-video system integration.

(Editor: Zhang Xiaojing)

Note: Figure translations are in progress. See original paper for figures.