Point of View

Networking Is Not an Island—or Shouldn't Be, Anyway

Why, and How, Networking Teams Need to Partner with Security

Divergent Perspectives on the Corporate Infrastructure

Networking and security teams see the same world from vastly different points of view. Networking professionals are primarily concerned with systems' availability and performance. These are the factors that they are evaluated on, and they hear—loud and clear—about any failures or connectivity issues. Thus, many networking teams see the organization's IT infrastructure as a utility. Their goal is to provide uninterrupted, quality service, and they monitor the network's success from a high level.

Meanwhile, security staff have an inverse, highly granular point of view. They are responsible for preventing cyberattacks, which means they are charged with determining whether each specific network packet should be allowed to go wherever it's headed. Performing effective analyses requires a focus on the minute details of network traffic.

Neither perspective is the inherently "right" way to view a technology infrastructure. In fact, both are crucial to providing the environment that a modern business requires. But the differences between them can lead to conflict and ultimately challenges in delivering business initiatives.

It's worth noting that the dichotomy in viewpoints originated in the traditional division of labor between network and security operations. Because all important IT assets used to be contained within the company's network perimeter, security and networking professionals generally agreed that if the organization could keep bad actors out, it would have security under control. The security team focused on protecting the network edge, while the networking team took responsibility for everything happening inside that perimeter.

Today, limiting security activities to the network edge is dangerously inadequate. As more and more employees are now working remotely, and business applications have started moving to SaaS and cloud models, the new business landscape has dramatically expanded the corporate attack surface. This has forced network and security teams to find new ways to enable connectivity while actively protecting traffic flows throughout the modern network, inspecting data moving among internal systems, out to the network edge, and up into the cloud.

The relationship between networking and security teams should reflect this natural evolution in responsibilities—but in many companies, it doesn't.

According to a study by Enterprise Management Associates:

75%

More than 75% of IT organizations have seen an increased need, over the past few years, for collaboration between networking and cybersecurity teams.

39%

Only 39% of organizations believe these collaborations have been fully successful.[1]

[1] Shamus McGillicuddy. "3 steps to better collaboration between networking and security pros," Network World, Nov. 15, 2021.

A Tradition of Dysfunction

The difference in perspectives across security and networking teams has resulted, at many companies, in a dysfunctional relationship that may harm the business's ability to innovate. When the networking group initiates an improvement project of some kind, security may be a mere afterthought. Rather than including security colleagues in the project design from the outset, networking professionals may wait until the initiative is near completion to bring them into the loop.

This essentially turns the security team into a stop sign. Projects designed to upgrade availability or network performance must clear the security hurdle before they can move forward. Those that don't pass muster with security decision-makers cannot proceed; the networking team may have to go back to the drawing board to better meet the company's security mandates. This approach opens the door for tensions between the two groups.

On a more granular and day-to-day level, security solutions may frequently prevent the network from delivering data packets to their intended destination. Whenever this happens, the networking team might have to field calls from users whose applications aren't performing as expected. In fact, they might have to prove that the problem is not a network outage before even bringing security into the conversation.

Both scenarios—projects that must be redesigned to meet security requirements, and security solutions that frequently block network traffic—can slow down business improvements and impede staff productivity. This can generate hard feelings between the teams, as well as blowback from the business. Neither team ends up looking very good to the broader organization.

> "We're brought in early in the networking team's development cycle to make sure the code created is truly secure. We aren't finding out just ahead of production so that we're left to decide if we let it go as 'insecure' or get accused of stopping progress."
>
> Tim Callahan, CISO,
> Aflac (quoted in Network World)[2]

Success: Networking and Security Working in Tandem

The alternative, which minimizes friction between security and networking, is to have the teams work together on every project, from its launch onward. With this approach, professionals from both functions routinely collaborate to build a technology infrastructure rooted in a zero trust framework that is simultaneously high-performing and secure. They join forces to enable distributed users, located outside the company's four walls, to safely and efficiently access corporate resources, some of which may reside in the cloud.

[2] Sandra Gittlen. "How to boost collaboration between network and security teams," Network World, Dec. 21, 2018.

When the security team is deeply involved in most everything the networking group does, life is better for everyone. Consider, for example, the improvement to productivity throughout both teams when security solutions' logs get dialed in effectively. As fewer false-positive alerts come through, the security group can focus their energies on stopping the true threats to the business. And the reduction in noise means the networking team no longer faces constant, unnecessary distractions related to security issues.

This might sound idyllic, but it is not easy without network security transformation. For most companies, the transition to such collaboration is daunting. Not only are human behaviors often stubbornly difficult to change, but most networks are replete with legacy assets, which may not even be capable of meeting current security standards. The key to success lies in the adage "How do you eat an elephant? One bite at a time." When a key category of security hardware, such as the network's firewalls, needs a refresh, networking and security can take a first step toward long-term collaboration by jointly evaluating whether the company's approach to network protection is still effective in the "new normal."

Another approach to security that can help foster the needed shift in mindset is zero trust. The concept, which entails not implicitly trusting anyone, makes sense to most security professionals who are no longer comfortable focusing only on the network edge. With zero trust, users can access only those resources they have been explicitly approved to access—and only after their identity has been confirmed.

A side effect of adopting a zero trust mindset is that the security team needs to be involved in every step of network architecture design and deployment. Zero trust essentially forces the networking team to meet with security architects on a regular basis. It creates a cohesive and collaborative approach to network and security improvements, because there is simply no way to implement a zero trust network architecture without involving security professionals in the earliest stages of planning and design.

Think of the networking team as a delivery driver. Packages are loaded onto their truck, and their responsibility is to transport those packages to their final destination. The delivery company may also have, somewhere in the organization, security personnel who are tasked with ensuring that drivers do not deliver dangerous packages. When a box looks suspicious, they may scan it to ensure that it does not contain malicious materials.

What zero trust does is place a security guard on each delivery truck. The guard is responsible for preventing delivery of anything suspicious, which means that the only way any packages can reach their destination is if the driver and security guard communicate about the safety and delivery route for each package. Like our delivery team, security and networking professionals must work closely together for a zero trust infrastructure to be successful.

---

[3] Sandra Gittlen. "How to boost collaboration between network and security teams," Network World, Dec. 21, 2018.

Where to Start

The first step in building a more collaborative culture for the networking and security teams is to establish a regular meeting schedule for the company's CISO and CIO. The appropriate frequency for these meetings will depend on the organization—including factors such as market segment and company size—but maintaining a regular schedule is crucial. Relationship building starts at the top.

When they meet, the leaders should discuss their teams' tactical goals and strategic objectives, clarifying whether networking and security are effectively aligned. Open, and ongoing, communication between the CISO and CIO helps ensure that their teams are moving in the same direction, rather than working at cross-purposes. From there, the collaborative spirit should naturally flow down into lower levels of the organization.

Partnerships between individual security and networking professionals need to be tight. Team members should have frequent meetings, and communication should be close to continuous among staff who are working together on specific projects. Bringing the granular security point of view and the big-picture networking perspective into the same room on a regular basis encourages both teams to jointly work through concepts, ideas, and project plans while there is plenty of time to tweak initiatives to meet everyone's needs.

In this era of rapid change and heightened business agility, delays in engineering and design cycles are not acceptable. But implementing changes that introduce security vulnerabilities is also not acceptable. The best approach to support corporate innovation is for security and networking professionals to work together from day one.

> "IT directors and security leaders must model the close relationship they want from their teams, because if they don't get along, their teams won't get along."
>
> Chris Calvert, Co-founder, Respond Software (quoted in Network World)

Initiatives That Test the Waters for Collaboration

Here are several ideas for launching specific projects that can build collaboration between networking and security teams.

Before selecting your first collaborative project, evaluate your organization's pain points.

- What are your network engineers spending their time on? What proportion is keep-the-lights-on activity (maintenance, patching, upgrades, etc.)?
- Where is security creating the most latency for users' interaction with applications or data?
- What would be the benefits of improving the pain points you uncover?
- Establish a combined set of goals rooted in a zero trust framework.

Consider securing web traffic as a first joint project.

- Companies have long used web filtering to prevent users from visiting off-limits sites, such as pornography or gambling sites.
- A traditional web filter is on-premises hardware, which means that all users' internet traffic is typically backhauled to the corporate data center.
- Backhauling remote users' web traffic to the data center is illogical.
- Security and networking groups can collaborate to find more efficient ways to secure web traffic from their distributed users going to distributed locations.
- What are your data governance and compliance requirements?

Consider finding a way to protect users without requiring virtual private network (VPN) access.

- VPNs also require backhauling traffic to the data center, which is tedious for remote users accessing cloud resources.
- Determine the priority of this project by looking at the proportion of users who work outside of corporate offices, and the proportion of applications that reside outside of the data center. It simply does not make sense to route all traffic through the data center when a majority of that traffic is now going to the web.
- Look at options for steering traffic directly to where it needs to go, such as to a hyperscaler, or SaaS app, while also providing necessary protections.
- This approach would probably increase application performance for users. It would also enhance security and performance of the internal network by decreasing the amount of unnecessary traffic passing through the data center. So, it's a win-win.
- For companies considering replacing their VPN, it would likely also make sense to add a zero trust strategy that removes implicit trust of anyone who's inside the data center perimeter, as well as to refine least-privilege access and continuously monitor.