perimeter 81

The Easy Way to M&A:
Merging Networks After an Acquisition



perimeter 81

In two words, you can sum up what it's like for companies to merge or for one to acquire the other: it's complicated. There are so many tasks to take care of from questions of corporate culture, to regulatory requirements to, yes, Information Technology. Here at Perimeter 81 we aim to make the latter part of this process as painless and seamless as it can be.

Sure, securing networks is no small task when an IT team is faced with managing two networks – or possibly more if the board's gone on a spending spree. It can be a real pain, because the overarching principle must be to maintain network stability. At the same time upper management wants to see a measure of unification between the two company networks.

Some companies may prefer to keep the networks separate–especially helpful when we're talking about an acquisition that will remain a subsidiary. However, when the acquired organization is going to be absorbed by the parent company then a complete merge between the two networks often makes sense.

Perimeter 81's platform can help in either of these scenarios since we can serve as the joining point between the two company networks. This makes it much easier to bring together disparate cloud services and on-prem resources into a single network, without sacrificing a lot of valuable time and resources.

Whether it's one, two, or three networks the basic strategy remains the same:

With Perimeter 81, CISOs can trust their IT teams to create, manage and monitor the company's network from a unified platform.



Gain control and visibility over the new networks



Move the new company under the Perimeter 81 umbrella as a separate tenant or network



Align identity providers (IdP) and implement single sign-on (SSO)



Begin the transition to a single network

All rights reserved. Perimeter 81 | 2023

perimeter 81

Gain Control and Visibility

The first step is to assess the acquired company's network and see what it includes in terms of user devices, servers, and cloud services. This may have been done to some extent during the original M&A process; however, it's always good to verify that all the information is still valid, and that no new services, servers, or appliances have been added or removed.

The final inventory list should include all important assets and resources that are inside the network such as primary data centers, and the various cloud services that the acquired company uses. In addition, user devices should take up a second list.

The point of this step is not only to understand what the various assets are inside a network, and how to manage them, but also to reveal commonly used applications or systems with the parent company. These can often be the first points where companies can merge or speed up some of the changes. A shared cloud provider, for example, may have easy ways for two accounts to merge into one, allowing you to view all company assets from a single account.

In addition to understanding what you have, it's critical to dig into the state of in-house servers. Are they up-to-date on patches, for example? Are there any issues in the logs that may indicate the presence of threat actors? How many legacy applications are running on outdated servers that will need to be moved over as-is, or is there a chance to use this merger as a chance to modernize the systems of the acquired company? These are all critical questions to figure out as part of the merger.

Once you have an understanding of everything that's in the acquired company's network, and gain access in order to control those endpoints and services, the next step is more likely to go smoothly.

Once you have an understanding of everything that's in the acquired company's network, and gain access in order to control those endpoints and services, the next step is more likely to go smoothly.

All rights reserved. Perimeter 81 | 2023

perimeter 81

Align Identity Providers and Implement SSO

One of the wonderful things about using Perimeter 81 to align networks is that the two companies don't necessarily need to start out with the same IdP. Perimeter 81 supports all of the major identity providers such as Azure Active Directory, Auth0, Google, Okta, OneLogin, and JumpCloud.

Perimeter 81 supports all of the major identity providers such as Azure Active Directory, Auth0, Google, Okta, OneLogin, and JumpCloud

To start, the acquired company can authenticate with their current logins to maintain network stability, and then IT can start changing them over to the company's standard IdP, if necessary.

We make it easy to transition since your primary IdP provider is already registered with Perimeter 81. We highly recommend, however, that you use an IdP that supports SSO, which will make it easier to integrate with cloud providers and reduce the number of times employees have to login per day.

Moving to the Perimeter 81 umbrella

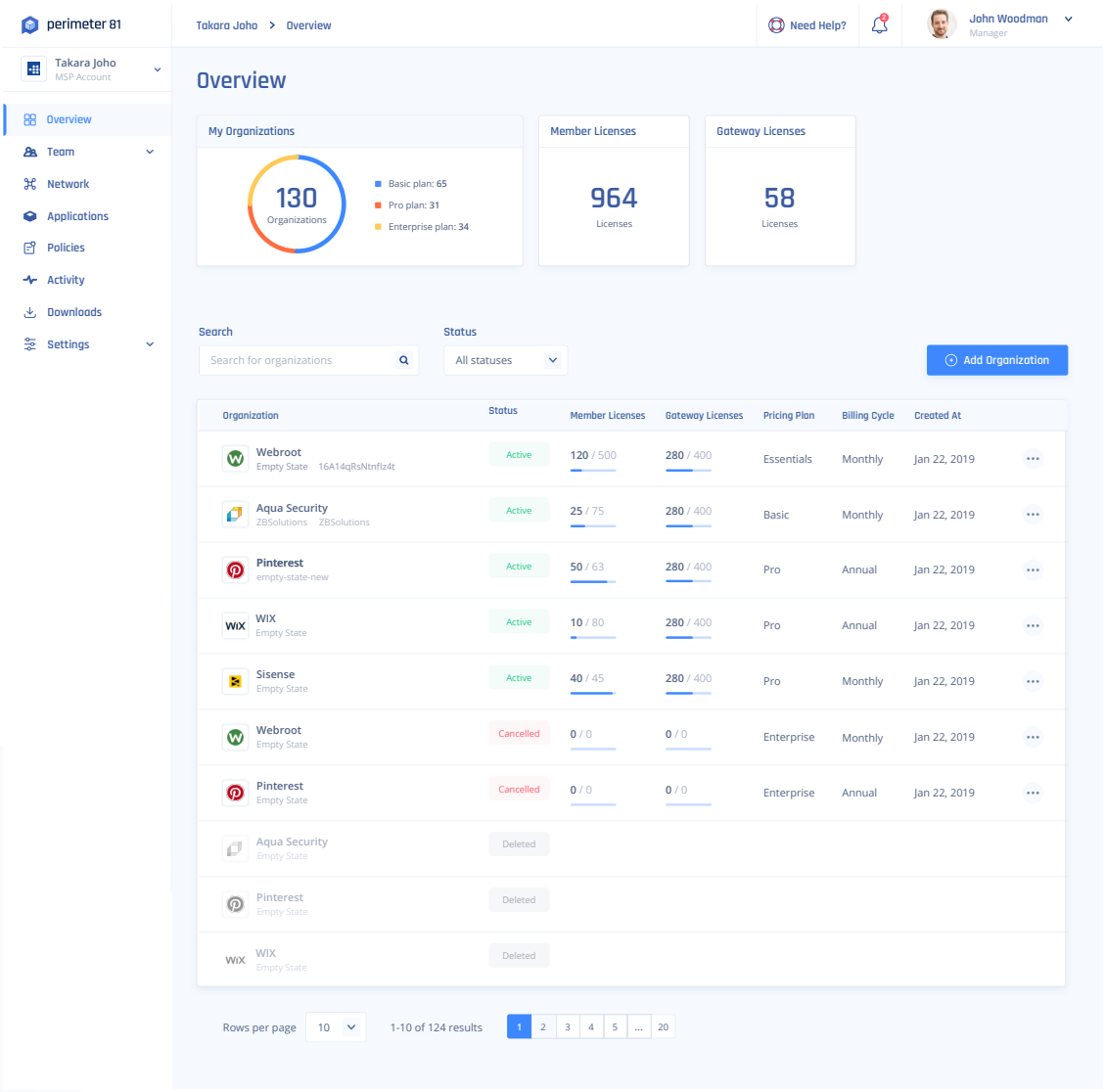
Now we're ready for the first major change for the acquired company. The aim is for the parent company to move the acquired company to Perimeter 81–the parent company in our scenario is already a customer. This will make it easier to combine networks later (if needed), and this step helps IT teams gain real-time visibility over both networks in one spot. In addition, it helps keep the networks stable, since while they may be under the Perimeter 81 umbrella, they will effectively operate independently for a smoother primary transition. Just how independently they operate depends on your particular circumstances.

There are many different requirements for businesses undergoing a merger, but it's often a gradual process. Perimeter 81 enables companies to take the time they need to go from total separation to an intermediate state to a fully completed consolidation. You can also skip any of these stages if they aren't relevant to your company, or even remain at one of these states indefinitely.

All rights reserved. Perimeter 81 | 2023

perimeter 81

Maximum Separation



Perimeter 81's multi-tenant platform is an ideal solution for companies that need to maintain complete separation. This can be due to regulatory requirements, for example, or because one company will remain a subsidiary of the other.

Our multi-tenant set-up offers complete data and privacy for both organizations, while allowing IT teams to manage both in one spot. Each company network will maintain separate assets such as gateways, logs, IDPs, employee rosters, firewall rules, and access to on-prem and cloud resources. IT teams can then switch between the two networks with a simple menu click from the management console.

A Multi-Tenant approach can be maintained indefinitely or only for a short period of time during the merger process.

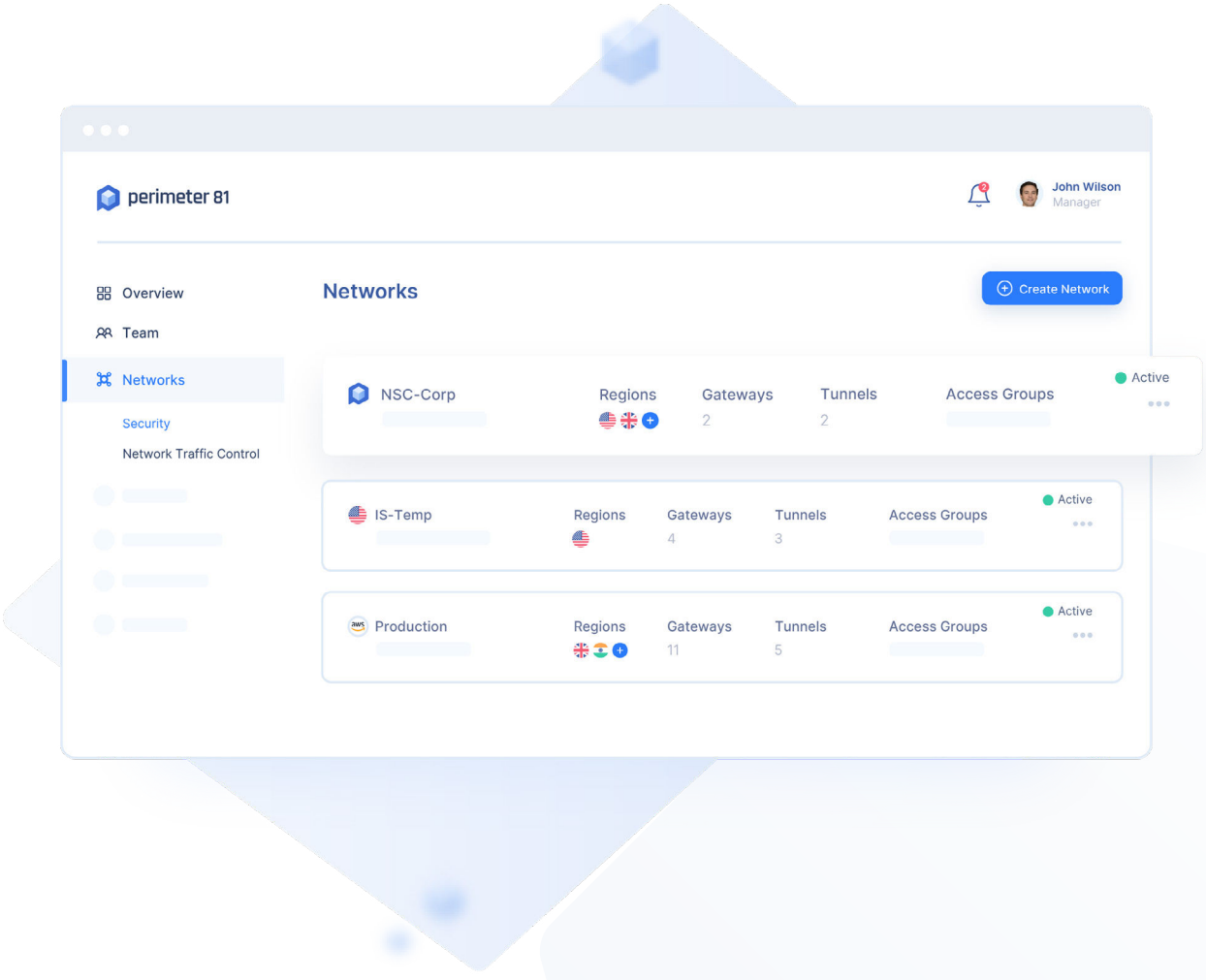
All rights reserved. Perimeter 81 | 2023

perimeter 81

Intermediate Separation

When complete separation isn't necessary, we recommend that IT teams define the new acquisition as its own separate network within the organization's current Perimeter 81 dashboard.

Under this scenario, the new users will be added to the parent company's Perimeter 81 account and given a separate subnetwork from the Networks dashboard. From the user's point of view all resource access will be separate. For the IT Manager, however, it will operate as a single company with combined team rosters, firewall rules, IDPs, logs, and multiple subnetworks. The IT team can then view all activity from a single pane of glass.



All rights reserved. Perimeter 81 | 2023

perimeter 81

Let's create a simple example to illustrate how this would work in practice. The National Stapler Company (NSC) just acquired International Staples (IS). The two companies are excited about the possibilities of remaking the stapler market worldwide with a variety of new staple types and advanced, next-generation staples.

Before all that magic can happen, however, they need to join their networks. NSC is already a Perimeter 81 customer, and they are creating a separate network inside their Perimeter 81 dashboard for IS.

So they create a new network called IS-Temp, they then assign all IS employees to a group called IS-Corporate. NSC then identifies all the various regions that the IS-Temp network will need. Then the team adds the appropriate number of gateways with connections to the IS servers and cloud resources–including secure tunnels between the gateway and the resources for added security. Then it's just a matter of distributing the Perimeter 81 agent to the desktops of IS employees.

Now, sysadmins and IT Managers can easily observe the IS network, see who's accessing what, and use web filtering rules and malware protection to protect the network from malicious threats.

While set-up times vary based on the size of each network, we can typically get the network for a midsize company up and running in hours.

Now that we have two or more networks under the same umbrella we can keep them running on their own to ensure stability, or move towards a single network.

All rights reserved. Perimeter 81 | 2023

perimeter 81

Transitioning to a Single Network

After the M&A has passed regulatory scrutiny, or the IT team is confident that all corporate subnetworks are stable under Perimeter 81, you can start moving the acquired company's assets into the parent organization's Perimeter 81 network. This is easiest to do by first moving to the intermediate stage where both companies are operating separate subnetworks on the same dashboard. At this point, most of the pieces are combined anyway including the IDPs, team member lists, logs, and so on.

To start, we'd suggest connecting the acquired company's cloud services to the parent company's network, which requires very little configuration, and each service can be typically transitioned in a few minutes. It's just a matter of adjusting the settings on the cloud service side to accommodate the parent company's gateway, and that's pretty much it.

Moving on-premises resources from one Perimeter 81 network to another can also be fairly simple. All you have to do is set-up the connection between the site and the Perimeter 81 service, but we highly recommend taking this one slowly since on-prem resources are typically less robust and more prone to configuration issues than cloud services where most of the server maintenance is taken care of for you.

Perimeter 81's management system is extremely intuitive and easy to use, and our award winning support team and account managers are always ready to help with any issues that could come up. We also offer advanced support services to help maintain and run your network smoothly.

Next Steps

With a completed transition to a single network, or set of networks under the Perimeter 81 umbrella, some good next steps include enhancing your Zero Trust Network Access (ZTNA) with context-based rules for company resources. This will add greater security for the entire organization and reduce the impact of threat actors who obtain company login credentials.

We'd also highly recommend following in the footsteps of National Stapler Company and adding the Hybrid Secure Web Gateway service for web filtering and malware protection to protect employees from malicious websites, and to secure your network against malware attacks.

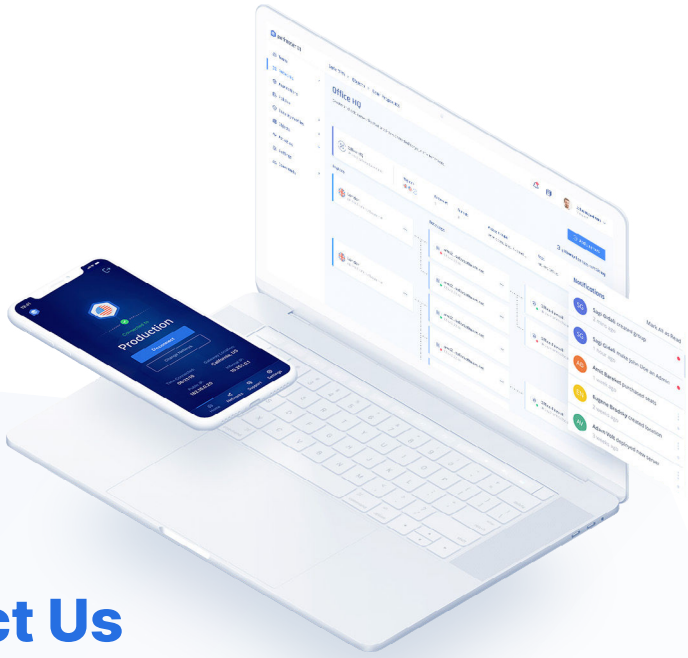
Whichever network security features you implement, Perimeter 81 is here to help you. Should you have any issues with a network transition please don't hesitate to reach out to your Customer Success Manager or contact our help team directly.

All rights reserved. Perimeter 81 | 2023

perimeter 81

About Perimeter 81

Perimeter 81 is a robust, yet easy-to-use, converged networking and network security platform which connects all users, in the office or remote, to all resources, located on-prem, or clouds. It is a cloud-native service that includes advanced capabilities such as Zero Trust remote access, Internet access control, malware protection and firewall as a service. It enables any business to build a secure corporate network over a private global backbone, without hardware and within minutes. The entire service is managed from a unified console and is backed by an award-winning global support team that has you covered 24/7.



Contact Us

Perimeter 81 Ltd.

sales@perimeter81.com

perimeter81.com

Request a Demo

All rights reserved. Perimeter 81 | 2023