NETWORK SECURITY

OVERVIEW

Data is the new currency of the digital world and the success of your business depends on keeping it safe.

But the reality is that threats to your organization will only continue to increase in number, danger, and cost as surface attack areas become more numerous and complex.

That's why TenFour offers a Network Security (NetSec) utility service that provides multiple levels of protection designed to give your team the time and resources it needs to focus less on routine operations and maintenance and more on defending your environment's most vital and vulnerable inner layers: Applications and Data.

We handle security and access in the Network and Host layers, so we reduce your in-house team's workload while providing the first line of defense. By minimizing the number of equipment variables and standardizing our security measures across the IT infrastructure we provide, your surface attack area doesn't expand even as your business grows and your infrastructure extends out to the IoT edge, making it far more difficult to infiltrate your network. To get to you they need to go through us.

We support your network security operations by monitoring for threats before they cost your business trust, productivity, or revenue, and updating each hardware or software component before it's become outdated or obsolete. We proactively seek new information about the latest bug notifications and security vulnerabilities, test new threat mitigation strategies, and implement the changes that make the most sense for your network. And because every component of your infrastructure is constantly generating data, we're able to look back in time and share past event information to assist your SOC remediation.

You already have enough things to worry about when it comes to managing your organization. We're here to help ensure network security is no longer one of them.

STRATEGIES

Our NetSec platform is comprised of three different strategies to provide more options and coverage:

Embedded Security Shield

Included standard in all TenFour IT infrastructure is an initial level of embedded security measures we call "Shield." From routers to switches and beyond, every component of the IT infrastructure we provide is set up to act as a security sensor, giving us end-to-end visibility of your network's access and operations at no additional cost. Performance, health, and security are monitored around the clock as part of this service, so you're assured your network's running optimally and suspicious activity is detected as quickly as possible.

Next-Generation Firewalls

Based on the needs of your network and operations, we offer three best-in-class, next-generation firewall options: Centralized, Distributed, or Extranet. Available on a pay-as-you-need basis as TenFour IT Units (ITUs), these advanced layers of protection provide more robust coverage, as well as more advanced command and control capabilities. As your operation's needs change over time and the network grows, we're able to keep your environment both flexible and responsive by adding or removing firewalls. Additionally, we can load our firewalls into the edge-computing devices associated with your host network to provide the same protection regardless of instance.

Command & Control Consoles

We offer three central console options as subscription-based ITUs that are designed to help monitor and manage your network's firewalls on top of the previous NetSec technology.

- Our Enterprise Security Management Console provides policy information, configuration details, threat detection reports, and more in one consolidated service designed to simplify administration of edge-based security instances.

- The NetFlow Visibility Console collects and sorts the flood of sensor data generated by our IT infrastructure services into a streamlined format ideal for remediation.

- Finally, our External DNS Console allows you to view and monitor all of your network's external-facing DNS activity for potential third-party incursions.

BUSINESS SOLUTIONS

Flexibility

The threats to your network are constant and evolving, so it's vital that any network security solution be agile enough to anticipate and respond to threats regardless of where it is deployed. Our NetSec platform is designed to be modular and flexible, and adapt to the specific performance and availability standards established for your network and business. By incorporating every IT infrastructure component in your organization's sites as a security sensor, we are able to supply your current security monitoring and analysis system with a wealth of new information about your operating environment.

Reliability

There are no days off when it comes to protecting your network and IT infrastructure. TenFour's NetSec platform provides the highest level of security, availability, and performance, with nearly instantaneous failover, and total network visibility for protection before, during, and after an attack. Our feature-rich defense system quickly identifies zero-day attacks using next generation technology with near real-time updates for intrusion prevention, advanced malware protection, and URL filtering. And our U.S.-based Network Operations Center is working around the clock to make sure any attempt to infiltrate your network is stopped at the door or detected for your attention.

$

Cost

As cyber security threats increase, the costs incurred stopping them will only continue to rise. TenFour has simplified the implementation, operations, administration, and ongoing lifecycle support process to ensure maximum efficiency and consistency. Our NetSec platform is constantly refreshed over the course of its five-year lifespan, and designed to anticipate and incorporate any new industry standards, software and equipment, all at a consistent, reduced cost to your organization. And by reliably defending against threats we help you avoid costly repercussions, such as disaster recovery, insurance payments, lost revenue, and potentially far worse.

SERVICE FEATURES

Reclaimed Resources

Our embedded security service allows you to move your security and IT resources from the Network and most of the Host/System layers to the Application and Data layers so you can focus on protecting the information that's critical to your differentiation.

Round-the-Clock Support

We provide up to 99.999% NetSec platform availability to all facets of your network and IT infrastructure, but if an issue arises, our 24x7x365, U.S.-based Network Operations Center (NOC) is always available to proactively or immediately remediate any problem.

Proactive Maintenance

Our on-going lifecycle support process keeps your software and hardware up to date in order to address critical vulnerabilities, bugs, or new functionality. Operating system and software code changes are always delivered in a proactive, systematic way to maximize code version control and minimize customer uncertainty.

Reliable & Refreshed Equipment

We use fully redundant and rigorously tested software and hardware components with our reference architectures to simplify equipment variables and standardize configurations throughout the IT infrastructure. We proactively test and implement critical patches and configuration changes to reduce surface attack areas.Plus, we refresh all equipment at regular, agreed-upon intervals so you never have to worry about technology debt.

Ironclad Security Standards

TenFour's fully embedded network cyber security solutions lower your surface attack area in support of attack prevention, risk reduction, and framework compliance requirements. We subject risky domains to URL and file inspection at the IP and DNS layers and block compromised devices before they can call home to stop data exfiltration and execution of ransomware encryption of your files and assets.

Location and Device Agnostic

It doesn't matter where your IT infrastructure sits or if it's public or private. We provide a location-agnostic approach designed to connect your business, its employees, and its customers cross the globe.

BUSINESS USE CASES

Large Organization Site with Enterprise Internet (Tier 1)

Business Problem:

- A large multinational organization's headquarters requires that a number of security operations work in parallel to support the business.

- First, the site's employees must be able to access a fully functional internet connection that is constantly checked for viruses and terminated should malicious threats appear.

- Second, a business partner working alongside the organization on several major projects must be able to safely access a specially crafted sub-network that is home to related applications and data.

- And third, all employees and select contractors must have remote access to their workstations and data from a number of fixed and variable locations off site, and with an array of security privilege levels.

TenFour Solution:

- TenFour's NetSec service features the highest level of security, availability, and performance for your site by deploying an array of firewall and security management services, while also delivering enterprise internet access at speeds up to 8.5 Gbps.

- Multiple Centralized Next-Generation Firewalls (CNGFW), an Enterprise Security Management Platform (ESMP), a Secure Visibility Platform (SVP), and a Secure DNS Platform (SDP) give you total network visibility by using infrastructure devices as security sensors.

- And with advanced malware protection, URL filtering, and a feature-rich suite of network admission control technologies we're able to automatically block risky sites at the DNS and IP layers and quickly identify zero-day attacks if infiltration does occur.

- TenFour's robust NetSec platform is designed to provide secure, redundant, and context-aware high-speed connectivity to local, cloud, and global networksprovide secure, redundant, and context-aware high-speed connectivity to local, cloud, and global networks.

Medium to Large Organization with Secondary Backup Site (Tier 2)

Business Problem:

- A medium-sized corporate headquarters is home to a small on-site workforce, but the technological nature of its business demands a relatively large IT staff be in constant communication with telecommuting employees.

- In order to introduce an additional layer of protection for its intellectual property, the business has also established an off-site, private data center, in which they store the majority of their proprietary application data.

- Availability and disaster recovery are very high priorities; the business must be able to retain a degree of online flexibility, but still have an iron-clad barrier against potential incursion.

TenFour Solution:

- TenFour's NetSec service features the highest level of security, availability, and performance for your site by deploying an array of firewall and security management services, while also delivering enterprise internet access at speeds up to 8.5 Gbps.

- A Centralized Next-Generation Firewalls (CNGFW), an Enterprise Security Management Platform (ESMP), and a Secure DNS Platform (SDP) give you total network visibility by using infrastructure devices as security sensors.

- And with advanced malware protection, URL filtering, and a feature-rich suite of network admission control technologies we're able to automatically block risky sites at the DNS and IP layers and quickly identify zero-day attacks if infiltration does occur.

- TenFour's robust NetSec platform is designed to provide secure, redundant, and context-aware high-speed connectivity to local, cloud, and global networks

BUSINESS USE CASES

Medium Organization or Manufacturing Site (Tier 3)

Business Problem:

- A medium-sized retail site with a relatively small workforce requires that its employees be able to access a secure network space focused on the business, while its customers access a screened and monitored complimentary internet connection that allows them to browse recreationally or order items from within the location.

- In addition, some employees require external internet access for third-party vendor coordination and to conduct customer service via the organization's website.

- This must all be made available while protecting vital infrastructure from manipulation and incursion

TenFour Solution:

- TenFour's NetSec service uses a Distributed Next-Generation Firewall (DNGFW) to facilitate external internet connections up to 2 Gbps while also protecting intranet operations at your site with an array of firewall and security management services.

- We give you total network visibility by using infrastructure devices as security sensors and with advanced malware protection, URL filtering, and a feature-rich suite of network admission control technologies we're able to block risky sites at the DNS and IP layers and quickly identify zero-day attacks if threats do arise.

- TenFour's robust NetSec platform is designed to provide secure, redundant, and context-aware high-speed connectivity to local, cloud, and global networks.

Small to Medium Organization Site (Tier 4)

Business Problem:

- A health provider organization with small- to medium-sized sites focused primarily on local operations needs to provide employees and customers with a reliable internet connection.

- Due to the sensitive nature of its operations it requires a high degree of protection, but its external connection must provide high availability and bandwidth.

- Though the site is not connected to a centralized data center, it does on occasion need to communicate with a headquarters site via the internet and does on occasion need to download or transfer potentially sensitive files.

TenFour Solution:

- TenFour's NetSec service uses a Small Next-Generation Firewall (SNGFW) to facilitate external connections at speeds up to 450 mbps while also providing your site with the highest level of security, availability, and performance.

- In conjunction with an array of firewall and security management services, our service provides total network visibility by using infrastructure devices as security sensors.

- And with advanced malware protection, URL filtering, and a feature-rich suite of network admission control technologies we're able to automatically block risky sites at the DNS and IP layers and quickly identify zero-day attacks if threats do arise.

- TenFour's robust NetSec platform is designed to provide secure, redundant, and context-aware high-speed connectivity to local, cloud, and global networks.

ADD-ON FEATURES

The following services can be purchased as part of TenFour's NetSec platform on top of the embedded Shield service to provide additional layers of threat-focused security features and capabilities:

- **Next-Generation Firewall:** Provides a live threat intelligence feed, as well as an Intrusion Prevention System (IPS), Advanced Malware Protection, and URL filtering, all at a throughput rate up to 8.5 Gbps.

- **Enterprise Security Management Platform (ESMP):** Provides security management via a single interface that controls administrative access to security devices and network admission for all end users.

- **Security Visibility Platform (SVP):** Provides total network visibility of all east-west traffic with encrypted traffic analysis revealing indicators of compromise via the ESMP.

- **Domain Name Services (DNS):** Screen and block malicious destinations via IP layer enforcement, intelligent proxy technology, and command and control callback blocking before a connection can be established.

END-TO-END

All of the elements of your digital environment depend on each other, but NetSec ensures each element is threat-free and able to perform as desired. In addition to NetSec, TenFour delivers the following services as utilities, all designed to work in harmony and transform your business.

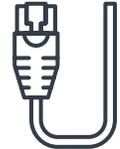| Wide Area Network	Local Area Network	Internet of Things	Data Center	Unified Communications & Collaboration	Physical Infrastructure

ABOUT TENFOUR

What got you through the Information Age won't get you through the Digital Age. You need new tools.

We've created a new type of IT infrastructure company. We build exceptional, private domain global IT infrastructure that is simplified, has fewer defects, and costs less to operate than traditional models. And we don't just build and operate IT infrastructures; we own them.

We're not a Cloud computing company, but we've taken the Cloud model and extended it beyond compute and storage to core components, platforms, and services, such as routers, switches, wireless access points, IP phones, IoT devices, and so much more which has traditionally been "uncloudable." The best part is: just like electricity and water utilities, you pay only for what you use, when you use it.

LET'S GET STARTED

You're building the future of your company, but you don't have to build it alone.

Reach out to **+1 973 267 5236** or email **hello@tenfour.com** to see how TenFour's IoT utility service can help ensure your organization's future is built on the strongest foundation possible.