White Paper

Historical and Future Roles for Firewall and Proxy Gateways

CONTENTS

INTRODUCTION

Who should read this paper?

Network and security VPs, architects, directors, and managers.

When to read this paper?

When planning future inline control points for threat and data protection.

Why read this paper?

The role of the firewalls and proxy gateways are changing driven by content and context for adaptive access, zero trust principles, and remote and hybrid work with security service edge (SSE) solutions.

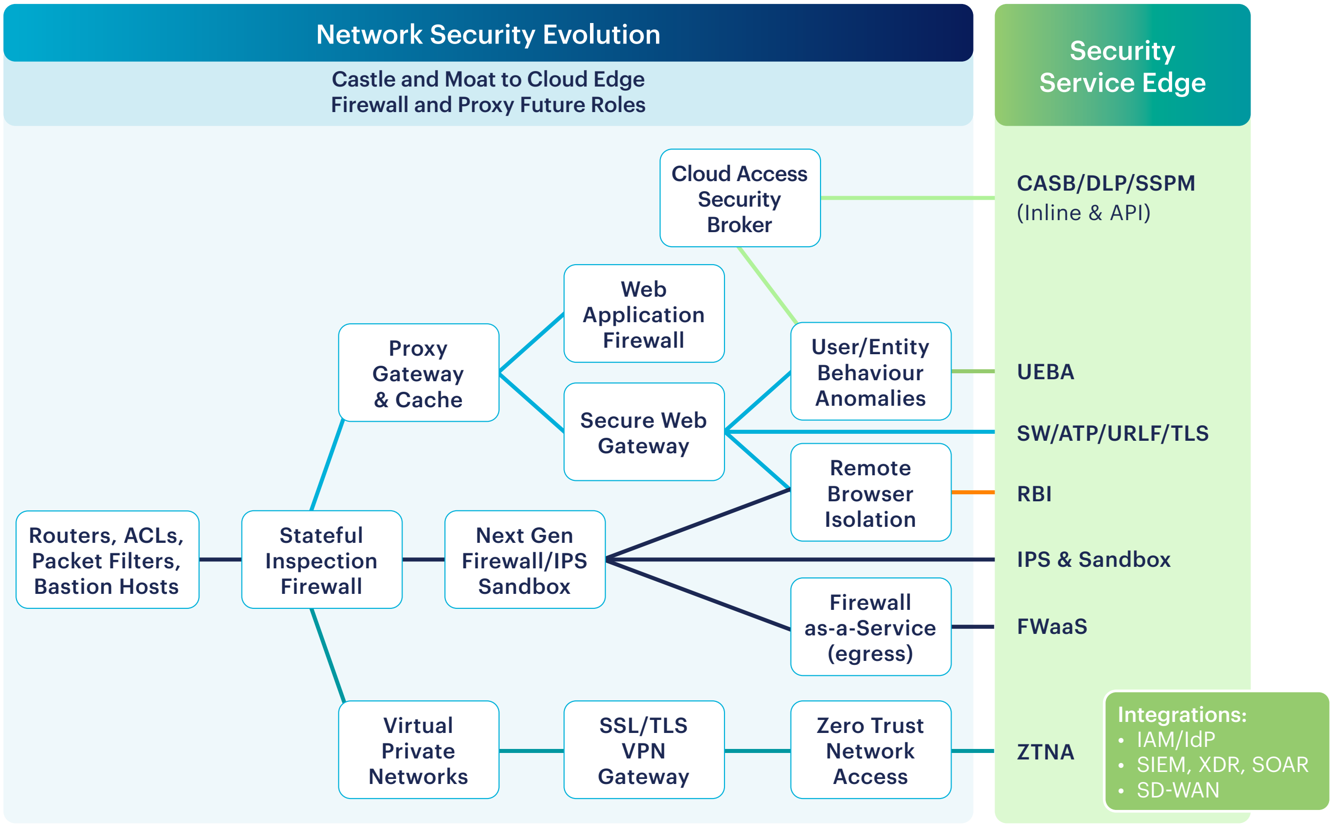
EXECUTIVE SUMMARY

Humans in general do not like change, and doing the same thing repeatedly and expecting improved results is one definition for insanity. Given the high-tech domain has a generational span of five to seven years where change is almost inevitable, these forces work against each other where the human resistance to change presses against the forward march of technology. The long-held debate of firewalls versus proxy gateways for inline network security has recently moved into a new generation. An understanding of the historical divides over the years and some more recent post pandemic role changes are putting it all into perspective.

> One of the clear drivers for generational change of firewalls and proxy gateways is AI and machine learning requiring content and context that many legacy inline defenses lack for real-time analysis.

The role of remote access has also changed with increased hybrid work while zero trust principles are challenging long held security perspectives. Years ago, proxy gateways were divided into separate roles for egress with secure web gateways (SWGs) and ingress with web application firewalls (WAFs). We are now seeing next generation firewalls (NGFWs) experience a similar divide for egress with cloud-hosted firewall-as-a-service (FWaaS) for hybrid and remote working within security service edge (SSE) platforms, while the ingress/egress firewall for inbound/outbound traffic remains in place to protect data centers, infrastructure, and on-site workers. Zero trust network access (ZTNA) is also replacing virtual private networks (VPNs) with public facing exploitable services and known lateral movement issues with a more secure “inside-out” connection model directly to desired applications or resources.

Most important is the impact on threat and data protection inline where a decades old model of file hash signatures for malicious files or sensitive data no longer scales, even with frequent threat intelligence sharing amongst the herd community for indicators of compromise (IOCs). Unknown and zero-day threats continue to increase and environments with dynamic, unstructured data (e.g., source code) change too fast for DLP data classification and registration. For these growing use cases the use of AI and machine learning are closing the gap in real-time while delivering a performant user experience. We are in a new generation, both the journey of how we arrived and what the new roles mean is key for network and security architecture. Analyzing content and context in real-time and accepting change will define success.


Network Security Evolution
Castle and Moat to Cloud Edge
Firewall and Proxy Future Roles
Security Service Edge
Cloud Access Security Broker
Web Application Firewall
Proxy Gateway & Cache
Secure Web Gateway
User/Entity Behaviour Anomalies
Remote Browser Isolation
Routers, ACLs, Packet Filters, Bastion Hosts
Stateful Inspection Firewall
Next Gen Firewall/IPS Sandbox
Firewall as-a-Service (egress)
Virtual Private Networks
SSL/TLS VPN Gateway
Zero Trust Network Access
CASB/DLP/SSPM (Inline & API)
UEBA
SW/ATP/URLF/TLS
RBI
IPS & Sandbox
FWaaS
ZTNA
Integrations:
• IAM/IdP
• SIEM, XDR, SOAR
• SD-WAN

EARLY DAYS AND THE DIVIDE

Routers, ACLs, Packet Filters, and Bastion Hosts

For most people the internet arrived in the mid-1990s via dial-up modems for what was mostly a text experience with static images, nothing like we have today. Access control lists (ACLs) defined outbound and inbound access on routers, while a small group of people on greatcircle.com shared their knowledge about early firewall designs including dual bastion hosts and the firewall toolkit (fwtk). The internet was an external destination and some even claimed it was the CB radio of the 1990s and would fade away. From the beginning a divide of egress and ingress was established for ACLs, routers, packet filters, and early firewall designs both proxy and network based.

Performance of Stateful Inspection Firewalls Wins the Day

Once the internet concept caught on to share information online, find birds of a feather, and learn new things there was no stopping the momentum. Some politicians may have even claimed to have created the internet due to its popularity. Speed was essential and the performance of stateful inspection network-based firewalls far surpassed proxy and dual bastion-host designs with 8-10X faster speeds. Egress ports were opened for approved policy requests and then closed after the session completed, or remembered for ingress traffic, an improvement of static ACLs leaving ports open. Traffic was defined for specific source and destination IP addresses, ports, and for specific protocols, known as 5-tuple firewall access controls. The firewall became the primary defense for network security teams to define the inside and the outside, plus DMZs for hosted services such as web and file sharing servers.

Virtual Private Networks and Next Generation Firewalls

Remote access quickly became a primary use case, and virtual private networks (VPNs) became a key feature of network-based firewalls eventually evolving into SSL browser-based remote access. VPNs enabled employees' remote access to specific network zones, plus contractors, partners, and third parties where they could access internal applications and data with some degree of lateral movement. Websites continued to expand capabilities, web filtering and URL categories matured, and the good, bad, and ugly sides of the internet were defined. Popular websites and domains began to take on application-like characteristics and the next-generation firewall (NGFW) emerged with app-ID, content-ID, and user-ID access controls, a step-up from 5-tuple firewall access controls.

The Proxy Divide into Secure Web Gateways and Web Application Firewalls

Proxy inspection had some degree of success while supporters argued for their more secure design, including re-constructing the content for security scanning versus using a stream-based antivirus applied by NGFWs. Proxy inspection also provided protocol compliance, header-based controls, and granular policies including the ability to filter, strip, or replace web objects. However, performance issues held proxies back compared to stateful inspection and NGFW performance with easier policy controls. Caching became a key proxy use case for frequently accessed content reducing the full trip to origin servers for content and improving the user experience. At its peak users could experience well over 30% of web content from caching, however, as websites became more dynamic and personalized the percentage fell. What caching did provide was a new design for proxy servers built on optimized operating systems designed for web objects versus files and executables and faster performance.

> The egress and ingress roles were divided for proxy servers with egress defined by secure web gateways (SWGs) and ingress by web application firewalls (WAFs). This divide will come for NGFWs, however, in several decades and after the pandemic.

BEFORE TLS DOMINATES AND EARLY HARDWARE SCALABILITY

Clear Text HTTP Inspection

NGFWs continued to scale performance as well as proxy gateways (or SWGs) as both had the advantage of HTTP clear text traffic to inspect and only a small percentage of encrypted SSL traffic, later to become TLS. Until this blind spot fully developed, it was easy for NGFWs, intrusion protection systems (IPS), and SWGs to inspect clear text content for web filtering, anti-virus file checks, and access control. One key issue developed when adverse internal users could hide their identity with release and renew commands to get a new IP address lease and thus mask their identity. Human resource teams could not be certain they had the right employee for policy violations, even worse when local or federal authorities came knocking for an individual. This led to an increase in interest in SWGs with integrated per-session authentication and authorization as user identity was court admissible no matter how many times IP address leases were changed. The second key issue was the evolution of threats where it became desirable to hold and trickle a file download, giving anti-malware defenses more time for detection. Today we call this patience zero protection.

The Emergence of Encrypted Traffic

SSL and eventually TLS traffic encryption increased in popularity, and it created a blind spot for network security defenses.

Turning on SSL/TLS traffic inspection could overload a NGFW appliance used to clear HTTP traffic inspection, so it was often avoided. Dedicated SWGs became more popular for SSL/TLS inspection, plus the ability to filter, strip, or replace any web object, and file trickle giving malware defenses more time. Static URL filtering also evolved into dynamic URL ratings with machine learning where high confidence ratings were in real-time. Add in a small benefit from content caching and stream splitting media and SWGs became the egress point for web traffic mainly on ports 80 and 443 while the NGFW kept guard across all ports and protocols plus providing remote VPN access. This was an era when SSL/TLS traffic encryption grew from 15% to 75% within a couple of years, even under-provisioned SWGs ran hot with the overload of encrypted traffic. This led to SSL acceleration cards and SSL offloading devices to serve in a layered defense stack for advanced threat protection.

Differences Between Enterprise and Mid-Market Solutions

A unique characteristic between large enterprise solutions and mid-market solutions for inline network security was the ability to manage the solution via scripting. Large enterprises will invest in automation and scripting to manage security solutions and are not that interested in a web administration UI. The opposite holds true for mid-market solutions where the web administration UI has an easy to use step-by-step policy process that is provided as a guide. Today, solutions have their core capabilities with an API layer and then a UI layer on top replicating the capabilities. Anything the UI can accomplish is driven through the API layer and thus it can also be scripted. User groups and communities, plus subject matter experts will often share scripts versus watching a UI demo with step-by-step instructions as one key indicator of enterprise administrators.

PRE-COVID ROLES

A Decade of Defined Roles for SWGs and NGFWs

Roles were stable for well over a decade for secure web gateways and next generation firewalls where almost every organization on the internet deployed a NGFW, however, only those rich with resources could afford SWGs. The slowly increasing agent of change was SSL/TLS encrypted traffic as it put a burden on firewall hardware appliances to decrypt traffic. NGFWs kept on inspecting packet headers, filtering domains, and analyzing visible content while SWGs became purpose-built for encrypted traffic inspection, content analysis, stricter user identification, and the ability to filter, strip, or replace web objects.

When it came to logging events, NGFWs focused mainly on alerts while SWGs would record detailed web transaction events with high volumes to often overwhelm reporting solutions. A SWG first deployed for encrypted traffic inspection would run at less than 10% capacity and by the end of its five-year lifespan up to 75% capacity utilization and ready for replacement if everything went well. However, not all deployments could sustain the high growth of encrypted traffic and the cloud adoption of Office 365 creating customer frustration and budgeting issues.

> Administrators knowledgeable on web proxy gateways were also in high demand in a time when IT security headcounts and budgets were limited.

The result was the pervasive use of NGFWs to define perimeters and the more limited use of SWGs for those rich with resources to decrypt and inspect web traffic for real-time analysis of content.

New Defenses for the Unknown

The security mantra of patching your systems and updating your signatures was challenged by new URLs, new content, and zero-day threats not seen before. This unrated and unknown content had two options, analyze it inline while the user waits or send it to background defenses for analysis and then update signatures. SWGs provided the advantage of encrypted traffic inspection for content visibility for real-time categorization ratings (vs human rater labs in the background) and could trickle and hold files until determined benign for download. NGFWs and SWGs also leaned into sandboxing of executable files to determine malicious threats to then update signatures.

> A driving theory at the time was the larger the herd of community members, the more exposure to new threats via patient zero infections and henceforth the faster new signatures could be developed and shared from a security vendor.

As an augmentation to SWGs, remote browser isolation (RBI) provided a pixel generated view of websites and unknown and potentially malicious content to protect users and their devices from attacks.

Endpoint and Gateway Threat Protection Strategy

Up until 2017, and the growth of fileless threats, the endpoint was best suited to analyze executable threats having access to the file system, runtime, and directory. Fileless attacks executed in memory avoid the file system using runtime scripts to create a new challenge. Plus, phishing attacks were content-based with no executables to analyze, along with other scams and tricks to collect access credentials and mislead users. SWGs became an important partner to endpoint threat protection with their ability to analyze content between origin servers and users as a man-in-the-middle (MITM) inspection point.

> Encrypted traffic inspection at scale and high performance became even more important to protect users and resources from file-based, fileless, and phishing attacks.

Dominance of VPNs for Remote Access

Initial virtual private networks (VPNs) required a managed client in an era when "yet another agent" would frustrate desktop management teams wrangling with conflicts between multiple endpoint agents. The innovation of SSL/TLS-based VPNs using web browsers' accelerated VPN adoption into a dominant role for remote access. At this point in time less than 20% of an organization's employees and workers were remote, requiring VPNs into company resources. Most employees, contractors, and workers would access a main office or branch office for their job duties working on a managed device on a company managed network behind a NGFW and in many cases a SWG.

> This on-site environment will become heavily challenged when the pandemic starts.

Early Days of SaaS/IaaS Adoption

While NGFWs and SWGs had well-defined roles, refresh cycles, and consistency for capabilities, an entirely new world was developing for SaaS applications and IaaS cloud services.

> Most administrators for NGFWs and SWGs did not consider the new kids on the block as their responsibility and for the most part ignored SaaS and IaaS before the pandemic.

Cloud access security broker (CASB) solutions focused on managed SaaS and IaaS using API inspection leveraging web hooks for new events or time-based analysis. The primary focus was data protection and DLP as the most popular SaaS applications contained data under compliance regulations. In a parallel universe, users were also adopting personal SaaS applications for email, social, IM, chat, personal communications, and cloud file storage. These company versus personal SaaS worlds will soon intersect with the pandemic.

To add another factor for the perfect pandemic storm, the growth of HTTPS for encrypted web traffic in many regions of the world for operating systems and web browsers was over 90%. For inline security defenses not decrypting and inspecting HTTPS this led to an increasing blind spot, more reliance on the herd community for threat intelligence to block known threats, and no visibility for data movement as SaaS/IaaS adoption increased. If you did manage encrypted traffic inspection and resources, you would have seen the near doubling of capacity required every few years to keep pace with both the increasing use of HTTPS and increasing web and SaaS/IaaS traffic.

End of the Castle and Moat Era

Early 2020 defined the end for the castle and moat security defense era. Security and networking administrators used to users in offices on their networks, managed devices, and applications and data in their data centers would soon be put to the test. A popular snarky T-shirt for IT admins of this era was “I read your email first.” Network TAPs could record any traffic into packet captures for replay and analysis, visibility was taken for granted.

Hybrid and Remote Work Arrives Further Increasing Digital Transformation

BAM! March 2020 isolates workers from offices with the pandemic for one of the largest resilience impacts in IT history.

> The perfect storm hits with limited VPN capacity, data center-based security defenses, blind spots for encrypted traffic inspection, and increasing SaaS/IaaS utilization.

The pandemic accelerated users, apps, and data into the cloud towards digital transformation and business agility. What may have taken years of adoption happened quickly to redefine the roles of legacy security defenses. Businesses had a choice to join the digital divide or fall behind, and with their choice add or lose critical IT talent and skills required for the journey.

VPNs Feel the Stress Backhauling Traffic

Almost immediately VPNs were put to the test for remote worker access to company resources, and in many cases were overwhelmed until more capacity was deployed. This increased costs, complexity, and opened the door to more security risks. VPNs use a public service port open to exploits, weak credentials enabled access compromise, and open lateral movement with access only expanded the attack surface. The user experience of backhauling VPN traffic to data centers and through legacy security defenses was often poor, resulting in users evading this path or being allowed direct access to SaaS/IaaS to enable productivity. In either case, visibility once taken for granted was lost.

SaaS Adoption Accelerates with Cloud First Strategy

Managed SaaS application adoption was growing over 18% year over year for office productivity suites, customer relationship management, marketing, and human resources as primary growth areas. At the same time personal SaaS quickly became a resilience option for remote workers to share files, move data, and get tasks completed with the least amount of friction.

> While managed SaaS could use API inspection, unmanaged SaaS and personal instances of popular SaaS applications developed quickly into a post-pandemic blind spot.

While networking and security teams understood for over a decade how to manage NGFWs and SWGs, they were new to CASB inline traffic inspection for company and personal use of SaaS and IaaS. Companies adopting a cloud first strategy had a new blind spot, they could not detect unknown or unapproved data movement or exfiltration.

NGFWs Divide into FWaaS for Remote Egress and ZTNA for Remote Access

For hybrid and remote workers, backhauling their business transactions to data center-based defenses makes little sense with a poor user experience. The role of the NGFW for these users is changing quickly where egress traffic is now protected by a Firewall-as-as Service (FWaaS) as part of an SSE security platform along with a combined proxy for web and SaaS/IaaS traffic inspection merging SWG and CASB Inline together at the core. Remote access via VPNs also transformed into zero trust network access (ZTNA) based on zero trust principles using a more secure "inside-out" connection. The traditional role of the NGFW now remains at data centers for ingress and egress traffic unless a company is 100% cloud first and retires their data centers. As seen with SWG appliances, the NGFW appliance will fade away as use cases change and cloud scale and performance for any user, device, and location prevail.

Whirlwind Consolidation of Security Service Edge

A few analysts predicted the consolidation of security defenses into cloud edge platforms before the pandemic, however, they quickly realized how accurate they were after the pandemic. What started out as secure access service edge (SASE) was further refined into security service edge (SSE) and SD-WAN. This caught NGFW and SWG vendors off guard with one SWG CEO trying to figure out how a CASB vendor was leading the SSE solution space. Both company and personal SaaS/IaaS traffic now surpassed web traffic in volume and requires both TLS decryption and SaaS/IaaS application decoding for content visibility. CASB solutions at the time were mostly regarded as API inspection of managed SaaS for DLP and compliance.

Now an 800-pound gorilla shows up with CASB inline traffic inspection for company and personal SaaS, IaaS, and web traffic to lead the SSE solution space. This new visibility post-pandemic quickly confirmed more than half of threats are cloud-delivered versus web, and data exfiltration and theft increase 300% the last 30 days of employment for departing employees.

> Traditional use cases for NGFWs and SWGs missed the growing adoption of SaaS and IaaS for company and personal use, plus the pandemic acceleration impact.

Blocking these domains only frustrates users and may also block a resilience option when primary applications have an outage. Understanding users, apps, and data movement moved to front and center with SSE, cloud first strategies, and digital transformation. The role of NGFWs and SWGs changed and were about to face one more challenge.

Zero Trust Principles Versus Marketing

Zero trust principles seek to remove implicit access, refine least privilege access, and continuously monitor. From these basic concepts, the marketing of zero trust is far removed from reality. Most of the marketing messages lean towards secure access for zero trust and miss the concept that data flows through all the other zero trust components (users, applications, devices, and networks).

> Zero trust principles do not function well with blind spots of legacy security defenses.

The concept of least privilege access for a business transaction based on its content and context only works if you have visibility. And if you want to continuously monitor to refine least privilege access, you need visibility of the user, data, app, device, and network. The result is SSE solutions combine CASB and SWG capabilities into a core inline proxy with FWaaS and ZTNA to redefine the traditional NGFW and VPN roles to support zero trust principles. As a cloud security edge platform, SSE has the scale and performance for any user, device, or location to provide a great user experience removing the trade-off of performance versus security for content visibility.

Cybercrime Advances Ransomware

> Ransomware at the core monetizes compromised remote access and reflects the need for zero trust principles.

Companies resting on legacy defenses including VPNs, remote access support solutions, traditional firewalls, and lacking the ability to detect access compromise for accounts, users, and devices became easy targets. If your first line of defense is to detect ransomware malware that encrypts data and manages the encryption keys, the data has already been exfiltrated in earlier kill chain stages and the extortion is set to happen. Remote access compromise and phishing are the leading entry points for ransomware and drive a multi-sector underground economy selling off access to desired targets.

Government regulations responded with multi-factor and strong authentication requirements, plus the eventual recommendation to replace VPN solutions open to compromise and zero-day threats. ZTNA using an inside-out connection specific to an application or resource is more secure, plus the use of dedicated egress IP addresses into managed SaaS applications from SSE platforms. Phishing requires real-time content analysis of web, email, SaaS, and IaaS traffic given fake login forms are often hosted in popular SaaS and IaaS cloud services. Ransomware will continue to drive the replacement of legacy security solutions when analyzed holistically and beyond the executable file malware itself.

Unknown and Unapproved Data Exfiltration, Theft, and Insiders

When the pandemic started workers took managed devices to their homes to access a wide variety of non-work-related content, plus multiple uses of laptops for education, personal, and social access. Adult content access spiked over 600% at first and then declined. No surprise there, when WiFi was first provided on commercial airlines the same thing happened, the airlines turned it off until web filtering was added. Employment and job changes were also in the mix given a new remote working experience with some people wanting to keep it long-term. Some savvy IT companies even published unlimited remote working ads to lure valuable employees from other firms requesting a return to offices.

What employees do on laptops at their company desk in an office with others watching and what they do remotely are two very different things. Exposure to more non-work-related content opens the door to more lures and threats.

> Employees, contractors, and partners also feel more entitled to data they see as valuable in future job roles.

This was supported when seeing a 300% increase in data exfiltration and theft during the last 30 days of employment before departure, and 74% of this data flowing into personal cloud storage. Unknown and unapproved data exfiltration, theft, and insider risks increased with hybrid/remote working where legacy defenses were blind to company versus personal use of SaaS and IaaS. The reality of less than 3% of SaaS applications being managed by IT and the other 97% adopted by business units and users marching towards digital transformation caught NGFW and SWG solutions off guard.

Content and Context are the Future for Real-time Adaptive Access Control

Inline inspection of SaaS and IaaS content and context in real-time is the future of access control for SSE solutions. Firewalls perfected the inspection for network traffic, SWGs did the same for web traffic, and now SSE brings these controls together with inline CASB content and context inspection. Based on application risk, behavior risk, device posture, activity, data sensitivity or other variables adaptive access control is applied to every business transaction for its content and context. If a user desires to delete 100 files of company sensitive data, adaptive access can request a step-up authentication or request a justification from the user. If another user may desire to access an unmanaged risky cloud storage application to move files, adaptive access can warn them and provide safer company-approved cloud storage options. The concept of real-time coaching is much like satellite navigation (or GPS) when driving today, users need guidance in real-time.

> We are in a new gray area between known good and known bad that requires adaptive access and guidance to protect users and data.

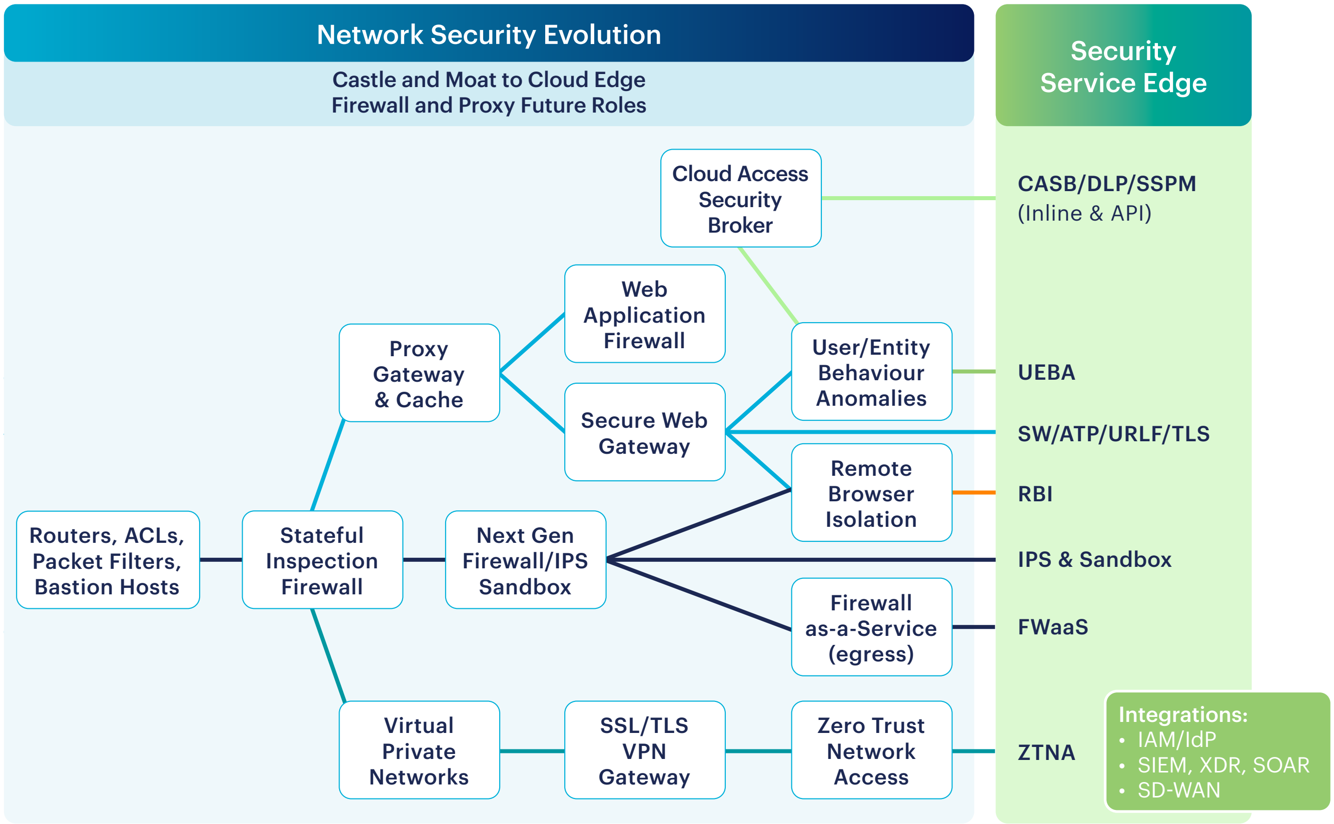
Role of AI and Machine Learning for Threat and Data Protection

Artificial intelligence (AI) and machine learning (ML) have been used in the background for many years for threat defense engines, data classification, URL dynamic ratings, and IT operation planning as a few examples. Now AI and ML-based defenses are moving inline to work in real-time to detect new unknown zero-day threats and identify sensitive data in documents and images. The AI boom itself enables both the good and bad to quickly develop new code, content, and learn quickly. AI is both a boom and lure with the potential to expose sensitive data. ChatGPT quickly became the leading accessed AI application and the most popular content supplied to it was source code. Legacy defenses were not in a position to allow company instances of AI versus controlling public and personal instances for users; nor provide the ability to identify content like source code being fed into AI applications. Inline AI/ML-based defenses are detecting malicious executable files, phishing attacks, and classifying dozens of documents and images, including source code today.

> AI/ML defenses inline providing real-time protection at T+0 only work with content visibility, and this defines the modern SSE platform.

Modern Roles for NGFW, SWG, CASB, VPN, and ZTNA for Zero Trust

The web gateway quickly divided into its egress SWG and ingress WAF roles for web traffic. While the NGFW has remained combined for egress and ingress of network traffic, post pandemic egress traffic flows into FWaaS for hybrid and remote workers, and VPN capabilities are being replaced with ZTNA as part of SSE platforms. Early on CASB was defined mainly by API inspection of managed SaaS and IaaS with DLP for data-at-rest. The often-overlooked inline capability of CASB to inspect thousands of managed and unmanaged applications and cloud services, including by company versus personal instance for hundreds of applications quickly became highly valued. Zero trust principles and their growing interest requires content and context visibility for least privilege access and continuous monitoring for each business transaction. This same content and context will drive the further evolution of real-time AI/ML defenses in SSE platforms.


Network Security Evolution
Castle and Moat to Cloud Edge
Firewall and Proxy Future Roles
Security Service Edge
Cloud Access Security Broker
CASB/DLP/SSPM
(Inline & API)
Web Application Firewall
Proxy Gateway & Cache
User/Entity Behaviour Anomalies
UEBA
Secure Web Gateway
SW/ATP/URLF/TLS
Remote Browser Isolation
RBI
Routers, ACLs, Packet Filters, Bastion Hosts
Stateful Inspection Firewall
Next Gen Firewall/IPS Sandbox
IPS & Sandbox
Firewall as-a-Service (egress)
FWaaS
Virtual Private Networks
SSL/TLS VPN Gateway
Zero Trust Network Access
ZTNA
Integrations:
• IAM/IdP
• SIEM, XDR, SOAR
• SD-WAN

SUMMARY

Investing in security defenses for infrastructure that no longer exists or will soon fade away is a costly mistake as companies embrace hybrid working and digital transformation. The NGFW, SWG, and VPN renewals should be analyzed carefully going forward knowing the shift to SaaS and IaaS inline inspection, visibility to content and context for inline AI/ML defenses and providing adaptive access with real-time coaching to users.

> Knowing how we arrived at this point and the drivers for change for egress and ingress network, web, and SaaS/IaaS traffic are important for everyone.

Innovators and early adopters quickly adapt seeing the signs of change as they drive innovation, roadmaps, and validate analysts' predictions. For the majority, how fast they recognize and adapt post pandemic will likely define their success, the IT talent they attract and keep, and to prepare for the next shift. The force of technology advancing against human resistance to change continues in all aspects of our lives.

WHY NETSKOPE

Netskope Intelligent SSE uniquely provides traffic inspection for web, SaaS, and IaaS for thousands of applications and cloud services to understand the content and context. The core architecture includes ZTNA for access to private applications and the full integration of SWG and CASB solutions for a single pass inspection of inline traffic from users or systems. This rich visibility enables the Netskope Zero Trust Engine to provide adaptive access controls, real-time coaching, and an understanding of company versus personal instances for hundreds of applications to detect unknown data movement. Least privilege access is provided with the ability for users to provide justifications to continue business transactions enabling policy refinement through continuous monitoring in support of zero trust principles.

To learn more, please read our **New Insights for Threat and Data Protection — What Legacy Vendors Want to Hide** eBook, infographic, and webinar-on-demand.

Netskope, a global SASE leader, is redefining cloud, data, and network security to help organizations apply zero trust principles to protect data. Fast and easy to use, the Netskope platform provides optimized access and real-time security for people, devices, and data anywhere they go. Netskope helps customers reduce risk, accelerate performance, and get unrivalled visibility into any cloud, web, and private application activity. Thousands of customers, including more than 25 of the Fortune 100, trust Netskope and its powerful NewEdge network to address evolving threats, new risks, technology shifts, organizational and network changes, and new regulatory requirements.

Learn how Netskope helps customers be ready for anything on their SASE journey, visit netskope.com.