NEXUSGUARD®

SECURING NATIONS

NEXUSGUARD'S BASTIONS SERVICES FOR GOVERNMENT CYBER PROTECTION

www.nexusguard.com

GATEWAY TO GOVERNMENT CYBERSECURITY WITH NEXUSGUARD BASTIONS SERVICES

Within the domain of government cybersecurity, ISPs (Inter Service Providers) face significant challenges when attempting to break into the sector. Established Managed Security Services are often dominated by big-name providers, limiting the opportunities for lesser-known ISPs in Asia Pacific. Nevertheless, the emergence of government tenders focused on safeguarding the integrity and accessibility of all government services has created a chance for these lesser-known ISPs to establish a foothold in this crucial industry.

Previously, the absence of DDoS protection services prevented them from bidding for government tenders due to the high costs and substantial effort required for productization. Fortunately, Nexusguard's Transformation Alliance Program (TAP), and deployment of Nexusguard Bastions now offers a solution to address this challenge, enabling these ISPs to overcome the barriers and establish a presence in this critical industry.

GOVERNMENT CYBERSECURITY: CHALLENGES AND REQUIREMENTS

Governments often grapple with unique challenges when it comes to implementing robust cybersecurity solutions. The sensitive nature of government operations demands a highly secure and reliable network infrastructure to protect against evolving cyber threats and ensure uninterrupted service delivery and data security. Below are key challenges faced by governments:

Data Sovereignty

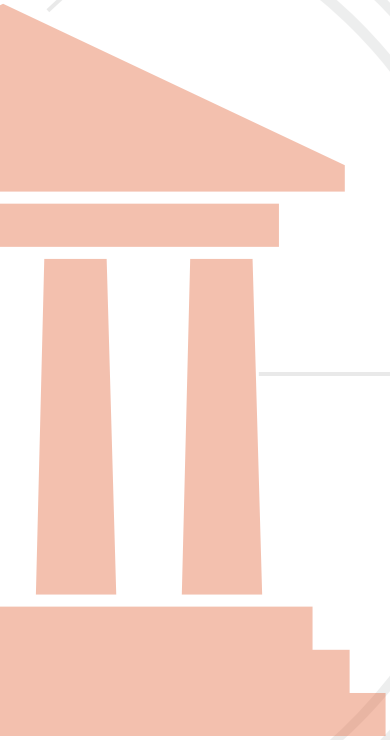
Government data and information are inherently sensitive, particularly for ministries like the Ministry of Defence, Home Affairs, and the Prime Minister's Office. These ministries prioritize data integrity and often favor a limited approach to data availability. Access from within the country's borders typically takes precedence over external access.

DNS Security

Cyber attacks spare no industry. Among the favored targets for threat actors lies the Domain Name System (DNS), vulnerable to exploitation in the absence of robust security protocols owing to its inherent openness. Within the governmental domain, DNS attacks pose significant threats. Given the vast repositories of highly confidential data managed by governments and their agencies, ranging from voter records to tax information, the aftermath of such attacks can be profound, making DNS security a critical component of any government's digital infrastructure.

Web Application and API Protection

Government websites require robust defenses against attacks targeting APIs and vulnerabilities in web applications due to several critical reasons. Interconnected government applications aim to streamline federal communication, but this connectivity can pose a significant risk if exploited by a proficient attacker. Disruptions preventing site access could have dire consequences during emergencies when crucial information must be disseminated. Moreover, the stakes are exceptionally high for government websites, as a breach of classified information could tarnish a country's reputation or even trigger international incidents.



Inter-Agency Coordination

In many countries, the Government comprises multiple agencies, each with its own services and systems. These agencies are typically centrally managed or overseen by an agency specifically created for this purpose. Central agencies are tasked with coordinating cybersecurity initiatives across various agencies and departments, necessitating a unified and collaborative approach to DDoS protection.

Incident Response and Crisis Management

Governments require robust incident response strategies to effectively handle and alleviate the impact of DDoS attacks promptly. This entails establishing a synchronized crisis management approach for public communication and swift service restoration, reducing reliance on service providers who solely act as communication conduits to vendors situated elsewhere globally.

THE NEXUSGUARD'S BASTIONS SOLUTION

Nexusguard Bastions stands at the forefront of comprehensive managed solutions, enabling the seamless deployment of Nexusguard services at on-premises or edge locations. Specifically designed for ISPs grappling with the repercussions of cyber attacks or seeking to augment their product offerings with advanced security capabilities, Nexusguard Bastions seamlessly combines carrier-grade hardware and cutting-edge technology.

Through the integration of our Bastions servers and strategically positioned Bastions PoPs (Points of Presence), ISP's can effortlessly extend the reach of our comprehensive security solutions to their clients within their local areas. This includes delivering a range of services, including Clean Pipe, Origin Protection, Application Protection and DNS Protection, all customized to meet the unique needs of organizations across various sectors, including government, healthcare, and education.

NEXUSGUARD BASTIONS ENABLED ISPs TO PROTECT THE GOVERNMENT SECTOR

Recognizing Nexusguard's expertise in the cybersecurity field, several ISPs joined forces with the company to bolster their bids for the government tender. Leveraging Nexusguard's acclaimed Bastions services, which offer advanced threat detection, mitigation capabilities, and a wide range of security solutions, these ISPs found optimal solutions to address governmental challenges and fulfill stringent security prerequisites effectively.

Clean Pipe Provided an Added Layer of Protection for Government Networks

Integrating Clean Pipe served two important purposes. Firstly, it helped ISPs to protect themselves by maximizing network availability and reducing congestion on downstream clients' Internet uplink caused by volumetric attacks. With Clean Pipe in place, government networks experienced a substantial boost in network performance and uninterrupted connectivity, ensuring smooth operations even in the face of volumetric attacks.

Secondly, it ensured that all data processing took place on-premise, eliminating any concerns related to data sovereignty. With this solution, governments could maintain complete control over their data, keeping it in-country within the confines of their own infrastructure, and ensure that sensitive information stayed under the jurisdiction of the respective government.

Nexusguard DNS Protection Maximized Availability for Governments' Authorized Name Servers

Nexusguard's DNS Protection operates continuously in an "always-on" mode, ensuring constant and reliable defense for government DNS infrastructures, serving as an impenetrable barrier against potential threats with unwavering watchfulness.

Additionally, Nexusguard's DNS Protection provides the option of deploying in ANYCAST mode, enabling the distribution of DNS traffic across diverse Points of Presence (PoPs), enhancing the reliability and resilience of government DNS infrastructures significantly.

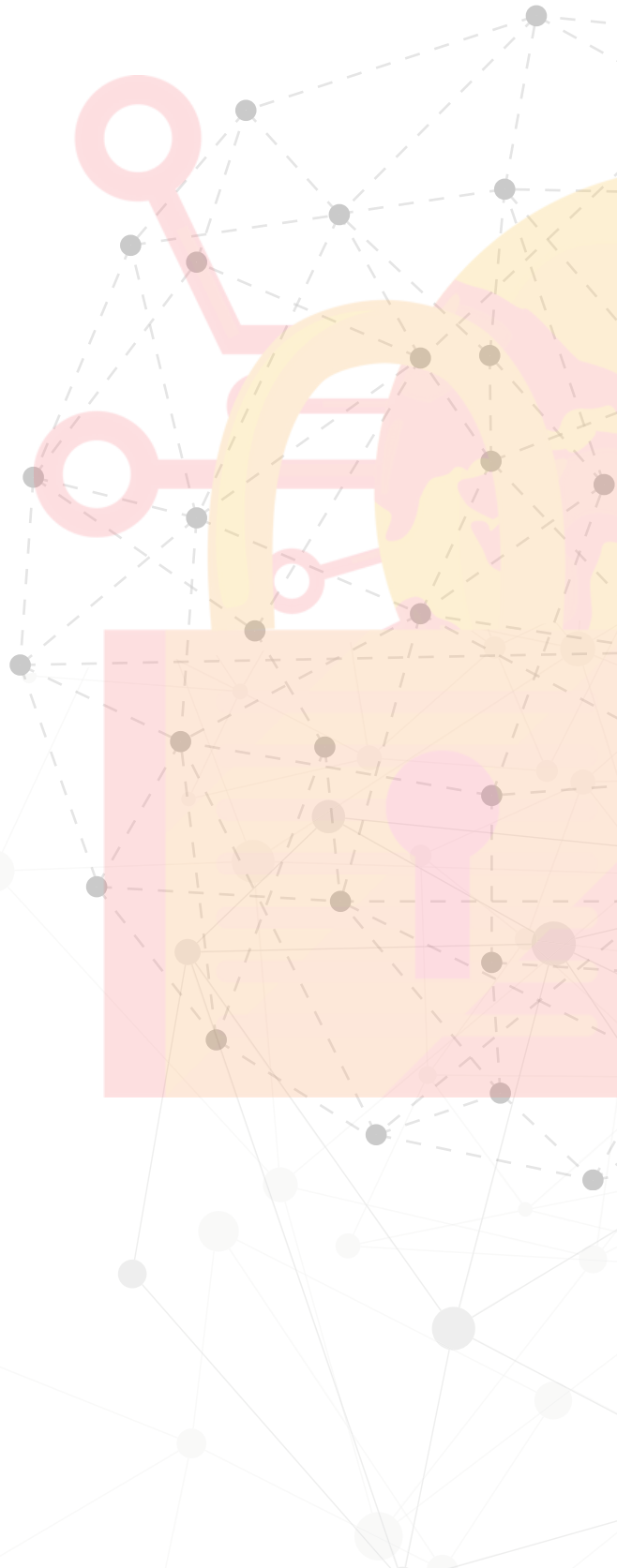
Moreover, Nexusguard leverages its robust cloud bandwidth to reinforce DNS Protection, guaranteeing smooth management of large traffic volumes. This capability enabled government DNS infrastructures to sustain peak performance levels even during periods of high usage.

Government Websites Secured by Nexusguard Application Protection & WAF

In an era marked by rapidly evolving threats, a robust solution is essential - one that strengthens multiple layers of both network and application security. This is where Nexusguard Application Protection, equipped with an enterprise-grade Web Application Firewall (WAF), made a significant impact in safeguarding government websites and applications.

Nexusguard Application Protection transcends the capabilities of traditional firewalls, offering a comprehensive security strategy that protects various layers of network infrastructure and applications. By leveraging advanced technologies and intelligent algorithms, it effectively detects and mitigates sophisticated cyber threats, ensuring the resilience and integrity of the entire system.

With the enhanced security provided by Nexusguard Application Protection, governments can confidently navigate the dynamic threat landscape through a secure environment for their APIs and web services.



Federated Multi-Agency Control Dashboards Simplified the Management of Security Measures for Governments

Nexusguard provides a multi-tiered and integrated dashboard that seamlessly integrates analytics, and visually presents a multitude of metrics, event logs and reports for governments to monitor and manage ministries, agencies, and individual departments. This offering enabled governments to maintain a comprehensive overview of the country's cybersecurity posture at any given moment, proving invaluable during emergencies. Enhanced visibility facilitates strategic resource reallocation during crises, while in peacetime, such visibility and control support strategic learning initiatives and capacity planning efforts.

24/7 Security Operations Center (SOC) Ensured Swift Response to Security Incidents and Emergencies

Nexusguard's Security Operations Center (SOC) is staffed by a team of highly skilled security experts who diligently monitor and defend against evolving threats round the clock. Wth access to leading-edge threat intelligence systems and real-time monitoring tools, the SOC ensures swift identification and resolution of security incidents, emergencies and crises, offering proactive defense for governmental entities.

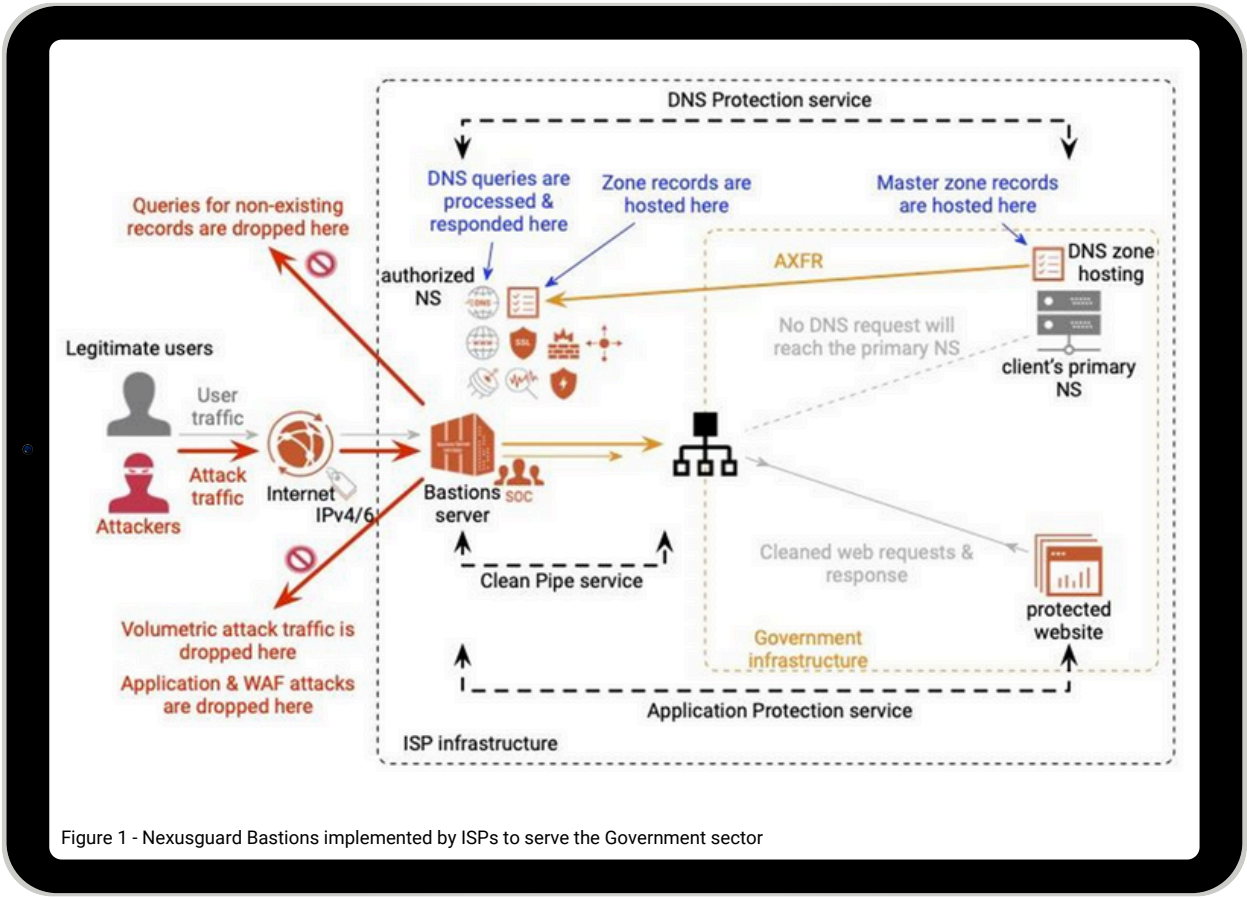


Figure 1 - Nexusguard Bastions implemented by ISPs to serve the Government sector

COMMERCIAL SUCCESS AND REVENUE GENERATION

Nexusguard's partnership with ISPs in Asia Pacific not only facilitated their entry into the government sector but also resulted in remarkable commercial success. By providing comprehensive managed services and seamlessly delivering multiple solutions through Nexusguard Bastions, ISPs not only tackled and resolved the challenges faced by governments, but also generated substantial revenue, enhancing their position in the industry. This successful venture exemplifies how collaboration with cybersecurity experts like Nexusguard can open new avenues for ISPs in previously untapped markets.

SOCIAL IMPACT: SAFEGUARDING NATIONS FROM CYBERSECURITY BREACHES

Beyond its commercial achievements, the partnership between Nexusguard and ISPs holds immense social significance. By safeguarding critical government services in departments such as immigration and law enforcement, ISPs played a vital role in protecting nations from potential cybersecurity breaches. Recent incidents, such as the compromise of Indonesia's national data centre by cyber attackers, disrupting immigration checks at airports, serve as stark reminders of the increasing cyber threats faced by nations globally. Through their collaborative efforts, Nexusguard and ISPs contribute to maintaining national security and fortifying digital resilience.

About Nexusguard

Nexusguard, a leading Singapore-based cybersecurity vendor, specializes in proven Anti-DDoS solutions. With 15 years of experience, Nexusguard protects major service providers, enterprises, and governments worldwide. Recognized by Gartner, Forrester, and other top research firms, Nexusguard delivers proven defense against the largest and most complex cyber attacks.

Contact Nexusguard today to fortify your defenses with Patriot Net! Reach out now to learn more.

contact@nexusguard.com www.nexusguard.com/patriotnet