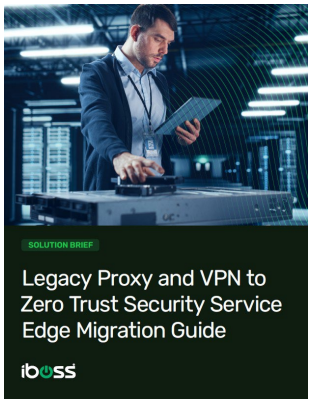

Legacy Proxy and VPN to Zero Trust Security Service Edge Migration Guide

Thank you for downloading this iboss solution brief. Carahsoft serves as iboss' Master Government Aggregator® making the company's cyber solutions and services available to the Public Sector through Carahsoft's network of reseller partners, Solutions for Enterprise-Wide Procurement (SEWP) V, Information Technology Enterprise Solutions – Software 2 (ITES-SW2), NASPO ValuePoint Cooperative Purchasing Contract, and other contract vehicles.

To learn how to take the next step toward acquiring iboss' solutions, please check out the following resources and information:

For additional resources:
carah.io/ibossResources

For upcoming events:
carah.io/ibossEvents

For additional iboss solutions:
carah.io/ibossSolutions

For additional iboss NetBackup solutions:
carah.io/ibossNetBackup

To set up a meeting:
iboss@Carahsoft.com
(703)-889-9710

To purchase, check out the contract vehicles available for procurement:
carah.io/ibossContracts

For more information, contact Carahsoft or our reseller partners:
iboss@carahsoft.com | (703)-889-9710

SOLUTION BRIEF

Legacy Proxy and VPN to Zero Trust Security Service Edge Migration Guide

iboss

Table of Contents

03 Overview

04 Architectural Overview

05 High Level Transition Process Outline

05 Mapping Connectivity and Security from Legacy On-Prem Proxies

06 Mapping Proxy Connectivity Method

07 Resource and Vendor Anchoring via Enterprise IP Space

07 Mapping Security Policies to the iboss Service

07 Mapping Authentication to the iboss Service

08 Mapping Security Policies to the iboss Service

09 Replacing On-Prem Policies with iboss Onsite Policy Enforcement Points

10 Connect Remote Users to the iboss Zero Trust Security Service Edge

11 Geo-Location Capabilities

11 Bypassing Traffic from the Service Edge

11 Ensuring the iboss Service Edge can Communicate with all Enterprise Resources

12 Leveraging iboss Browser Isolation to Replace VDI for Contractors, Guest & BYOD

13 Summary

Overview

The iboss Zero Trust Security Service Edge is a SaaS security service that provides the capabilities traditionally found in legacy on-prem proxies and traditional VPNs but delivers them using a cloud-based delivery model that follows modern Zero Trust principles which can connect and protect workers while offsite, while ensuring applications and data are only accessible by approved users. The iboss Zero Trust Security Service Edge follows the NIST 800-207 Zero Trust Architecture framework which is designed to protect users and resources regardless of location. The unique containerized architecture of the iboss Zero Trust Security Service Edge allows the service to deliver all connectivity and security capabilities using a single unified global service to ensure connectivity, security, policies and logging are consistent across the enterprise and can be configured through a centralized service that applies its capabilities consistently across the enterprise.

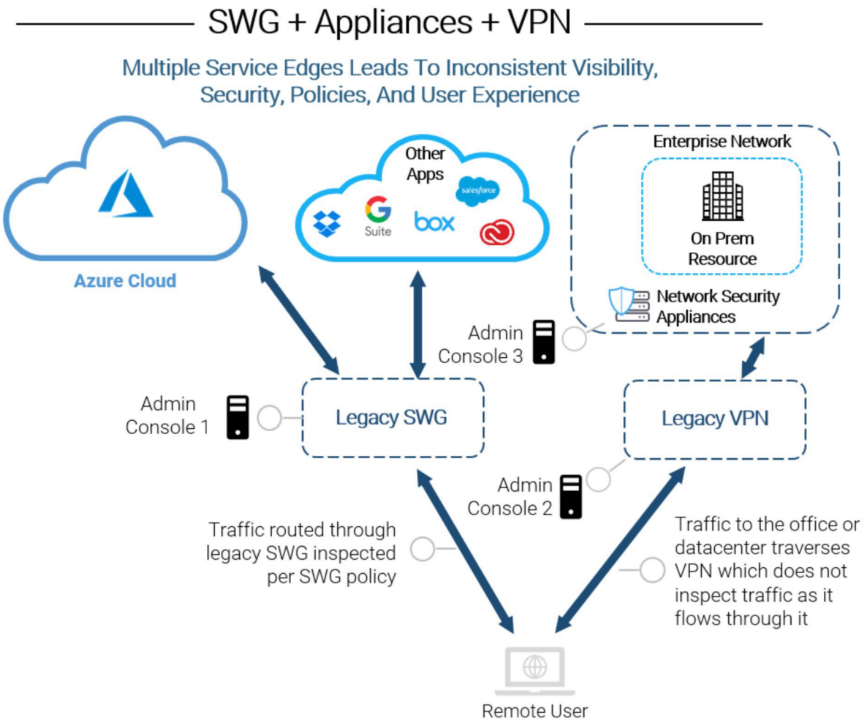

Figure 1- Complexities of found in legacy on-prem proxies and traditional VPNs

One of the key components that the iboss service provides is the ability to deliver "continuous adaptive access" decisions throughout every interaction between users and resources. This ensures that access to resources is terminated automatically when situations arise such as a device becoming infected with ransomware which prevents the spread of ransomware across the enterprise. This key concept is described in the NIST 800-207 Zero Trust Architecture which is implemented by the iboss service.

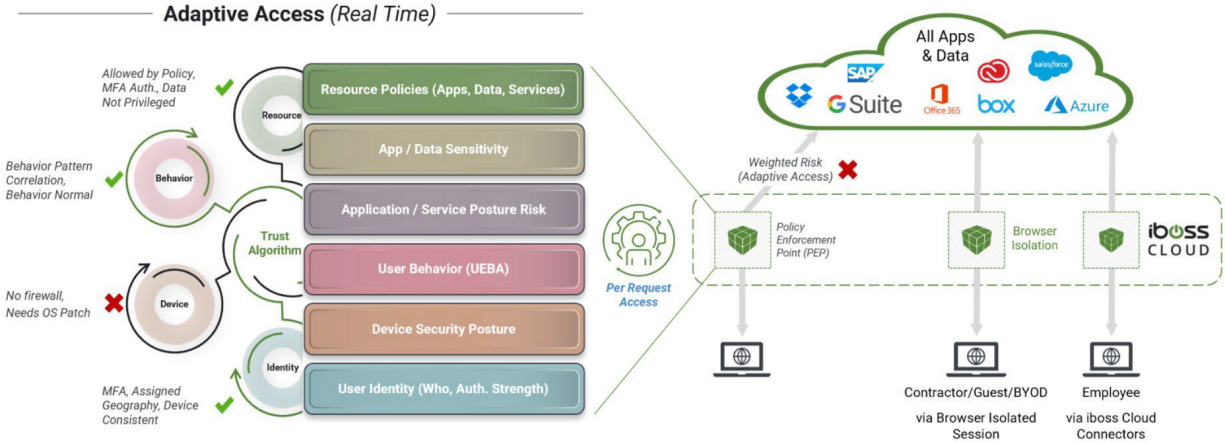

Figure 2 - iboss provides "continuous" adaptive access verifying every request before allowing access. This prevents the spread of ransomware, for example, as infected devices are immediately cut from accessing sensitive resources

© 2022 iboss, All Rights Reserved.

This guide is designed to provide guidance for migrating from legacy on-prem proxies, traditional VPNs and legacy VDI to iboss. This allows for the consolidation and reduction of costs while increasing security and enabling a work from anywhere model. The capabilities found within the iboss Zero Trust Security Service Edge are extensive and can replace all of the functionality that is found in enterprise-grade on-prem proxies without network redesign or restructuring. This makes a quick transition possible without disruption to the organization.

Architectural Overview

The transition to the iboss Zero Trust Security Service Edge expands security and visibility, while reducing costs, by ensuring all users and resources are protected regardless of location and without reliance on the enterprise datacenter. Connections from users will traverse directly through the iboss service edge before reaching the final destination of the connection without the need to send those connections back through the datacenter. The service edge is responsible for running CASB, malware defense, data loss prevention, and logging. The unique advantage of the iboss service is that it maintains a single service edge globally so security and visibility is equally applied to all users and resources regardless of location. This also ensures continuous adaptive access decisions are applied to every connection, between every user and resource, regardless of location as well.

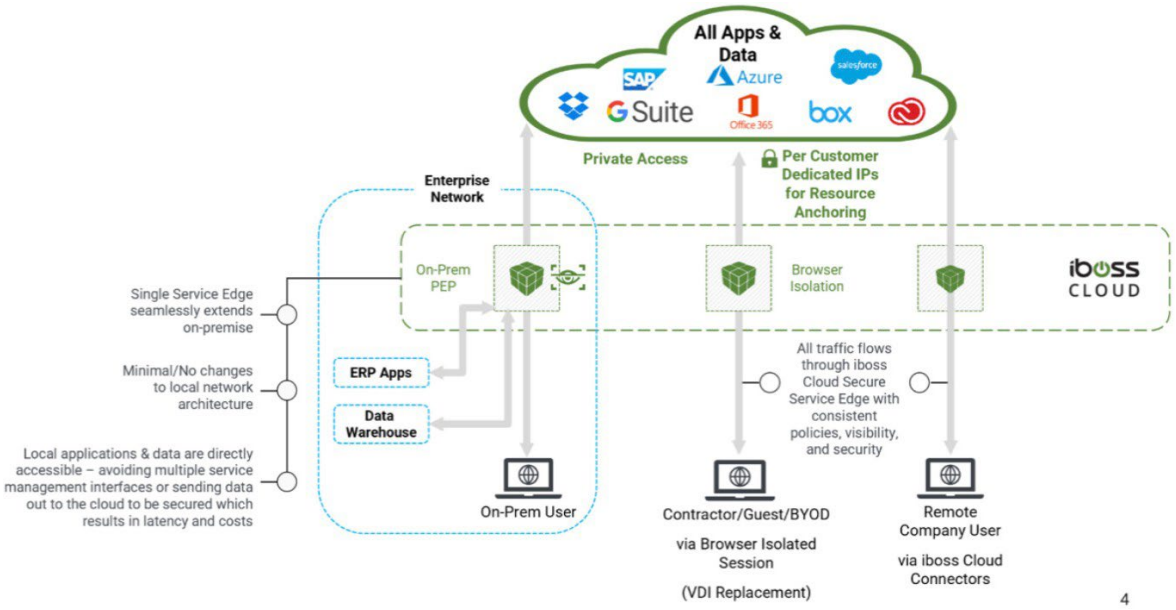

Figure 3 - iboss maintains a single, global Security Service Edge (SSE) that extends gateways into the datacenter to replace legacy on-prem proxy appliances. This provides consistent security, policies, compliance and logging across all users and resources

In the diagram above, notice that the iboss service edge has the ability to extend into the datacenter while still maintaining a single Zero Trust Security Service Edge. This is an important concept to understand as it is this ability that makes it possible to replace legacy on-prem proxy appliances without changing the datacenter network topology. It also provides on-prem users direct access to on-prem resources without needing to send connections out to the cloud security edge and back creating a "trombone" effect. Finally, it allows onsite resources to gain the benefits of complete isolation and continuous adaptive access protection which is provided by the iboss Zero Trust service which increases the security posture of the organization.

© 2022 iboss, All Rights Reserved.

It is important to note that moving to a Zero Trust Security Service Edge is not a one-shot, one refresh cycle journey. It is an iterative process that can be done by first modernizing the security and connectivity approach by replacing legacy technologies such as on-prem proxies and VPN, then continuing on by tightening access to resources and tuning adaptive access policies for even more protection. This allows an enterprise to transition budgets to modernize the connectivity and security approach quickly while providing the foundation that will benefit the organization for years to come.

High Level Transition Process Outline

Transitioning from legacy proxies and VPN to the iboss Zero Trust Security Service Edge can follow the process outlined below:

1. Map legacy proxy policies to the iboss service. All policies found in legacy on-prem proxies can be ported to the iboss service with its extensive policy engine.
2. Replace legacy on-prem proxies with iboss Gateway/Policy Enforcement Points with no network changes to the datacenter. At this point, legacy proxies are decommissioned and budget for on-prem proxies is eliminated.
3. Connect work-from-anywhere users to the iboss Security Service Edge via cloud connectors. Cloud connectors are iboss agents that encrypt and steer traffic through the iboss service automatically and provide device posture checks to ensure devices have their firewall enabled, antimalware enabled, have critical patches installed and perform other checks to ensure device health.
4. Ensure the iboss Zero Trust Security Service Edge can communicate with all apps and data, including those located within the datacenter, so that it can provide access to users regardless of location. There are many options available to achieve this including creating tunnels between the iboss cloud gateways and the datacenter or allowing the cloud gateways to communicate with the onsite gateways which can broker connections to onsite resources. At this point, legacy VPNs are eliminated including the budget used for VPN access as the iboss service can now connect users to any application or data.
5. Connect contractors, guests, high-risk users such as call center agents and BYOD to applications and data via iboss Browser Isolation which provides VDI-like access to resources but instead accomplishes this leveraging the end user browser to separate the user from the data. At this point, VDI budget can be consolidated.

This guide will walk through the five steps above. Remember, not all steps need to be accomplished at once and during the first pass to get the benefits of cost reduction and increased security benefits.

Mapping Connectivity and Security Policies from Legacy On-Prem Proxies

There are two key components to consider when replacing legacy on-prem proxies. The first is ensuring the connectivity method being used is supported to minimize network changes. The second is porting the security and logging policies to the new platform. Typically, ensuring the connectivity method being used matches the new platform during the transition makes things easier but is not a hard requirement. As long as a connectivity method is supported that allows the devices, including OT and IoT, to connect to the proxy, it will be enough to ensure a smooth transition. Ensuring the security and logging policies are supported by the new platform is typically a requirement that must be met. The iboss platform includes an extensive connectivity and policy engine which ensures that a transition to the iboss Zero Trust Security Service Edge is possible, easy and smooth.

© 2022 iboss, All Rights Reserved.

Mapping Proxy Connectivity Method

In this step, first identify the connectivity method being used by the legacy on-prem proxy that is being replaced by iboss. The iboss supports a vast amount of connectivity methods and will likely support the method currently being used. Below is a list of the most common connectivity methods:

Connectivity Methods	Description
F5 Load Balancing to Proxies	In this scenario, an F5 load balancer is used to distribute proxy requests across an array of on-prem proxies. The containerized nature of iboss allows this method to be easily supported. The F5 load balancers will distribute the load across horizontally scaling iboss Policy Enforcement Points which replicate their policy across the cluster.
Cisco WCCP	In this scenario, Cisco routers or switches transparently redirect traffic to the on-prem proxies via the WCCP protocol. The iboss service supports WCCP.
Cisco ITD	Similar to WCCP, the Cisco ITD protocol is configured within Cisco switches and routers and transparently redirects traffic to on-prem proxies. The iboss platform supports ITD and onsite iboss Policy Enforcement Points will take the place of legacy on-prem proxies.
Explicit Proxy Settings	In this scenario, on-prem devices are configured with proxy settings or a Proxy Auto-Configuration script (PAC) that causes the devices to send their traffic through the on-prem proxies. The iboss platform supports explicit proxy and PAC settings. The iboss platform also supports the ability to create multiple proxy ports, each with different default policies so that they can be applied to different sets of users and devices.
SOCKS proxy	Typically used for IoT and OT, traffic is redirected to the proxies to support non-HTTP protocols. The iboss platform supports SOCKS proxy and can drop-in replace this functionality.
FTP Relay	This is used for scenarios where OT/IoT need to perform FTP functions but do not support proxy settings. The proxies simulate the destination FTP server and relay the traffic between the client and the destination. The iboss platform supports FTP relay.
Agents	In this scenario, a software agent is installed on devices/laptops to redirect traffic to the proxies. The iboss cloud connectors are specialized for this purpose and support on and off-prem traffic redirection as well as device health posture checks. The iboss cloud connectors also support automatically performing encrypted DNS via DoH and install the root MITM decryption certificate needed for HTTPS inspection.
DNS	In this scenario, DNS queries are redirected to a service which inspects the queries for malware and security policies. This is typically used for BYOD or IoT/OT scenarios. The iboss platform provides this capability. Client DNS settings are pointed to iboss which performs DNS resolution and security/logging functions.
Tunnels	In this scenario, tunnels are created to a cloud security service to redirect traffic from branch offices or the datacenter automatically to the cloud security service. The iboss platform supports GRE and IPSec tunnels as well as integration with SD-WAN to automatically capture traffic and send it to the cloud security edge.
ICAP	The iboss platform supports ICAP with the ability to send objects it processes to other ICAP services. This includes decrypted objects and other request attributes that can be used to integrate with additional DLP engines and other analysis services.

Figure 4 - iboss supports all network data redirections found in legacy on-prem and cloud proxies to make migrations frictionless and easy

© 2022 iboss, All Rights Reserved.

Resource and Vendor Anchoring via Enterprise IP Space

In many scenarios, vendors are tied to the enterprise by creating virtual wires using ACLs that include the enterprise IP Address space. For example, LexusNexus only allows access from traffic originating from the enterprise datacenter. In addition, anchoring resources to the Security Service Edge prevents users from accessing those resources directly and allows continuous adaptive access as well as security policies to be applied before access is granted. This is typically achieved using ACLs to datacenter IP space to create a virtual wire to the application from the proxies.

The iboss Zero Trust Security Service Edge provides dedicated IP address space for each customer. This ensures that vendor integrations and resource anchoring is possible, even in cases where a user is working from home and connecting directly to a SaaS application, such as Microsoft Office 365, without traversing the enterprise datacenter first. This is a unique capability of the iboss platform which allows offloading traffic from the datacenter for fast connections and reduced costs while meeting the requirements from anchored vendors and resources.

Mapping Security Policies to the iboss Service

The iboss service includes an extensive policy and security engine. This process typically consists of two parts. Mapping user identity to a directory service, such as Active Directory or Azure AD, and mapping the connectivity and security policies from the legacy proxies to the iboss service.

Mapping Authentication to the iboss Service

The iboss platform supports a wide variety of user authentication methods with some of the most popular authentication methods found in legacy proxies listed below.

Connectivity Methods	Description
NTLM	The iboss platform supports NTLM for authentication. NTLM is typically used for on-prem users in traditional environments as NTLM is an on-prem authentication protocol. With the need to transition authentication so that users are authenticated both on and off prem, typically NTLM is replaced with authentication via agents which can leverage SAML via Federated Identity Providers.
Kerberos	The iboss platform supports Kerberos. Similar to NTLM, this is typically replaced with authentication via the iboss cloud connectors. However, for on-prem devices such as OT/IoT, this can be leveraged as well.
SAML	Used for authentication against Federated Identity Providers, the iboss platform supports SAML for integration with Identity Providers such as Azure AD, Okta and Ping. The iboss platform can also extract login attributes such as user groups from the SAML authentication assertion.
OIDC	OIDC is typically used for Azure AD authentication. OIDC integration to Azure AD is supported by the iboss platform.
Statistic User Authentication	The iboss platform supports defining static users with username and password stored within the iboss platform.
Statistic IP assignment	In some cases, assigning an identity to OT/IoT is performed by mapping IP addresses to those devices. The iboss platform supports static IP mapping to device names and specific policies.

© 2022 iboss, All Rights Reserved.

Connectivity Methods	Description
Agent Based Authentication	The iboss cloud connectors can extract the currently logged in user from devices automatically based on the user that logged into the OS. The agents also support step-up authentication and SAML.
SAML + MFA for legacy applications	The iboss platform can perform SAML and MFA checks before access is granted to legacy applications. This provides the ability to perform MFA in cases that the application only supports legacy authentication methods, such as basic auth.

Figure 5 - iboss supports a wide variety of authentication methods to ensure any method currently used for authenticating users is easily migrated to the new service

For authentication, choose the method that makes the most sense for the business outcome being achieved. For example, if users are able to work remotely, choose the iboss cloud connectors which provide authentication in addition to providing data encryption and redirection to the cloud service and device health posture checks. Then use similar authentication methods for OT/IoT/Guests/BYOD to ensure a seamless transition.

Mapping Security Policies to the iboss Service

The next step is to map security policies to the iboss service. The iboss platform supports multiple security groups as well as a concept named policy layers. Typically, users and devices get unique default policies based on one of many groups that can be configured. Policy layers are dynamic policies that are added to each request and can be linked to users, groups, OUs or IP subnets. They contain lists of allow lists, block lists and categories that are applied to each connection. Policy layers are a great strategy for mapping legacy proxy "policy objects" that serve a similar function. The process of migration typically involves mapping policy objects to iboss policy layers.

In addition, the iboss service contains all policy constructs found in legacy enterprise proxies to ensure a one-to-one mapping of policies. This includes categories, allow lists, block lists, keyword matching, malware content analysis, threat feeds including CnC callback detection and more. Proxy combinatorial rules provide the ability to create rules that match any aspect of a request and take an action such as block or forward the request to another proxy or service.

The process of mapping the security policy from the legacy proxy typically involves exporting the policy configuration from the legacy proxies and using that to create those policies within the iboss service. If help is needed in this process, iboss provides professional services support that has extensive experience mapping Broadcom, McAfee and other proxy configuration to the iboss platform which minimizes overhead on staff.

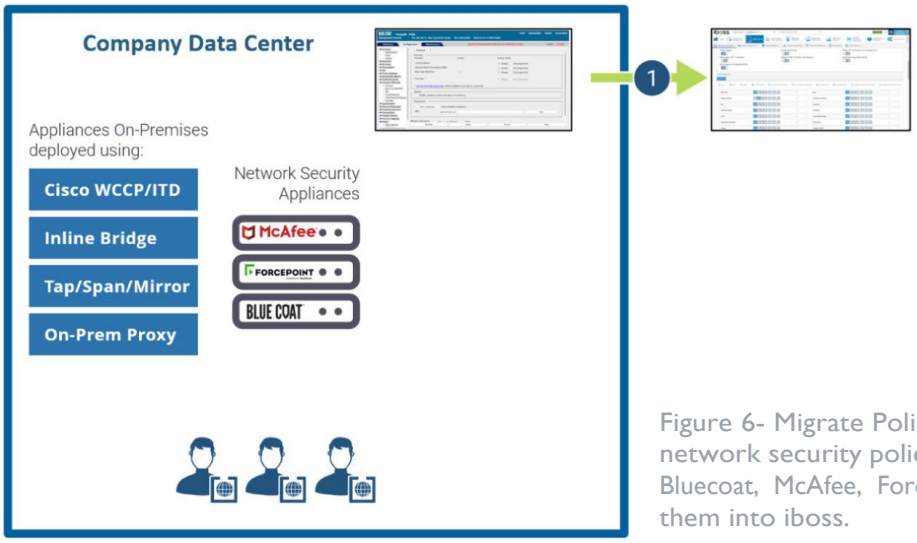

Figure 6- Migrate Policies & Configuration - Take existing network security policies & configuration from Broadcom Bluecoat, McAfee, Forcepoint, WSA, Palo Alto and import them into iboss.

© 2022 iboss, All Rights Reserved.

Replacing On-Prem Proxies with iboss Onsite Policy Enforcement Points

Once connectivity, authentication and policies are ported, the iboss Policy Enforcement Points can be used as drop-in replacements for legacy on-prem proxies without disrupting the network topology in the datacenter. The difference between iboss onsite Policy Enforcement Points and legacy proxies are substantial:

1. Unlike legacy on-prem proxies that only provide security and logging for on-prem users, iboss PEPs are just an extension of the single unified Security Service Edge meaning policies, security and logging applied to traffic through onsite PEPs will match traffic that traverses the iboss cloud PEPs from remote workers. This ensures a unified connectivity and security policy.
2. Traffic flowing through the iboss onsite PEPs has all security applied locally without needing to send the traffic through iboss cloud PEPs, which allows the traffic to exit the datacenter directly and reach the destination without additional hops. It does this while ensuring remote user traffic is never sent through the datacenter and instead sent through the iboss cloud PEPs which send traffic directly to the destination which reduces datacenter costs and improves performance.
3. Resources that are local to the datacenter can be accessed through the iboss onsite PEPs with the traffic never leaving the datacenter while maintaining the same global security and logging. This provides direct, in datacenter connections.
4. The iboss onsite PEPs receive all of their configuration automatically through the global cloud security service which is configured through a unified single admin console. This ensures they are treated as another Point of Presence (POP) and not standalone appliances as is the case with legacy on-prem proxies.
5. The onsite iboss PEPs can act as connection brokers, if desired and configured, receiving encrypted connections from iboss cloud PEPs allowing remote users to access datacenter resources using Zero Trust principles and without the need to configure tunnels to the iboss cloud service.
6. The iboss onsite PEPs support full continuous adaptive access to protect on-prem resources and provide micro-segmentation to all datacenter resources eliminating direct user access while onsite.

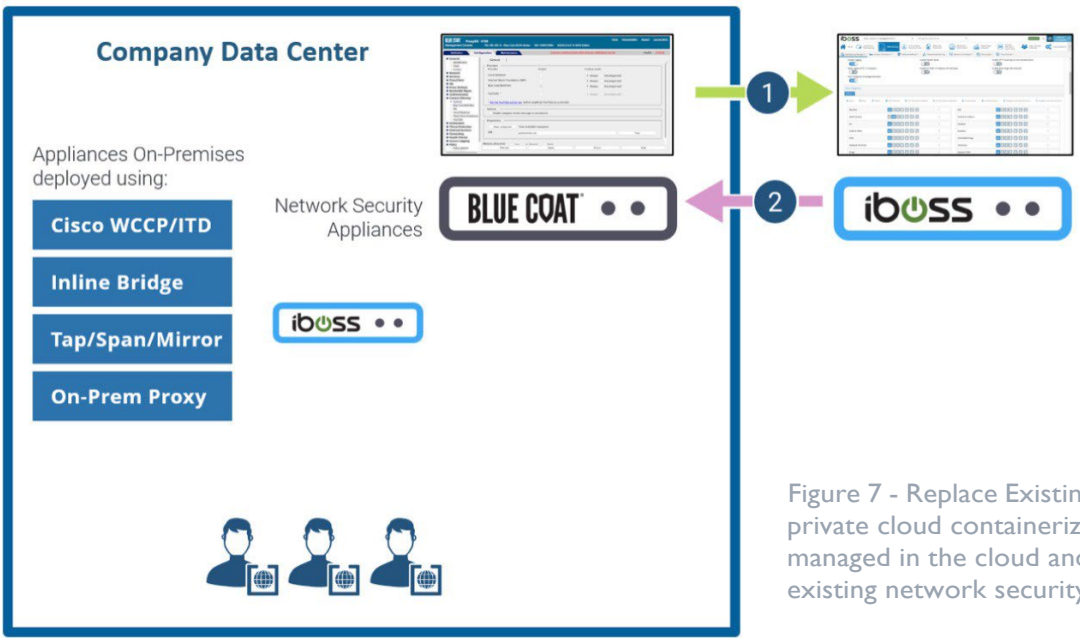

Figure 7 - Replace Existing Hardware - Take iboss private cloud containerized gateways that is managed in the cloud and easily drop-in replace existing network security hardware.

© 2022 iboss, All Rights Reserved.

When replacing legacy proxies, the IP Addresses of the legacy proxies can also be transferred to the iboss onsite PEPs. This can reduce configuration changes on devices such as OT and IoT. This is not required, however, and an alternative approach is to configure the iboss onsite PEPs with new IP addresses which allow traffic to be steered off of the legacy proxies to the iboss PEPs. Regardless of the approach, the onsite PEPs will simply be an extension of the single global cloud security service and apply consistent security across the enterprise.

Connect Remote Users to the iboss Zero Trust Security Service Edge

The next step involves connecting remote users to the iboss Zero Trust Security Service Edge. This ensures:

1. All user traffic is automatically steered through the iboss service before reaching any destination for security and logging
2. Traffic is secured and logged without having to traverse the data center first
3. Continuous adaptive access is applied while users are remote when accessing enterprise resources
4. The legacy VPN is eliminated as users are connected to all enterprise resources including SaaS and on-prem data and applications

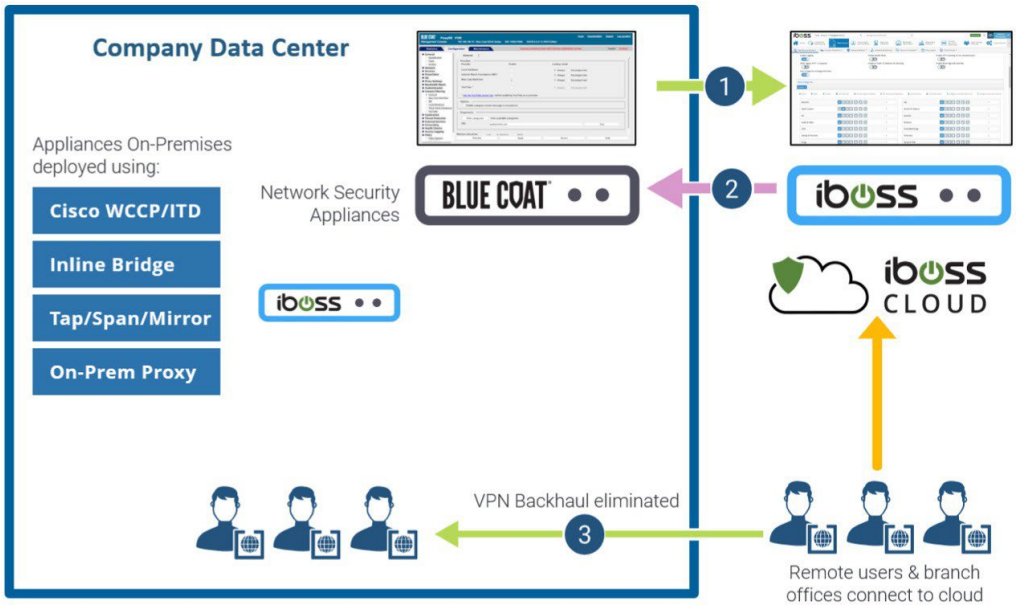

Figure 8- Connect Users - Remote users directed to closest iboss cloud resource and eliminate backhaul with VPN's to data center.

This step is easily accomplished by deploying the iboss cloud connectors with iboss supplied agents that perform all of the needed functions to ensure users are securely connected to the iboss service edge. The agents are designed to be bulk pushed and silently installed. For example, the iboss cloud connector for Windows comes in a MSI format that can be silently bulk pushed through SCCM. Other options include pushing the agents via MDM.

This process usually involves deploying the iboss cloud connector on a handful of devices. The agent can be installed manually on Windows, for example. The agents are downloaded from the iboss admin console pre-configured for the account. Once installed, the agents perform key functions that include:

© 2022 iboss, All Rights Reserved.

1. Automatically steering traffic to the iboss security edge regardless of user location
2. Performing device health posture checks (i.e. firewall is on, disk is encrypted, critical patches are installed)
3. Automatically intercept DNS queries and encrypt them, sending them to the cloud service for resolution. This helps easily meet compliance requirements and ensures local DNS attacks are mitigated.
4. Install the MITM root certificate needed for HTTPS decryption automatically. The root certificate is downloaded from the iboss cloud service and can be an existing enterprise decryption certificate that is already in place. This allows copying the original MITM certificate to the iboss platform.
5. Have the ability to perform step-up authentication Traffic is secured and logged without having to traverse the datacenter first

Once installed, users can go on and off-prem while traffic is always redirected to the iboss Zero Trust Security Service Edge for security and logging.

Geo-Location Capabilities

The iboss platform includes the ability to geo-locate users and steer traffic automatically through the closest iboss Policy Enforcement Point. This also includes determining when a user is on-prem and steering traffic through onsite PEPs automatically. Geo location is performed by mapping the user's public IP to the user location. Zones can also be created within the iboss platform to force traffic to remain within region (i.e. for GDPR) or redirect traffic through specific PEPs to get to a destination (Software Defined Perimeter/SDP).

Bypassing Traffic from the Service Edge

Traffic can be bypassed from the service so that it reaches its destination directly rather than through the service edge. Bypasses can be configured to be applied only when a user is at a certain location or coming from a particular geo-region. For example, it may be desirable to have the enterprise video and voice service go direct between devices and the destination. This is not required but can be a preference.

If a PAC file was already being used with bypasses in place, the settings from within the PAC are copied to the iboss service. The iboss service also hosts the PAC configuration which eliminates the need to host the PAC file on servers if that was the case previously. The iboss service contains intelligent and dynamic PAC generation based on criteria such as region or location.

Ensuring the iboss Service Edge can Communicate with all Enterprise Resources

The iboss Zero Trust Security Service Edge allows only approved users to connect to enterprise applications and data across SaaS, cloud infrastructure (AWS, Azure) and on-prem locations. Unlike a VPN which requires a user to be aware of the location of the resource, the iboss service completely abstracts the location and uses dynamic access policies to determine who should be allowed to connect to what resource, regardless of where the resource is located. This provides a better end-user experience as the user does not need to ever enable or disable a VPN to gain access to enterprise resources. The user is always connected to the resources they need regardless of where those resources are located.

In order to broker connections to on-prem applications and data, the iboss service edge must be able to communicate with that resource via a network path. This can be accomplished via a variety of methods. This includes creating tunnels between the cloud gateways and the locations hosting those resources or providing a path to those resources via the onsite

© 2022 iboss, All Rights Reserved.

hosted iboss PEPs which extend the service into the datacenter. All iboss PEPs have unique and dedicated IP addresses per customer. This allows ACLs to be created between cloud PEPs and onsite PEPs which will communicate via encrypted connections to provide access to datacenter resources. This model is referred to as the "enclave model" within the NIST 800-207 Zero Trust Architecture framework.

When this phase is completed, the legacy VPN can be completely retired.

Leveraging iboss Browser Isolation to Replace VDI for Contractors, Guests & BYOD

The iboss platform supports Browser Isolation which provides VDI-like access to applications and data with complete separation between the end-user device and the resource being accessed. The end-user's browser is used to provide the pane of glass which is a stream of pixels that is sent from the iboss service. Typically, this is used to connect non-enterprise owned devices or users performing high risk functions such as call center agents accessing customer data. Using iboss Browser Isolation also provides additional benefits such as:

1. Eliminates the need for hosting and managing VDI infrastructure which results in substantial cost savings
2. Because the data is run through the same global service edge and PEPs, continuous adaptive access can be applied for isolated access scenarios
3. Logging for each access request and click within the isolated application
4. Log forwarding of all accesses to the enterprise SIEM for all interactions within the browser isolated session
5. Ability to provide access to only the applications needed without a full desktop

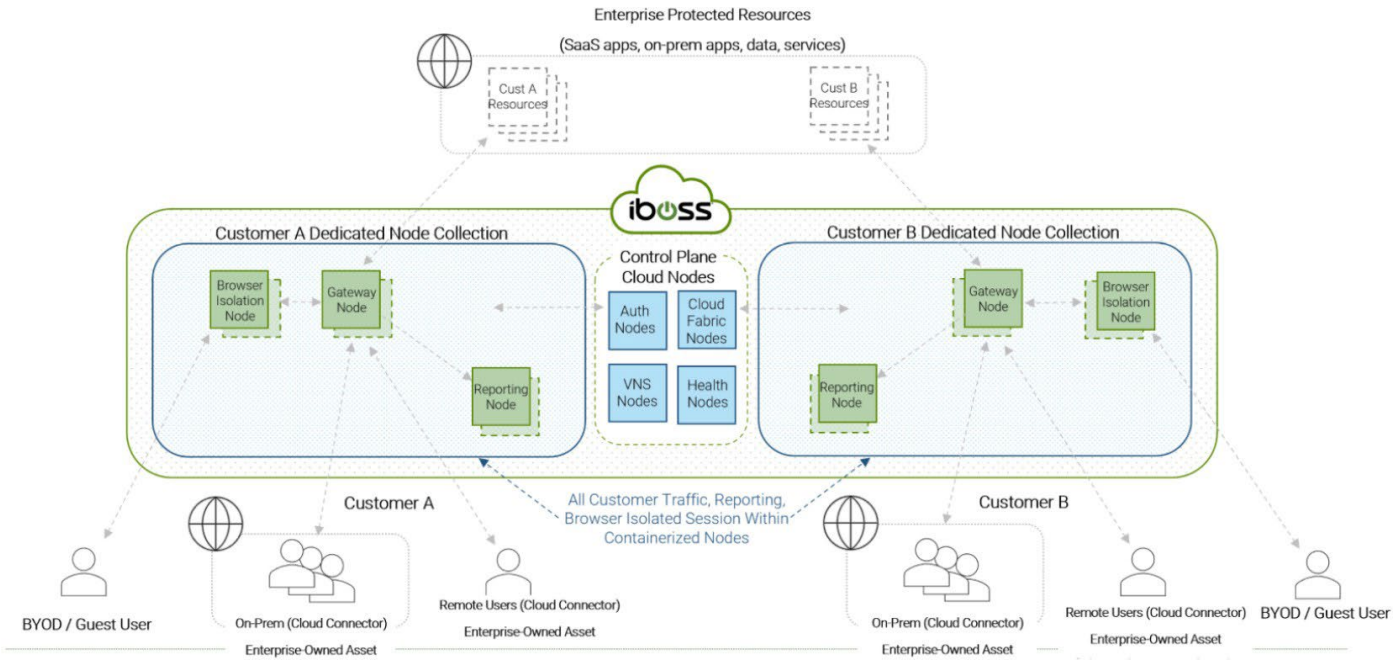

Figure 9 - iboss provides natively integrated Browser Isolation which replaces legacy VDI to provide resource access for contractors, call center agents, guests and BYOD

© 2022 iboss, All Rights Reserved.

As seen above, BYOD/Guest Users will connect through a Browser Isolated session while the connections from that session are run through the same gateway Policy Enforcement Points that are servicing enterprise owned devices. This results in the same global unified service to protect all devices and all resources equally and consistently.

Browser Isolation is typically the last step taken in a migration process and can be performed during a completely different phase that is decoupled from the initial migration process.

Summary

The iboss Zero Trust Security Service Edge has a single unified edge design that makes migrations from legacy on-prem proxies, VPN and VDI possible within a short time frame. The extensive connectivity methods, authentication methods, security and policy engines, and ability to extend natively into the datacenter make it the ideal choice to modernize a legacy security strategy to a global Zero Trust Security Service Edge that can secure and connect all users and resources regardless of location.

© 2022 iboss. All Rights Reserved.

+1 877.742.6832
sales@iboss.com

101 Federal St
Boston,MA 02110

iboss is a cloud security company that enables organizations to reduce cyber risk by delivering a Zero Trust service designed to protect resources and users in the modern distributed world. Applications, data and services have moved to the cloud and are located everywhere while users needing access to those resources are working from anywhere. Built on a containerized cloud architecture, iboss delivers security capabilities such as SWG, malware defense, browser isolation, CASB and data loss prevention to protect all resources, via the cloud, instantaneously and at scale. This shifts the focus from protecting buildings to protecting people and resources wherever they are located. Leveraging a purpose-built cloud architecture backed by 230+ issued and pending patents and more than 100 points of presence globally, iboss processes over 150 billion transactions daily, blocking 4 billion threats per day. More than 4,000 global enterprises trust the iboss Cloud Platform to support their modern workforces, including a large number of Fortune 50 companies. iboss was named one of the Top 25 Cybersecurity Companies by The Software Report, one of the 25 highest-rated Private Cloud Computing Companies to work for by Battery Ventures, and CRN's top 20 Coolest Cloud Security Companies of 2022. To learn more, visit www.iboss.com