

iPass® Policy Orchestration

Introduction

With increasing regularity, enterprises and their employees are firmly embracing the business and personal benefits of working outside the confines of the enterprise network. Consequently, remote access into the enterprise network environment is essential from anywhere Internet connectivity is present – wired or wireless - and users increasingly view a lack of connectivity to critical business applications as unacceptable in the modern organization – whether the user is at a customer or business partner site, in transit, in a public setting, or at home.

In addition, an increasing number of users operate as virtual single-person offices of the enterprise - spending extended periods of time connecting through the Internet to their communities of constituents and non-enterprise Web resources before they dock back into the enterprise environment either remotely or on-site. This leaves them often without VPN protection and out of reach of the protection afforded by enterprise-mandated updates to security and operating system software.

Also, as virtual offices, their laptops or other endpoint devices have become repositories of sensitive information (e.g., business plans, financial statements, sales proposals, private customer records, etc.) that they must retrieve on a moment's notice to accomplish their business objectives. Considering the business, regulatory, and legal risk faced from leaked or stolen information, these endpoint devices should have the same security precautions as the enterprise network servers.

Serious security risks are associated with this mushrooming level of remote access activity and decentralized information storage. The malicious element is forever present, propagating destructive viruses and worms faster and exploiting the weakest point in the connection between users and the enterprise network with increasing sophistication. A significant point of vulnerability is at the origin of remote communication, that is, at the remote and mobile endpoint device. *Unless a protective layer for these devices continuously exists and adapts constantly to the ever-changing characteristics of security threats, the ability of these devices to serve the remote worker as an effective business tool is compromised, the confidentiality of sensitive information is breached, and an unwitting conduit into the enterprise network is created.*

In this paper, we will review how enterprises maintain secure communication with their remote user communities. Since this security is, in reality, a composite of multiple security applications, it is important to understand the protective function that each application performs in order to appreciate how these seemingly standalone applications can be optimally combined to create a more robust remote access security solution. To that end, we

will examine the iPass Policy Orchestration approach to secure connectivity as a new architecture that enables tightly coordinated security for remote and mobile users.

Remote Access Security Foundation

It is well known that communication over the Internet has inherent security risks. The Internet, by its very nature, is an open and shared network for use by anyone with access. Moreover, unless Internet users undertake explicit action, their Internet communication is potentially viewable by other Internet users. This is the first problem that must be solved in using the Internet for business communication involving remote users, that is, *creating private communication over a shared and open network*.

Next, since the Internet user community is not a closed community of known and trusted users, the risk of user falsification is present. This represents the second problem to solve: *establishing a trust relationship with remote users seeking access to the enterprise network*.

Last, by being a member of the Internet community, each member can communicate with potentially any other member. However, a two-way street exists and any other member of the Internet can attempt to communicate with the remote user and the endpoint device without the user's consent or knowledge. With a set of Internet members having malicious intent, probes of unprotected and under-protected endpoint devices followed by infection, information theft, and disruption in operation can and does occur. This situation represents the third problem to solve: *ensuring the remote endpoints are continually protected during Internet communication and can be trusted for access into the enterprise network*. Fortunately, a number of solutions have been developed to address, at least partially, these three problems. Those solutions are:

Addressing Problem #1 – Creating private communication over a shared and open network: Deploy a VPN

Virtual Private Networks (VPNs) – Whether using IPSec (Internet Protocol Security) or SSL (Secure Sockets Layer) Internet security protocol, VPNs have the objective of making Internet communication private by encrypting the packets between communicating devices and ensuring payload integrity.

Addressing Problem #2 – Establishing a trust relationship with remote users seeking access to the enterprise network: Authentication and authorization¹

Although session data is protected from being sniffed from outside the VPN tunnel, procedures should be followed to ensure that the user is authentic and trustworthy. This is the domain of authentication and authorization.

Authentication – There are many authentication methods, with the use of plaintext static passwords being the most common. Being the most common, however, does not equate to being the strongest. Enterprises are recognizing that passwords require too much user

¹ A trust relationship with the user should also include establishing a trust relationship with the user's device. Due to the unique operations involved to establish a trust relationship with the user and the user's device, we will examine each trust relationship separately.

diligence to be an effective method of authentication by themselves and fast-acting spyware exists that can crack even highly complex passwords.

These password shortcomings give rise to the use of two and three-factor authentication methods such as token-based or biometric systems. By adding more factors into the authentication process, the means to falsify a legitimate user's identity or device is more difficult. The enterprise dilemma in using multi-factor authentication methods is that higher costs are associated with layering new systems on top of old, as well as requiring more items (e.g., a token) that a user can misplace or can be stolen, all of which affects user productivity and adds to user support and training costs. Consequently, enterprises should evaluate the added security and cost of multi-factor authentication against the sensitivity of the data and systems being accessed.

Another relevant consideration of the authentication process is credential security, that is, whether the remote users' credentials, especially passwords, are encrypted before leaving their endpoint devices. This is especially critical if user credentials transit the Internet.

Last, two-way or mutual authentication between user and enterprise network equipment adds another layer of protection by ensuring there is mutual agreement between the two entities that communication should occur.

All these factors – authentication method, private communication of user credentials, and mutual authentication – are considerations for the enterprise in choosing the most appropriate authentication process. It is for this reason that access control standards such as IEEE 802.1X and the Wi-Fi Association's WPA specification are growing in popularity, to provide a standardized credential protection scheme between the endpoint and network infrastructure that includes both mutual authentication and credential encryption.

Authorization – Having established procedures to ensure Internet communication privacy and integrity and having chosen the appropriate authentication method, the next step is to define user access rights and privileges. That is, what activities remote users can conduct in the enterprise network. This too has become more sophisticated as enterprises need to better control the level of user access.

Variables used to assign access rights include: who the user is (e.g., rank and responsibility), user affiliations (e.g., department and company), authentication method, and the trustworthiness of the endpoint device (more on this trust relationship in the next problem area). In practice, authentication and authorization operate in a complementary fashion with the most highly trusted users granted the highest level of authorization.

Addressing Problem #3 - Ensuring remote endpoints are continually protected during Internet communication and can be trusted for access into the enterprise network

Just as a trust relationship must be established with the user based on an authenticated identity, a trust relationship must be established with the endpoint device. Devices can be infected with a malicious agent that allows an open door to threats to the enterprise network routed through the endpoint. Authentication and authorization as previously described do not establish a trust relationship with the endpoint device. Originally trusted when "imaged" by the enterprise IT staff, these devices quickly become vulnerable through installation of rogue applications (e.g. peer-to-peer software), unprotected Internet use, or new

vulnerabilities discovered in previously “trusted” application and operating system software. Furthermore, as virus propagation times shorten, delays in delivering virus list updates, security policy updates, and new patches to all endpoints endanger both endpoints and network resources.

Endpoint vulnerability assessment, remediation, and enforcement solutions can reduce endpoint security risks

Recognizing vulnerabilities associated with insecure software applications and Internet-based threats, security and network infrastructure vendors have developed and are refining their solutions to assess the current security state of the endpoint device. Through this assessment, decisions can be made on whether security applications such as anti-virus and personal firewalls are present, up-to-date, properly configured, and operating correctly on the endpoint device and whether the latest critical patches for operating systems have been installed.

If the security applications are resident on the endpoint device but not in operation, the user can be required to launch them or this will be completed automatically. If determined that the anti-virus definitions file, personal firewall rules or the applications or operating system software itself is out-of-date (relative to the enterprise’s policies), options include directing the user to a protected site for a software update (also known as remediation), limiting his/her access rights and privileges (restricted authorization), or disallowing access to the enterprise network entirely. These solutions can be Internet-hosted, hosted within the enterprise demilitarized zone (DMZ), or run from within the network through a VPN tunnel.

There is also emerging a new breed of solutions that enforce remote endpoint policy compliance at the enterprise network edge. These come from well-known companies such as Cisco Systems (Network Access Control), Microsoft (Network Access Protection), and Nortel Networks (Tunnel Guard). Each of these offer solutions that initiate when the user touches the enterprise network and operate as a pre-VPN enforcement process based on a separate compliance agent running on the endpoint. These solutions may provide a remediation capability as well or may shunt the endpoint to a 3rd-party remediation product that actually brings the endpoint into compliance through software updates.

Finally, a number of SSL VPN vendors also offer similar tools to assess the security state of the endpoint device and some offer the means to create a virtual desktop within the endpoint device. This virtual desktop insulates the remote user’s SSL VPN session from “malware” that may be present on the endpoint device. With this technology, virus signatures or their variants do not need to be known in order to be blocked.

Endpoint assessment solutions have limitations

Although these endpoint assessments represent a material improvement in checking the spread of worms and viruses from the endpoint device to the enterprise network and reducing the risk of backdoor entry to the enterprise network, they are not without limitations.

1. **Endpoint assessment solutions from most vendors are designed to protect the enterprise network, not the endpoint devices.** These assessments only occur when the remote user initiates a connection request to the enterprise network. Given that a growing number of remote workers operate as virtual offices that rely on

direct Internet access, they are not afforded this protection on a continual basis. Whether just for an hour or for days at a time, the damage and potential productivity loss from compromised sensitive information can be extreme to the enterprise in light of regulations regarding proper care for corporate financial (Sarbanes-Oxley) and customer (Health Insurance Portability and Accountability Act, California SB1386, and the European Union's Directive 95/46/EC) information.

2. **These solutions operate at the edge of the enterprise network, which presents a number of potential vulnerabilities.** First, establishing even a brief connection between the endpoint device and the enterprise network even at a protected network edge can create a seam of vulnerability for malicious code to launch its assault. Second, conducting assessments and remediation at the enterprise may create a processing bottleneck and single point of failure unless designed for peak scalability and automatic fail-over – both representing additional costs for the enterprise.

iPass Policy Orchestration

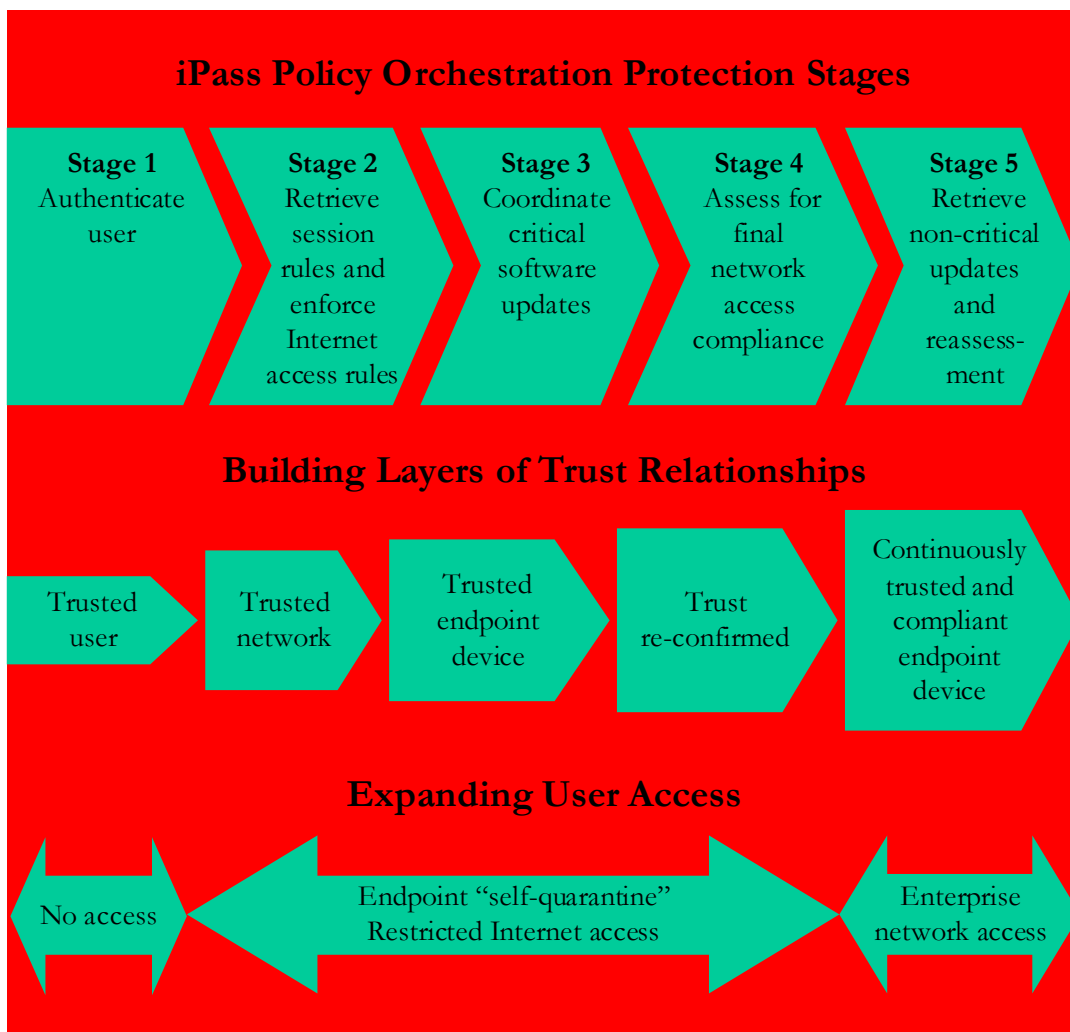
With this review of remote access security complete, we now turn our attention to the iPass Policy Orchestration initiative. To understand the value of iPass Policy Orchestration, one first must recognize that remote connections to an enterprise network consist of multiple, incremental stages. As the endpoint moves through the stages of the connection procedure, different security vulnerabilities are present and, to combat these vulnerabilities, increasing layers of trust and protection should be established through a logical, coordinated process. The challenge is to identify all vulnerabilities and then ensure that the proper security tools deployed to combat them are installed, up-to-date, and have successfully completed their tasks. Only then should Internet and enterprise access be allowed. This is accomplished through a sequence of events coordinated in a manner that balances the dual goals of minimizing remote user inconvenience and maximizing protection of the mobile endpoint and enterprise network. This coordinated process is one of the central attributes of iPass Policy Orchestration.

Another central attribute of iPass Policy Orchestration is that it is driven by the iPass virtual network platform, which provides control points on the endpoint device, at the Internet provider, on the enterprise network, and on the Internet. This allows iPass to enforce different policies at different points in the connection process. As trust relationships are confirmed through the iPass Policy Orchestration process, secure and safe connections between the endpoints with the Internet and to the enterprise network can be confidently established.

The endpoint component of this platform, the iPassConnect client software, acts as a control agent on the endpoint device to throttle endpoint-originated communication to the enterprise network until the appropriate level of trust relationships can be confirmed. This is the same client software that coordinates with iPass provider partners and the iPass virtual network platform to provide dial-up, wired broadband, and wireless broadband Internet access for remote users from tens of thousands of global locations. In addition, coordination between the iPassConnect client software and the iPass virtual network platform can also include coordination with 3rd-party security solutions to deliver a system that is both highly controlled and versatile.

Finally, by following a hosted model, iPass Policy Orchestration allows enterprise customers to gain the benefits of policy enforcement without having to install and manage additional infrastructure at the edge of their networks or allow endpoints to touch the network while less than fully trusted.

As will be discussed below, iPass Policy Orchestration can help address many of the problems of remote and mobile access stated above and specifically the limitations highlighted around establishing a trust relationship with the endpoint device. Our illustration of the iPass Policy Orchestration flow shown below provides an overview of the entire process. Descriptions of each stage follow the illustration. These descriptions assume the reader has a basic understanding on how the iPass connectivity service operates. A short network demonstration on the iPass website, www.ipass.com provides additional clarification.



Stage 1 – Authenticate user

Several distinctive aspects exist within the iPass Internet-based service relative to an enterprise-hosted authentication process. Each aspect adds to protection of the enterprise network and the confidentiality of the user's credentials. In terms of enterprise network protection, there is no direct communication between the user or the local PROVIDER and the enterprise network until trust has been established. Instead, information exchange is mediated through one of many redundant iPass Transaction Centers located around the world, ensuring that the enterprise will only receive authentication requests from validated iPass users. In addition, by acting as a mediation point, the iPass service insulates sensitive information about the enterprise from the Internet access providers.

With regard to confidentiality of the user's credentials, iPass utilizes SSL as an integral layer of the iPass protocol stack. In the iPass virtual network, 100% of the authentication communications are protected in dual 128-bit SSL tunnels supported by digital certificate exchange, one from the local PROVIDER to the iPass network core and another from the iPass core to the enterprise, to ensure no information is passed in the clear over the Internet. This ensures that interlopers on 3rd-party Internet access and backbone networks cannot view or manipulate user identity information. Also credentials are protected over natively less secure Internet on-ramps such as public broadband and Wi-Fi hotspots by required use of the GIS specification, which provides mutual authentication as well as encryption of the authentication request. Finally, use of the optional iSEEL service extends additional password encryption out to the client, protecting passwords over potentially insecure "first mile" connections.

Stage 2 – Retrieve session rules and enforce network-based Internet access rules

These session rules reflect enterprise IT and security policies pertaining to connectivity usage and dictate the parameters under which users are allowed Internet and enterprise access. Representative rules include the following categories and can be changed dynamically by the IT manager:

Category	Examples
Internet access methods	Define allowable access means (e.g., dial-up, shared broadband, and Wi-Fi) for security or cost reasons.
Access origination	Exclude Internet access from certain countries or locations prone to Internet-based attacks.
Security requirements	Require specific security software versions and operating system patches that must be present and operating on the endpoint device before access to the Internet and the enterprise network is granted.
Application use	Exclude use of disallowed endpoint applications (e.g., peer-to-peer) to lower infection risk.
Financial controls	Define session length limits, idle timeouts. Exclude expensive locations or access methods.

The session rules are obtained from iPass servers located within the secure iPass network core. These rules are set by IT management using the secure iPass Portal. As part of its Policy Orchestration initiative, iPass will in the future dynamically link these servers to enterprise management systems such as Microsoft Active Directory, allowing enterprise IT to affect policy changes pertaining to connectivity directly from their native systems.

During this stage there is also rule enforcement pertaining to the location being used for Internet access; namely rights to use a specific access method (e.g. Wi-Fi hotspots), connect from certain geographic locations to control expense and security risks, or use of optional security features such as iSEEL password encryption. This enforcement is done to block originating access from risky or expensive methods or locations. This Internet usage enforcement logically precedes endpoint software policy enforcement as a user must first have basic Internet access rights before proceeding to assessment and remediation of endpoint software.

Starting with Stage 2 the endpoint is placed in a highly restricted state. The iPassConnect™ client software instructs the personal firewall to “self-quarantine” the endpoint, only allowing communication between the iPassConnect client and the iPass policy servers located in an iPass Transaction Center. All other network-aware applications resident on the endpoint device (e.g., Instant Messaging) are blocked from external communication. Independent of the communication with the endpoint device, the iPass policy server retrieves session rules from the iPass RoamServer software running on the enterprise network through a separate SSL tunnel, maintaining separation of the still-untrusted endpoint and the enterprise network.

Stage 3 – Coordinate critical software updates

Once session rules have been retrieved, the iPassConnect client software will orchestrate the running of an assessment and remediation service that validates session rule compliance and updates endpoint software as appropriate. Assessment and remediation services are available in the market today from several vendors including iPass (their Endpoint Policy Management service). For any of these services to function effectively and securely, communication must be coordinated among the relevant software elements on the endpoint device and the update server.

With iPass Policy Orchestration, communication occurs among the iPassConnect client software, the endpoint personal firewall, and an update agent present on the endpoint. The assessment process begins with the personal firewall receiving instructions from the iPassConnect client software to “self-quarantine” the endpoint and allow access only to the critical update server. If the customer has deployed Endpoint Policy Management from iPass, then the update agent is part of the iPassConnect client and the update server is located within the iPass network (i.e., Internet-based). The update server may also be a third-party hosted service or a server located within the enterprise DMZ.

Next, the assessment service determines through information exchange with the update agent whether critical software updates are required for endpoint compliance. When required, updates will be sent and installed on the endpoint device. During this entire process, iPass will ensure users are only able to access the update server and will only open the proper ports. Examples of critical updates are those that patch security holes in the

endpoint operating system, VPN client, personal firewall, or anti-virus software as well as proper versions of configuration, policy rules, and data definition files.

Once the critical update process is completed, the software will report back to the iPassConnect client software on its completion status and either move onto Stage 4 or act as dictated by enterprise security policies (e.g., retry assessment, terminate connection).

Stage 4 – Assess for final network access compliance

The next step is to orchestrate a final network compliance check. This stage can be thought of as a final network protection step that supplements the endpoint protection provided in Stages 2 and 3. To this end, iPass Policy Orchestration is designed to be able to coordinate with today's compliance tools as well as upcoming solutions such as Cisco Network Admissions Control, Microsoft Network Access Protection, or the APIs to be promulgated by the Trusted Computing Group. This provides a final reconfirmation of compliance that is designed as a hard requirement for the establishment of a VPN tunnel between the endpoint and the enterprise network.

During this stage, iPassConnect will instruct the personal firewall to “self-quarantine” endpoint access to the VPN server and interactions between the network compliance agent and iPassConnect will validate that the endpoint is trustworthy at the point of VPN launch. At the completion of this stage, a VPN tunnel is established and the endpoint “self-quarantine” is lifted. The trusted user and endpoint now have enterprise network access.

Stage 5 – Retrieve non-critical software updates and reassessment

In Stage 3, enterprises control which software updates are critical and should be installed before granting the remote user Internet access and subsequently establishing a VPN tunnel to the enterprise network. The enterprise may have chosen to defer certain endpoint software updates based on the severity of the faults they address or the level of inconvenience the user would face waiting for the update. In Stage 5, software updates that were not deemed as critical in Stage 3 can “trickle down” to the user in the background.

In addition, continuous reassessment of session rule compliance occurs at this stage. During the VPN session, users might intentionally or accidentally disable the personal firewall or anti-virus software. This compromises the trust relationship that was established through Stage 4 and elevates the security risk to the enterprise network and the user's endpoint device. That is why in Stage 5, the iPassConnect client software performs continuous compliance confirmation. If an out-of-compliance situation is encountered, steps can be taken to either quarantine and remediate the endpoint device or automatically tear down both the enterprise and Internet sessions.

Conclusion

For a remote connectivity solution to deliver the benefits of business continuity, protection of intellectual property, and regulatory compliance an enterprise requires, it must uniformly protect all elements of the information ecosystem - user identities, endpoint devices, session data, and the enterprise network. While focused security tools are available to protect each element, the interrelationships that exist among elements leaves other elements vulnerable if

any one element is compromised (e.g., a stolen identity can lead to a compromised endpoint and enterprise network). Therefore, for enterprises to receive the full protection benefit from all of their security components, an orchestrated approach that accounts for these interrelationships is essential.

iPass Policy Orchestration endeavors to provide such a solution through a coordinated, stepwise approach to remote access security. By sequentially opening the gates of user Internet and enterprise network access as the most appropriate security operations are successfully completed, the iPass approach ensures user and endpoint device trust relationships are created and/or confirmed before access to the enterprise network is permitted.

Finally, the iPass approach helps streamline overall management of the secure connectivity process, allowing enterprise IT to maintain fine-grained control over policy management by providing for self-service configuration of policies, integration between iPass policy management mechanisms and a company's broader management systems, and real-time visibility into user compliance with policies.

Michael Suby
Senior Research Analyst
Stratecast Partners, A Division of Frost & Sullivan