



网络准入控制（NAC）技术 与 **Sygate Compliance on Contact**

Richard Langston, Product Line Manager, Sygate

目 录

概要	2
介绍	2
什么是网络准入控制(NAC)?	3
SYGATE COMPLIANCE ON CONTACT 解决方案	4
结论	10

概要

今天,员工对系统的滥用、错误配置以及恶意访问导致企业业务面临很多现实的安全威胁。事实上,根据Gartner 的估计,大约20%的受控系统已经遭受不同程度的安全危害。此外,Gartner 估计企业网络中20%的系统是完全不受控的。显然,这会导致大多数企业容易遭受网络攻击,引起生产力损失、机密信息的泄露,以及其它的代价高昂(和尴尬)的损失。

网络准入控制(Network Access Control, NAC)是一个过程。通过强制作为网络访问前提条件的IT安全策略,来减少网络安全事件,增强对企业安全制度的遵从。尽管“网络准入控制(NAC)”是一个新定义类别,Sygate 技术公司却是策略强制领域多年来的领导厂商,先后在网络准入控制方面率先实现了VPN (IPSEC和SSL), LAN (802.1x), 客户端代理自我强制(Self-Enforcement)技术。

今天,Sygate 拥有很多实施了完整NAC解决方案的大型企业客户。NAC解决方案需要多种强制方法和高度的策略灵活性才能覆盖整个企业网络。客户应该仔细评估他们的环境和需求,权衡各种可行方案。作为在NAC解决方案的革新者,Sygate 提供最全面和灵活的选项集来部署网络准入控制,最大程度的满足企业的需求。

介绍

今天企业面临很多IT挑战。其中的关键挑战是与日趋频繁的安全事件做斗争,努力维护企业安全制度的遵从。滥用,错误配置,恶意访问关键的企业系统渐臻盛行。这些挑战中一个共同的主线是确保网络端点的保护和控制。例如,很多安全事件是由简单的桌面配置错误和安全补丁未及时升级造成的。类似地控制哪些应用可在那些端点上运行,也还有很长的路要走才能迎接管理的挑战。

现有的技术,例如补丁和脆弱性管理系统,属于被动的方式来保持系统主机的更新,它们没有强调一个真正的解决方案应该具备的要素:将那些没有升级到最新或是不符合企业安全策略的系统与网络断开,并建立一种方法在不需要IT支持人员介入的情况下修复。

网络准入控制技术解决这一问题的方法是在端点连接到网络之前对它们的安全状态进行审计,并在连接到标准企业网络之前进行适当的更新。从而将蠕虫和病毒屏蔽在网络之外,也能强制应用级的安全策略。

部署最简单的NAC解决方案仍然需要大量的规划来将许多不同厂商的网络部件联动在一起。Sygate 技术公司作为NAC方面的先驱,于2002年发布其首个具备NAC功能的产品。初期产品主要针对保护公司网络免遭不符合企业安全策略VPN用户的威胁,现在Sygate已经扩展它的NAC解决方案,包含有On-Demand和基于局域网的解决方案。沿着这个方向,Sygate在如何构建大规模高效的NAC 解决方案,如何显著提高企业网络面对安全事件的可用性和弹性方面,形成了自己独到的见解。

从本白皮书中,我们将着眼于网络准入控制技术背后的理论,包括Gartner 组织关于NAC

解决方案的定义。我们也将突出许多被Sygate标识为成功要素的必要条件。

什么是网络准入控制(NAC)?

几个行业分析机构对网络准入控制（NAC）技术进行了思考，每家都使用了不同的术语集和差异很小的网络准入控制定义。例如，Forrester使用“网络隔离（Network Quarantine）”，而Meta用“端点访问控制（Endpoint Access Control）”。

Gartner 也为网络准入控制创建了一个参考设计，这个设计是一个回环的过程，维护一个全局的策略，来评估端点，减少安全问题，准许系统接入网络，实时监控系统和企业安全策略的一致性。

因为Gartner 架构是最完备的设计之一，它所定义的过程以及如何使NAC工作起来的内容值得借鉴。Gartner 的NAC过程从安全策略的定义开始。策略勾勒了管理员希望强制的安全配置，这些配置会作为网络访问的前提条件。这些策略能够包括任何的系统或第三方软件配置，完全视企业的需要而定。

对大多数企业来说，典型的策略是强制验证操作系统补丁是否更新，反病毒软件是否在运行及病毒库是否更新，端点防火墙软件是否在运行及被适当的配置。管理员也可能希望执行更多高级策略，检查定制安全软件或特殊安全配置是否存在。

一旦策略创建完成，就有了在系统连入网络时可参照的安全基线。一个重要的考量是无论系统是如何接入网络的，该基线评估必须进行。为了保证网络安全，局域网（LAN），广域网（WAN），无线（Wireless），IPSec，和SSL VPNs全部必须执行安全基线评估。

基于该基线评估结果，访问控制（Access Control）授予该连接系统相应级别的访问权限。例如，一个达标的系统将会获得全部的网络访问权限。不达标的系统或者被彻底阻止，没有任何的网络访问权限，或者为了减少对网络的威胁（通常也为了修复），将授予该系统某一隔离级别的网络访问权限，并帮助恢复达到安全策略的要求。为了使NAC真正有价值，修复过程必须自动化。换句话说，就是不要求助技术支持小组，系统自动恢复到符合安全策略的要求。

一旦系统经过隔离修复处理，被允许连接入网络，就需要一种监控技术确保这些系统保持达标的状态，不要出现反常的情况。反常的系统必须被隔离，直到它们被修复。

因此，网络准入控制解决方案需要：

1. 创建一个中央的安全策略视图；
2. 当一个系统或用户连接入网时，对其安全状态进行评估；
3. 一旦系统连接入网，对其安全状态进行连续监控；
4. 基于系统状态，执行网络访问和系统修复策略。

除了Gartner的NAC框架定义的功能之外，高效的NAC解决方案需要几个其它的特征来满足今天大企业的需求。这包括：

- 多种网络接入方式支持（远程访问VPN IPsec，拨号，SSL VPN，无线，LAN，DHCP，802.1X，WEB访问等）。为了成功，一个NAC方案必须从第一天起就能守护网络的所有入口。如果后门或窗子都敞开着，仅仅锁住前门不能防止任何人的进入。
- 企业级扩展能力和易管理性，包括灾难恢复和冗余，保证NAC方案能够扩展以适应企业发展和需要。
- 强大的策略隔离、管理功能隔离的信息管理工具。组织内不同角色经常需要不同的安全配置，很多大公司将策略制订委派给各业务部门，但仍然需要一个策略的全局视图。
- 业经证实的灵活的部署策略。例如像“学习模式”之类的功能，使NAC方案可以最初以审计模式部署，从而大大缩减引入新IT实践所带来的痛苦。
- 可扩展，可定制策略。允许管理员创建自定义NAC规则，不需要从NAC厂商处获取帮助。
- 灵活机动基于处所的策略，可减少NAC对终端用户工作习惯的影响。例如，旅行的用户处于公共网络时，通常需要一个更高级别的安全防护。而位于办公室中，这个高级别的安全防护会影响到企业应用和信息共享（甚至打印！）。类似的例子也适用于企业无线网，派出机构等等。
- 多厂商兼容，开放的解决方案，可支持今天和今后几年企业网络中不同的技术组件。NAC技术仍然在发展进化之中。今天，在市场有可实施，业经证明的方法。然而，投资于单一技术，例如Cisco NAC或者Microsoft NAP，可能不会产生期望的结果。

Sygate Compliance on Contact 解决方案

使用Sygate 管理服务器，IT管理者能中央管理它们的网络访问策略。这些策略包括内建对知名反病毒软件，个人防火墙，反间谍软件，操作系统和系统补丁检查。也包括一个高级工具箱，用于创建定制检查，检查可以针对系统上发现的文件，正在运行的应用，注册表设置，文件日期和校验和，以及其它类似条件。自适应策略允许强制不同策略，这取决于用户使用的网络连接类型，例如：用户使用IPSEC VPN 连接，由于他们裸露于公网，因此需要一个更高级别的准入检查。

例如，一个组织可以配置策略，让所有的Windows 2000 系统安装Service Pack 4，所有的Windows XP 系统安装Service Pack 2，全部的系统运行赛门铁克反病毒软件并保持最新的病毒库更新。或除了启用以上全部检查外，再附加检查其它定制的安全应用，和IT部门定制的注册表键值等。

一旦策略创建，所有安全策略在网络连接时将受到Compliance On Contact（连接之际安全之时）的强制。Compliance on Contact 在公司网络上的每一连接点进行策略符合性检查。

包括在用户经过IPSec VPN、SSL VPN、有线以太网和无线网络连接到公司网络时，执行整套的NAC安全基线检查。下图“Sygate通用NAC解决方案”，阐述被Compliance on Contact使用的网络连接点、连接方法。下表列出所支持和测试的网络基础架构厂商。

API 集成	802.1x (W) LAN NAC集成	On-Demand NAC集成
Aventail	Airespace (Cisco)	AEP (Formerly Netilla)
Checkpoint	Alcatel	Aventail
Cisco	Aruba	Aruba
iPass	Cisco	Juniper
Juniper	Enterasys	Nortel
Nortel	Extreme	V-One
	Foundry	Whale
	HP Procurve	
	Nortel	

强制协同工作图

一旦设定了安全基线，访问控制（Access Control）是解决方案中接下来的一步。如果系统符合安全策略要求，它们可以连接到公司网络。用于访问控制的技术随着连接类型的不同而不同。Sygate代理自动执行一个预配置的操作，在不需要用户干预的情况下帮助系统恢复到安全基线以上。一旦得以更新，系统会重复此过程，由于它已符合安全策略要求，将获得对企业网络的访问。参见下图了解一个完整的工作过程。

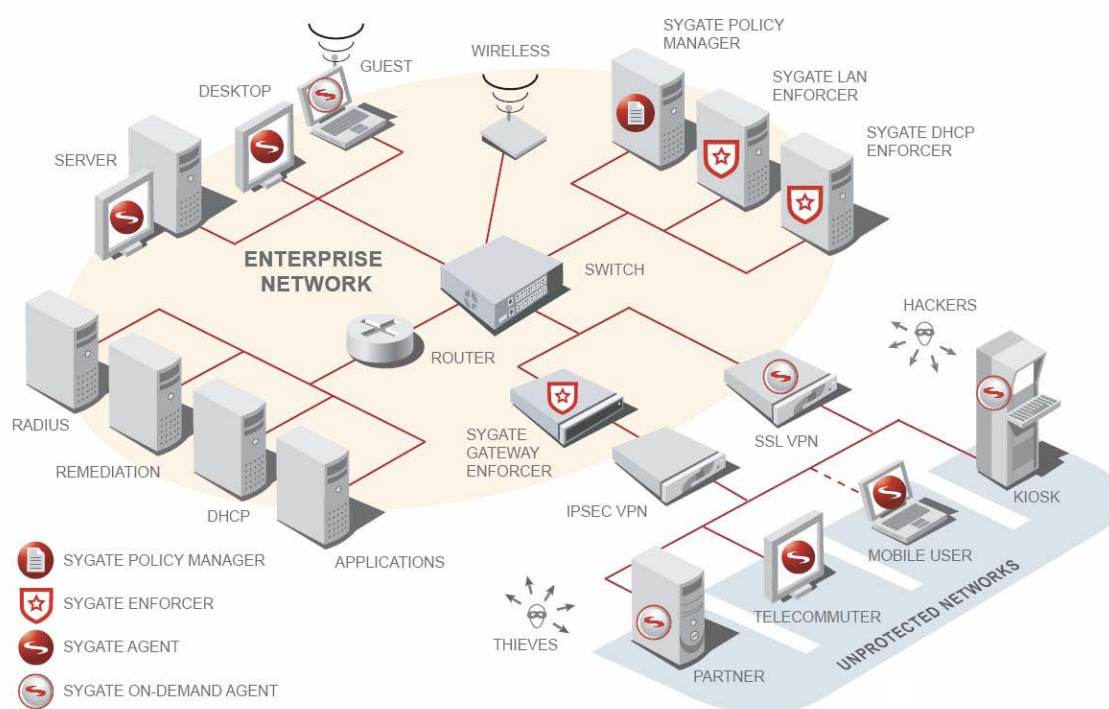
Compliance on Contact连续监控客户端状态，在系统违背策略的情况下，采取行动限制该系统。

Sygate使用六种不同技术实现完整的通用NAC解决方案：

1. 基于API与IPSEC VPNs 集成

2. 网关强制—适用任何网络的透明（in-line）强制
3. 通过“Sygate On Demand 代理”的 On-Demand applets 实现SSL VPN 强制
4. 用于局域网和无线网络基于802.1x标准的强制
5. 基于DHCP 的强制，可用于任何架构之上的局域网和无线网络
6. 用于Cisco路由器的第一版的Cisco NAC技术。

以下看每种方式是如何工作的。



Sygate Universal NAC Solution Diagram

Sygate API 集成

当用户通过IPSEC VPN连入网络，Sygate API 被使用与安装在远端系统的Sygate 安全代理通信，判断该系统是否与安全策略一致。为了使该种方式工作，IPSEC VPN 网关必须支持Sygate 的通用强制API。为了确保Sygate API 的兼容性，Sygate 与绝大多数VPN 厂商一起工作，包括Cisco, Nortel, Juniper, Aventail, AEP, Array Networks。对于不支持Sygate

API 的VPN 网关，Sygate的透明（in-line）网关强制服务器可以被插入在VPN网关后边，执行本功能。

Sygate On-Demand NAC

SSL VPNs 的引进产生了另外一个面向WEB 的NAC组件的需求。为了满足这个需求，Sygate 开发了Sygate On-Demand 代理（SODA）。SODA 包括一个随需的，透过Java发放的NAC组件，该组件可以评估一个系统的安全策略状态，无需预先安装常驻式的代理。SSL VPN 网关可以通过它们的WEB验证界面发放此代理，确保系统符合策略要求后，才被允许访问受该网关控制的公司资源。Juniper, Array Networks, Netilla 和Aventail 这些SSL VPN厂商在它们产品中均包括了基于SODA的NAC支持。

Sygate Gateway NAC

除了VPN 访问，管理者可能想控制对关键网络资源的访问。例如数据中心或者到远程办公室的广域网链路。Sygate 的透明（in-line）网关强制服务器用于实现这个任务。网关强制服务器拦截流量，根据所配策略决定是否放行。如果系统不符合企业安全策略的要求，它们会被禁止访问位于强制服务器之后的网络资源。

Sygate 802.1x-Based NAC for LAN and Wireless

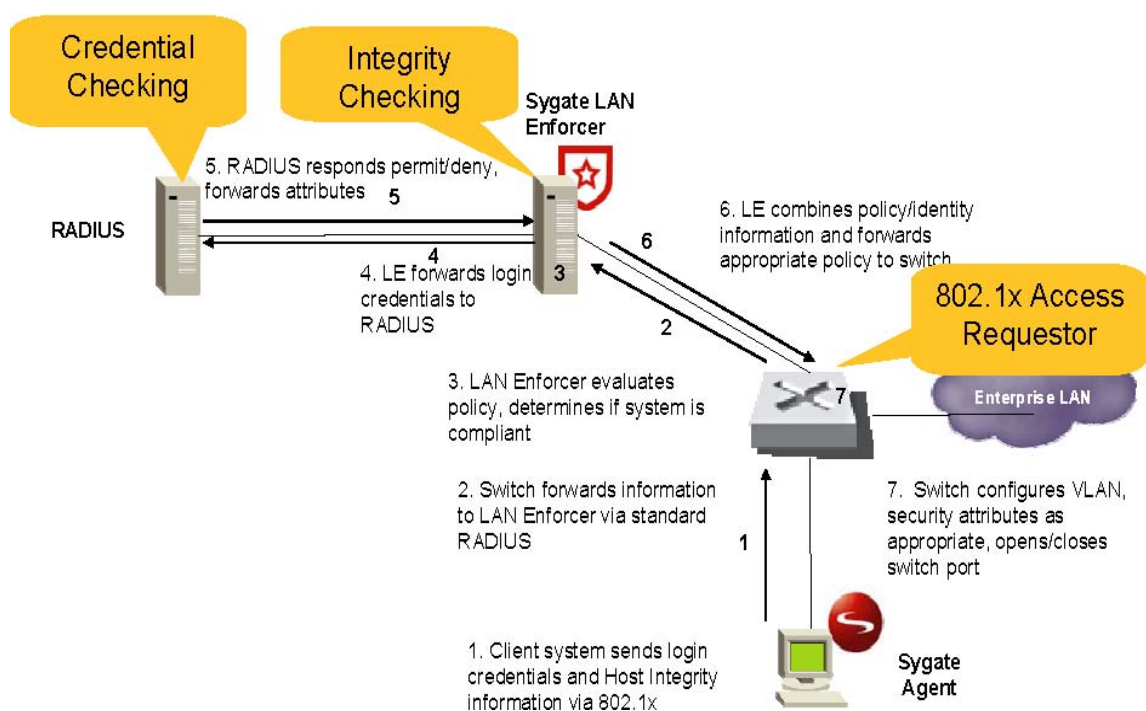
Sygate 于2004 年六月发布最早的基于局域网的NAC技术。该技术增强利用了IEEE 的802.1x准入控制协议，几乎所有有线和无线以太网交换机制造商都支持该协议。Sygate 使用这个链路级协议评估端点是否符合安全策略要求，提供自动问题修复，并允许达标的系统进入公司网络。

802.1x 是一个认证协议，在用户访问计算机网络之前，需要提供有效的凭证来增加安全。802.1x 较通常的Windows PC 登录更为安全，因为网络端口—不仅仅PC本身，在认证之前是被锁住无法访问的。用户提供登录凭证，例如用户名和密码，交换机传递这些凭证到验证服务器。通常，验证服务器是一个RADIUS 服务器。如果凭证正确，RADIUS 服务器将发送一个认证消息到交换机或接入点，授权该用户对网络的访问，并配置该用户连接的服务属性。

在LAN强制策略过程中，端点上的Sygate代理使用802.1x协议传递策略符合性信息到网络交换机，网络交换机再中继到一个Sygate 的LAN强制服务器。这个LAN 强制服务器作为一个RADIUS 代理服务器，验证策略符合性信息并可选择咨询RADIUS 服务器验证用户名和密码或者多因素认证。

如果系统不符合企业安全策略要求，LAN强制服务器将该系统放入到隔离区，在该区域中该系统会得到修复，同时又不影响那些符合要求的系统。一旦Sygate 完成自动修复，802.1x 协议将重新验证用户。由于系统已经达标，将被授予访问企业网络权限，如下图所示。

Sygate LAN Enforcement Using 802.1x



Sygate 局域网强制过程图

Sygate DHCP-Based NAC

基于802.1xNAC提供最大化安全。然而，它需要接入层交换架构支持802.1x协议。即使交换机支持802.1协议，开启它仍需要仔细计划。Sygate的基于DHCP的NAC方案可以解决这些问

题，在现存网络环境下不需要升级任何硬件或软件。

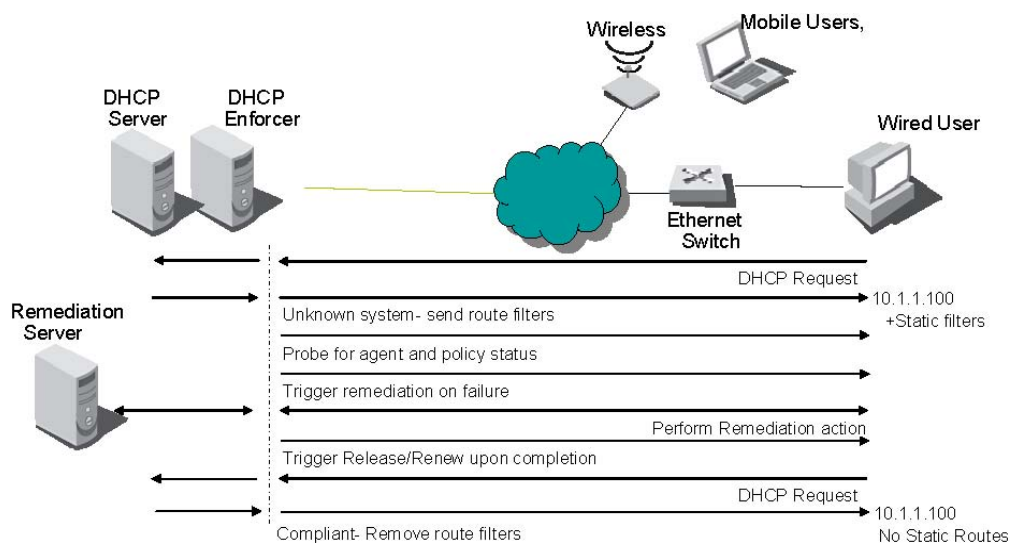
Sygate 的DHCP NAC被内嵌 (in-line) 部署在DHCP 服务器和网络之间。如果用户没有运行一个代理或用户当前NAC策略符合性是未知的，该用户将被分配一个“不可路由的”或“隔离的” IP地址。这些地址不能随意访问网络，只有受限的权限。这有两种方式实现。或者这些客户端被分配一个不同IP网段的特殊IP地址，在路由器上通过访问控制列表控制这些特殊IP地址可以访问的网络，或者客户端被分配正常网段的IP地址，但是设定了特殊的静态路由，仅容许访问所需的服务器，并没有到整个网络的缺省路由。

一旦客户端有了一个IP地址，DHCP 强制服务器将和客户端上Sygate 代理通讯，确定客户端的策略是否及时更新，是否符合企业安全策略的要求。如果不符合，该代理将触发所需的修复动作，使该系统与企业安全策略相一致。一旦符合要求，该客户端将发起一个DHCP 释放和更新。一旦DHCP 强制服务器接收到一个更新的请求，它将联系代理，确定客户端已经达标。系统将被授予一个正常生产网络的DHCP 租约，给予全部的网络访问权限。

因为DHCP NAC作为一个透明 (in-line) 的DHCP 代理服务器，可以与现存的任何DHCP基础架构兼容。部署这种NAC方法涉及在DHCP 服务器前放置DHCP 强制服务器，决定一种隔离IP 地址策略，在DHCP 服务器上改变某些设置。下图为一个通讯封包流程示例。

没有安装代理的系统可以有两种方式授予访问权限。第一种方式是，对于一个非Windows系统可以免除此NAC过程。第二种方式是，可以设置一个基于MAC 地址的免查表。这个MAC地址列表可以接受通配符，可以容许整个一类系统免受检查，例如IP电话使用它们组织唯一标识符。

DHCP NAC Packet Flow



Sygate NAC 方法回顾

NAC 方法	Sygate 产品开始支持	需要的最小版本Sygate 软件
Gateway Enforcement	2001年6月	SSE 2.0
API Enforcement	2001年12月	SSE 3.0
Self-Enforcement	2003年8月	SSE 3.5
802.1x (W)LAN Enforcement	2004年7月	SSE 4.0
Cisco NAC v1	2005年6月	SNAC 5.0, SEP 5.0
DHCP	2005年6月	SNAC 5.0, SEP 5.0

结论

网络准入控制技术预期能显著减少安全事件的数量和严重程度，帮助对安全制度的遵从。Sygate 的Compliance on Contact 技术通过在多种网络协议和网络接入方式上强制策略交付了今天NAC方案的承诺。其灵活的解决问题的方式可确保成功的实现以及对IT投资的保护。