

Napera 网络

Napera选择GlobalSign EmbeddedSSL安全网络访问控制解决方案

Napera
www.napera.com



2008年2月，Napera开始了一个试点项目，成为第一批将有效的、经过全面审查的X509数字证书用于通过HTTPS管理的网络设备的公司之一。

Napera N24和N24S网络设备利用基于web的管理服务来进行报告、日志记录、警报和备份服务。

合作
GlobalSign
www.globalsign.cn



通过利用GlobalSign的高度普及的SSL证书，Napera在其解决方案中采用了广泛可信的安全方法，确保只有健康的计算机和授权用户才能访问公司网络，并使客户能够受控地访问互联网或打印机。Napera为中小型企业构建了它的解决方案，以提供易于管理和可负担的企业级网络访问控制。确保最高级别的安全而不复杂是Napera的重点，这就是为什么GlobalSign解决方案可以完美地满足其需求。

行业
存储设备

利用可信的方法确保新产品的安全

在网络安全行业的一个突破性的举动，Napera已经成为第一个利用有效的，完全审查的X509数字证书通过HTTPS(超文本传输协议安全)管理的网络设备的公司之一。通过HTTPS，网络管理人员可以安全地、无缝地访问Napera创新的网络访问控制设备的嵌入式web管理服务。

结果
Napera的网络访问控制技术结合GlobalSign的SSL证书，允许用户安全地控制和加强设备健康、身份和网络访问，并提供计算机和网络安全状态的可见性和实时报告。

产品

Napera的网络访问控制解决方案包括一个设备和一个基于web的日志、报告和警报管理服务，名为MyNapera.com。Napera N24设备与MyNapera.com一起工作，以确保用户得到授权，计算机是健康的，网络是安全的。Napera N24是一个综合的解决方案，它结合了受控的客户和员工访问、Windows和Mac系统的计算机健康强制执行、身份强制执行以及有线和无线环境的增强安全性。

- 10分钟内部署
- 易于使用和管理
- 千兆性能
- 利用微软网络访问保护

Napera正在使用GlobalSign经过验证的SSL技术与新的综合管理服务接口，以及利用GlobalSign提供的灵活API将SSL证书导入Napera N24设备。通过向每个设备唯一的完全合格域名颁发证书，Napera快速有效地试验了一个程序，在他们的设备上制造SSL证书，成为历史上第一个在通过HTTPS管理的网络设备中嵌入有效服务器证书的网络安全公司。服务器证书将设备和Napera标识为一个组织，该组织还向用户提供保证，即地址正确，连接是加密的。

“公司希望善待他们的客人，这有时意味着给他们提供互联网接入。然而，让它们插入你的网络可能是一个巨大的安全风险。网络访问控制技术有助于实现正确的平衡。客户机访问已经成为它必须面对的挑战之一，因为它试图平衡安全性和工作效率。尤其是在经济低迷时期，企业更多地依赖外包和承包商来完成工作，而不是雇佣新员工”。



挑战

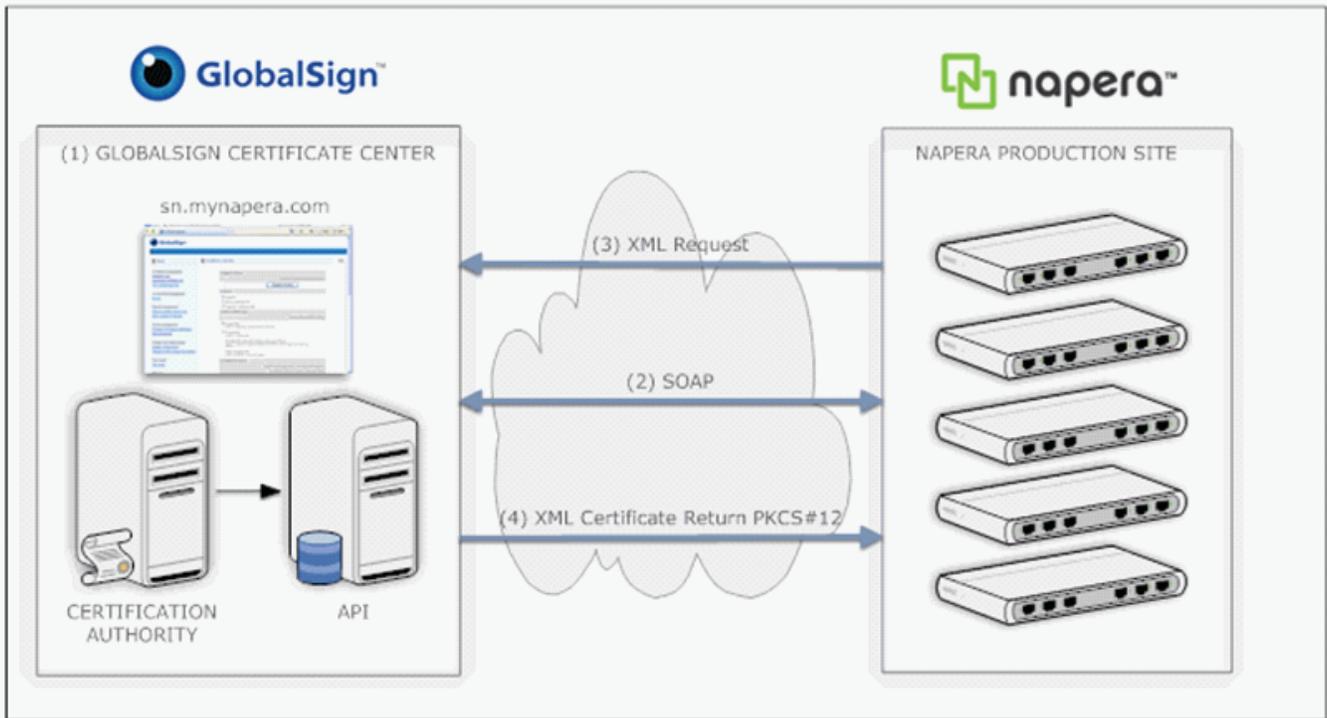
- 允许用户安全地远程或现场访问其控制面板，而不影响网络安全。
- 向那些可能没有内部CA或流程为其设备购买SSL证书的客户id提供SSL证书。
- 限制最终用户和系统管理员“点击通过”自签名证书或来自不可信证书颁发机构的证书警告。(许多使用HTTPS的安全设备依赖于自签名证书，这使得管理员“点击通过”警告)。

标签

CEO Napera Networks
(Technewsworld.com
7/16/08)

解决方案

- 利用GlobalSign的SSL证书的已知和经过验证的技术，所有互联网浏览器和大多数移动设备都天生信任该证书。
- 通过利用现有投资，Napera的客户不必获得自己的证书。
- 通过使用来自可信证书颁发机构的SSL证书，N24网络设备继承了此类证书提供的信任和普遍性，因此加强了终端用户和系统管理员对SSL的正确使用。
- Napera的网络访问控制技术结合GlobalSign的SSL证书，允许用户安全地控制和加强设备健康、身份和网络访问，并提供计算机和网络安全状态的可见性和实时报告。



(1) 证书管理门户

GlobalSign证书中心(GCC)是一个SaaS平台，允许通过基于web的门户或Napera的自动化API访问服务。Napera通过批准的API(应用程序编程接口)在线向GlobalSign提交格式适当的证书请求。在使用预先审查的域名mynapera.com进行身份验证后，GlobalSign要么直接或通过API颁发证书，要么将证书发送到证书应用程序最初发出的电子邮件地址。利用预先审查的域名mynapera.com立即签发组织验证证书。

GlobalSign通过检查域名所有权或域名使用权以及任何其他适当的信息来验证提交的信息。这可能还包括检查第三方数据库或资源，与标准组织(如互联网工程任务组(IETF)或互联网名称与数字地址分配公司(ICANN))进行比较，并通过电话进行独立验证。

(2) API 通信函数

应用程序编程接口(API)允许Napera的制造系统和GCC之间进行通信，以便在Napera N24和N24S设备上申请、生成、发送、接收和安装经过组织验证的SSL证书。

(4) 私钥代码样本

```
Private-Key: (2048 bit)
modulus:
 00:dd:3c:f6:9a:be:d2:66:20:0c:7d:0c:ae
  cc:f4:e8:89:8d:16:b3:5c:16:75:06:33:f9
  d6:9b:f4:6b:e7:4d:0f:44:af:8b:87:dc:79
  e8:e4:20:19:df:f0:0d:04:4d:2c:4c:ad:19
  8c:6a:4d:a6:d6:0e:e8:ae:e2:37:75:8d:d5
  31:15:3c:f4:4d:ad:5d:f8:d0:23:c2:72:de
  9b:ef:f7:84:25:b0:cf:92:4d:39:4a:18:41
  81:28:ac:5b:f2:7d:74:e2:8f:f9:a7:c1:c0
  dd:cd:b1:4c:23:23:63:27:30:4c:da:8e:72
  77:c2:22:e2:b4:43:bb:9d:ca:36:59:fc:98
  da:c4:2c:34:03:0c:e5:91:51:e2:23:20:ae
  30:8f:9e:f5:a5:2c:e4:bf:ab:2f:fb:82:03
  ff:5e:90:a8:f0:be:b0:4d:aa:f3:af:2c:27
  7e:7a:d2:c3:e8:5b:53:8d:86:db:ae:f6:7c
  35:b6:52:9d:a0:c1:e0:da:ac:6b:68:05:7e
  41:62:63:56:b3:47:6e:11:d8:d4:6c:92:be
  f2:a5:72:3d:4e:d9:d2:e2:8d:42:92:3e:cf
  63:89
publicExponent: 65537 (0x10001)
privateExponent:
 5c:a2:77:1b:6a:45:0c:af:e4:aa:c3:91:b2
  ea:ec:27:14:25:6a:2a:67:d8:ce:25:1a:e4
  f2:31:10:b1:43:c9:dd:d7:a7:13:d7:14:21
  15:27:ff:cd:8d:64:d5:e5:3e:64:48:a2:95
  3f:75:8e:22:d9:11:42:90:c3:e9:fb:de:3d
  d4:db:b5:eb:84:68:f1:92:ad:36:71:04:b4
```

(3) API代码示例

```
<?php
require_once 'SOAP/Client.php';
$url = 'http://xxx.globalsign.com/services/GasOrder';
$nameSpace = 'http://xxx.globalsign.com';
class Order {
    var $client;
    var $nameSpace;
    function Order($url,$nameSpace) {
        $this->client = new SOAP_Client($url);
        $this->client->_namespace = $nameSpace;
    }
    function PVOrder($request) {
        $res = $this->client->call('PVOrder',$request,$this->nameSpace);
        return $res;
    }
}
$rek = new Order($url,$nameSpace);
$req['Request']['OrderRequestHeader']['AuthToken']['UserName'] = '';
$req['Request']['OrderRequestHeader']['AuthToken']['Password'] = '';
$req['Request']['OrderParameter']['ProductCode'] = "OV";
$req['Request']['OrderParameter']['OrderKind'] = "new";
$req['Request']['OrderParameter']['Licenses'] = "1";
$req['Request']['OrderParameter']['ValidityPeriod']['Months'] = "12";
$req['Request']['OrderParameter']['CSR'] = "
-----BEGIN CERTIFICATE REQUEST-----
xxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxx
-----END CERTIFICATE REQUEST-----";
$req['Request']['ContactInfo']['FirstName'] = "xxxx";
$req['Request']['ContactInfo']['LastName'] = "yyyy";
$req['Request']['ContactInfo']['Phone'] = "55555";
$req['Request']['ContactInfo']['Email'] =
"admin@test.com";
$res = $rek->PVOrder($req);
print_r($res);
?>
```

Napera在以下三个主要场景中使用了GlobalSign的SSL证书技术:

- 1.因为GlobalSign证书本质上是受所有互联网浏览器信任的, Napera使用它们来确保用户安全地远程或现场访问MyNapera.com基于web的管理服务。
- 2.当无线接入点(WAP)针对Napera N24作为无线网络访问控制基础设施的一部分进行身份验证时, GlobalSign证书确保了更高的安全性。
- 3.当终端设备(如笔记本电脑)在网络访问期间使用802.1x对Napera N24进行身份验证时, 就会利用GlobalSign证书。

通过嵌入证书技术, Napera向那些可能没有内部证书颁发机构(CA)或购买SSL证书流程的客户提供了SSL证书。这些受信任的SSL证书通过防止用户“点击通过”自签名证书所显示的证书警告, 帮助最终用户和系统管理员正确使用SSL证书。许多依赖于HTTPS连接的安全设备依赖于自签名证书, 因此制约系统管理员和最终用户“点击通过”警告消息。

Napera的网络访问控制技术与GlobalSign的SSL证书允许用户控制和加强设备健康, 身份和网络访问的安全性。

使用SSL的基于浏览器的用户界面的优点安全性

为每个Napera N24提供一个完全验证和公开信任的X509数字证书可以为Napera的客户提供许多安全好处。由于Napera使用的是独特的软件即服务模式, 因此没有考虑为N24和N24S设备使用其他类型的安全来解决这一特定挑战。对于这个基于浏览器的服务, Napera总是使用安全的HTTPS连接进行管理。

GlobalSign的区别:

在与多个SSL证书机构和供应商交谈后, Napera选择了GlobalSign, 因为它愿意提供灵活的解决方案, 例如一个可行的SOAP API, 以将SSL证书嵌入Napera的网络设备。GlobalSign与Napera密切合作, 其他供应商不会继续进行讨论, 除非预先订购大量的证书。

Napera Networks的创始人兼首席技术官Chris Boscolo说:“GlobalSign为我们提供了一个灵活、可用的SOAP API, 无缝地集成到我们的制造过程中, 允许我们使用预先审查的域名和序列号来订购证书。”“没有其他人会在这个层面上与我们合作, 为我们的解决方案提供所需的尖端安全。”

GlobalSign公司首席执行官Johan Sys评论道:“GlobalSign和Napera都在发送移动性和安全性信息, 合作是很有意义的。我们很高兴能够帮助Napera使用我们无处不在的SSL证书保护其网络设备的安全。他们对安全的承诺, 以及专注于他们最擅长的事情, 将证明是一种互利的伙伴关系, 无论是现在还是未来。”

了解更多信息

www.napera.com
www.globalsign.cn