UNIVERSIDADE TECNOLÓGICA FEDERAL DO PARANÁ
PROGRAMA DE PÓS-GRADUAÇÃO EM TECNOLOGIA
ESPECIALIZAÇÃO EM TELEINFORMÁTICA E REDES DE COMPUTADORES

ALAN FLÁVIO FOLLMANN

IMPLANTAÇÃO DE NAC EM AMBIENTES CORPORATIVOS

MONOGRAFIA DE ESPECIALIZAÇÃO

CURITIBA
2011

ALAN FLÁVIO FOLLMANN

IMPLANTAÇÃO DE NAC EM AMBIENTES CORPORATIVOS

Monografia apresentada como requisito parcial à obtenção do título de Especialista em Teleinformática e Redes de Computadores, do DAELN, da Universidade Tecnológica Federal do Paraná,.

Orientador: Prof. Kleber Kendy Horikawa Nabas

CURITIBA
2011

Ministério da Educação
Universidade Tecnológica Federal do Paraná
Diretoria de Pesquisa e Pós-Graduação do *Campus* Curitiba
Departamento Acadêmico de Eletrônica
Especialização em Teleinformática e Redes de Computadores

TERMO DE APROVAÇÃO

Título da Monografia

Implantação de NAC em Ambientes Corporativos

por

Alan Flávio Follmann

Esta monografia foi apresentada às 18:00 do dia 02. de setembro de 2011 como requisito parcial para a obtenção do título de ESPECIALISTA EM TELEINFORMÁTICA E REDES DE COMPUTADORES, Universidade Tecnológica Federal do Paraná. O candidato foi argüido pela Banca Examinadora composta pelos professores abaixo assinados. Após deliberação, a Banca Examinadora considerou o trabalho aprovado com a nota 9,0 (NOVE INTEIROS)

Prof. Walter Godoy Junior
(UTFPR)

Prof. Kleber Kenay Horikawa Nabas
(UTFPR)

Visto da Coordenação

Prof. Dr. Walter Godoy Júnior
Coordenador do Curso

RESUMO

Este trabalho apresenta uma abordagem teórica sobre a implantação da tecnologia NAC para o controle de acesso às redes de dados, tendo o foco em ambientes corporativos. Evidencia a necessidade de investimentos em segurança dinâmica por parte das empresas, com o objetivo de controlar os diferentes tipos de usuários e dispositivos conectados à rede. Apresenta as questões que devem ser levantadas durante a preparação e execução do projeto. Discute de forma detalhada as fases de implantação, abordando os obstáculos a serem superados e as boas práticas a serem seguidas para o sucesso do projeto, com base na literatura pertinente ao texto.

Palavras-chave: Autenticação. Avaliação. Autorização. Remediação. NAC.

ABSTRACT

This paper presents a theoretical approach on deploying NAC technology to control access to data networks, with focus in corporate environments. Highlights the need for dynamic security investments by firms in order to control the different types of users and devices connected to the network. It presents the issues to be raised during the preparation and execution of the project. Discusses in detail the deployment, addressing the obstacles to be overcome and the good practices to be followed for the success of the project, based on the literature pertaining to the text.

Keywords: Authentication. Assessment. Authorization. Remediation. NAC.

SUMÁRIO

1 INTRODUÇÃO

NAC é uma sigla do inglês (Network Access Control) que significa Controle de Acesso à Rede, sendo algumas vezes também referenciado como Controle de Admissão à Rede. É um termo com uma história de utilização entre os fabricantes de infraestrutura de rede, sistemas operacionais e softwares de segurança. Os fabricantes de infraestrutura de rede originalmente introduziram tecnologias de controle de acesso com soluções baseadas em autenticação e autorização para controle da comunicação dos usuários e equipamentos. Os sistemas baseados nas credenciais dos usuários e equipamentos permitiram as organizações de TI administrar de forma centralizada quem e o que estava permitido comunicar na rede.

Com o tempo esse conceito de controle de acesso a rede começou a evoluir para incluir um conjunto de informações mais sofisticadas, usadas para determinar quem e o que é permitido comunicar na rede a partir de uma determinada localização em um determinado horário. Fabricantes de sistemas operacionais e softwares de segurança poderiam fornecer informações sobre os sistemas finais, que poderiam ser utilizadas em adição com as credenciais no processo de autenticação. A avaliação da “saúde” dos sistemas finais, incluindo a ameaça que os sistemas finais poderiam causar para o ambiente de rede, e a vulnerabilidade dos sistemas finais para ficarem infectados com vírus e *worms* (subclasse de vírus), poderia ser parte do contexto usado no processo de autenticação e autorização.

A partir dessa abordagem múltipla para determinar quem e o que deveria ser permitido na rede, e quando e onde um sistema final deveria ter acesso, veio a promoção da indústria para o agora comumente usado termo NAC. As soluções de NAC atuais podem ajudar a proteger uma organização do uso indesejado da rede, ameaças de segurança intencionais e não intencionais, e ataques de negação de serviço propagados por *worms* e vírus através de sistemas finais vulneráveis. As soluções NAC podem também ajudar a impor políticas de comunicação, permitindo melhor alocação de recursos de rede para que os processos sejam tão eficientes quanto possível. O benefício para uma organização ao implementar a solução NAC é um ambiente de negócios mais seguro e eficiente. O desafio está em entender as

muitas tecnologias envolvidas nas várias soluções NAC do mercado, e encontrar uma abordagem de arquitetura que ofereça várias funções críticas:

- Visibilidade e gestão de identidade dos vários sistemas finais conectados na rede;

- Avaliação dos sistemas finais, antes deles estarem com acesso permitido na rede (pré-conexão) e depois que eles estiverem conectados na rede (pós-conexão);

- Assistências de remedição para sistemas finais e/ou usuários que não estiverem em conformidade com as políticas de segurança da rede;

- Relatórios de conformidade que detalhem onde os sistemas finais estão na rede e o que eles estavam fazendo na rede.

Poucas empresas hoje são entidades fechadas com perímetros de segurança bem definidos. As empresas se esforçam para fornecer acesso às informações aos usuários a qualquer hora e de qualquer lugar. Usuários móveis, serviços terceirizados, acesso remoto, visitantes, necessitam de acesso à rede para executarem seus trabalhos; trazendo seus equipamentos para dentro e fora dos escritórios. Assim, as empresas acabam expondo suas redes às ameaças e ataques. Violações da rede podem levar à perda de informação, privacidade pessoal, propriedade intelectual e outros dados críticos (CISCO, 2009).

A habilidade de uma organização em gerenciar o acesso do usuário e a segurança do sistema final é um componente crítico para garantir segurança global e disponibilidade de sua infraestrutura de TI. As soluções que fornecem tecnologias proativas e reativas para garantir a continuidade dos negócios irão providenciar um significativo retorno nos investimentos. O NAC é um elemento essencial para uma arquitetura de segurança geral para proteger confidencialidade, integridade e disponibilidade das informações.

2 ENTENDENDO O NAC

Apesar de NAC ser um termo comum hoje em dia para as organizações de TI, há muita discussão em torno do que o NAC envolve e o que não envolve. Alguns vêem o NAC como simplesmente o registro e autorização das máquinas conectadas na rede. Alguns vêem NAC como uma solução para proteger o ambiente de rede dos vírus e *worms*. Outros vêem o NAC como um “porteiro” da rede, com a função de controlar como as máquinas, que não estão em conformidade com as diretrizes corporativas de computação, podem acessar a rede. Uma solução NAC bem planejada é na verdade todas essas coisas.

NAC é um termo que descreve várias tecnologias desenvolvidas para controlar/restringir acesso aos usuários finais à rede, baseado em sua “saúde”. O conceito básico é que sistemas finais vulneráveis e perigosos não deveriam comunicar na rede de negócios porque eles poderiam causar um risco de segurança para serviços e processos críticos. Uma solução de NAC iria prevenir um sistema final “doente” de acessar a rede de uma maneira normal até que o sistema final fosse determinado como “saudável” (NAC WHITEPAPER, 2008).

A verificação da saúde de um equipamento conectado na rede é também conhecida como avaliação do sistema final. Sistemas finais podem ser os PCs tradicionais, impressoras, telefones IP, câmeras de segurança IP, etc. Uma avaliação deveria descobrir o nível de vulnerabilidade e o nível de ameaça de um sistema final. Elementos como *patch* de segurança, presença de antivírus, atualização de assinaturas de antivírus, aplicações sendo executadas, portas abertas, etc..., podem ser investigadas para determinar a saúde geral do sistema final.

Uma abordagem desejável de NAC deveria permitir a avaliação de qualquer tipo de sistema final conectado na rede. Isso é criticamente importante devido ao aumento da diversidade dos sistemas finais conectados nas redes. Para ter uma postura abrangente e proativa para a segurança da rede, cada sistema final conectado na rede (não interessa qual tipo de equipamento) deve ser “desafiado” por uma solução de NAC. A função atual de avaliação pode ser fornecida por várias aplicações. A aplicação de avaliação pode requerer um agente instalado no sistema

final, ou pode funcionar completamente independente dos sistemas finais, de uma maneira sem agente instalado.

Muitos vendedores de soluções NAC atuais não contam com um desafio de autenticação para os sistemas finais, como parte do processo de controle de acesso. Autenticação deveria ser um fundamento crítico para qualquer solução de NAC, e é necessária para obter escalabilidade, flexibilidade, visibilidade, e para fazer cumprir os requerimentos de uso da rede e políticas de segurança. Uma vez que um usuário ou máquina está autenticado (as credenciais foram verificadas) o processo de autorização toma lugar, alterando a configuração da porta de rede de origem física ou virtual, para permitir comunicação baseada em um conjunto de regras de políticas. Avançadas tecnologias de autorização deveriam utilizar contextos adicionais como localização, hora do dia, endereço MAC, etc.., resultando em uma solução robusta. A flexibilidade de autenticação multiusuário, multimétodo em um vendedor de solução NAC significa que não há necessidade de substituição de qualquer dos switches de borda para ganhar visibilidade e controle sobre aqueles usuários e equipamentos conectados (JABBUSH, 2010).

Depois que o processo de avaliação e autorização dos sistemas finais é realizado, se for determinado que um sistema final está fora de conformidade com as políticas de segurança da rede, o sistema final é colocado em um estado de quarentena na rede. O processo de execução de política de quarentena deve envolver políticas de comunicação na rede bem granulares (não simplesmente atribuição de VLAN). Além do que, colocar todos os sistemas finais “doentes” dentro da mesma VLAN de quarentena apenas significa que eles irão infectar uns aos outros com novas vulnerabilidades.

Remediação é o ato de retificar um problema para deixar em conformidade com as políticas pré-definidas. O processo de remediação como parte da solução NAC permite aos usuários colocados em um estado de quarentena a ficarem em conformidade. É importante que o usuário de rede esteja envolvido no processo de remediação para que a eficiência do processo de negócios seja maximizada. Quando um usuário ou seu sistema final tem um problema, eles deveriam ser capazes de consertar isso sem ter que envolver a equipe de TI. Isso irá impedir que a equipe de suporte seja bombardeada com problemas de configurações e conformidade dos sistemas finais. Para que esse processo seja efetivo, a solução NAC deve fornecer uma notificação ao usuário quando um sistema final é colocado

em quarentena na rede. As políticas de comunicação devem ser aplicadas como parte do estado de quarentena para permitir comunicação segura aos serviços necessários para deixarem o sistema final em estado de conformidade.

Autenticação, avaliação, autorização, aplicação de políticas e remediação são todas partes críticas de um solução de NAC abrangente. Há muitos produtos e tecnologias disponíveis de múltiplos vendedores que oferecem algumas dessas partes. Uma solução de NAC integrada, com arquitetura aberta deverá fornecer todos essas partes críticas trabalhando juntas.

3 PREPARANDO PARA O NAC

Se aplicado em toda empresa, a implantação do NAC pode ser um projeto extenso e irá requerer muita preparação. As informações a seguir irão descrever algumas das preparações que podem ser tomadas por uma organização de TI para garantir o sucesso do projeto NAC.

3.1 Principal Objetivo

Antes de embarcar em um projeto de implantação de solução NAC, é importante entender os principais benefícios para os negócios que se deseja alcançar com o NAC. Um exemplo poderia ser o seguinte:

"*Nós gostaríamos de implementar NAC para garantir que nossos visitantes possam acessar a internet em nossas salas de reunião. Aos visitantes não deve ser permitido comunicação com a rede interna da empresa. Todos os sistemas finais conectados na rede devem ter um nível mínimo de segurança*." (UNDERSTANDING NAC, 2010)

Com esse exemplo, os elementos fundamentais de um projeto NAC podem ser determinados:

- Quem é permitido conectar na rede?
- Como eles são permitidos conectar?
- O que eles estão autorizados a conectar?
- Onde eles devem ter acesso?

O NAC geralmente é um processo, e pode ser separado em:
- Função (quem?)
- Direitos (como?)
- Recursos (o que?)
- Localização (onde?)

Um componente de tempo também pode ser adicionado (quando alguém pode acessar?)

3.2 Sistemas Finais e Usuários a Serem Suportados

Um dos desafios de uma implementação NAC é a integração com os diferentes tipos de sistemas finais. Considerando as diversas opções de identificação, autenticação e avaliação no ponto de acesso à rede, pode ser difícil garantir uma cobertura completa com uma solução NAC. Para garantir a aplicação do NAC de forma abrangente, será necessário saber com antecedência que tipos de sistemas finais existem e quais direitos eles deveriam ter no ambiente de rede. Grupos e recursos precisam ser atribuídos para sistemas finais bem como para usuários. Os grupos não deveriam ser muito específicos para não tornar o trabalho administrativo muito difícil.

Algumas questões para preparação:

- Todos os tipos de equipamentos e usuários de rede são conhecidos?
- Todos os recursos necessários para os grupos definidos foram identificados?
- Há alguma restrição física ou lógica?
- Os recursos podem ser agrupados juntos?
- Deve ser concedido o acesso em geral e negado especificamente, ou vice-versa?

Mesmo que o projeto comece com apenas alguns equipamentos ou grupos de usuários, é necessário ter uma visão completa do projeto inteiro para escolher a arquitetura de NAC correta. Uma solução baseada em agente, por exemplo, não seria aplicável a todos os tipos de equipamentos como impressoras, telefones IP, e outros. Isso pode causar problemas após a implantação pelo fato de muitos dos clientes não serem gerenciáveis (TIPPINPOINT NAC, 2008).

4 IMPLANTAÇÃO

Uma abordagem baseada em fases é o método preferido para a implantação de solução NAC. Em geral, uma implantação NAC pode ser separada nas seguintes fases (UNDERSTANDING NAC, 2010):

Fase 1: Detecção e rastreamento dos sistemas finais
Fase 2: Autorização dos sistemas finais
Fase 3: Autorização dos sistemas finais com avaliação
Fase 4: Autorização dos sistemas finais com avaliação e remediação

Fase 1: Coleta de informação sobre todos os sistemas finais, sem causar nenhuma alteração nas conexões existentes. Isso é basicamente um inventário dos sistemas finais conectados na rede. Pode ser feito com ou sem autenticação.

Fase 2: Considera as regras pré-definidas e restrições relacionadas ao acesso a rede. Isso tipicamente requer autenticação para garantir que políticas de acesso a rede específicas possam ser aplicadas para cada sistema final e usuário.

Fase 3: Avaliação de todos os sistemas finais. Esse dado pode ser acessado via um sistema de gerenciamento externo (por distribuição de software), um agente, ou por *scan* de rede. As informações típicas são: sistema operacional, vulnerabilidades, portas abertas.

Fase 4: Depois que as políticas de acesso a rede são aplicadas aos sistemas finais individualmente, usando o resultado dos dados da avaliação. Os usuários deveriam ser informados sobre essa avaliação e deveriam receber a oportunidade de remediação caso não estejam em conformidade com as políticas de segurança apropriadas.

As próximas seções irão detalhar as tecnologias empregadas para a implantação de NAC em fases.

5 DETECÇÃO E AUTENTICAÇÃO

Todos deveriam ser capazes de acessar a rede a qualquer hora e de qualquer lugar, e a rede deveria reagir dinamicamente e automaticamente de acordo com as regras definidas para os equipamentos e/ou usuários fazendo conexão.

Para que isso aconteça é necessário saber quem está conectado na rede e onde eles estão localizados. A documentação manual da rede deveria ser desnecessária. Com NAC, a empresa deveria ser capaz de realizar uma documentação automática da rede.

“Como pode um sistema final ou usuário ser identificado?”

Os equipamentos *inline* têm um método óbvio para fazer a identificação. Os sistemas finais estão diretamente conectados neles, e assim são imediatamente vistos pelo sistema.

Onde não há equipamentos *inline* para identificação, uma variedade de métodos pode ser utilizada para identificação dos equipamentos que estão se conectando na rede. Endereços MAC e IP são os métodos mais comumente utilizados para identificação, mas eles podem mudar em menos de alguns minutos, sendo portanto adequados de forma limitada. Na verdade, a identificação de um sistema final anda de mãos dadas com sua autenticação. O mesmo mecanismo que é usado para autenticação é freqüentemente também usado para identificar os sistemas finais. Autenticação é o método pelo qual a solução NAC identifica os usuários ou equipamentos como sendo autorizados na rede (EDWARDS, 2009).

Contudo, a questão que precisa ser feita antes de decidir sobre qualquer método utilizar, é:

“qual autenticação é suportada pelo sistema final?”

Existem muitos métodos que podem ser utilizados para autenticação de sistemas finais e usuários. Uma solução de NAC abrangente deveria ser capaz de suportar múltiplos métodos:

- 802.X port based (via RADIUS)
- MAC based (via RADIUS)
- Web based
- Static port/Mac configuration
- Dynamic port/MAC configuration (SNMP)
- Kerberos Snooping

Outros contextos como *hostname* (nome da máquina) ou endereço IP podem ser utilizados para identificação. Isso pode ser bastante útil, especialmente para sistemas que não sejam computadores.

É importante notar que algumas soluções NAC omitem a funcionalidade de autenticação, e utilizam apenas o método de identificação em combinação com a avaliação para determinar se o usuário ou equipamento deveriam estar na rede (NAC COMPARISON, 2007).

6 AVALIAÇÃO

Uma forte integração do processo de registro para avaliação de sistemas finais ainda não é comum. O processo de registro é um componente importante da implantação do NAC. Os padrões de avaliações são a Microsoft (Network Access Protection) e TNC (Trusted Network Connect). O IETF também está trabalhando nisso, mas ainda não tem uma solução completa até o momento. A função de avaliação vai além da porta do switch e tenta avaliar o sistema final em si (FRATTO, 2007).

A Avaliação, ou verificação da saúde, pode ser separada em dois métodos:

Sem Agente:

1. Baseado na Rede – um *scanner* de rede varre os sistemas finais remotamente (utilizando a rede).
2. Baseado em *Applet* – uma *applet* Java é usada para lançar funções de avaliação nos sistemas finais (baseado em navegador).

Com Agente:

1. Agente Temporário – também conhecido como agente dissolvível. Pode ser carregado e descarregado do sistema final. Não requer direito administrativo para executar as verificações de conformidade.
2. Agente Permanente – um conjunto permanente de software com firewall e detecção de intrusos instalado no sistema final.

Durante uma avaliação, os sistemas finais são verificados para saber se estão em conformidade e/ou vulneráveis. Isso também inclui testes do firewall instalado no sistema final e outras aplicações, a procura de vulnerabilidades.

A escolha de qual método de avaliação é o mais apropriado para um ambiente em particular é baseada no que se deseja verificar e quais possibilidades o sistema final permite. Obviamente seria um grande desafio conseguir instalar um agente em uma impressora ou em um telefone IP. Por outro lado, um *scanner* de

rede pode ter problemas com um antivírus local quando tentar varrer o sistema final a procura de assinaturas de vírus.

O tempo de avaliação e a carga produzida na rede também são bem diferentes para cada método. Um *scanner* de rede varre a rede e, conseqüentemente causa uma carga maior, requerendo mais banda. Um agente realoca essa carga dentro do cliente e irá necessitar somente de recursos locais até que o relatório final seja enviado para a administração. Os recursos locais requeridos por um Agente Permanente podem ser grandes, uma vez que eles trabalham com aplicações próprias para servir como firewall e sistemas de prevenção de intrusos. O tempo estimado para varredura com qualquer um desses métodos é difícil de medir, pois depende de testes e os propósitos. Uma varredura rápida no firewall local é com certeza mais simples e rápida do que uma varredura abrangente com testes de vulnerabilidades em milhares de portas em camada 4 do modelo OSI.

Uma avaliação extensiva pode não somente fornecer informações sobre o estado da saúde dos sistemas finais, mas também informações adicionais para propósitos de inventário e auditoria (JABBUSH, 2010).

6.1 Sem Agente

A extensão dos testes de sistemas finais depende em parte do software utilizado para a avaliação. Há um grande mercado para *scanners* de vulnerabilidade, oferecendo uma enorme variedade de programas que são projetados somente para isso e são continuamente atualizados com conjuntos de novos testes.

Geralmente uma avaliação inclui os seguintes passos (sem ordem particular):
1 – Disponibilidade e identificação – Ping, DNS lookup
2 – Portscan – TCP/UDP
3 – Identificação de vulnerabilidades
4 – Exploração de vulnerabilidades

Cada um desses passos deveria ser configurado separadamente e um passo poderia utilizar os resultados de qualquer outro passo. Por razões de carga e

desempenho, faz sentido somente procurar por vulnerabilidades nas portas abertas. Alguns *scanners* de rede podem se conectar ao próprio cliente (com usuário e senha) e executar testes locais no cliente. É necessário muito cuidado na realização dos testes de vulnerabilidade, uma vez que isso pode causar um colapso no sistema final.

A desvantagem desse método é a precisão dos resultados. Por um lado, é possível fazer a verificação somente das vulnerabilidades conhecidas. Por outro lado, os serviços e versões não podem ser identificados com precisão através de comunicação remota na rede. Outro problema é a grande carga (causada pelo *scan*) no próprio servidor de *scan*. Na verdade, é quase impossível fazer *scan* de milhares de sistemas finais com um único servidor de *scan*. Uma vantagem desse método de avaliação é a extensão dos testes, que geralmente são maiores do que um agente poderia fazer. Também, em um ambiente com visitantes, não é necessário forçar eles a instalarem nenhum software.

A maior vantagem desse método é a capacidade de varrer sistemas finais que não permitem a instalação de nenhum agente, que com certeza, aumenta o número de equipamentos incluídos em uma implantação de NAC.

6.2 Com Agente

Um agente é uma parte independente de um software que roda em um sistema final, e fornece informações sobre a saúde do sistema final, e em alguns casos, trabalha proativamente contra ameaças. A grande vantagem de um agente é a opção de requisitar e verificar todos os dados de um sistema. Mas também há desvantagens nesse método. Desde que um agente precisa ser instalado em um sistema final, pode haver limitações na capacidade de cobertura em um ambiente de rede corporativo.

Em áreas com múltiplos sistemas operacionais e aplicações, pode ser necessário fazer muitos ajustes de configurações nos clientes, e é comum que às vezes nem haja essa opção. O agente tem que ser muito “social” e tem que ser capaz de se comunicar com seu ambiente. Isso pode causar problemas em ambientes com múltiplos fabricantes. A maioria dos fabricantes de NAC oferece

também seus próprios agentes para tornar suas soluções NAC mais fortes, e restringir a integração com outras soluções.

Estão sendo realizados trabalhos para desenvolver agentes para múltiplos fabricantes. A Microsoft oferece seu *Network Access Protection* (NAP) como uma interface entre agentes e NAC no próprio sistema operacional. Geralmente deve-se considerar a sustentabilidade e compatibilidade de permanecer flexível para futuras decisões envolvendo a implantação de NAC.

Uma avaliação de agente normalmente oferece as seguintes informações:
- O firewall está ativo e sendo executado?
- Há algum software de antivírus instalado e com assinaturas atualizadas?
- Qual o sistema operacional rodando?
- Qual o nível de patch do sistema?
- Existe uma conexão com o agente?
- Quais softwares estão instalados?
- Quais processos e serviços estão sendo executados?

As possibilidades de testes são muitas, mas testes específicos acrescentam complexibilidade uma vez que o agente primeiro precisa aprender o que deveria ser testado e como diferenciar entre bom e mau. Um agente é capaz de executar uma avaliação e fornecer os resultados mais rápido que os outros métodos. Ele também aloca a maior parte da carga para o sistema final. Isso faz da solução baseada em agente mais escalável para ambientes de redes maiores. Em alguns casos o agente também pode executar a auto remediação, como por exemplo, ativar o firewall local do sistema final. Também há a opção de gerenciar os visitantes com agentes dissolvíveis, onde o agente é instalado na RAM do sistema final e se “dissolve” depois da próxima iniciação do sistema (CISCO 2009).

Não há uma solução única de avaliação para todos os sistemas finais. A melhor implementação seria com agentes onde possível e com *scanner* de rede onde fosse preciso. Os dois métodos se complementam, e em ambientes com grande nível de segurança, às vezes faz sentido utilizar os dois métodos ao mesmo tempo. Outra vantagem, independente das informações de segurança dos sistemas finais, é a documentação de todos os equipamentos de rede.

7 AUTORIZAÇÃO

Depois de detectar, autenticar e avaliar um sistema final, uma arquitetura NAC bem planejada pode aproveitar a informação aprendida para autorizar os sistemas finais a acessarem a rede e serviços específicos.

Autorização é o processo pelo qual uma solução NAC aplica decisões sobre acesso à rede para um sistema final. A autorização é modo pelo qual o sistema conduz ações, como por exemplo, mover os sistemas finais para diferentes VLANs (Virtual LAN), aplicar restrições de acesso via ACL (*Access Control List*) ou garantir acesso adicional. As opções de autorização variam muito entre as soluções NAC.

A autorização é de longe a função mais desafiadora de uma solução NAC para implementar e integrar na rede porque ela necessita modificar de alguma maneira o sistema final ou a própria rede, para aplicar as mudanças dos direitos de acesso.

O processo de autorização aplica todas as regras planejadas durante a fase de preparação da implementação NAC. Como discutido anteriormente, há múltiplas opções disponíveis em relação à autorização de serviços para os sistemas finais. Essas opções podem ser dependentes do desempenho da rede, e em particular, da capacidade da solução NAC. Além disso, a escolha da opção de autorização depende do nível de segurança requerido, bem como do desenho da infraestrutura em si. É importante saber se mais do que um sistema final precisa compartilhar portas ou se equipamentos, usuários, portas, ou fluxos de tráfego individuais precisam ser considerados (UNDERSTANDING NAC, 2010).

Algumas questões para considerar na escolha do método de autorização:

- Qual nível de granularidade é necessário? Na porta, usuário, equipamento, camada de tráfego?
- Tudo deveria ser negado por padrão e somente permitido caso por caso? Ou vice-versa?
- Como é manipulada a autorização de vários equipamentos na porta do switch?

Os principais métodos de autorização são:

a) ***Inline***: O equipamento autorizador fica entre os sistemas finais e o restante da rede,

b) ***Software***: Instalado nos sistemas finais para aplicar regras ditadas por um controlador NAC instalado na rede,

c) ***Out Of Band (OOB):*** Utiliza um controlador NAC central que se comunica com um servidor de autenticação (Radius) e com todos os *switches* de borda da rede.

Cada método apresenta seus prós e contras, que não serão discutidos nesse trabalho.

8 REMEDIAÇÃO

O NAC deve ter a função de remediação completamente integrada na solução. Sem opções para remediação, uma solução NAC simplesmente irá bloquear o acesso do sistema final em não conformidade, sem fornecer uma maneira de trazer o equipamento para conformidade. Estará impedindo que um número significativo de sistemas finais se conecte aos serviços necessários para manter a continuidade e produtividade dos negócios.

Remediação é o processo de apoiar os sistemas finais a atingirem o nível necessário de conformidade, para depois, permitir o acesso a rede. Para diminuir o processo de remediação manual, os problemas com os sistemas finais devem ser resolvidos automaticamente ou pelo usuário, ao invés de envolver o suporte técnico de TI (CISCO, 2007).

Remediação automática é possível com a utilização de agentes. Em alguns casos um software de gerência pode ser acionado pela solução NAC para resolver essa questão.

A solução mais comum para remediação manual é um servidor de remediação web específico para o qual os usuários são redirecionados. A vantagem disso é uma gerência centralizada do processo de remediação disponível, com a execução distribuída para os usuários finais.

Conteúdo importante de um portal Web:

- Informação sobre o status do sistema final: em quarentena, permitido na rede, etc.
- Especificação das violações do sistema final: Firewall desabilitado, base de assinaturas desatualizadas, etc.
- Detalhes para resolução do problema: habilitar firewall, se conectar ao servidor de atualizações, etc.
- Informações sobre os serviços disponíveis: servidor de atualização do sistema operacional, etc.
- Link para se reconectar depois de seguir as instruções.

As remediações deveriam ser automáticas para diminuir a intervenção do usuário. Quanto melhor o processo de remediação, menor a carga de trabalho administrativo, uma vez que a maioria das soluções dos problemas pode ser redirecionada para o agente ou usuário.

Questões relevantes para o processo de remediação:

- Quem é o responsável pela remediação? Um agente, o usuário ou o administrador?
- Quanto tempo leva o processo de remediação e reconexão?
- O portal de remediação está acessível para todos?

9 MONITORAMENTO

Até agora a discussão centrou-se na avaliação de sistemas finais na fase de pré-conexão. Mas quem garante que mudanças não são feitas para tirar o sistema final da conformidade após a conexão na rede? Ferramentas para avaliação e monitoramento contínuo são frequentemente empregadas. Dependendo do método, intervalos diferentes de tempo podem ser usados para avaliação pós-conexão. Um agente ou um *scan* remoto do sistema final podem executar avaliações contínuas a cada espaço de tempo determinado.

A solução NAC também deveria incluir uma variedade de opções para atender os requisitos da rede. A solução NAC escolhida deveria trabalhar de forma flexível, mas baseada em modelos para diminuir o trabalho administrativo e facilitar a resolução de problemas (ROBINSON, 2007).

Alguns parâmetros para considerar:
- Os sistemas deveriam ser avaliados toda vez que eles conectarem?
- Qual o intervalo que os sistemas deveriam ser reavaliados (toda semana, mês)?
- Os clientes podem permanecer conectados durante a avaliação, ou eles deveriam ser colocados em quarentena, por padrão?

Além disso, o NAC é um perfeito complemento para soluções de segurança baseadas em comportamento e anomalias. Essas soluções geralmente analisam os fluxos de comunicação de dados e detectam ataques de camada 3-7(Modelo OSI), mas não são capazes de aplicar qualquer ação de combate na infraestrutura de rede. Esse tipo de monitoramento pode ser integrado com uma solução de NAC bem planejada para fornecer proteção efetiva após conexão. Outra opção é a combinação de um Sistema de Detecção de Intrusos (*IDS-Intrusion Detection Sistem)* e uma solução NAC para detectar os ataques e também ter uma resposta automática do sistema.

Quanto mais aberta for a interface do NAC, mais soluções de segurança podem utilizar essa interface, e maior seu valor para a rede.

10 CONCLUSÃO

A coisa mais importante a saber sobre NAC é que ele não é um produto, e sim um processo. Produtos podem estar envolvidos, mas as partes mais importantes do NAC não envolvem tecnologia e sim o gerenciamento de pessoas e riscos.

Um projeto NAC não tem que ser complexo e nem difícil. A implementação NAC pode ser dividida em etapas lógicas ou fases. E os benefícios incrementais podem ser rapidamente percebidos através do processo de implementação. O sucesso do projeto NAC depende realmente de um bom começo. Quanto mais informações estiverem disponíveis e melhores as políticas forem definidas, mais fácil será a implementação.

11 REFERÊNCIAS

CISCO NAC – EXECUTIVE OVERVIEW. 2009. Disponível em: http://www.cisco.com/en/US/solutions/collateral/ns340/ns394/ns171/ns466/net_implementation_white_paper0900aecd80557152.pdf. Acesso em: 09 abril 2011.

NAC WHITEPAPER. 2008. Disponível em: http://www.enterasys.com/company/literature/nac-wp.pdf. Acesso em: 05 março 2011.

JABBUSH, Jennifer. Universal NAC Feature Model. 2010. Disponível em: http://securityuncorked.com/2010/03/universal-nac-feature-model-document. Acesso em: 20 abril 2011.

UNDERSTANDING NAC. 2010. Disponível em: http://www.enterasys.com/company/literature/enterasys-nac-guide.pdf. Acesso em: 12 março 2011.

TIPPINPOINT NAC. 2008. Disponível em: http://www.netevents.tv/output/tippingpoint/downloads/401079-001_TippingPointNAC.pdf. Acesso em: 7 maio 2011.

FRATTO, Mike. Tutorial Network Access Control. 2007. Disponível em: http://www.networkcomputing.com/data-protection/229607166?pgno=1. Acesso em: 21 maio 2011

EDWARDS, John. The Essential Guide to NAC. 2009. Disponível em: http://www.focus.com/briefs/essential-guide-nac/. Acesso em: 02 abril 2011.

NAC COMPARISON GUIDE. 2007. Disponível em: http://www.networksecurityjournal.com/whitepaper/pdf/nac-comp-guide-nsj_8-07.pdf. Acesso em: 16 abril 2011.

CISCO NAC: HELP CUSTOMERS IMPROVE SECURITY. 2007. Disponível em: http://www.cisco.com/en/US/solutions/collateral/ns340/ns394/ns171/ns466/net_implementation_white_paper0900aecd8051f9e7.pdf. Acesso em: 09 abril 2011.

ROBINSON, Brian. What You Need to Know About NAC. 2007. Disponível em: http://www.itsecurity.com/features/what-you-need-to-know-about-nac-072607/. Acesso em: 2 abril 2011.

DEPLOY AN INTEROPERABLE AND STANDARDS-BASED NAC SOLUTION. 2007. Disponível em: http://www.cisco.com/en/US/solutions/collateral/ns340/ns394/ns171/ns466/net_implementation_white_paper0900aecd8067e368.pdf. Acesso em: 09 abril 2011.

360^{O} NETWORK ACESS CONTROL WITH TIPPINGPOINT NAC. 2007. Disponível em: http://www.netevents.tv/output/tippingpoint/downloads/503188-001_360NACwithTippingPoint.pdf. Acesso em: 7 maio 2011.

WILSON, Tim. Annual CSI Study. 2007. Disponível em: http://www.darkreading.com/security/perimeter-security/208804727/annual-csi-study-cost-of-cybercrime-is-skyrocketing.html. Acesso em: 21 maio 2011

JUNIPER NETWORKS. Disponível em: http://www.juniper.net. Acesso em: 11 junho 2011.

SYMANTEC. Disponível em: www.symantec.com. Acesso em: 11 junho 2011