

Uma solução segura de acesso remoto via VPN para manutenção de Controladora de Discos de *Mainframe* da Empresa Beta baseada na Norma NBR ISO/IEC 17799

Edvaldo Queiroga¹, Leila Maria M V Galvão², Marcio Petiz³ e Sergio Venut⁴

Universidade Católica de Brasília (UCB), Campos Universitário II, SGAN 916
Módulo B – Brasília – DF – Brasil

***Abstract.** The remote access used to effectuate the preventive maintenance and to answer problem events to a Mainframe Disc Controlling is not safe and do not follow the rules of NBR ISO/IEC 17799:2001. This article intends to present a safe solution to remote access via VPN in order to maintain the Mainframe Disc Controlling, based on NBR ISO/IEC 17799:2001 recommendation.*

***Resumo.** O acesso remoto utilizado para se efetuar manutenção preventiva e em resposta a eventos de problemas a uma Controladora de Discos de Mainframe da empresa Beta é inseguro e não segue as normas NBR ISO/IEC 17799:2001. Este artigo se propõe a apresentar uma solução segura de acesso remoto via VPN para manutenção de Controladoras de Discos de Mainframe baseada nas recomendações NBR ISO/IEC 17799:2001.*

1. Introdução

Durante anos, o acesso remoto para manutenção foi tipicamente caracterizado por técnicos remotos acessando recursos privados de uma organização através de uma rede de telefonia pública, com a conexão discada terminando em um servidor de acesso (*Remote Access Server – RAS*) ou simplesmente um modem. A segurança deste acesso remoto geralmente era baseada em uma autenticação simples com *login* e senha, somada a uma confirmação da origem da ligação telefônica, *Call-back* e às vezes com a implementação de servidor para autenticação, autorização e *log* de auditoria.

O acesso remoto para manutenção e gerência da Controladora de Discos de *Mainframe* da empresa Beta, utiliza esta estrutura antiga e precisa ser melhorado para adquirir a segurança necessária e requerida nos tempos atuais.

A enorme difusão da *Internet* e a crescente disponibilidade de acesso de banda larga, em conjunto com o desejo de redução dos altos custos do acesso discado, têm conduzido ao desenvolvimento de mecanismos de acesso remoto baseados na *Internet*.

Esse tipo de acesso remoto, comumente chamado de acesso remoto VPN, utiliza a tecnologia de redes privadas virtuais (VPN), possibilitando que uma infraestrutura de rede pública, como a *Internet*, seja utilizada como backbone para a comunicação do técnico remoto e a rede privada. Na VPN são implementados mecanismos de segurança para que a conexão, mesmo através de uma rede pública como a *Internet*, seja segura.

Os mecanismos de segurança que são implementados na VPN visam garantir a integridade, confidencialidade e disponibilidade, que são pilares do Código de prática para a gestão da segurança da informação, mais conhecido como norma NBR ISO/IEC 17799:2001.

Com base nestes princípios, na solução de acesso remoto via VPN e na norma NBR ISO/IEC 17799:2001, em que vários tópicos abordam a segurança no acesso a terceiros, que este trabalho foi desenvolvido.

Os tópicos da NBR ISO/IEC 17799:2001 relacionadas a acesso remoto são os seguintes: política de utilização dos serviços de rede, rota de rede obrigatória, autenticação para conexão externa de usuários, autenticação de nós e proteção de portas de diagnósticos remotas.

Conforme descrito na NBR ISO/IEC 17799:2001 no item proteção de portas de diagnósticos remotas, convém que o acesso às portas de diagnósticos seja seguramente controlado. Muitos computadores e sistemas de comunicação estão instalados com recursos que permitem o diagnóstico remoto por *dial-up* para uso dos engenheiros de manutenção. Se desprotegidas, essas portas de diagnóstico proporcionam um meio de acesso não autorizado.

Convém que elas, portanto, sejam protegidas por um mecanismo de segurança apropriado, por exemplo uma chave de bloqueio e um procedimento para garantir que elas sejam acessíveis somente através de um acordo entre o gestor dos serviços computadorizados e o pessoal de suporte de *hardware* e *software* que solicitou o acesso.

Neste trabalho, após apresentada a realidade atual da topologia de acesso remoto para manutenção da Controladora de Discos da empresa Beta, mostrados os conceitos e o funcionamento de uma VPN, além das principais práticas da NBR ISO/IEC

17799:2001 para acesso de terceiros e finalmente, será proposta uma solução de acesso remoto baseado em VPN para manutenção das Controladores de Discos de *Mainframe* da empresa Beta.

2. Funcionamento do acesso remoto atual a Controladora de discos de *Mainframe* para manutenção

Existem basicamente dois tipos de conexão estabelecidas para a Controladora de Discos de *Mainframe*: *Inbound* e *Outbound*.

Conexão *Outbound* – Iniciadas pelo sistema proprietário interno da Controladora de Discos de *Mainframe* e ocorrem nas seguintes situações e periodicidade:

- Diariamente, para teste de conexão e envio de status;
- Semanalmente, para envio de configuração atualizada;
- Por evento, na ocorrência de falha/erro ou diagnóstico preditivo.

Conexão *Inbound* - Iniciadas externamente pelo sistema proprietário remoto, ocorrendo somente na seguinte situação:

- Falha/Erro de Alta Criticidade (*System Down*), para os quais foi definido *CASE ID* e determinado que o atendimento é realizado com o auxílio remoto por Especialistas de 2º Nível.

Os técnicos e especialista podem efetuar alguns tipos de manutenção definidos pelo funcionamento do sistema:

- sistema proprietário não possibilita acesso aos dados do cliente;
- Nenhum acesso remoto (Conexão *Inbound*) é realizada sem o conhecimento do Engenheiro de local/residente. O processo para estabelecimento deste tipo de conexão exige a presença do mesmo, para fornecimento das seguintes informações:
 - Liberação do acesso remoto no sistema;
 - *Start* do Programa de acesso remoto;
 - Inserção do número de Telefone para Conexão *Inbound* pelo programa de acesso remoto.
 - Habilitação (através de *password* da sessão remota).

Após o estabelecimento dessa conexão, somente a transferência de arquivos e informações referentes ao erro de hardware investigado são acessadas pelos especialistas de 2 Nível.

O acesso remoto através de conexão *Inbound* funciona da seguinte forma:

- Para iniciar uma sessão com o sistema da Controladora de Discos, o especialista de 2 Nível localizado remotamente, deve discar para a Controladora utilizando uma senha especial do programa remoto;

- Uma vez conectado, o especialista de 2 Nível deve também fornecer uma senha adicional para habilitar o sistema proprietário remoto;

- Esta senha adicional deve ser conferida contra a senha trocada (*downloaded*) pelo par de sistemas proprietários durante as chamadas diárias para o *software* localizado na empresa prestadora de serviços;

- Especialista de 2 Nível fornece então um número de telefone para o sistema da controladora de discos (*call-back*) e o software da controladora inicia uma conexão *outbound* para o número fornecido. Efetivada a conexão, o especialista de 2 Nível está conectado remotamente.

A segurança dessa solução se baseia nos seguintes pontos:

- Protocolo proprietário de comunicação, não compatível com nenhum protocolo padrão de mercado;

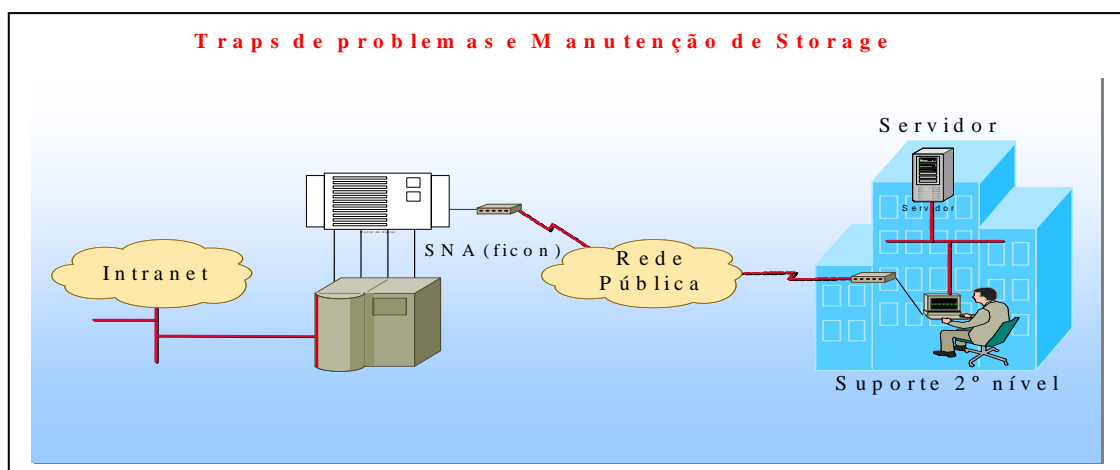
- Utilização de um sistema que trabalha em topologia *peer-to-peer*, não possibilitando a comunicação sem o par dos sistemas;

- Utilização de estrutura de comunicação baseada em *hex streams*, impossibilitando o reconhecimento de códigos de caracteres como EBCDIC, ASCII, ou outros;

- Infra-estrutura de *software* e *hardware* que não possibilita o acesso aos dados.

dos clientes.

Figura 1 – Topologia de acesso remoto atual



3. Conceitos e funcionamento de uma VPN

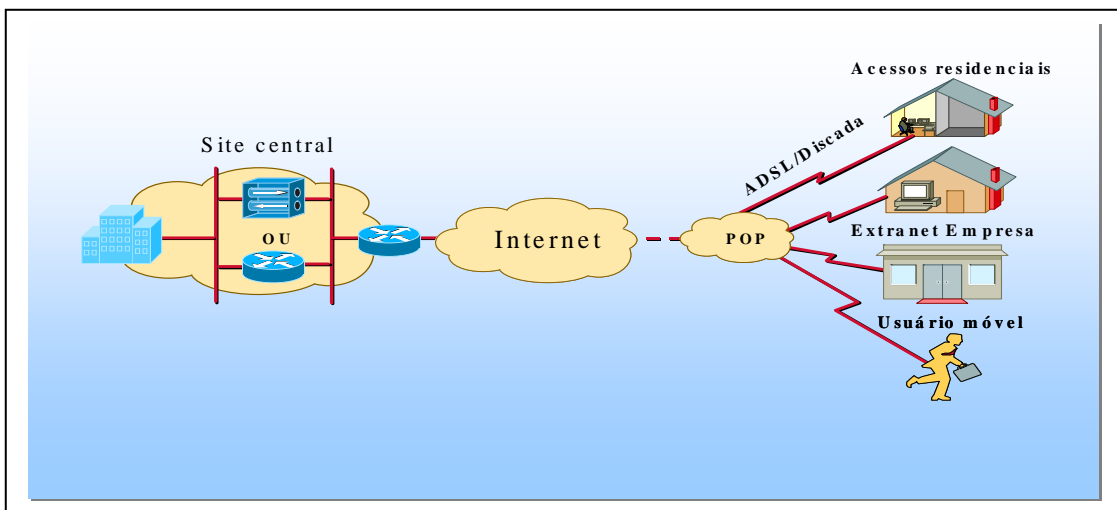
VPN (*Virtual Private Network*) é uma conexão criptografada entre duas redes privadas através de uma rede pública, como a Internet.

A VPN é utilizada para transferência de informações, de modo seguro, entre redes corporativas e/ou usuários remotos.

Os tipos básicos de VPN são: acesso remoto e *Site-to-Site*.

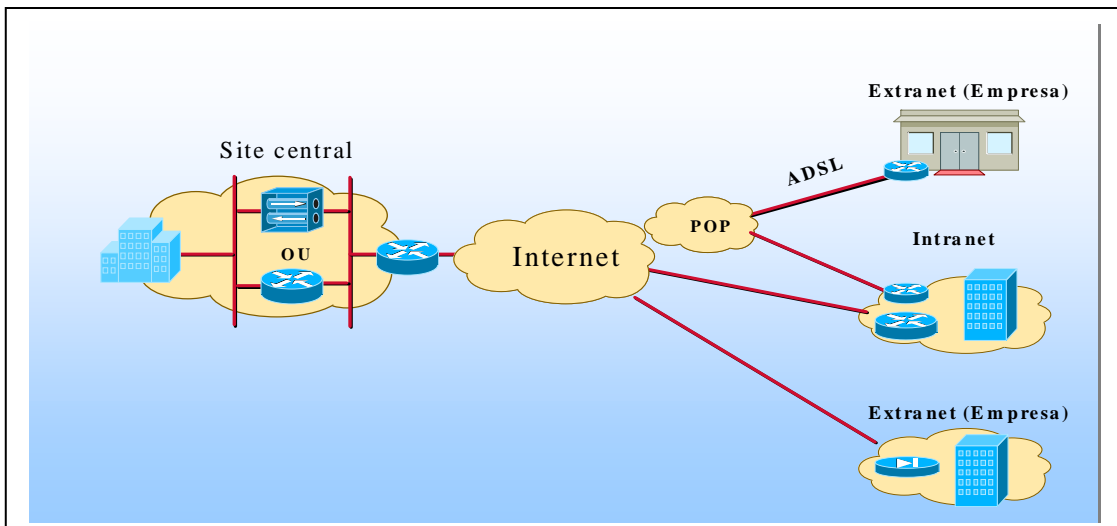
Acesso Remoto – É utilizada para acessos residenciais, de pequenos escritórios e usuários móveis. Veio para agregar e até substituir os acessos dial (linha discada). Para se conectar via VPN ao site central, geralmente instalamos um *client* em nossa estação/notebook ou utilizamos *WebVPN*.

Figura 1 – Acesso Remoto



Site-to-Site – É utilizada para conectar *sites* corporativos e outras empresas. Veio para trazer outra opção de conexão, além *Link* dedicado e *Frame-Relay*.

Figura 2 – Acesso Site-to-Site



Para que a conexão segura seja estabelecida, utilizamos o *IPSec* (*IP Security*). O *IPSec* é um conjunto de protocolos padronizados (RFC 2401 – RFC 2412) desenvolvidos pela *IETF*. O *IPSec* oferece transferência segura de informações através da rede IP pública ou privada. Uma conexão *IPSec* envolve sempre três etapas:

Negociação do nível de segurança;

Autenticação e Integridade;e

Confidencialidade;

Para implementar essas três etapas o *IPSec* utiliza-se de três mecanismos:

AH – Authentication Header;

ESP – Encapsulation Security Protocol;e

IKE – Internet Key Exchange Protocol

Além de ser um padrão aberto *IETF* que está sendo adotado por todos os fabricantes de equipamentos de redes de computadores e desenvolvedores de sistemas, por definição o *IPSec* possui uma arquitetura aberta no sentido de possibilitar a inclusão de outros algoritmos de autenticação e criptografia.

Criptografia é a combinação de uma chave de um algoritmo matemático baseado em uma função unidirecional. Este algoritmo é aplicado aos dados, juntamente com a chave, de modo a torná-los indecifráveis para qualquer um que os veja. O modo que isso é feito garante que somente é possível se obter os dados originais caso se possua o algoritmo e a chaves usados inicialmente.

Autenticação é também a combinação de uma chave com um algoritmo matemático baseado em uma função unidirecional. A diferença em relação a criptografia, é que este algoritmo, quando aplicado sobre os dados, não produz dados indecifráveis mas sim um assinatura digital para eles. Essa assinatura é gerada de tal forma que qualquer pessoa que desconheça o algoritmo ou a chave utilizados para gerá-la seja incapaz de calculá-la. Quando uma assinatura digital é gerada, ela passa a ser transmitida para o destino junto com os dados. Caso estes tenham sofrido quaisquer alterações no caminho, o recipiente quando calcular a assinatura digital dos dados recebidos e compará-la com a assinatura recebida, irá perceber que as duas são diferentes e concluir que os dados foram alterados.

A autenticação é uma operação bastante rápida quando comparada com a criptografia, porém sozinha não consegue impedir que os dados sejam lidos. Ela deve ser usada apenas nos casos onde se necessita confiabilidade dos dados mas não sigilo. Caso se necessite de ambos, usa-se autenticação em conjunto com a criptografia.

Mantendo-se um destes dois componentes secretos (no caso, a chave), faz-se com que a visualização dos dados por terceiros se torne impossível.

Através do processo de autenticação descrito acima, é possível se garantir a origem das mensagens em uma comunicação entre duas partes. Entretanto, para que isso seja possível, é necessário que as entidades que estão se comunicando já tenham previamente trocado informações através de algum meio fora do tráfego normal dos dados. Esta troca de informações normalmente consiste no algoritmo a ser utilizado par a autenticação e sua chave.

O problema surge quando se torna necessário assegurar a origem das mensagens de uma entidade com a qual nunca existiu comunicação prévia. A única forma de se resolver este problema é delegar a uma terceira entidade o poder de realizar estas autenticações (ou em termos mais técnicos, realizar a certificação da origem de uma mensagem). Esta terceira entidade é chamada de Entidade Certificadora e, para que seja possível ela assegurar a origem de uma mensagem, ela já deve ter realizado uma troca de informações com a entidade que está sendo certificada.

Certificado digital é um documento fornecido pela Entidade Certificadora para cada uma das entidades que irá realizar uma comunicação, de forma a garantir sua autenticidade.

4. Proposta de acesso remoto via VPN a Controladora de Discos de Mainframe da empresa Beta

O acesso remoto a controladora de discos de *Mainframe* da empresa Beta é efetuado através de linha discada. Após o estabelecimento da conexão, um sistema proprietário derruba a conexão e se confirmada a origem cadastrada, efetua a conexão de forma reversa com o dispositivo remoto. Para acessar efetivamente a controladora de discos, é utilizada uma senha única, de conhecimento do técnico remoto e do técnico residente.

Através de uma auditoria interna de segurança efetuada na empresa Beta, percebeu-se que o acesso remoto para manutenção da Controladora de Discos de *Mainframe*, era uma caixa preta. Foi elaborado um questionário baseado na NBR ISO/IEC 17799:2001 e solicitado para a empresa responsável que respondesse estas perguntas. Com a análise deste questionário, foi constatado que apesar dos mecanismos utilizados para segurança do acesso remoto, como: protocolo proprietário de comunicação, utilização de um sistema proprietário em topologia *peer-to-peer* e utilização de estrutura de comunicação baseada em *hex streams*, além de infra-estrutura de software e hardware que não possibilita o acesso aos dados dos clientes, a empresa Beta precisa necessitar auditar o processo e controlar os acessos. Esta auditoria teria de ser presencial e seria de difícil execução.

Com estes problemas documentados, partiu-se para o projeto de uma solução que pudesse garantir os princípios de segurança pilares da norma NBR ISO/IEC 17799:2001: confiabilidade, integridade e autenticidade.

A solução a ser implementada funcionaria da seguinte forma:

a) Acesso remoto via VPN para manutenção

- O técnico de suporte nível 2 se conectaria a Controladora de Discos de *Mainframe* através de VPN pela *Internet* a partir de software Cisco VPN *client* instalado em sua estação remota. Em sua estação remota, estaria associado ao *software* Cisco VPN cliente, um certificado digital no nome do técnico;

- O túnel VPN seria fechado junto ao equipamento de concentração de VPNs localizado na *Extranet* da empresa Beta;

- O túnel seria baseado na porta TCP 443 com *IPSEC*;

- Após conectado no *peer* VPN da empresa Beta, e após validado o seu certificado, o técnico de nível 2, se autentica em um servidor Tacacs, com chave e senha. A partir deste momento, o técnico é autorizado e seu acesso começa a ser auditado.

- Depois de autenticado pelo servidor *Tacacs*, o técnico remoto, se autentica na Controladora de Discos de *Mainframe* em um *software* de configuração. Esta autenticação seria efetuada com chave e senha, e seria possível dar os perfis de leitura, escrita e gravação, conforme a necessidade. Somente via barramento *ethernet* é possível a utilização deste *software* para autenticação dos técnicos remotos de acordo com o perfil escolhido. Este acesso é isolado e não permite acesso do técnico aos dados do disco. Os comandos efetuados pelo técnico são todos auditados e registrados em *log*.

b) Conexão via VPN *Site-to-Site* para envio de eventos de problemas

- O software de gerenciamento da Controladora de Discos de *Mainframe* percebe que há um problema no funcionamento do equipamento e inicia um pedido de conexão *https* para o servidor localizado remotamente na empresa provedora dos serviços de manutenção;

- Este pedido de conexão passa chega ao equipamento VPN Concentrador localizado no site *Extranet*, que abre uma conexão VPN sob demanda para o equipamento de VPN remoto;

- Após estabelecida a VPN *Site-to-Site*, o *software* de gerenciamento da Controladora de Discos de *Mainframe*, se autentica em um servidor via certificado digital e depois os alarmes são transmitidos para o servidor de destino. A autenticação utilizada na VPN *Site-to-Site* será através de chaves simétricas (*pre-shared keys*).

Para implementar esta solução, foram definidas as seguintes ações no projeto, com relação a infra-estrutura:

- Compra de dois *switches* de pequeno porte para criação de uma rede local *ethernet* e conectar a Controladora de Discos de *Mainframe* via cabo UTP categoria 5e, padrão de cabo utilizado pela empresa;

- Instalação e configuração da rede local, com a implementação da infra-estrutura física, lógica e elétrica;

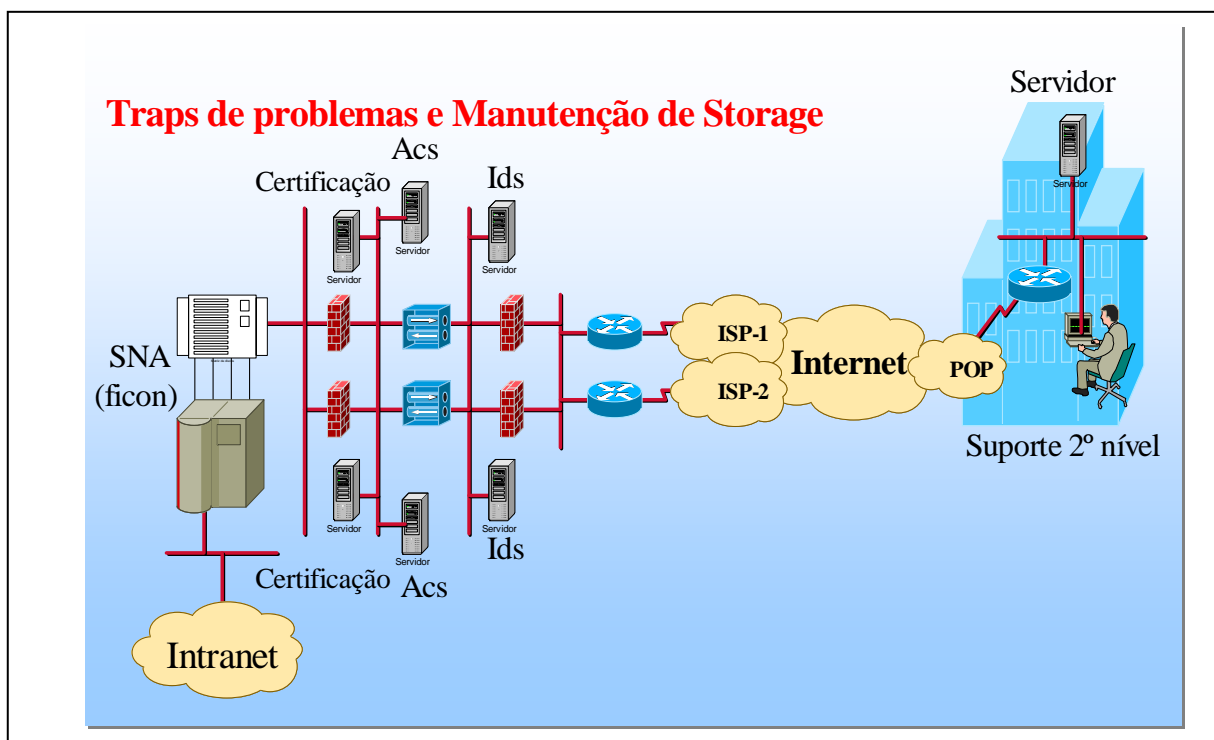
- Interligação da rede local ao *firewall* interno da rede DMZ da empresa;

- Configuração dos equipamentos de segurança e rede para permitir os acessos devidos: Regras de *firewall*, fechamento da VPN, autenticação Tacacs, validação de certificado, etc...;

- Configuração da Controladora de Discos de *Mainframe* para funcionamento em rede local e permitir o acesso dos técnicos remotamente.

- Criação de perfis de acesso, chaves e senhas na Controladora de Discos de *Mainframe* para os técnicos remotos.

Figura 3 – Topologia de acesso remoto proposta



5. DISCUSSÃO

Somente a implementação da VPN, o controle de acessos, a auditoria e as outras configurações de segurança garantiriam um acesso seguro ?

Devido a características particulares apresentadas pelos cenários de acesso remoto, algumas categorias básicas de requisitos como a autenticação dos extremos do túnel, a configuração do sistema remoto e a passagem por intermediários, devem ser tratadas prioritariamente para o desenvolvimento de uma solução segura e funcional.

Não basta implementar a política de segurança. Deve haver, também, um gerenciamento da implementação desta política, para verificação de tentativas de burlar a segurança.

O que acontece geralmente nas empresas que implantam este tipo de solução de segurança é que após implementada, não há manutenção ou atualização.

Com certeza, o controle da empresa Beta sobre os acessos irão melhorar, juntamente com a responsabilidade e os serviços de análise das informações dos **logs** de auditoria.

Uma equipe terá de ser montada para suporte a esta política.

6. Conclusão

O acesso remoto VPN possui uma grande aplicabilidade em um ambiente corporativo, ao permitir que uma organização externa deixe de realizar ligações interurbanas para manter suas soluções em hardware no ambiente do cliente, acessando recursos de TI, utilizando um túnel virtual criado através da *Internet*.

Neste artigo, demonstramos como um problema de falha na segurança em acesso remoto pode ser resolvido através da aplicabilidade da Norma NBR ISO/IEC 17799:2001.

Como resultado deste trabalho apresentamos uma solução de acesso remoto VPN baseada no software Cisco VPN *Client* para acesso remoto de manutenção e VPN *Site-to-Site* para envio de alarmes de problemas no equipamento Controladora de Discos de *Mainframe* da empresa Beta.

Após a implementação desta solução, a empresa Beta será capaz de controlar não somente os acessos dos técnicos, mas também terá o controle de todas as configurações efetuadas por eles.

7. Referências

- Norma NBR ISO/IEC 17799:2001
- Estudo de caso Empresa Beta – Manutenção de Controladoras de Discos Mainframe
- Arquitetura IP *Security* – Parte I – Adailton J. S. Silva, Renata Cicilini Teixeira, junho 1999
- RFC 2401 - *Security Architecture for Internet Protocol* <ftp://ftp.ietf.rnp.br/rfc/rfc2401.txt>
- RFC 2412 - *The OAKLEY Key Determination Protocol* . <ftp://ftp.ietf.rnp.br/rfc/rfc2412.txt>